UNIVERSIDAD DE GRANADA

A FRAMEWORK BASED IOHT FOR COMPREHENSIVE, INTELLIGENT, AND ADAPTIVE SOLUTION IN THE HEALTH DOMAIN

Programa de Doctorado en Tecnologías de la Información y la Comunicación (B25.56.1)

Student: Nour Mahmoud Bahbouh

ID 101741

Supervisors

Prof. Juan Francisco Valenzuela Valdés

Prof. Sandra Sendra Compte

2020-2024

Editor: Universidad de Granada. Tesis Doctorales
Autor: Nour Mahmoud Bahbouh
ISBN: 978-84-1195-730-4
URI: https://hdl.handle.net/10481/102871

Acknowledgement

I express my sincere gratitude to my supervisors, Professor Juan Francisco Valenzuela Valdés and Professor Sandra Sendra Compte, for their unwavering support, guidance, and encouragement throughout the entire journey of my thesis. Their meticulous review and valuable suggestions have significantly contributed to the refinement of this thesis. Additionally, I extend my appreciation to Dr. Adnan Abi Sen for his collaboration and scientafic and technical support in researching.

I would like to dedicate my thanks to the memory of my father, who was my primary supporter. May he rest in the highest paradise. My heartfelt gratitude also goes to my mother her continuous support and praying. In addition to my parents in law, I appreciate their prayers on my behalf.

To my loving husband, in your unwavering support and boundless love, I find the strength to conquer academic heights. This achievement is as much yours as it is mine. With gratitude and love, this thesis is dedicated to you.

To my beloved siblings, Dr. Jamal, Dr. Kamal, Pharmacist Fatima, and Dr. Thanaa, Thank you for your constant encouragement, guidance, and inspiration. Each of you has been a source of strength throughout my journey, and I am deeply grateful.

To my beloved Obadah, Mohammad, and my little princess Sham, Your joy lights my academic path, and this thesis is dedicated to you, my little inspirations. May your childhood be filled with happiness and your dreams know no bounds.

Lastly, I express my gratitude to the University of Granada for providing the academic environment that facilitated the completion of this thesis.

Contents

Resumen

La vida y la felicidad están directamente relacionadas con la salud, por lo que podemos afirmar que no hay nada más importante. En sistema de salud y sus mejoras sirven como un indicador clave del progreso social y del nivel de atención a los individuos. Por lo tanto, el sector de la salud ha atraído una atención significativa de los investigadores después de la revolución digital y los avances significativos en las herramientas tecnológicas. Una de las últimas tecnologías y conceptos es el Internet de las Cosas de la Salud (IoHT) / Internet de las Cosas Médicas (IoMT), que actúa como un paraguas para todas las etapas de desarrollo en este sector, comenzando por E-Health, luego M-Health, S-Health, seguido de I-Health, U-Health y, finalmente, llegando a IoHT. A pesar de que IoHT introdujo muchas aplicaciones inteligentes basadas en Internet de las Cosas e inteligencia artificial, todos los sistemas de atención médica, incluso los más avanzados, enfrentaron desafíos durante la prueba real de la pandemia de Covid-19. Esta tesis analiza los desafíos a los que se enfrentan los sistemas de atención médica basados en IoHT. Estos desafíos han impactado la capacidad de los sistemas para enfrentar pandemias, han afectado la efectividad de los sistemas de atención médica y han amenazado su futuro. La tesis aborda los diferentes desafíos extremadamente importantes dado el sector en el que se aplican, es decir, el ámbito de la salud. Los desafíos abordados son:

1- El desafío más significativo es la falta de una plataforma o marco unificado integral en el sector de la salud. En cambio, existen miles de servicios, aplicaciones y sistemas independientes que abordan diversos problemas o cuestiones relacionados con la salud.
2- Proporcionar datos confiables en tiempo real de diferentes fuentes para garantizar soluciones efectivas mediante la utilización de ciencia de datos, inteligencia artificial, algoritmos y modelos asociados.
3- Rendimiento y capacidad de respuesta a casos de emergencia, que requieren potencia computacional para procesar grandes volúmenes de datos generados a partir de diversas fuentes de datos.
4- Disponibilidad de servicios y movilidad independientemente de las circunstancias.
5- Interoperabilidad a nivel de dispositivo, servicio, protocolo y datos heterogéneos, lo que dificulta la capacidad de colaborar e integrar varios servicios y sistemas de atención médica.
6- Seguridad y confiabilidad de los datos, un problema importante para todas las tecnologías modernas, que gana importancia con la sensibilidad de los datos y servicios de atención médica.
7- La privacidad de los datos es uno de los mayores desafíos en el sector de la salud debido a la naturaleza de los datos y su importante conexión con los usuarios, además de la necesidad de mantener la precisión de los datos de atención médica al mismo tiempo que se los protege.
8- Pandemias, revelaron debilidades en la respuesta de los sistemas de atención médica a las pandemias y la ausencia de protocolos específicos para la gestión de pandemias.
9- Las concentraciones masivas de salud, que no se han abordado adecuadamente a pesar de un aumento significativo de eventos a gran escala en los últimos años en varios dominios (religioso, cultural, político), complican las cosas durante las pandemias y resultan en la muerte de miles de personas.
10- Atención especial a las personas con discapacidad, los ancianos y las personas con enfermedades crónicas, ya que requieren servicios y tratamientos especiales para crear sistemas efectivos que les permitan llevar su vida diaria con normalidad.
11- La sociedad y el medio ambiente, con poco enfoque en la concienciación de la comunidad y la necesidad de abordar cuestiones de contaminación, energía y salud vegetal y animal.

La intención o el objetivo de esta tesis es que tras su elaboración, ésta pueda usarse como un mensaje humanitario que aborde todos los puntos anteriores. Para garantizar la validez de nuestra afirmación en el objetivo principal del mensaje, que es construir un marco integral basado en IoHT para crear sistemas de atención médica efectivos y resilientes capaces de resistir pandemias y otros desafíos al tiempo que garantiza la seguridad y la privacidad de sus usuarios. Como parte de los subobjetivos del mensaje, trabajamos extensa y profundamente en los once desafíos mencionados anteriormente. Revisamos las soluciones existentes para cada desafío, discutimos sus debilidades y presentamos nuestra solución de una manera que no impacte negativamente otros desafíos.

Para abordar el primer, segundo, tercer y cuarto desafío, diseñamos un marco integral que consta de cinco capas integradas, cada una con sus elementos y funciones que contribuyen colectivamente a resolver uno o más desafíos. La mayoría de las tecnologías modernas se han empleado en el marco propuesto, incluyendo, entre otras, Internet de las cosas, Crowdsourcing, Modelos informáticos, Drones, Teléfonos inteligentes y dispositivos inteligentes y, Ciencias de datos y algoritmos de inteligencia artificial

- La primera capa fue la capa de detección responsable de proporcionar datos de múltiples fuentes (dispositivos de IoT como etiquetas RFID o sensores de malla inalámbricos, sensores portátiles, teléfonos inteligentes, redes sociales y crowdsourcing de los propios usuarios para proporcionar datos en tiempo real desde todas partes, además de datos de sistemas de atención médica, aplicaciones y servicios).
- La segunda capa fue Fog Computing para aliviar la carga en la nube al realizar el procesamiento inicial de datos localmente y brindar respuesta en tiempo real sin demora, especialmente en emergencias. La integración entre la niebla y la computación en la nube tuvo un impacto positivo en la mitigación de todos los demás desafíos, especialmente la disponibilidad y la movilidad. La tercera capa fue una propuesta de capa de computación intermedia llamada Light Cloud, más fuerte que la niebla y más rápida que la nube, para distribuir mejor la carga de trabajo, crear Federated Learning para datos agregados y administrar mejor los nodos de niebla. Además, esta capa respalda la movilidad al proporcionar instalaciones de borde móviles y confiar en drones en muchos servicios.
- La cuarta capa es la nube, responsable de agregar todos los datos de las otras capas y proporcionar una inmensa potencia informática para ejecutar algoritmos de ciencia de datos, incluida la minería de datos, el aprendizaje automático, la minería de texto y el aprendizaje profundo, además de algoritmos y herramientas de inteligencia artificial. Esta capa ha contribuido a preservar los datos de forma permanente para formar datos históricos que, a través del análisis, pueden generar una gran cantidad de conocimiento y reglas que respalden la gestión de la atención médica y las decisiones gubernamentales, así como mejorar la adaptabilidad e inteligencia de los servicios de atención médica.
- La quinta capa es la capa de Servicios y Aplicaciones, y se ha propuesto el concepto de una Super App para la Salud, donde todos los servicios de atención médica se pueden proporcionar a través de una aplicación integral. La Super App contribuirá a crear una competencia justa entre los proveedores de servicios para ofrecer servicios de mejor calidad, permitiendo la autoselección del mejor servicio para el usuario en función de sus preferencias, contexto, calidad del servicio y evaluación.

El quinto desafío, la interoperabilidad y la resolución del problema de los datos heterogéneos, implicó categorizar todas las soluciones propuestas en el campo de la interoperabilidad en una encuesta. Las soluciones abarcaron todos los niveles de interoperabilidad (hardware, protocolos, formatos y sintaxis, bases de datos, datos y semántica). En realidad, no existe una única solución integral, por lo que propusimos un enfoque híbrido que integra múltiples soluciones, junto con sugerir el diseño de una ontología integral para unificar nuevos sistemas y servicios y respaldar la interoperabilidad entre ellos. Para los sistemas heredados, se propuso un servicio basado en TM para transformar los mensajes de estos sistemas para alinearse con la ontología.

El sexto desafío, la seguridad de los datos y la confiabilidad, vio las mejores soluciones propuestas en investigaciones anteriores que se basaban en Blockchain. Sin embargo, el desafío fue que los algoritmos de consenso actuales no eran adecuados para operar durante las pandemias. Por lo tanto, se realizó un estudio de algoritmos de consenso, lo que condujo a la propuesta de un nuevo algoritmo de consenso llamado Proof of Reputation, adecuado para los servicios de atención médica, que proporciona datos confiables a prueba de manipulaciones e irrefutables. Además, la naturaleza descentralizada de blockchain era compatible con la computación en la niebla, lo que ofrece un mayor nivel de protección de datos. Además, para datos altamente sensibles y confidenciales, se propuso un nuevo método de ofuscación liviano y altamente seguro, que supera a otros métodos en términos de confianza, robustez, rendimiento y resistencia a los ataques.

El séptimo desafío, la privacidad de los datos, implicó revisar todos los enfoques principales para la protección de la privacidad y sus métodos asociados, como Dummy, ofuscación, Third Trusted Party, Cloak Area, Mix Zone, Private Information Retrieval y Encryption. Todos estos métodos sufren inconvenientes relacionados con su impacto en la precisión o el rendimiento de los datos, lo cual es inaceptable en el sector de la atención médica. Se propuso un enfoque especial para la protección de la privacidad que preserva la precisión de los datos sin un impacto significativo en el rendimiento. Además, se sugirió un enfoque específico para la protección de la privacidad de los datos de crowdsourcing para alentar a los usuarios y voluntarios a contribuir al suministro de datos manteniendo la privacidad.

El octavo desafío, que aborda específicamente las pandemias, propuso un protocolo especial para operar en este marco. El protocolo considera la prestación de servicios especializados y el apoyo a las alertas tempranas para tomar las precauciones necesarias mediante algoritmos de clasificación del nivel de amenaza o evaluación de infecciones. Además, enfatiza el papel de los centros de salud móviles, los servicios de atención médica a distancia y la dependencia de drones y voluntarios, así como la mejora de la concienciación sobre la salud y el distanciamiento social durante las pandemias. Todo lo anterior se implementó al tiempo que se garantizaba la fiabilidad de los datos agregados, se evitaban los rumores durante las pandemias y se preservaba la privacidad de las personas.

El noveno desafío es mejorar la salud y la seguridad durante las reuniones. Las investigaciones anteriores se han centrado predominantemente en abordar la congestión y la seguridad de las multitudes más que en las preocupaciones sanitarias. Sin embargo, después de la COVID-19, se hizo evidente la importancia de las medidas sanitarias en las multitudes, lo que hizo necesarias soluciones para gestionar eficazmente las multitudes y garantizar la salud y la seguridad. Se propuso la integración de varias soluciones dentro de un marco general, junto con un algoritmo de monitoreo ligero especializado basado en ML y TM. Además, se sugirieron soluciones de desinfección inteligente y alerta inteligente, junto con una aplicación móvil para proporcionar servicios específicamente para los participantes en las reuniones. También se propusieron puertas inteligentes y caminos digitales para controlar eficazmente el flujo de multitudes.

El décimo desafío implica atender a las personas con necesidades especiales mediante la asignación de un conjunto de servicios adaptados a ellas, junto con servicios de detección temprana de enfermedades crónicas y servicios para ancianos y niños también.

El undécimo desafío se centra en el cuidado comunitario y ambiental. Se propuso una plataforma para apoyar la concienciación de la salud de la comunidad con un motor de búsqueda de temas de salud (enfermedades, centros de salud, medicamentos y artículos de salud). Además, se desarrolló una aplicación para gestionar el proceso de donación de sangre y proporcionar un suministro de sangre oportuno. Además, se ha puesto en marcha un servicio para promover el voluntariado en materia de primeros auxilios. Además, se están realizando esfuerzos para mejorar la sanidad vegetal y se está desarrollando una plataforma para la gestión de residuos y la reducción de la contaminación.

Por último, hemos señalado algunos trabajos futuros y áreas en las que se pueden realizar más contribuciones para ofrecer soluciones adicionales.

Resume

Life and happiness are directly related to health, so we can state that nothing is more important. The healthcare system and its improvements serve as key indicators of social progress and the level of care for individuals. Therefore, the healthcare sector has attracted significant attention from researchers after the digital revolution and important advancements in technological tools. One of the latest technologies and concepts is the Internet of Healthcare Things (IoHT) / Internet of Medical Things (IoMT), which acts as an umbrella for all stages of development in this sector, starting from E-Health, then M-Health, S-Health, followed by I-Health, U-Health, and finally reaching IoHT. Even though IoHT has introduced many smart applications based on the Internet of Things and artificial intelligence, all healthcare systems, even the most advanced ones, faced challenges during the real test of the COVID-19 pandemic. This thesis analyzes the challenges faced by healthcare systems based on IoHT. These challenges have impacted the ability of systems to deal with pandemics, affected the effectiveness of healthcare systems, and threatened their future. The thesis addresses the different challenges that are extremely important, given the sector in which they are applied, i.e. the health field. The challenges addressed are:

1- The most significant challenge is the lack of a comprehensive unified platform or framework in the healthcare sector. Instead, there are thousands of independent services, applications, and systems addressing various health-related issues or problems.

2- Providing reliable real-time data from different sources to ensure effective solutions through the utilization of data science, artificial intelligence, algorithms, and associated models.

3- Performance and responsiveness to emergency cases, requiring computational power to process large volumes of data generated from various data sources.

4- Availability of services and mobility regardless of circumstances.

5- Interoperability at the device, service, protocol, and heterogeneous data levels, hindering the ability to collaborate and integrate various healthcare services and systems.

6- Data security and reliability, a major issue for all modern technologies, gaining importance with the sensitivity of healthcare data and services.

7- Data privacy, is one of the biggest challenges in the healthcare sector due to the nature of data and its significant connection to users, in addition to the need to maintain the accuracy of healthcare data while protecting it.

8- Pandemics, revealed weaknesses in healthcare systems' response to pandemics and the absence of specific protocols for pandemic management.

9- Mass gatherings health, not adequately addressed despite a significant increase in large-scale events in recent years across various domains (religious, cultural, political), complicating matters during pandemics and resulting in the deaths of thousands.

10- Special attention to people with disabilities, the elderly, and those with chronic diseases, as they require special services and treatment to create effective systems enabling them to lead their daily lives normally.

11- Society and the environment, with little focus on community awareness and the need to address issues of pollution, energy, and plant and animal health.

We wanted our thesis to be a humanitarian message addressing all the previous points, not just focusing on one aspect. To ensure the validity of our claim in the main message goal, which is to build a comprehensive framework based on IoHT to create effective and resilient healthcare systems capable of withstanding pandemics and other challenges while ensuring the security and privacy of its users.

As part of the sub-objectives of the message, we worked extensively and in-depth on the eleven aforementioned challenges. We reviewed existing solutions for each challenge, discussed their weaknesses, and presented our solution in a way that does not negatively impact other challenges.

To address the first, second, third, and fourth challenges, we designed a comprehensive framework consisting of five integrated layers, each layer having its elements and functions that collectively contribute to solving one or more challenges. Most modern technologies have been employed in the proposed framework, including but not limited to (Internet of Things, Crowdsourcing, Computing models, Drones, Smart phones and smart devices, Data sciences and Artificial Intelligent Algorithms).

- The first layer was the Sensing Layer responsible for providing data from multiple sources (IoT devices such as RFID tags or wireless mesh sensors, wearable sensors, smartphones, social media, and crowdsourcing from users themselves to provide real-time data from everywhere, in addition to data from healthcare systems, applications, and services).
- The second layer was Fog Computing to alleviate the burden on the cloud by performing initial data processing locally and providing real-time response without delay, especially in emergencies. The integration between fog and cloud computing had a positive impact in mitigating all other challenges, especially availability and mobility.
- The third layer was a proposed Intermediate Computing layer called Light Cloud, stronger than fog and faster than the cloud, to better distribute the workload create Federated Learning for aggregated data and better manage fog nodes. Additionally, this layer supports Mobility by providing mobile edge facilities and relying on drones in many services.
- The fourth layer is the Cloud responsible for aggregating all data from the other layers and providing immense computing power to execute data science algorithms, including data mining, machine learning, text mining, and deep learning, in addition to artificial intelligence algorithms and tools. This layer has contributed to preserving data permanently to form historical data that, through analysis, can yield a wealth of knowledge and rules supporting healthcare management and government decisions, as well as improving the adaptability and intelligence of healthcare services.
- The fifth layer is the Services and Applications layer, and the concept of a Super App for Health has been proposed, where all healthcare services can be provided through one comprehensive application. The Super App will contribute to creating fair competition among service providers to deliver better quality services, enabling Auto-Selection for the best service for the user based on their preferences, context, service quality, and evaluation.

The solution of the fifth challenge, interoperability and resolving the issue of heterogeneous data, involved categorizing all solutions proposed in the field of interoperability in a survey. Solutions spanned all levels of interoperability (hardware, protocols, formats and syntax, databases, data, and semantics). In reality, there is no single comprehensive solution, so we proposed a hybrid approach integrating multiple solutions, along with suggesting the design of a comprehensive ontology to unify new systems and services and support interoperability between them. For legacy systems, a service based on TM was proposed to transform messages from these systems to align with the Ontology.

The sixth challenge, data security, and trustworthiness saw the best-proposed solutions in previous research relying on Blockchain. However, the challenge was that current consensus algorithms were not suitable for operation during pandemics. Therefore, a survey of consensus algorithms was conducted, leading to the proposal of a new consensus algorithm called Proof of Reputation, suitable for healthcare services, providing trustworthy data that is tamper-proof and non-repudiable. Additionally, the decentralized nature of blockchain was compatible with fog computing, offering a higher level of data protection. Furthermore, for highly sensitive and confidential data, a new lightweight and highly secure obfuscation method was proposed, surpassing other methods in terms of trust, robustness, performance, and resistance to attacks.

The seventh challenge, data privacy, involved reviewing all major approaches to privacy protection and their associated methods such as Dummy, obfuscation, Third Trusted Party, Cloak Area, Mix Zone, Private Information Retrieval, and Encryption. All these methods suffer from drawbacks related to their impact on data accuracy or performance, which is unacceptable in the healthcare sector. A special approach to privacy protection was proposed that preserves data accuracy without a significant impact on performance. Additionally, a specific approach for privacy protection of Crowdsourcing data was suggested to encourage users and volunteers to contribute to data provision while maintaining privacy.

The eighth challenge, specifically addressing pandemics, proposed a special protocol for operation within this framework. The protocol considers providing specialized services and supporting early warnings to take necessary precautions through threat-level classification algorithms or infection assessment. Additionally, it emphasizes the role of mobile health centers, remote healthcare services, and reliance on drones and volunteers, as well as enhancing health awareness and social distancing during pandemics. All of the above was implemented while ensuring the reliability of aggregated data, preventing rumors during pandemics, and preserving individuals' privacy.

The ninth challenge is enhancing health and safety during gatherings. Previous research has predominantly focused on addressing crowd congestion and safety more than health concerns. However, following COVID-19, the importance of health measures within crowds became evident, necessitating solutions for effectively managing crowds while ensuring both health and safety. Integration of various solutions within a general framework was proposed, along with a specialized lightweight monitoring algorithm based on ML and TM. Additionally, smart sanitization and smart alert solutions were suggested, along with a mobile application to provide services specifically for participants in gatherings. Smart gates and digital pathways were also proposed for effectively controlling crowd flow.

The tenth challenge involves catering to individuals with special needs by allocating a set of services tailored to them, along with early detection services for chronic diseases and services for the elderly and children as well.

The eleventh challenge focuses on community and environmental care. A platform to support community health awareness with a search engine for health issues (diseases, health centers, medications, and health articles) was proposed. Additionally, an application was developed to manage the blood donation process and provide timely blood supply. Furthermore, a service to promote volunteering in first aid was introduced. Moreover, efforts are underway to enhance plant health, and a platform for waste management and pollution reduction is being developed.

Finally, we pointed out some future work and areas where further contributions can be made to provide additional solutions.

Chapter 1 - Introduction

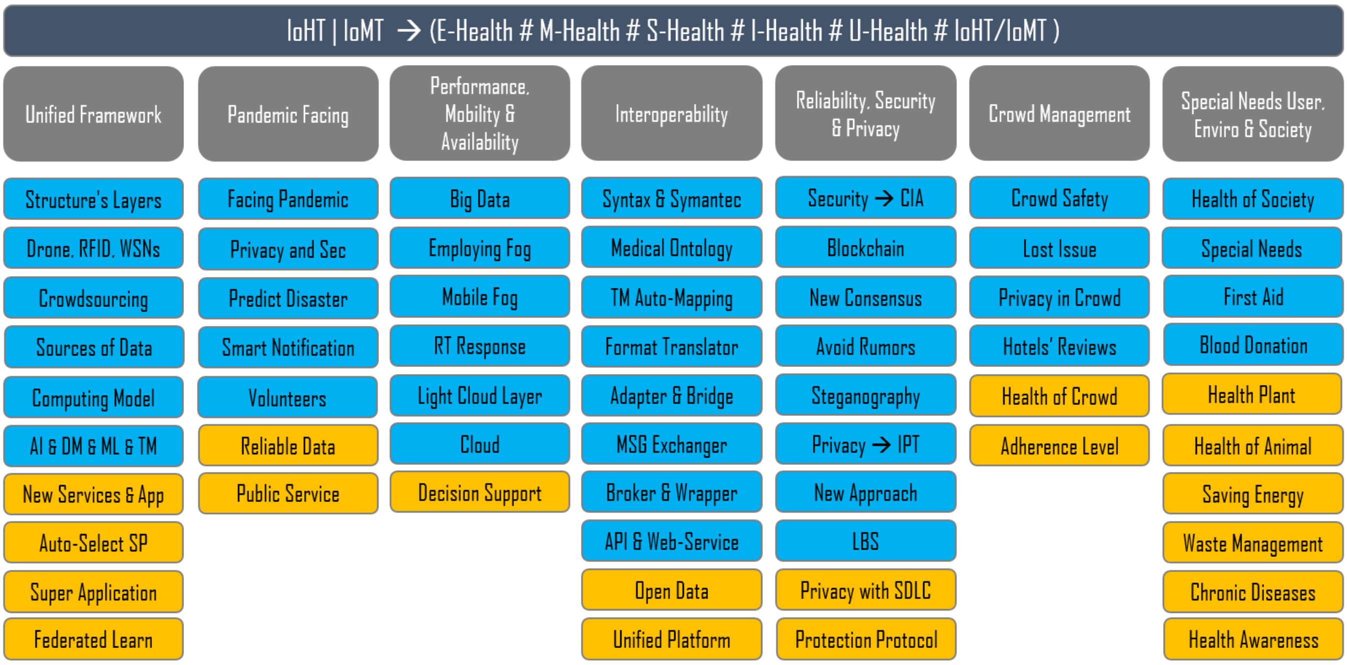
We designed this thesis document as a list of published or under reviwing papers. This section outlines the mechanism for organizing and reviewing the whole thesis, along with arranging its main chapterss, and what each chapter contains. Additionally, it presents the problems addressed by the thesis and the objectives it aims to achieve.

Map of Thesis

Each chapter within the thesis will present a published or prepared-for-publication research in each related areas of our map as the following:

- Chapter 1 is the introduction and maproad of the thesis organization.
- Chapter 2 includes a published paper that serves as a comprehensive reference study on the Internet of Health Things (IoHT). In conclusion, it reviews the proposed comprehensive framework to enhance the resilience of the healthcare sector.
- Chapter 3 discusses the issue of pandemic preparedness and related matters. The section contains a draft of a comprehensive framework for the healthcare sector based on the Internet of Health Things (IoHT). This framework enables healthcare systems to confront pandemics. Additionally, the section includes a published paper that provides a solution to ensure the security, privacy, and reliability of health data during pandemics. It also encompasses a framework for natural disaster management utilizing ML and IoT, along with creating intelligent alerts in disaster situations (draft paper).
- Chapter 4 discusses the issue of interoperability and presents a study of a published paper on the proposed solutions to support interoperability, along with a hybrid solution suggested for this challenge.
- Chapter 5 discusses the issue of health within crowds through a published research paper on crowd management. In addition to it introduces a paper on protecting the privacy of data coming from crowd-sourcing.
- Chapter 6 discusses the issue of security and privacy through several research papers in the fields of blockchain, steganography, and privacy.
- Chapter 7 presents several papers in the field of enhancing community health, such as blood donation, a framework to support people with special needs, and a model to assistance for deaf parents.
- Chapter 8 is a comprehensive summary of what has been accomplished during the thesis, along with points and future directions, whether they are currently being worked on or will be addressed in the future.

Figure 1 provides also an overview map of the thesis, illustrating the subdomains and related areas of the health, in addition to our contributions and ideas, and used tools and technologies which are utilized within the proposed comprehensive framework.



IoHT | IoMT → (E-Health # M-Health # S-Health # I-Health # U-Health # IoHT/IoMT)

Unified Framework	Pandemic Facing	Performance, Mobility & Availability	Interoperability	Reliability, Security & Privacy	Crowd Management	Special Needs User, Enviro & Society
Structure's Layers	Facing Pandemic	Big Data	Syntax & Symantec	Security → CIA	Crowd Safety	Health of Society
Drone, RFID, WSNs	Privacy and Sec	Employing Fog	Medical Ontology	Blockchain	Lost Issue	Special Needs
Crowdsourcing	Predict Disaster	Mobile Fog	TM Auto-Mapping	New Consensus	Privacy in Crowd	First Aid
Sources of Data	Smart Notification	RT Response	Format Translator	Avoid Rumors	Hotels' Reviews	Blood Donation
Computing Model	Volunteers	Light Cloud Layer	Adapter & Bridge	Steganography	Health of Crowd	Health Plant
AI & DM & ML & TM	Reliable Data	Cloud	MSG Exchanger	Privacy → IPT	Adherence Level	Health of Animal
New Services & App	Public Service	Decision Support	Broker & Wrapper	New Approach		Saving Energy
Auto-Select SP			API & Web-Service	LBS		Waste Management
Super Application			Open Data	Privacy with SDLC		Chronic Diseases
Federated Learn			Unified Platform	Protection Protocol		Health Awareness

Figure 1. Map of thesis

Problem Statement

The rapid technological development, especially in the field of data science and the Internet of Things, brings with it a lot of hope and promises to our world in various fields. Technology seeks to create a more sophisticated world and smarter services that adapt to the behavior and nature of each user. The health domain still attracts a greater share of scientific research in order to preserve people's lives, provide healthcare, reduce ailments, and serve people with special needs (disabilities, old age, cultural barriers, and communication, and other issues). Unfortunately, the ongoing Covid-19 pandemic has exposed major weaknesses in the current health systems despite the great development in the number of new services, systems, and devices. The main reason for this weakness is the lack of effective and real integration among these services, systems, tools, and devices. Moreover, there are no special protocols to deal with exceptional cases. Therefore, most countries, including the developed countries were unable to control the spread of the pandemic, which has so far has caused millions of deaths and greatly affected all sectors, including education and the economy. The ongoing pandemic has prevented gatherings, crowds, and events since March 2020 in most of the countries. In summary, our lives have become dramatically different, and working towards having an integrated health system has become the desired goal.

Main Challenges in IoHT

1- There is no comprehensive framework provides integration between all new technologies, tools, services, solutions, and applications in the health domain.
2- There is no specific protocol for dealing with pandemics like Covid-19 or natural disasters.
3- There is no trust method for health news with pandemics and prevent rumors.
4- There is no specific plan for dealing with users’ health in crowded events
5- Interoperability issue between heterogeneous devices, protocols, technologies, and data formats.
6- Privacy and security issues of users’ data in IoHT
7- Performance of managing different types of data
8- Energy issue of IoHT systems and devices

The Objective

This research seeks to activate the concept of IoHT in the most effective way, by building a more robust, intelligent, and flexible health system to deal with various conditions and situations. This would be achieved by building a comprehensive framework based on the integration of many modern technologies such as the Internet of Things, Data Science, Artificial Intelligence, Cloud, Fog, and Mobile Computing. This framework would provide a smart environment to stimulate cooperation among heterogeneous systems, services, and devices in the health domain through a special designed module for managing interoperability. Moreover, it would enable users to obtain the best services according to the prevailing circumstances and context. Moreover, the framework would enable governments to implement special protocols to appropriately confront future medical pandemics, prevent them from becoming catastrophes and limit their negative impact. The platform would provide a method to manage crowds and ensure the health and safety of people at large events. In addition, it would make contributions to many smart applications and services to help people in emergency cases, help people with special needs. Finally, the framework would provide a new approach to solve the problem of preserving the privacy and security of user data in the health sector, which one of the biggest challenges is faced by modern technologies.

The proposed research will demonstrate, through implementation and simulation, the efficacy of the proposed framework, methods, algorithms, and services by projecting them on several case studies. Based on the research, many recommendations and prospects for future development would be made.

Main Goals

1- Provide survey and classification for previous contributions in the IoHT
2- Provide comprehensive framework-based IoHT for smarter, more effective, and adaptive solutions
3- Propose a new component and ontology for enabling Interoperability in IoHT.
4- Propose a new protocol and algorithm to support a government to face any future pandemic.
5- Propose plans and algorithms to enable the government to observe and control the health in crowds.
6- Support cooperation among Cloud, Mobile, and Fog computing to address the performance issues.
7- Propose a new approach for preserving privacy and security in IoHT
8- Propose low-cost smart devices to enhance the health of communities and help disabilities.
9- Propose a smart mask for more protection and safety in epidemic cases.
10- Propose a smart solution for pollution observing, reporting, and hazardous waste management.
11- Propose new services and applications for a healthier community for users and animals.
12- Propose a platform for managing services in the health domain of different SPs
14- Simulate and implement for proposed methods, techniques, approaches, services, and apps

****

Chapter 2 - IoHT and Unified Framework

This chapter serves as the literature review for the entire thesis. It includes a survey paper on the Internet of Health Things (IoHT) that was published in a Scopus journal. The paper reviews the developmental stages of the healthcare sector, starting from electronic health and culminating in IoHT. It then presents all the definitions of IoHT, along with its applications and related fields. Additionally, it categorizes all the challenges associated with IoHT, forming the main axes of work and research throughout the thesis. We worked on providing solutions to these challenges. Towards the end of the paper, we presented a comprehensive framework that served as a High-Level Architecture, upon which different solutions could be built throughout the thesis in addressing various challenges or open issues.

An Empirical Investigation into the Altering Health Perspectives in the Internet of Health Things

Bahbouh, N. M., Compte, S. S., Valdes, J. V., & Sen, A. A. A. (2023). An empirical investigation into the altering health perspectives in the internet of health things. International Journal of Information Technology, 15(1), 67-77.

Abstract

Healthcare is on top of the agenda of all governments in the world as it is related to the well-being of the people. Naturally, this domain has attracted the attention of many researchers globally, who have studied the development of its different phases, including E-Health and the Internet of Health Things (IoHT). In this paper, the difference between the recent concepts of healthcare (E-health, M-Health, S-Health, I-Health, U-Health, and IoHT/IoMT) is analyzed based on the main services, applications, and technologies in each concept. The paper has also studied the latest developments in IoHT, which are linked to existing phases of development. A classification of groups of services and constituents of IoHT, linked to the latest technologies, is also provided. In addition, challenges, and future scope of research in this domain concerning the wellbeing of the people in the face of ongoing COVID-19 and future pandemics are explored.

Keywords: IoHT, E-Health, M-Health, S-Health, I-Health, U-Health, IoT, Covid-19.

Introduction

Throughout the ages and in all societies, the health sector has witnessed a special and great interest in its direct relationship to people's lives and their pain on the one hand, and its impact on all other sectors on the other hand [1]–[4]. What the world witnessed recently with the Corona pandemic [5], greatly affected all aspects of our lives and its fields such as the economy, education, and even the performance of daily tasks and social relations. Nothing can be better than a healthy life without disease, pain, deficiency, or disability. The healthiest societies are the more capable of giving and developing. But these societies still need more work and research in the health field to face future challenges, as the Corona pandemic has shown the inadequacy of the current situation in dealing with such crises [6]–[8].

With the beginnings of the modern digital revolution and the emergence of various communication technologies via the Internet, the health sector witnessed a similar revolution in converting many manual tasks into electronic tasks [2], [9]. Then computers and medical devices appeared that provided additional services, and then the development of Internet speed and the spread of smartphones created a new dimension of mobile medical services [10]. In the last decade, the Internet of Things came, which changed the concepts, and the search for systems and services became more intelligent and adapted to users, at lower costs, and with higher quality and availability [11], especially with its integration with other technologies such as cloud computing [9], fog computing [13], 5G [11], virtual reality [14], to name a few [13], [14].

There is no standard (unified) definition of the Internet of Things [15],[16], but we can define it as the concept that seeks to transform everything around us into smart things, with an identity, and ability to sense data, share with others, and integrate Machine-to-Machine (M2M) [15]–[17]. Since the elements of the Internet of things are limited in resources (power, storage, and processing or computing capacity) [18], therefore, all Internet of things systems depend on protocols that consume little power, In addition to their reliance on external computing and storage power such as cloud and fog computing models [19]–[22].

Below, Figure 1 shows a common architecture of the Internet of Things and its basic layers, as well as the most important protocols, tools, and their application fields, with a brief description of the most important applications and their fields [9], [23].

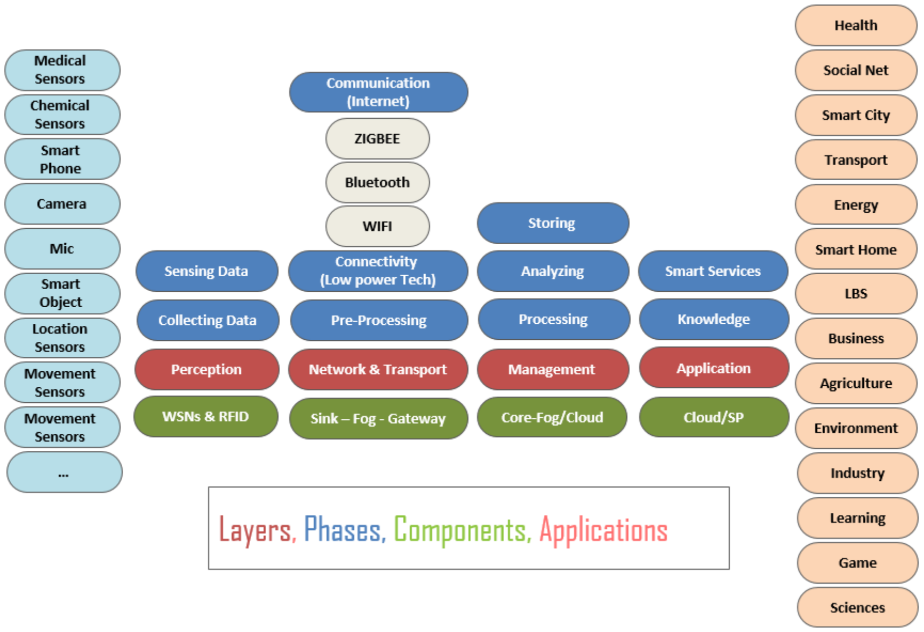


Fig 1. General Layers, Phases of Data, Components and Domains of IoT

There are two main elements in IoT, first Wireless Sensors Networks (WSNs) [24], second Radio Frequency Identification (RFID) [25] which have a critical role in the IoHT, it collects data about the patient in real-time (RT) and that produce many new smart services such as online treatment, permanent observing, and tele healing. WSNs are a group of different kinds of sensors that measure the physical conditions in the surrounding environment [26]. Recently WSNs became wearable (WBAN) [27], [28] which enables monitoring the human body's vital metrics continuously [29]. While RFID can identify objects to contact with them, which enables systems to track these objects everywhere [27]–[29].

In this article, we have provided a comparison of different healthcare phases of development, and a classification of various attributes of the IoHT domain is carried out in detail. Moreover, the challenges and future trends in this domain are streamlined. The remainder of this paper is organized into Section 2, a discussion of the history of health phases and concepts, Section 3, classifications of various constituents of the IoHT domain, Section 4, significance, and challenges, along with the future trend for the research, and Section 5, conclusions.

Historical Development of Health Phases

In this section, we provide a brief overview of the stages (main milestones) of development the health domain until IoHT (See Figure 2):

Over the years, the health sector is the most important sector because it is related to people's lives. It always attracts researchers to employ any new technology to serve medicine to reach a healthier life and be more resistant to diseases [2],[3]. It helps people with special needs or chronic diseases to live a normal life. With the beginnings of the digital revolution, information technology was employed to develop the health sector [2]. Computers, some medical devices, and software systems were provided to automate some tasks in hospitals and medical centers [9]. In addition, web services began to appear, such as reservations, appointments, inquiring about doctors' information, departments, offers, etc. [10]. All the above is called Electronic Health (E-Health) [30].

With the increase in progress, the number of electronic services increased, and smart phones and tablets began to spread and develop rapidly [7, 35], in line with the development in the speed and availability of the Internet, which enabled the user to make video calls [31]. The concept of Mobile Health (M-Health) appeared, medical centers began to provide their mobile services via smart phones, which provided ease and flexibility in use [33]. The features of these phones have encouraged creating many new useful services. The most important of which are: activating electronic consultations, supporting remote interviews between the doctor and the patient, and enabling the patient to enter and save some of his information periodically [31], [34]. So, the patient can share it with the doctor at the time of need for medical advice [34]. In addition, many mobile apps have appeared to support public health and provide advice and information to the user about a disease, medication, or any abnormal condition [35]. A new type of mobile health is the provision of services through ambulances or mobile medical centers, such as early detection or examination services for a specific disease and others [31]–[35].

The emergence of the Internet of Things [36], [37] also created a new trend and a great development in the health field. Smart Health (S-Health) [38], [42] has emerged in line with the concept of smart cities. The user no longer requires entering his data manually. Radio Frequency Identification (RFID) [27] and Wireless Sensors Network (WSNs) [29] will do the task automatically accurately. In addition to unlimited storage capabilities in the cloud [18], [39], and many useful new medical tools including wearables (such as a bracelet, belt, shoes, etc.), which contain sensors that measure the temperature, pressure, sugar, heart, respiratory, etc. [40],[41], [61]. More than that, S-Health is concerned with measuring the conditions of the environment, not just the person's biometric data to provide intelligent and adaptive services with context [42]. Alert service appeared for any sudden danger indicators in biometric values from the general average threshold. These contributions have raised RFID the level of safety and public health [39]–[41].

With the increase in the number of IoT objects and devices that continuously monitor the health of users with unlimited storage of their data, huge amounts of data have accumulated in the clouds [20]. With the availability more computing power like cloud computing [43], mobile computing [44], or edge computing such as fog [18], [45], it had become possible to analyze this data with intelligent algorithms (Data Mining, Text Mining, and Machine Learning) [6], [46]–[48]. These algorithms greatly helped in serving the medical field and supporting it with additional knowledge, such as predicting the probability of a particular disease, revealing characteristics associated with a new disease, or like expert systems to describe the patient’s condition automatically [48]-[50]. In addition to more powerful applications in processing for medical images to support automated disease detection, and relieve pressure on the medical staff, in addition to more adaptive services. This became known as Intelligent Health (I-Health) [51], [52]

The effects of the Internet of things began to appear in other areas as well, and smart homes [53], [54] appeared and spread widely, in addition to location-based services [56], [57], and others. Health researchers have sought to employ new features to find economic and effective solutions, especially for elderly patients, people with chronic diseases, and people with special needs [54], [55]. To achieve that they depended on transforming smart homes into a special care room for these people, which makes it easier for their families and the medical team to track their condition permanently, obtain continuous information, vital signs, and alert to any emergency directly [58]. all the above have contributed to saving expenses, reducing congestion in hospitals, and improving the level of health care [59] and thus what is known as the concept of Ubiquity Health (U-Health) [60] appeared, especially with services to track the patient anywhere and not only in his home [7], [58]–[60].

Recently, the concept of the Internet of Health Things (IoHT) or Internet of Mobile Things (IoMT) [59], [61] has emerged as a new concept for an integrated and proactive healthcare system based on IoT to provide and process data in Real-Time (RT). IoHT is a container for all the previous concepts. It has other new features such as awareness, smart medical devices, robots, Tele-health, as well as the development of medical education using virtual reality (VR) techniques, the use of holographic sensory communication, and 3D imaging for better diagnosis of the disease [7], [61]. Moreover, the great attention to the health of society by monitoring and collecting data remotely from everywhere, analyzing it, and finding useful information that helps governments and medical teams to face future medical pandemics and control the health of the crowd [7], [12], [61].

In short, IoHT seeks to create an independent entity for the health sector to distinguish it and its importance from the rest of the sectors to reach an ideal healthy society that is more robust, developed, free of many diseases, and capable of facing future epidemics [62], [63].

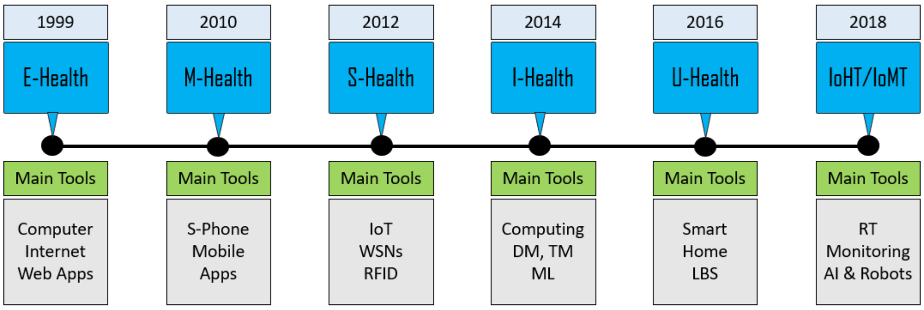


Fig 2. The Main Milestones of Evolution the Health Domain

According to the importance of IoHT, many researchers provided a review of different aspects of it. Table 1 summarized comparing of this research and a few recent surveys in the IoHT.

Table 1. Comparing contributions of a few recent surveys in IoHT

Ref No.	The main contributions
[126]	• Presented a comprehensive review of sensing devices in the health domain
[127]	• Discussed the recent technologies, protocols, and applications of IoHT
[128]	• Focused on the fog computing and its role and applications with IoHT
[129]	• Concerned about the blockchain for privacy and security in IoHT
[130]	• Viewed the structure of IoHT which they divided into three layers (sensing, personal server, and medical server) • Classified the applications of IoHT to monitoring, assisting, remoting, and analyzing. • Discussed the challenges in which the security and privacy were the most important one
This Research	• Provided historical narrative for integration between technologies and health domain starting from E-Health until IoHT/IoMT • Posed a more comprehensive classification for IoHT technologies and applications especially for dealing with the health of disabled users or during a pandemic or crowded events • Classified most of the challenges which researchers have to deal with it in future

IoHT Definition, Domains, and Applications

In this section, we have reviewed definitions, characteristics, and application of IoHT.

3.1 Definitions IoHT (IoMT | MIoT)

There are many definitions for IoHT, this research proposes a comprehensive definition by integrating all previous ones. IoHT is a concept that refers to an integrated healthcare system based on IoT [59], so the patient stays connected with the health facilities [7]. IoHT allows collecting data, monitoring it continuously, and making it available in RT when needed, especially for people with special needs, patients, the elderly, or in emergencies [36]. It also refers to the provision of diagnostic and proactive health care adapted to the context and at low treatment costs [38]. Finally, IoHT supports smart hospitals by supporting preventive health, providing patient-centered care with the help of home health systems and digital health systems with the aim of creating a smart health community [59], [64], [65].

3.2 A Classification of different levels of the IoHT Domain and applications

As we discussed before, IoHT can be considered as an umbrella for all previous phased of development health, so it includes many domains which this research classified into five domains wherein each domain we will refer to many different applications and services (to name a few). Hint, all the domains integrate to provide more adaptive and smart services.

❖ Mobile Health & Monitoring in RT [66], [67]: it is the services that are provided by smart phones, or by smart ambulances to enable access services everywhere. in addition to providing monitoring and tracking, data storage, alerting, etc. Many examples of applications and services related to this class are [7], [62], [66], [67]:
  - Medical calculator like help pregnant women to tracking her status by time
  - Medical news and advice
  - Online consultations
  - Early diagnosis like service for prediction about potential infect in diabetes
  - Activities recording like number of steps per day
  - Smart ambulance guides normal users to do the right actions in emergency cases during the time of waiting for an ambulance which will depend on the map to arrive at the accurate location of the case or event [32], [39].
  - Digital Health Systems and medical record (EHR/EMR) for information storage, searching, medication management, etc. [55], [68]

❖ Artificial Intelligence (AI) with IoHT: it depends on the new medical devices to provide smart, remote, and automated services [6], [12], [69].
  - Tele-surgeries: now the medical team can do surgery for patients living on the other side of the world without the need to be in the same locations by depending on very accurate devices and speed stable connection [11].
  - Holographic, new technology for 3D image for the human body enable physicians to get more accurate data about cases [12].
  - Haptic medicine, here employs new technology like hologram and VR to transfer virtual sensitivity [12],[70]
  - telemedicine interviews
  - Wearable Devices: There are many wearable sensors (watches, bracelets, glasses, clothes, shoes, hats, etc.) that collect different types of data to enable the log of this data in RT [70], [71].
  - Robots and smart hospitals: to achieve tasks instead of humans, especially in the pandemic situation like a robot for delivering medicines or samples. There are small micro-robots now can enter the body and do some tasks [72]–[74].

❖ Data Sciences (DS) with IoHT: we need DS algorithms to analyze big data that is collected by different devices and systems for predictive, and early diagnostic, or to process some data like a medical image for automatic and speed detection to reduce the overhead on physician and decision support.
  - Analysis the daily activities [75]
  - Detect the pests and diseases of the skin by image processing [76], [77]
  - Studying and understanding the chronic diseases [78]
  - Predict about infected cased of new virus like covid-19 [79]
  - Voice Recognition to provide voice command and help disabled users [80].
  - Data analysis by machine learning (ML), statistics, reports and visualization, medical image processing, early detection [81]–[83].

- ❖ Ambient Assisted Living: This domain concerns disabled users, the elderly, and people with chronic diseases. IoHT enables them to have independent life without needing assistance from others. Examples of some services in this domain are [54], [60], [84]:
  - Ubiquity health which enables systems to monitor and care about elderly or patients in RT and in their homes and outside.
  - Smart home and smart hospital.
  - Monitoring the effect walking on the chronic diseases and rehabilitation
  - Help blind users to do shopping by themselves
  - Rapid response, ambulance management, fast detection of emergencies, etc. [5], [85]–[88].
- ❖ Community Health: The health issue is not related to individuals only [89], [90]. There are many issues linked to community and environment [91], [92]
  - Monitoring air quality and pollution [93].
  - Dealing with epidemics like Covid-19 [5].
  - Raise awareness and cognitive about new disease, infection, bad habits, or food, etc. [91].
  - Disease prevention
  - Energy saving
  - Save health of crowd or in the congestion area [13].
  - Support the personal health as health monitoring, fitness & daily activities, obesity, preventive, etc. [94]
  - Cooperation for healing and treatment among health centers and experts for scientific cooperation, studying the characteristics of chronic diseases, confronting pandemics, discovering treatments, developing smart devices and services, etc. [85], [94].

Challenges in IoHT Domain

After analyzing many of research articles and surveys in health domain and IoHT, we have streamlined the challenges, in tandem with [95]–[97]. The challenges are:

4.1 Interoperability due to heterogeneity between diverse services, devices, and systems in IoHT

Interoperability is one of the most remarkable challenges that must be addressed in IoHT, as it relies on the Internet of Things, which does not yet have a standard architecture or protocols. It also depends on various medical devices of individual ownership, in addition to heterogeneous modern technologies [98]. Therefore, we need a means or method that enables these tools, services, and systems to cooperate, so that this cooperation creates new, more advanced services [99].

Some solutions have been presented in this field, such as relying on standardized protocols and technologies (like Constrained Application Protocol (COAP), Data Distribution Service (DDS)), relying on intermediary structures as a third-party intermediary (like the cloud), using standard technologies (like Extensible Markup Language (XML) or JavaScript Object Notation (JSON)) to represent and share data between different services and applications, or relying on dictionaries and ontology for unifying concepts used to describe future services [99], [100]. But so far, this issue is still open and needs more attention to find more efficient and effective future solutions, especially for the old systems that already exist, while respecting the principle of ownership and privacy [98]–[100].

4.2 Security and privacy of medical data

All technologies depend mainly on data, which has become the real wealth in this era [101]. But, on the dark side, collecting a lot of data about our lives and our surroundings, storing, and analyzing them make these technologies able to discover a lot of sensitive information about each person, and may also discover information that the person himself does not know about his behavior, habits, and character [95]. Thus, the development in technologies and smart services has accompanied the emergence of a new challenge related to the issue of protecting the security and privacy of this data [102]. No one is satisfied to disclose his data (for example, his medical data [91]) to the public, where its data may be exploited maliciously and greatly affect his life. The most dangerous is dealing with a malicious or hacked service provider (SP) [101],[103], who can exploit users' data to reveal information outside the scope of the announced service, which is called a privacy violation [104], [105].

In general, privacy can be defined as the person's right to determine who, when, how, why, and where his data will be used [106]. As well as his right to access and manage this data completely and ensure that his identity is not revealed to others to make a profile and link it to his identity [107]. Finally, the user must be not tracked [108],[109]. As for security [110], it is an older concept than privacy and it is imperative to protect the confidentiality and integrity of data (not to modify it), in addition to the availability of services [111], [112]. The following Figure 3 illustrates the most important concerns about data privacy and data security [95], [113]. It clarifies the basic difference between both concepts. For more details, see [114].

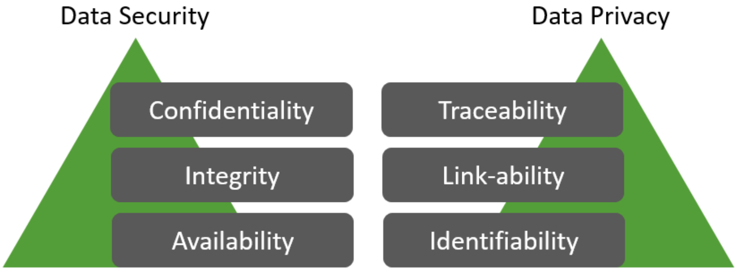


Fig 3. General Comparison between Privacy and Security

Security and privacy are very important and critical issues with IoHT which depends on collecting data in RT [111]. This data is sensitive and private, but at the same time, the user has to share this data with health centers, physicians, research centers, etc. Any attack on health data can cause a threat to the life of the user [112]. Moreover, many countries start applying laws and roles to preserve the privacy of users like GDPR Europe law [115], where security and privacy is a critical issues in the health domain [113]. Many solutions have been provided so far to protect the security of medical data, most of them are based on encryption or blockchain technology [116] to prevent data modification and create transparency in any process that takes place on this data [117],[118]. Many technologies have been presented to protect privacy in the medical field [95], [114]. But unfortunately, until now there is no comprehensive solution for privacy or security, and all the previous solutions are only discussing a specific application, so privacy and security are an open issue so far [119].

4.3 Health of crowds

Concern for the health of crowd participants is still an open topic for discussion, but with IoHT, we can propose smart solutions to continuously monitor participants' conditions in real-time, track any abnormal condition, early detection of any potential disease and thus reduce the spread of infection and disease within the crowd. So far, the health department needs more contributions, especially in large crowds, such as the pilgrimage [13], [92].

4.4 Threats posed by pandemics

The Corona pandemic showed the fragility of health systems, even in developed countries, in the face of pandemics [85]. Life around the world was affected in all its fields, which prompted many countries to apply precautionary measures to the entire population and to stop all activities, and this had a very severe impact on the economic situation in this country, and also greatly affected education and other fields [79]. The health sector was suffering the most, the medical centers were unable to absorb the large numbers of patients, which raised the number of deaths significantly, and some countries failed to control the infection, and some of them surrendered to the pandemic relying on what is known as herd immunity [86]. All the above emphasizes the need to develop an integrated platform with special scenarios and protocols to work at the time of pandemics to avoid them turning into a disaster and to mitigate and overcome their effects without major damage [6], [85], [86].

4.5 Big data and Speed of response

IoHT has created an environment based on collected data from everywhere and all the time through wearable sensors, sensors in the surrounding environment, data that comes from social media, or smartphone applications. Therefore, the amount of collected data will be huge, and since we need a quick response in medical applications as it is sensitive to time delays, this creates a real challenge in finding an effective way to transfer data and process and analyze big data quickly and in real-time [9], [120].

4.6 Mobility and scalability

IoHT must support mobile services strongly, which is considered a challenge especially in environments where the appropriate infrastructure is not available, also medical systems must be able to accommodate the large increase in the number of users or the increase in the amount of data generated that needs to be processed and analyzed [1], [120].

4.7 Energy issue

The energy problem is fundamental, especially with medical systems, as they are more demanding than other systems to save energy [121]. IoHT is highly dependent on the Internet of Things, and since the purposes of IoT are limited in resources, the issue of energy is also a real challenge facing medical systems and effective saving models must be proposed [22], [122].

4.8 Availability of services with tolerance for errors or failure (Fault-Tolerance)

The availability of medical systems and services is very critical, even if some services fail or some devices stop working, the main medical systems and their other services must remain effective and available at any time and from anywhere, and it is also a challenge that needs to propose alternative solutions that fully support availability and fault tolerance [123], [124].

4.9 Lack of a standard framework or architecture in the field of health

According to the nature of IoT which has many owners, there is no one base framework at least for each domain [4]. Each owner develops his services through his style, platforms, and tools. So, each service deals with a specific issue, and it will not be able to provide complete solutions and management for all issues in a specific domain like the health one. That affects the future of services and limits invention. For that, it is very important to find a comprehensive framework that can manage integration among all services to create a comprehensive and more efficient solution. Where the cooperation between services will enable the development of more adaptive and smarter services [16].

Moreover, the framework will enhance the quality of services, where many services providers generate services for the same goal, and the competition between them will enhance the quality and enable the framework to find new important function “Auto Selection Services” according to qualities attributes, user’s preferences, and context [16], [20].

Conclusion

This research presented a review study on the history of health systems development, and it explained the difference between the main stages that they passed (E-Health, M-Health, S-Health, I-Health, U-Health, and IoHT). Then it presented an integrated definition of IoHT and classification for its most important fields. In addition, the research mentioned many important applications and services in each field. Finally, it reviewed future challenges and open problems in the health field that needs effective and standard solutions.

It is very clear the importance of health for everyone or country. That justifies existing all these development stages, technologies, and services in this domain. However, on the other side, there are still many challenges to creating a robust health system, where these challenges affected the ability of countries to face Covid-19 effectively. The IoHT (the latest concept in the phases of health development) promises a lot in the health field through its integration with other advanced technologies, in addition to its interest in many sensitive issues such as pandemics, crowds, people with special needs, chronic diseases, etc.

In the next work, we will focus on creating a comprehensive framework for a smart healthy society that can face any challenge or pandemic and deal effectively with it (pandemic). This framework must address the interoperability issue, in addition to security and privacy issue. Moreover, this framework will enable service providers to cooperate and competed to provide higher quality services. Finally, we plan to implement this framework in Saudi Arabia (KSA) especially in the Mecca and Al Madinah cities which witness the crowded event (Hajj) annually, and the government seeks to transfer these cities to smart health ones.

References

1. A. Albesher and A. A. Albesher, “IoT in Health-care: Recent Advances in the Development of Smart Cyber-Physical Ubiquitous Environments,” 2019.
2. S. K. Goudos, P. I. Dallas, S. Chatziefthymiou, and S. Kyriazakos, “A Survey of IoT Key Enabling and Future Technologies: 5G, Mobile IoT, Sematic Web and Applications,” *Wireless Personal Communications*, vol. 97, no. 2, pp. 1645–1675, Nov. 2017, doi: 10.1007/s11277-017-4647-8.
3. Bhattacharya, Sudip, et al., "Applications of m-Health and e-Health in Public Health Sector: the challenges and opportunities," *International Journal of Medicine and Public Health* 8.2, 2018)
4. A. C. Tokognon, B. Gao, G. Y. Tian, and Y. Yan, “Structural Health Monitoring Framework Based on Internet of Things: A Survey,” *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 619–635, Jun. 2017, doi: 10.1109/JIOT.2017.2664072.
5. M. Kamal, A. Aljohani, and E. Alanazi, “IoT meets COVID-19: Status, Challenges, and Opportunities,” Jun. 2020, [Online]. Available: http://arxiv.org/abs/2007.12268
6. Jesmin, S., Kaiser, M. S., & Mahmud, M. (2020, September). Artificial and internet of healthcare things based Alzheimer care during COVID 19. In *International Conference on Brain Informatics* (pp. 263-274). Springer, Cham.
7. M. B. Yassein, I. Hmeidi, M. Al-Harbi, L. Mrayan, W. Mardini, and Y. Khamayseh, “IoT-based healthcare systems: A survey,” Dec. 2019. doi: 10.1145/3368691.3368721.
8. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, “internet of things for health care: A comprehensive survey,” *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015, doi: 10.1109/ACCESS.2015.2437951.
9. Aceto, Giuseppe, Valerio Persico, and Antonio Pescapé., "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0," *Journal of Industrial Information Integration* 18, 2020.
10. D. M. Castro, W. Coral, J. L. Cabra, J. D. Colorado, D. Méndez, and L. C. Trujillo, “Survey on iot solutions applied to healthcare,” *DYNA (Colombia)*, vol. 84, no. 203, pp. 192–200, Dec. 2017, doi: 10.15446/dyna.v84n203.64558.
11. R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, “Tactile internet and its applications in 5G era: A comprehensive review,” *International Journal of Communication Systems*, vol. 32, no. 14, Sep. 2019, doi: 10.1002/dac.3981.
12. Kaiser, M. Shamim, et al. "6G Access Network for Intelligent Internet of Healthcare Things: Opportunity, Challenges, and Research Directions." *Proceedings of International Conference on Trends in Computational and Cognitive Engineering*. Springer, Singapore, 2021.
13. M. Yamin, A. M. Basahel, and A. A. Abi Sen, “Managing Crowds with Wireless and Mobile Technologies,” *Wireless Communications and Mobile Computing*, vol. 2018, 2018, doi: 10.1155/2018/7361597.
14. Solangi, Z. A., Solangi, Y. A., Solangi, I. A., Chandio, S., Maher, Z. A., Rang, A. R., & Shaikh, N. A. (2020). Internet of Health Things: A Review. *Egyptian Computer Science Journal*, *44*(3).
15. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues,” *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2. Institute of Electrical and Electronics Engineers Inc., pp. 1191–1221, Apr. 01, 2020. doi: 10.1109/COMST.2019.2962586.
16. M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, “A survey on technologies, standards and open challenges in satellite IoT,” *IEEE Communications Surveys and Tutorials*, vol. 23, no. 3. Institute of Electrical and Electronics Engineers Inc., pp. 1693–1720, Jul. 01, 2021. doi: 10.1109/COMST.2021.3078433.
17. Ganesan, M., & Sivakumar, N., “A survey on IoT related patterns,” *International Journal of Pure and Applied Mathematics*, *117*(19), 365-369. 2017.
18. A. A. A. Sen and M. Yamin, “Advantages of using fog in IoT applications,” *International Journal of Information Technology (Singapore)*, vol. 13, no. 3, pp. 829–837, Jun. 2021, doi: 10.1007/s41870-020-00514-9.
19. A. A. Mutlag, M. K. Abd Ghani, N. Arunkumar, M. A. Mohammed, and O. Mohd, “Enabling technologies for fog computing in healthcare IoT systems,” *Future Generation Computer Systems*, vol. 90, pp. 62–78, Jan. 2019, doi: 10.1016/j.future.2018.07.049.
20. M. Asif-Ur-Rahman *et al.*, “Toward a heterogeneous mist, fog, and cloud-based framework for the internet of healthcare things,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4049–4062, Jun. 2019, doi: 10.1109/JIOT.2018.2876088.
21. A. Mukherjee, S. Ghosh, A. Behere, S. K. Ghosh, and R. Buyya, “Internet of Health Things (IoHT) for personalized health care using integrated edge-fog-cloud network,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 943–959, Jan. 2021, doi: 10.1007/s12652-020-02113-9.
22. A. Mukherjee, D. De, and S. K. Ghosh, “FogIoHT: A weighted majority game theory based energy-efficient delay-sensitive fog network for internet of health things,” *Internet of Things (Netherlands)*, vol. 11, Sep. 2020, doi: 10.1016/j.iot.2020.100181.

23. Hassan, W. H., "Current research on Internet of Things (IoT) security: A survey," *Computer networks*, *148*, 283-294. 2019.

24. Baloch, Z., Shaikh, F. K., & Unar, M. A. (2018). A context-aware data fusion approach for health-IoT. *International Journal of Information Technology*, *10*(3), 241-245.

25. J. E. Camacho-Cogollo, I. Bonet, and E. Iadanza, "RFID technology in health care," in *Clinical Engineering Handbook, Second Edition*, Elsevier, 2019, pp. 33–41. doi: 10.1016/B978-0-12-813467-2.00004-3.

26. H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "review of iot sensing applications and challenges using RFID and wireless sensor networks," *Sensors (Switzerland)*, vol. 20, no. 9. MDPI AG, May 01, 2020. doi: 10.3390/s20092495.

27. L. Cui, Z. Zhang, N. Gao, Z. Meng, and Z. Li, "Radio frequency identification and sensing techniques and their applications—A review of the state-of-the-art," *Sensors (Switzerland)*, vol. 19, no. 18. MDPI AG, Sep. 02, 2019. doi: 10.3390/s19184012.

28. Vinutha B and Raghunandan G H, "Structural Health Monitoring of Bridges Using WSNs," 2021.

29. D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, "Applications of wireless sensor networks: An up-to-date survey," *Applied System Innovation*, vol. 3, no. 1. MDPI AG, pp. 1–24, Mar. 01, 2020. doi: 10.3390/asi3010014.

30. S. K. Lee, M. Bae, and H. Kim, "Future of IoT networks: A survey," *Applied Sciences (Switzerland)*, vol. 7, no. 10, Oct. 2017, doi: 10.3390/app7101072.

31. J. A. Kim, "Book Review: The Internet of Healthy Things," *Healthcare Informatics Research*, vol. 22, no. 3, p. 250, 2016, doi: 10.4258/hir.2016.22.3.250.

32. Fang, Y., "Digital health and Internet of Health Things (IoHT)," *Digital Innovation*, 2016

33. Yu, Ping, et al. "The challenges for the adoption of m-health." *2006 IEEE International conference on service operations and logistics, and informatics*. IEEE, 2006.

34. S. Prinja, R. Nimesh, A. Gupta, P. Bahuguna, M. Gupta, and J. S. Thakur, "Impact of m-health application used by community health volunteers on improving utilisation of maternal, new-born and child health care services in a rural area of Uttar Pradesh, India," *Tropical Medicine and International Health*, vol. 22, no. 7, pp. 895–907, Jul. 2017, doi: 10.1111/tmi.12895.

35. Nisha, Nabila, Mehree Iqbal, and Afrin Rifat. "The changing paradigm of health and mobile phones: an innovation in the health care system." *Journal of Global Information Management (JGIM)* 27.1 (2019): 19-46.

36. E. Tsekleves and R. Cooper, "Design Research Opportunities in the Internet of Health Things: a review of reviews," Jun. 2018. doi: 10.21606/drs.2018.288.

37. J. Al-Jaroodi, N. Mohamed, and E. AbuKhousa, "Health 4.0: On the Way to Realizing the Healthcare of the Future," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3038858.

38. H. Dino *et al.*, "Impact of IoT Frameworks on Healthcare and Medical Systems Performance," 2021, doi: 10.5281/zenodo.4423394.

39. E. AbuKhousa, "Analytics and Telehealth Emerging Technologies: The Path Forward for Smart Primary Care Environment," *Journal of Healthcare Communications*, vol. 02, no. 04, 2017, doi: 10.4172/2472-1654.100108.

40. M. Muhib and A. Lambay, "sSurvey: Mutual Authentication Mechanism for Smart City Healthcare (SHC2) Applications," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 9, 2013, [Online]. Available: www.ijcstjournal.org

41. B. N. Karthik, L. Durga Parameswari, R. Harshini, and A. Akshaya, "Survey on IOT & Arduino Based Patient Health Monitoring System," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT*, vol. 1, no. 3, pp. 1414–1417, 2018, [Online]. Available: www.ijsrcseit.com

42. Solanas, Agusti, et al. "Smart health: A context-aware health paradigm within smart cities." *IEEE Communications Magazine* 52.8 (2014): 74-81.

43. Satyanarayanan, Mahadev. "The emergence of edge computing." *Computer* 50.1 (2017): 30-39.

44. K. Peng, V. C. M. Leung, X. Xu, L. Zheng, J. Wang, and Q. Huang, "A survey on mobile edge computing: Focusing on service adoption and provision," *Wireless Communications and Mobile Computing*, vol. 2018. Hindawi Limited, 2018. doi: 10.1155/2018/8267838.

45. J. Ren, G. Yu, Y. He, and G. Y. Li, "Collaborative Cloud and Edge Computing for Latency Minimization," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 5, pp. 5031–5044, May 2019, doi: 10.1109/TVT.2019.2904244.

46. A. Choudhuri, J. M. Chatterjee, and S. Garg, "Internet of Things in Healthcare: A Brief Overview," in *Internet of Things in Biomedical Engineering*, Elsevier, 2019, pp. 131–160. doi: 10.1016/b978-0-12-817356-5.00008-5.

47. R. Manikandan, R. Patan, A. H. Gandomi, P. Sivanesan, and H. Kalyanaraman, "Hash polynomial two factor decision tree using IoT for smart health care scheduling," *Expert Systems with Applications*, vol. 141, Mar. 2020, doi: 10.1016/j.eswa.2019.112924.

48. G. Verma and S. Prakash, "Internet of Things for Healthcare: Research Challenges and Future Prospects," in *Lecture Notes in Electrical Engineering*, 2021, vol. 668, pp. 1055–1067. doi: 10.1007/978-981-15-5341-7_80.

49. M. A. Sayeed, S. P. Mohanty, E. Kougianos, and H. P. Zaveri, "Neuro-Detect: A Machine Learning-Based Fast and Accurate Seizure Detection System in the IoMT," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 359–368, Aug. 2019, doi: 10.1109/TCE.2019.2917895.

50. Yoon, Jee-Eun, and Chang-Jin Suh. "Research Trend Analysis by using Text-Mining Techniques on the Convergence Studies of AI and Healthcare Technologies." *Journal of Information Technology Services* 18.2 (2019): 123-141, doi: 10.9716/KITS.2019.18.2.123.

51. X. Briffault, M. Morgiève, and P. Courtet, "From e-health to i-health: Prospective reflexions on the use of intelligent systems in mental health care," *Brain Sciences*, vol. 8, no. 6, 2018, doi: 10.3390/brainsci8060098.

52. A. A. Abdellatif *et al.*, "I-Health: Leveraging Edge Computing and Blockchain for Epidemic Management," Dec. 2020, [Online]. Available: http://arxiv.org/abs/2012.14294

53. M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, "A review of smart home applications based on Internet of Things," *Journal of Network and Computer Applications*, vol. 97. Academic Press, pp. 48–65, Nov. 01, 2017. doi: 10.1016/j.jnca.2017.08.017.

54. N. Agoulmine, M. Jamal Deen, J. S. Lee, and M. Meyyappan, "U-Health Smart Home: Innovative solutions for the management of the elderly and chronic diseases," *IEEE Nanotechnology Magazine*, vol. 5, no. 3, pp. 6–11, 2011, doi: 10.1109/MNANO.2011.941951.

55. T. Edoh and J. Degila, "IoT-Enabled Health Monitoring and Assistive Systems for in Place Aging Dementia Patient and Elderly," in *IoT and Smart Home Automation [Working Title]*, IntechOpen, 2019. doi: 10.5772/intechopen.86247.

56. H. Huang, G. Gartner, J. M. Krisp, M. Raubal, and N. van de Weghe, "Location based services: ongoing evolution and research agenda," *Journal of Location Based Services*, vol. 12, no. 2, pp. 63–93, Apr. 2018, doi: 10.1080/17489725.2018.1508763.

57. Basiri, Anahid, et al. "Indoor location based services challenges, requirements and usability of current solutions." *Computer Science Review* 24 (2017): 1-12.

58. Stewart, Christopher James. *Mackenzie Health: An Analysis of a" Smart" Internet of Things Approach to Healthcare*. Diss. University of Toronto (Canada), 2018.

59. J. Lucas, R. Vieira, and L. Antonio Da Ponte Junior, "An Introduction to the Internet of Healthcare Things."

60. J. Kim and S. O. Park, "U-Health Smart system architecture and ontology model," *Journal of Supercomputing*, vol. 71, no. 6, pp. 2121–2137, Nov. 2015, doi: 10.1007/s11227-014-1334-3.

61. J. J. P. C. Rodrigues *et al.*, "Enabling Technologies for the Internet of Health Things," *IEEE Access*, vol. 6, pp. 13129–13141, Jan. 2018, doi: 10.1109/ACCESS.2017.2789329.

62. L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electronics (Switzerland)*, vol. 8, no. 7, Jul. 2019, doi: 10.3390/electronics8070768.

63. M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. le Moullec, "survey on the roles of communication technologies in IoT-Based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36611–36631, Jul. 2018, doi: 10.1109/ACCESS.2018.2853148.

64. S. Noulas, "School of Social Sciences Master in Business Administration (MBA) Postgraduate Dissertation 'Factors influencing consumers'' intention to use Internet of Things (IoT) technology based solutions",'" 2018.

65. Mp, Sebastian. *Smart Hospitals: Challenges and Opportunities*. No. 315. Indian Institute of Management Kozhikode, 2019.

66. L. Minh Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," *Electronics (Switzerland)*, vol. 8, no. 7, Jul. 2019, doi: 10.3390/electronics8070768.

67. S. H. Almotiri, M. A. Khan, and M. A. Alghamdi, "Mobile health (m-Health) system in the context of IoT," in *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, Oct. 2016, pp. 39–42. doi: 10.1109/W-FiCloud.2016.24.

68. Dr. K. C. Benson, Dr. L. Jonassen, and Dr. B. Tran, "Cyber security for Medical Devices Using Block chain," *International Journal of Applied Science and Technology*, vol. 9, no. 4, 2019, doi: 10.30845/ijast.v9n4p2.

69. Hasan, I., Dhawan, P., Rizvi, S. A. M., & Dhir, S. (2022). Data analytics and knowledge management approach for COVID-19 prediction and control. *International Journal of Information Technology*, 1-18.

70. F. Patlar Akbulut and A. Akan, "A smart wearable system for short-term cardiovascular risk assessment with emotional dynamics," *Measurement: Journal of the International Measurement Confederation*, vol. 128, pp. 237–246, Nov. 2018, doi: 10.1016/j.measurement.2018.06.050.

71. B. M. Eskofier *et al.*, "An overview of smart shoes in the internet of health things: Gait and mobility assessment in health promotion and disease monitoring," *Applied Sciences (Switzerland)*, vol. 7, no. 10. MDPI AG, Sep. 25, 2017. doi: 10.3390/app7100986.

72. Deshkar, Sankalp, R. A. Thanseeh, and Varun G. Menon. "A review on IoT based m-Health systems for diabetes." *International Journal of Computer Science and Telecommunications* 8.1 (2017): 13-18.

73. Sasubilli, Satya Murthy, Abhishek Kumar, and Vishal Dutt. "Improving Health Care by Help of Internet of Things and Bigdata Analytics and Cloud Computing." *2020 International Conference on Advances in Computing and Communication Engineering (ICACCE)*. IEEE, 2020.

74. F. Zhou, X. Wang, and M. Goh, "Fuzzy extended VIKOR-based mobile robot selection model for hospital pharmacy," *International Journal of Advanced Robotic Systems*, vol. 15, no. 4, Jul. 2018, doi: 10.1177/1729881418787315.

75. M. Abdel-Basset, H. Hawash, R. K. Chakrabortty, M. Ryan, M. Elhoseny, and H. Song, "ST-DeepHAR: Deep Learning Model for Human Activity Recognition in IoHT Applications," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4969–4979, Mar. 2021, doi: 10.1109/JIOT.2020.3033430.

76. A. Khamparia, P. K. Singh, P. Rani, D. Samanta, A. Khanna, and B. Bhushan, "An internet of health things-driven deep learning framework for detection and classification of skin cancer using transfer learning," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 7, Jul. 2021, doi: 10.1002/ett.3963.

77. A. Khamparia, D. Gupta, V. H. C. de Albuquerque, A. K. Sangaiah, and R. H. Jhaveri, "Internet of health things-driven deep learning system for detection and classification of cervical cells using transfer learning," *Journal of Supercomputing*, vol. 76, no. 11, pp. 8590–8608, Nov. 2020, doi: 10.1007/s11227-020-03159-4.

78. X. Chen, R. Duan, Y. Shen, and H. Jiang, "Design and evaluation of an intelligent physical examination system in improving the satisfaction of patients with chronic disease," 2020, doi: 10.21203/rs.3.rs-23074/v1.

79. M. Yamin, A. A. A. Sen, Z. M. Al-Kubaisy, and R. Almarzouki, "A novel technique for early detection of COVID-19," *Computers, Materials and Continua*, vol. 68, no. 2, pp. 2283–2298, Apr. 2021, doi: 10.32604/cmc.2021.017433.

80. Bugajski, Mark. "Future of voice control for consumer interactions with internet of things systems: in the context of integration with other services offered by traditional service providers." (2016): 35-11.

81. M. Shoaib, M. Imran, F. Subhan, and I. Ahmad, "Towards a Low Complexity Scheme for Medical Images in Scalable Video Coding," *IEEE Access*, vol. 8, pp. 41439–41451, 2020, doi: 10.1109/ACCESS.2020.2976715.

82. C. M. J. M. Dourado, S. P. P. da Silva, R. V. M. da Nobrega, P. P. Reboucas Filho, K. Muhammad, and V. H. C. de Albuquerque, "An Open IoHT-Based Deep Learning Framework for Online Medical Image Recognition," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 541–548, Feb. 2021, doi: 10.1109/JSAC.2020.3020598.

83. Emmanouilidou, Maria. "The Internet of Healthcare Things: A European Perspective and a Review of Ethical Concerns." *International Journal of Humanities and Social Sciences* 13.5 (2019): 675-679.

84. E. Wianto, E. Sarvia, and C. H. Chen, "Authoritative parents and dominant children as the center of communication for sustainable healthy aging," *International Journal of Environmental Research and Public Health*, vol. 18, no. 6, pp. 1–19, Mar. 2021, doi: 10.3390/ijerph18063290.

85. R. P. Singh, M. Javaid, A. Haleem, and R. Suman, "Internet of things (IoT) applications to fight against COVID-19 pandemic," *Diabetes and Metabolic Syndrome: Clinical Research and Reviews*, vol. 14, no. 4, pp. 521–524, Jul. 2020, doi: 10.1016/j.dsx.2020.04.041.

86. M. Vangeti, C. Wata Dereso, R. Rudrapati Assistant Professor, M. Akhila, and M. Muturaman Assistant Professor, "Article ID: IJARET_11_09_014 Cite this Article: Madhuri Vangeti, Chala Wata Dereso, Ramesh Rudrapati, Miriyala Akhila and Maheswaran Muturaman, Applications of Internet of Things (Iot) to Track Covid-19 in Real Time," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, no. 9, pp. 134–140, 2020, doi: 10.34218/IJARET.11.9.2020.014.

87. M. Gusev, A. Stojmenski, and I. Chorbev, "Challenges for development of an ECG m-Health solution," *Journal of Emerging research and solutions in ICT*, vol. 1, no. 2, pp. 25–38, Dec. 2016, doi: 10.20544/ersict.02.16.p03.

88. T. Edoh, "Internet of Things in Emergency Medical Care and Services," in *Medical Internet of Things (m-IoT) - Enabling Technologies and Emerging Applications*, IntechOpen, 2019. doi: 10.5772/intechopen.76974.

89. J. C. Tsai *et al.*, “Design and Implementation of an Internet of Healthcare Things System for Respiratory Diseases,” *Wireless Personal Communications*, vol. 117, no. 2, pp. 337–353, Mar. 2021, doi: 10.1007/s11277-020-07871-5.

90. J. Y. Lee, C. P. Wong, and S. W. H. Lee, “m-Health views and perception among Malaysian: findings from a survey among individuals living in Selangor,” *mHealth*, vol. 6, pp. 6–6, Jan. 2020, doi: 10.21037/mhealth.2019.09.16.

91. C. A. Tschider, “The Consent Myth: Improving Choice for Patients of the Future.” [Online]. Available: https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/12

92. T. Edoh, “Risk Prevention of Spreading Emerging Infectious Diseases Using a HybridCrowdsensing Paradigm, Optical Sensors, and Smartphone,” *Journal of Medical Systems*, vol. 42, no. 5, May 2018, doi: 10.1007/s10916-018-0937-2.

93. E. Svertoka, M. Bălănescu, G. Suciu, A. Pasat, and A. Drosu, “Decision support algorithm based on the concentrations of air pollutants visualization,” *Sensors (Switzerland)*, vol. 20, no. 20, pp. 1–15, Oct. 2020, doi: 10.3390/s20205931.

94. D. Vital, P. Gaire, S. Bhardwaj, and J. L. Volakis, “An Ergonomic Wireless Charging System for Integration with Daily Life Activities,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 69, no. 1, pp. 947–954, Jan. 2021, doi: 10.1109/TMTT.2020.3029530.

95. A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” *International Journal of Information Technology (Singapore)*, vol. 10, no. 2, pp. 189–200, Jun. 2018, doi: 10.1007/s41870-018-0113-4.

96. Ianculescu, Marilena, and Adriana Alexandru. "Internet of health things as a win-win solution for mitigating the paradigm shift inside senior patient-physician shared health management." *International Journal of Computer and Information Engineering* 13.10 (2019): 569-573.

97. V. Jain, R. Wason, J. Moy Chatterjee, D.-N. le Ontology-Based, N. Malik, and S. Kumar Malik, “Using IoT and Semantic Web Technologies for Healthcare and Medical Sector,” 2020. [Online]. Available: https://www.who.int/hdp/.

98. S. Jabbar, F. Ullah, S. Khalid, M. Khan, and K. Han, “Semantic interoperability in heterogeneous IoT infrastructure for healthcare,” *Wireless Communications and Mobile Computing*, vol. 2017, 2017, doi: 10.1155/2017/9731806.

99. A. Jaleel, T. Mahmood, M. A. Hassan, G. Bano, and S. K. Khurshid, “Towards Medical Data Interoperability through Collaboration of Healthcare Devices,” *IEEE Access*, vol. 8, pp. 132302–132319, 2020, doi: 10.1109/ACCESS.2020.3009783.

100. S. Yang and R. Wei, “Semantic Interoperability through a Novel Cross-Context Tabular Document Representation Approach for Smart Cities,” *IEEE Access*, vol. 8, pp. 70676–70692, 2020, doi: 10.1109/ACCESS.2020.2986485.

101. B. Wu, S. Nazir, and N. Mukhtar, “Identification of Attack on Data Packets Using Rough Set Approach to Secure End to End Communication,” *Complexity*, vol. 2020, 2020, doi: 10.1155/2020/6690569.

102. A. Attaallah, M. Ahmad, M. T. J. Ansari, A. K. Pandey, R. Kumar, and R. A. Khan, “Device security assessment of internet of healthcare things,” *Intelligent Automation and Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021, doi: 10.32604/iasc.2021.015092.

103. S. R. Sree, “Secure Data Transmission on Internet of Healthcare Things,” *International Journal of Engineering Trends and Applications (IJETA)*, vol. 7, 2014, [Online]. Available: www.ijetajournal.org

104. H. Aranha, M. Masi, T. Pavleska, and G. P. Sellitto, “Securing Mobile e-Health Environments by Design: A Holistic Architectural Approach,” in *International Conference on Wireless and Mobile Computing, Networking and Communications*, Oct. 2019, vol. 2019-October, pp. 300–305. doi: 10.1109/WiMOB.2019.8923479.

105. D. Sparrell, "Cyber-safety in healthcare IoT." *2019 ITU kaleidoscope: ICT for health: networks, standards and innovation (ITU K)*. IEEE, 2019. doi: 10.23919/ITUK48006.2019.8996148.

106. A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for IoT,” *Sensors (Switzerland)*, vol. 19, no. 2, Jan. 2019, doi: 10.3390/s19020326.

107. Anagnostopoulos, Aris, et al. "Random Projection to Preserve Patient Privacy." *CIKM Workshops*. 2018.

108. A. M. Elmisery, S. Rho, and D. Botvich, “A fog based middleware for automated compliance with OECD privacy principles in internet of healthcare things,” *IEEE Access*, vol. 4, pp. 8418–8441, 2016, doi: 10.1109/ACCESS.2016.2631546.

109. F. Angeletti, I. Chatzigiannakis, and A. Vitaletti, “Towards an architecture to guarantee both data privacy and utility in the first phases of digital clinical trials,” *Sensors (Switzerland)*, vol. 18, no. 12, Dec. 2018, doi: 10.3390/s18124175.

110. J. J. Kang, “Systematic Analysis of Security Implementation for Internet of Health Things in Mobile Health Networks,” in *Intelligent Systems Reference Library*, vol. 177, Springer, 2020, pp. 87–113. doi: 10.1007/978-3-030-38788-4_5.

111. S. S. Rani, J. A. Alzubi, S. K. Lakshmanaprabu, D. Gupta, and R. Manikandan, “Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers,” *Multimedia Tools and Applications*, vol. 79, no. 47–48, pp. 35405–35424, Dec. 2020, doi: 10.1007/s11042-019-07760-5.

112. L. Wang, Y. Ali, S. Nazir, and M. Niazi, “ISA Evaluation Framework for Security of Internet of Health Things System Using AHP-TOPSIS Methods,” *IEEE Access*, vol. 8, pp. 152316–152332, 2020, doi: 10.1109/ACCESS.2020.3017221.

113. M. Mahmud *et al.*, “A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience Applications,” *Cognitive Computation*, vol. 10, no. 5, pp. 864–873, Oct. 2018, doi: 10.1007/s12559-018-9543-3.

114. A. A. A. Sen and A. M. Basahel, "A Comparative Study between Security and Privacy," *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2019, pp. 1282-1286.

115. E. ben van Veen, “Observational health research in Europe: understanding the General Data Protection Regulation and underlying debate,” *European Journal of Cancer*, vol. 104, pp. 70–80, Nov. 2018, doi: 10.1016/j.ejca.2018.09.032.

116. E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O. Y. Song, A. K. Bashir, and A. A. A. El-Latif, “DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems,” *IEEE Access*, vol. 8, pp. 111223–111238, 2020, doi: 10.1109/ACCESS.2020.2999468.

117. K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, “Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare,” *Blockchain in Healthcare Today*, Mar. 2018, doi: 10.30953/bhty.v1.20.

118. Shah, R., & Rajagopal, S. (2022). M-DPS: a blockchain-based efficient and cost-effective architecture for medical applications. *International Journal of Information Technology*, *14*(4), 1909-1921.

119. M. A. Rahman, M. Shamim Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, “Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach,” *IEEE Access*, vol. 8, pp. 205071–205087, 2020, doi: 10.1109/ACCESS.2020.3037474.

120. L. Zhu *et al.*, “A Survey of Fall Detection Algorithm for Elderly Health Monitoring,” in *Proceedings - 2015 IEEE 5th International Conference on Big Data and Cloud Computing, BDCloud 2015*, Oct. 2015, pp. 270–274. doi: 10.1109/BDCloud.2015.35.

121. J. J. Kang, M. Dibaei, G. Luo, W. Yang, P. Haskell-Dowland, and X. Zheng, “An energy-efficient and secure data inference framework for internet of health things: A pilot study,” *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–17, Jan. 2021, doi: 10.3390/s21010312.

122. B. K. Sovacool and D. D. Furszyfer Del Rio, “Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies,” *Renewable and Sustainable Energy Reviews*, vol. 120. Elsevier Ltd, Mar. 01, 2020. doi: 10.1016/j.rser.2019.109663.

123. F. Farhin, M. S. Kaiser, and M. Mahmud, “Towards Secured Service Provisioning for the Internet of Healthcare Things,” Oct. 2020. doi: 10.1109/AICT50176.2020.9368580.

124. M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” *Journal of Information Security and Applications*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.

125. Wang, Qin, et al., "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." *arXiv preprint arXiv*:2105.07447, 2021.

126. Baali, H., Djelouat, H., Amira, A., & Bensaali, F. (2017). Empowering technology enabled care using IoT and smart devices: a review. *IEEE Sensors Journal*, *18*(5), 1790-1809.

127. Alam, M. M., Malik, H., Khan, M. I., Pardy, T., Kuusik, A., & Le Moullec, Y. (2018). A survey on the roles of communication technologies in IoT-based personalized healthcare applications. *IEEE Access*, *6*, 36611-36631.

128. Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N. A., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, *90*, 62-78.

129. Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications*, *154*, 223-235.

130. Ketu, S., & Mishra, P. K. (2021). Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications*, *192*, 103179.

****

Chapter 3 - Facing Pandemic and IoHT Issues

This chapter is considered the most crucial in the research as it provides solutions to three significant challenges. The first challenge focuses on designing a comprehensive healthcare framework to enhance and support healthcare systems. The second addresses empowering healthcare systems to effectively combat pandemics. Finally, the challenge of performance, big data, and rapid response is tackled by employing various forms of computational models.

This chapter consists of four research papers, with two of them published in ISI journals and two still under review. The first paper (not yet published) details the proposed comprehensive healthcare framework. The framework presents a specific working protocol for pandemic situations. Within the proposed framework, we discussed various challenges at each layer and briefly suggested solutions. This paper serves as the nucleus for all our other ideas and work. The proposed model relies on fog and cloud computing, introducing a Mediating Computing model (Light-Cloud) between them. Additionally, it incorporates modern technologies such as drones and smart services. The framework also relies on diverse sources to provide data.

The second paper, published in an ISI journal, discusses a method to enhance community collaboration during pandemics while ensuring the privacy and data security of individuals. The paper introduces a new approach to achieve this during pandemics.

The third paper (Under Reviewing), presents another approach to pandemics, focusing on natural disasters. The paper provides a solution to mitigate the effects of disasters, such as floods, to safeguard the lives of individuals. The solution relies on the Internet of Things and machine learning algorithms for early disaster detection, threat level classification in each area, and alerting residents accordingly. Moreover, we enhance enhances the accuracy of the classification algorithm by incorporating crowdsourcing. In addition, the paper introduces the concept of smart alerting and volunteers, along with a companion application for smartphones.

C-IoHT: A Comprehensive Framework for Real-Time Healthcare Data Management During Pandemics

Not published yet

Abstract

The success of healthcare systems greatly depends on the availability of real-time information, which remains a significant challenge due to data volume, heterogeneity, security, and privacy concerns. The current COVID-19 pandemic has highlighted the need for reliable real-time information to effectively respond to exceptional circumstances. In this regard, this study proposes C-IoHT, a comprehensive framework that addresses these challenges and enables the development of a robust healthcare system. C-IoHT offers solutions to the triad of challenges through five layers that rely on the Internet of Health Things (IoHT) and data sciences. It includes three computing layers, namely fog and cloud, and a newly proposed "Light-Cloud" model that addresses performance and responsiveness issues. Additionally, C-IoHT proposes a specific ontology managed by Tri-computing to achieve data homogeneity and support interoperability between medical services. The framework also uses Tri-computing to manage blockchain, ensuring data security and privacy. Furthermore, C-IoHT suggests a real-time classification algorithm for early warning of pandemics and controlling the spread of infection. The study proposes essential healthcare services during pandemics and presents a suggested dashboard for healthcare decision support. The efficiency of C-IoHT is demonstrated through simulations, which show the enhancement of performance after adding the Light-Cloud layer, the effectiveness of using blockchain, and the accuracy enhancement of the classification algorithm when tested on the COVID-19 dataset.

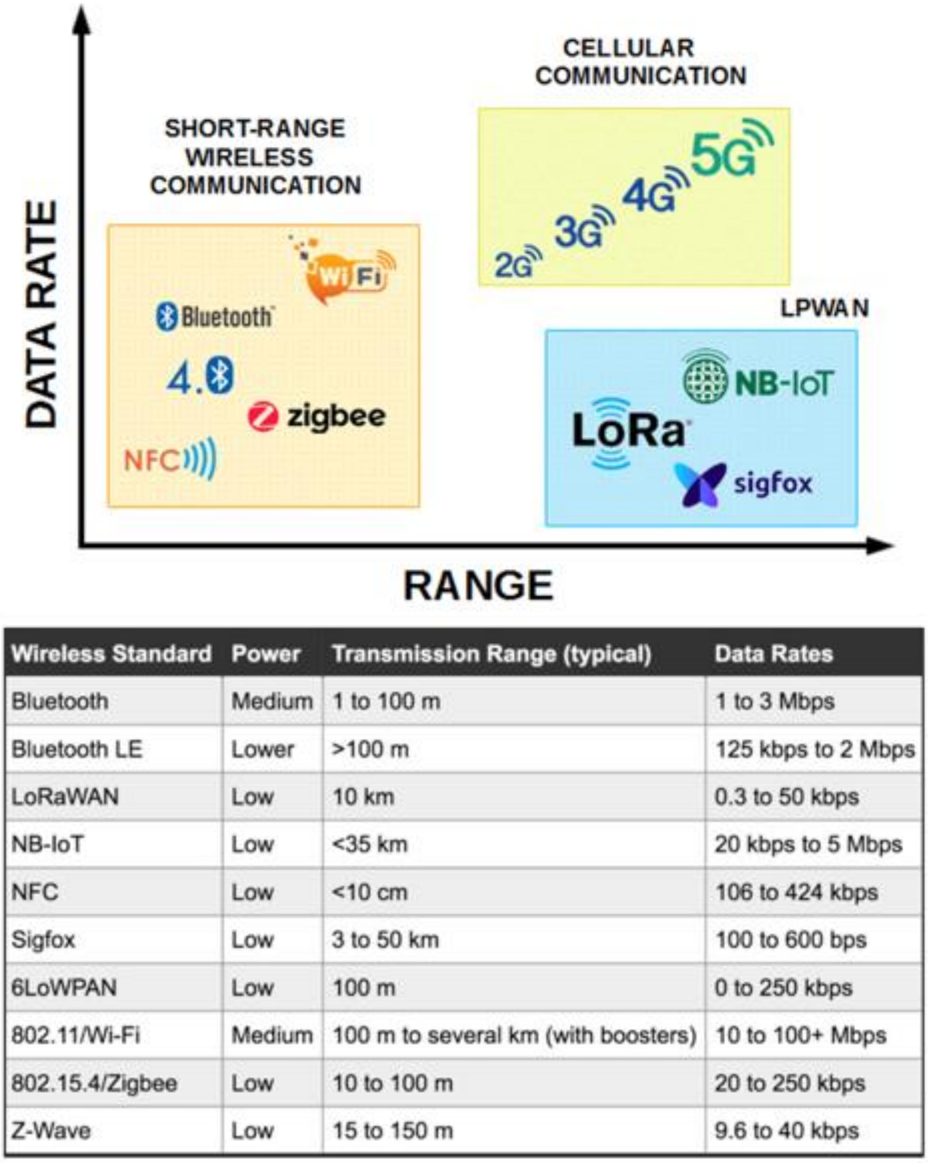
Keywords—IoHT, Interoperability, Fog, Light Cloud, Blockchain, Ontology, Machine Learning.

Introduction

In recent years, healthcare applications and services have undergone significant development, becoming more intelligent and user-friendly. This progress can be attributed to the digital revolution, data revolution, and modern technologies [1]. Among the cutting-edge technologies that have had a significant impact on healthcare are the Internet of Things (IoT) [2], wireless sensor networks (WSNs) [3], radio frequency identification (RFID) [4], and various computing models like cloud and fog [5]. Additionally, various communication protocols such as Wi-Fi, Bluetooth, Zigbee, 5G, and 6G have played a crucial role (see Figure 1) [6-7]. These technologies, among others, have been employed in the healthcare sector under one umbrella called the Internet of Healthcare Things (IoHT) [8].

The term IoHT, also known as Internet of Mobile Things (IoMT), appeared in 2018 after several stages of development in the healthcare field and its concepts, such as Electronic Health (EHealth), Mobile Health (MHealth), Smart Health (SHealth), Intelligent Health (IHealth), and Ubiquity Health (UHealth) [9]. IoHT can be defined as the utilization of the Internet of Things, artificial intelligence, and data science to create services that are more adaptable and cost-effective for individuals in the community, including patients, people with special needs, seniors, and even ordinary people [10] [11]. These services aim to provide smart and community healthcare everywhere and at any time. They also contribute to enabling remote care with continuous monitoring and immediate response to emergency cases, alerting or predicting them before they occur to minimize their effects [12] [13]. IoHT has introduced many new services primarily based on real-time data aggregation from various networked sensors that can be located anywhere around us, in the streets, in buildings, or even on our bodies, such as wearable sensors like clothing, shoes, accessories (such as rings, bracelets, glasses, etc.), known as Body Area Networks (BAN) [14] [15].

Despite significant progress and advancements in healthcare, the emergence of the COVID-19 pandemic in late 2019 exposed the limitations of current healthcare systems [16]. Even advanced countries struggled to contain the outbreak, highlighting weaknesses, and emphasizing the need for more advanced and efficient healthcare systems to address global crises [17]. The number of deaths in 2020 exceeded three million people, and the economic damage exceeded hundreds of billions of dollars, as most countries-imposed curfews and closed most commercial activities to limit the spread of the virus [18]. Moreover, a vast amount of fake news and rumors spread quickly throughout the crisis. One of the most important reasons for the failure to control the pandemic was the lack of cooperation and coordination between medical centers and governments [19]. Most research focused on addressing specific problems during the pandemic, such as predicting the number of infections [20], finding an appropriate vaccine [21], tracking the affected individuals [22], and monitoring adherence to precautionary measures [23].



Wireless Standard	Power	Transmission Range (typical)	Data Rates
Bluetooth	Medium	1 to 100 m	1 to 3 Mbps
Bluetooth LE	Lower	>100 m	125 kbps to 2 Mbps
LoRaWAN	Low	10 km	0.3 to 50 kbps
NB-IoT	Low	<35 km	20 kbps to 5 Mbps
NFC	Low	<10 cm	106 to 424 kbps
Sigfox	Low	3 to 50 km	100 to 600 bps
6LoWPAN	Low	100 m	0 to 250 kbps
802.11/Wi-Fi	Medium	100 m to several km (with boosters)	10 to 100+ Mbps
802.15.4/Zigbee	Low	10 to 100 m	20 to 250 kbps
Z-Wave	Low	15 to 150 m	9.6 to 40 kbps

Fig 1: Properties and Features of Wireless Protocols

Our research presents a comprehensive and robust framework for addressing the challenges posed by pandemics and other health emergencies. Our approach leverages the potential of IoHT and advanced data analysis tools to ensure that healthcare providers have the necessary information to make informed decisions and respond quickly and effectively to any crisis. Our framework integrates advanced data analysis and statistical tools, empowering health administrators and practitioners to make informed decisions based on real-time information. Collaborating with various medical centers and institutions ensures the accuracy and timeliness of data, providing a comprehensive and reliable view of the situation.

A key aspect of our framework is the development of specific protocols and services tailored to address pandemics and other health emergencies. These protocols ensure that healthcare systems have the necessary resources and infrastructure in place to respond promptly and effectively to any crisis. By implementing our IoHT-based framework, healthcare providers can access critical information in real-time, enabling them to make informed decisions and take proactive measures to mitigate the spread of disease and prevent future outbreaks. With the appropriate tools and resources, healthcare systems are better equipped to manage the challenges posed by pandemics and other public health emergencies.

Briefly, our contributions within the framework are numerous and include:

- Providing a roadmap and framework for addressing pandemics
- Offering various methods for data collection from diverse sources (IoT, WSNs, RFID, Smart Phones, Mobile Apps, Crowdsourcing, social media, Drones, GPS, Health Centers, Research Centers, Volunteers, etc.)
- Addressing the problem of interoperability and data integration by designing a public health ontology and unifying data representation (Syntax and Semantic Solutions)
- Employing Fog Computing to process data in real-time and ensure a rapid response when needed.
- Utilizing Cloud Computing to manage and process big data and applying data science algorithms to extract important insights.
- Adding an additional computing layer between the cloud and fog to increase the effectiveness of the framework.
- Improving the security, privacy, and reliability of data by employing blockchain technology between medical centers
- Proposing a classification and early warning algorithm during pandemics
- Suggesting some essential and smart healthcare services that should be available during pandemics.
- Conducting simulations to demonstrate the effectiveness of our proposed framework (C-IoHT) and testing the proposed classification algorithm on real data sets.

The rest of the paper is structured as follows; Section II outlines the most relevant contributions in the literature where different algorithms are used for sending and receiving data. Section III presents the main challenges and the proposed solutions. Section IV details the overall description of our proposed framework. The results are discussed in Section V. Finally, Section VI summaries the conclusion and future work.

Related Works

This section shows an overview of the existing frameworks and approaches for outbreak pandemic management. Outbreaks of infectious diseases and pandemics pose significant threats to public health and can have devastating consequences on economies and societies. In recent years, the world has witnessed several outbreaks of infectious diseases, such as Ebola, Zika, and COVID-19 [24]. The global response to these outbreaks has highlighted the need for effective frameworks and approaches.

Mackenzie et al. [25], in 2014, developed a framework to support decision-making during outbreaks and health emergencies. The framework is designed to provide guidance on outbreak detection, risk assessment, and response. It can be used by public health officials and other stakeholders to coordinate response efforts and implement interventions to mitigate the spread of disease. Cox et al. [26], in 2014, developed a risk management framework for pandemic influenza. This framework is designed to support decision-making during a pandemic by providing guidance on risk assessment, mitigation strategies, and resource allocation. It is intended to be used by public health officials, policymakers, and other stakeholders to develop effective response plans and implement interventions to reduce the impact of a pandemic.

Huron et al. [27], in 2022, developed a framework for assessing the severity of a pandemic. The framework is designed to support decision-making by providing guidance on how to categorize the severity of a pandemic based on various factors, such as the virulence of the pathogen, the extent of community transmission, and the impact on healthcare systems. The framework can be used to help public health officials and other stakeholders prioritize response efforts and allocate resources. Wolfe et al. [28], in 2021, developed an IDSR framework to support surveillance and response to infectious diseases. The framework is designed to help countries develop effective surveillance systems for detecting and responding to outbreaks, and it includes guidance on risk assessment, case management, and communication strategies.

Firda and Haksama. [29], in 2020, developed a framework to support the resilience of health systems during crises, such as pandemics. The framework provides guidance on how to build and maintain resilient health systems that can respond to emergencies, and it includes recommendations on strengthening health system governance, workforce capacity, infrastructure, and financing. Turenne et al. [30], in 2019, proposed a conceptual framework to guide the analysis of health system resilience in the context of pandemics. Wood et al. [31], in 2012, proposed a framework for studying zoonotic disease emergence and its drivers, using the spillover of bat pathogens as a case study.

Zusook et al. [32], in 2020, proposed a framework for assessing and managing the risk of COVID-19 in the workplace, which includes risk assessment, risk management, and communication strategies. Azzopardi-muscat et al. [33], in 2014, proposed a framework for pandemic risk management based on the lessons learned from the H1N1 pandemic. WHO [34], in 2021, provided a framework for the sharing of influenza viruses and access to vaccines and other benefits in the context of pandemic influenza preparedness. Sharma et al. [35], in 2021, provided overview of the COVID-19 pandemic, including its epidemiology, clinical features, and public health measures. It also discusses the challenges in managing the pandemic and the role of technology in addressing these challenges.

Islam et al. [36], in 2021, proposed an integrated pandemic monitoring and management system that utilizes various technologies such as the Internet of Things (IoT), cloud computing, and artificial intelligence (AI) to collect and analyze data related to pandemics. The system can be used to monitor the spread of pandemics, predict their future trends, and inform decision-making. Philippe et al. [37], in 2022, reviewed various digital health interventions that have been used for pandemic management, including telemedicine, mobile health apps, and wearable devices. The authors compare the effectiveness of these interventions in terms of improving patient outcomes and reducing the burden on healthcare systems. Moss et al. [38], in 2022, described the development of a decision support system for pandemic influenza planning based on the lessons learned from the H1N1 outbreak. The system uses epidemiological data to predict the spread of the disease and provides recommendations on the allocation of resources and implementation of control measures. Knauer et al. [39], in 2022, provided a review of the pandemic planning guidance provided by federal, state, and local agencies in the United States. The authors compare the guidance provided by these agencies and identify areas where improvements could be made to better prepare for future pandemics.

Briefly, the related works provided include various frameworks and approaches for managing and responding to pandemics and infectious diseases. The WHO Global Outbreak Alert and Response Network (GOARN) Framework, the Pandemic Influenza Risk Management Framework, and the Pandemic Severity Assessment Framework are examples of frameworks developed by WHO and the CDC to guide decision-making during outbreaks and pandemics. The Integrated Disease Surveillance and Response (IDSR) Framework focuses on developing effective surveillance systems for detecting and responding to outbreaks. The Health System Resilience Framework provides guidance on building and maintaining resilient health systems that can respond to emergencies. Other works propose conceptual frameworks for analyzing health system resilience and studying zoonotic disease emergence and its drivers. Some papers focus on specific technologies, such as digital health interventions and an integrated pandemic monitoring and management system. The decision support system for pandemic influenza planning and the review of pandemic planning guidance provided by federal, state, and local agencies provides insights into the development of response plans and policies.

Challenges for framework

This section classifies the main challenges that can face building a new framework, especially in the field of health where there are many complex factors to consider. So, the challenges that may be encountered when building a new health framework include:

1. Interoperability [40]: Interoperability is closely related to data integration and sharing. It refers to the ability of different systems and devices to exchange and use data in a standardized way. Interoperability

is crucial for effective coordination and communication among healthcare providers, as well as for ensuring that patients' health information is accurate and up to date.

2. Data Integration and Sharing [41]: One of the biggest challenges in building a new health framework is integrating and sharing data from different sources. Health data is often siloed within different healthcare systems and organizations, making it difficult to combine and analyze. This challenge can be addressed by implementing standardized data formats and protocols, as well as promoting data sharing and collaboration among stakeholders.

3. Performance issue [41]: Collecting data from different resources will generate huge amount of data “Big Data”. Processing big data will cause delays and bottlenecks in the cloud. Most health services are sensitive to latency, so cloud cannot manage the big data alone. The cloud must integrate with other computing models like edge computing for facing and addressing this challenge.

4. Privacy and Security [43]: Another major challenge in building a new health framework is ensuring the privacy and security of patients' health information. With the increasing use of digital health technologies, there is a risk of data breaches and cyber-attacks. To address this challenge, healthcare organizations must implement robust security measures, such as data encryption and access controls, and comply with data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA).

5. Governance and Regulation [44]: Building a new health framework also requires strong governance and regulation to ensure that the system is effective, efficient, and ethical. This includes developing policies and procedures for data management and sharing, as well as establishing clear roles and responsibilities for different stakeholders. It also involves complying with regulatory frameworks, such as those related to patient safety and data privacy.

To summarize, the development of a new healthcare framework necessitates overcoming numerous obstacles related to data integration and sharing, interoperability, privacy and security, governance and regulation, and stakeholder engagement. Each of these hurdles demands meticulous consideration and strategic planning to ensure the efficacy, efficiency, and ethicality of the framework. The subsequent subsections provide a more in-depth analysis of each challenge and their corresponding solutions.

Interoperability

Interoperability is an important challenge that needs to be addressed when building a comprehensive health framework. In healthcare, many different systems and devices are used to collect, store, and share health data. These systems and devices often use different formats and protocols for data exchange, which can make it difficult to share data between them. Interoperability is closely related to data integration and sharing, as it refers to the ability of different systems and devices to exchange and use data in a standardized way. This means that data can be easily transferred between different systems and devices and that the data can be interpreted and used by different systems and devices consistently and reliably [45].

Interoperability is crucial for effective coordination and communication among healthcare providers. For example, if a patient is referred to a specialist, the specialist needs access to the patient's health information to make an accurate diagnosis and provide appropriate treatment. Without interoperability, it may be difficult or impossible for the specialist to access the patient's health information, which can lead to delays in treatment and potentially negative health outcomes. Interoperability is also important for ensuring that patients' health information is accurate and up-to-date. If different systems and devices are not able to exchange data in a standardized way, it can lead to discrepancies in patients' health information. For example, if a patient's medication list is not updated in one system, but is updated in another system, this can lead to confusion and potentially harmful medication errors.

To address the challenge of interoperability, several strategies can be employed. One strategy is the use of standardized data formats and protocols for data exchange. For example, the use of the Health Level Seven (HL7) standard can ensure that different systems and devices can exchange data in a standardized way [46]. Another strategy is the use of application programming interfaces (APIs) to enable different systems and devices to communicate with each other [47]. Table I shows common solutions for the interoperability issue:

TABLE I Solutions for the interoperability issue

Method Name	*Mechanism*	*Limitation*
Middleware [48]	Create publisher and subscriber place to exchange messages among different systems.	It is required from all systems to subscribe then register its services and functions which is not acceptable for many of them.
Mapping [49]	Change data from a format to another one like from XML to JSON	It is not enough, and many systems dealing with raw data like text.
Wrapper [50]	Capsulate the legacy systems to read their data	It is only work with legacy systems
Translator [50]	Translate data between client and server	It needs a static code for each service or system
Data Adapter [51]	Connect to different database systems	It needs full access on the systems databases or open databases
API - application programming interface [52]	Create public functions for each system to provide data to others	APIs need an interoperability method for integration among them
Service-oriented architecture (SOA) [53]	Create public webservices for each system to provide data to others	It needs an interoperability method for integration among them
Ontology [54]	Create shared dictionary of common concepts to be used by services	There is no general ontology for health domain, in addition it requires all old systems to updates their data description.
Unified Developing Platform [55]	Create a platform for developer to generate homogeneity services	It supports only the systems that will be developed on the platform.
Web Mining [56]	Try to understand the meaning of messages among systems	If there are no common concepts used, the accuracy will be adversely affected.

In summary, interoperability is a crucial challenge that needs to be addressed when building a comprehensive health framework. It is important for effective coordination and communication among healthcare providers, as well as for ensuring that patients' health information is accurate and up to date. Strategies such as the use of standardized data formats and protocols and the use of APIs can help to overcome this challenge.

Data Integration and Sharing

Data integration and sharing play a critical role in the development of a new health framework. The ability to integrate and share data from various sources can facilitate more comprehensive and accurate assessments of health outcomes, which in turn can inform policy decisions, resource allocation, and disease prevention efforts. However, integrating and sharing health data can be a challenging task due to the complexity and diversity of data sources. Healthcare data is often siloed within different healthcare systems and organizations, and it may be stored in different formats, using different terminologies, and collected for different purposes. As a result, data integration and sharing require the establishment of standardized data formats and protocols that can enable the exchange and analysis of data across different systems and organizations [57].

Standardization is crucial to ensure that data from various sources can be integrated and analyzed accurately [58]. Standardization can include the use of standardized terminologies, coding schemes, and data exchange protocols that allow healthcare providers to exchange and use data in a consistent and interoperable manner. For example, standardized coding systems such as ICD-10 (International Classification of Diseases) and SNOMED CT (Systematized Nomenclature of Medicine-Clinical Terms) can be used to describe medical conditions and procedures consistently across different healthcare systems and organizations [59]. Promoting data sharing and collaboration among stakeholders is also crucial for ensuring that health data can be used effectively to improve health outcomes. Data sharing and collaboration can involve the creation of data-sharing agreements, establishing data governance structures, and implementing secure data exchange mechanisms. Data sharing and collaboration can also require the involvement of various stakeholders, including healthcare providers, patients, researchers, and policymakers.

In summary, data integration and sharing are critical for developing a new health framework. The establishment of standardized data formats and protocols, as well as the promotion of data sharing and collaboration, can enable more comprehensive and accurate assessments of health outcomes, which in turn can inform policy decisions, resource allocation, and disease prevention efforts.

Big Data Processing and Performance Challenge

One of the additional challenges to building a new health framework is the processing and analysis of big data [60]. With the emergence of data science techniques, such as machine learning and data mining, it has become possible to analyze data related to specific diseases, predict the number of infected individuals, and study the impact of the epidemic on various activities, such as curfews and air quality. The amount of data generated from various sources is vast, which poses a challenge for service providers and cloud computing [61]. To address this challenge, some researchers have proposed using fog or edge computing to reduce the burden on service providers and cloud computing. While fog computing offers several advantages over cloud computing, it cannot replace it, but they must work together to achieve effective collaboration [62].

Fog computing enables the processing and analysis of data closer to the source, which leads to lower latency and faster response times. This technology can be particularly useful in healthcare, where timely response is critical in decision-making processes. By reducing the burden on cloud computing, fog computing can also help to reduce costs associated with data processing and analysis. Moreover, the integration of fog computing and cloud computing can enable the creation of a hybrid infrastructure that offers the best of both worlds [63]. The combination of the two can offer scalability, reliability, and security, as well as cost-effectiveness. This approach can be applied to various healthcare use cases, such as remote patient monitoring, real-time data analysis, and predictive analytics. Table II depicts a comparison between cloud and fog computing [64].

In summary, the processing and analysis of big data are essential for building a new health framework. By leveraging fog computing and cloud computing, healthcare providers can create a hybrid infrastructure that offers scalability, reliability, security, and cost-effectiveness.

TABLE II Comparison between cloud and fog

Factor	Fog	Cloud
Nodes Number	Large number of nodes	One or few servers
Storage Type	Caching	Permanent
Cooperation	Mostly Cooperatively	Mostly Independently
Connection	Wireless	Internet
Location	Closed to user in the edge of network	Far from users
Distribution	Dense	Central
Application	Supports applications need RT interactive	Support applications need high computing power
Real Time	Strong Supported	Weak Supported
Mobility	Strong Supported	Weak Supported
Accountability	Weak	Strong

Challenge of Data Security and Privacy

In recent years, there has been an increasing need for enhanced data security, protection, reliability, and privacy [65]. Blockchain technology can offer decentralization, transparency, and significant data security advantages. Although blockchain technology initially emerged with digital currency applications, its use has quickly expanded to new applications such as smart contracts, preventing fake news on social media, and ensuring the safety and reliability of stored data [66]. Many medical research studies have also employed blockchain technology in other applications [67] that can be classified into five essential categories:

- Data Storage and Availability: Secure and reliable storage of patient data with fast access and availability of the distributed db.
- Access Management: Access policies have significantly changed for medical services during the COVID-19 pandemic.

- Supply Chains: For supplying vaccines or special drugs during pandemics and fighting against manipulation or corruption.
- Smart Contracts: Smart contracts with infected individuals for tracking cases in real-time and detecting contact cases.
- Data Sharing: Whether for educational or collaborative purposes.

Researchers in a reference study have pointed out the possibility of employing blockchain technology to create a system that supports data exchange between trusted parties during pandemics, reducing the time required for clinical trials [68].

In this study, blockchain technology will be employed to protect the security of healthcare data in the IoHT environment, which we have classified into six main categories:

- Continuous Monitoring and Mobile Health
- Medical Artificial Intelligence and Smart Devices
- Wearable Sensors and Applications
- Medical Data Analytics
- Assistance for the Elderly, Chronic Disease Patients, and People with Special Needs
- Community Health

In summary, there is a significant need to build a unified working platform in the healthcare sector at the city level, at least, that supports the collection of data from various sources and services scattered everywhere in real-time. The platform should solve the challenges of non-homogeneous data while ensuring the security, reliability, and privacy of this data and its users, and provide the necessary infrastructure for using blockchain technology. Furthermore, the platform should support different applications and stakeholders to create a more efficient, effective, and equitable healthcare system.

Governance and regulation

Governance and regulation are essential components of any healthcare system, and the proposed platform is no exception. Building a new health framework requires the development of strong governance and regulatory frameworks to ensure that the system is effective, efficient, and ethical. This involves several critical aspects, including data management and sharing policies, stakeholder roles and responsibilities, and compliance with regulatory frameworks. One critical aspect of governance and regulation is the development of data management and sharing policies. These policies outline how healthcare data is collected, stored, accessed, and shared, as well as who has access to the data and for what purposes. Developing effective policies requires consideration of ethical and legal frameworks, as well as the diverse needs and expectations of different stakeholders, including patients, healthcare providers, and researchers [69].

Establishing clear roles and responsibilities for different stakeholders is another important aspect of governance and regulation. The proposed platform involves multiple stakeholders, including patients, healthcare providers, researchers, regulators, and technology providers. Defining the roles and responsibilities of each stakeholder is crucial to ensure that everyone works together towards a common goal. Compliance with regulatory frameworks is also essential. Healthcare is subject to various regulations that ensure patient safety and data privacy. Examples of regulatory frameworks include the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Complying with these regulations requires developing effective policies and procedures for data management and sharing, as well as ensuring that all stakeholders understand and adhere to them [70].

To summarize, governance and regulation are crucial components of the proposed healthcare platform. Developing effective policies for data management and sharing, defining clear stakeholder roles and responsibilities, and complying with regulatory frameworks are all critical to ensuring that the platform is effective, efficient, and ethical.

Proposed C-IoHT framework

To address the challenges previously presented and classified during the literature review of previous research and business in the healthcare sector, and to build a robust healthcare system capable of coping with pandemics, the research proposes a comprehensive framework for managing a unified healthcare system. The framework relies on medical IoT and different models of computing, in addition to data sciences algorithms and blockchain technology besides many necessary services in various fields that can play an important role during pandemics. C-IoHT is divided into five main layers, each of which addresses an issue or challenge of the challenges, and all of these layers collaborate to create a robust system. Figure 2 illustrates the five layers with the basic objects of each layer, while Figure 3 provides more details about the layers' main functions, i.e. the tools and resources for data collection, in addition to the proposed services and applications.

The C-IoHT framework proposes to establish a system for healthcare data that is secure, dependable, and respects privacy, which can be accessed and shared by authorized entities. The framework consists of the following main goals (which are distributed on five layers to address most of the challenges) which are:

1. Data acquisition and management: the framework is responsible for collecting data from various sources and devices, such as wearable sensors, medical devices, and social media. The layer includes tools and resources such as cloud computing, edge computing, and big data analytics to manage and process the collected data.

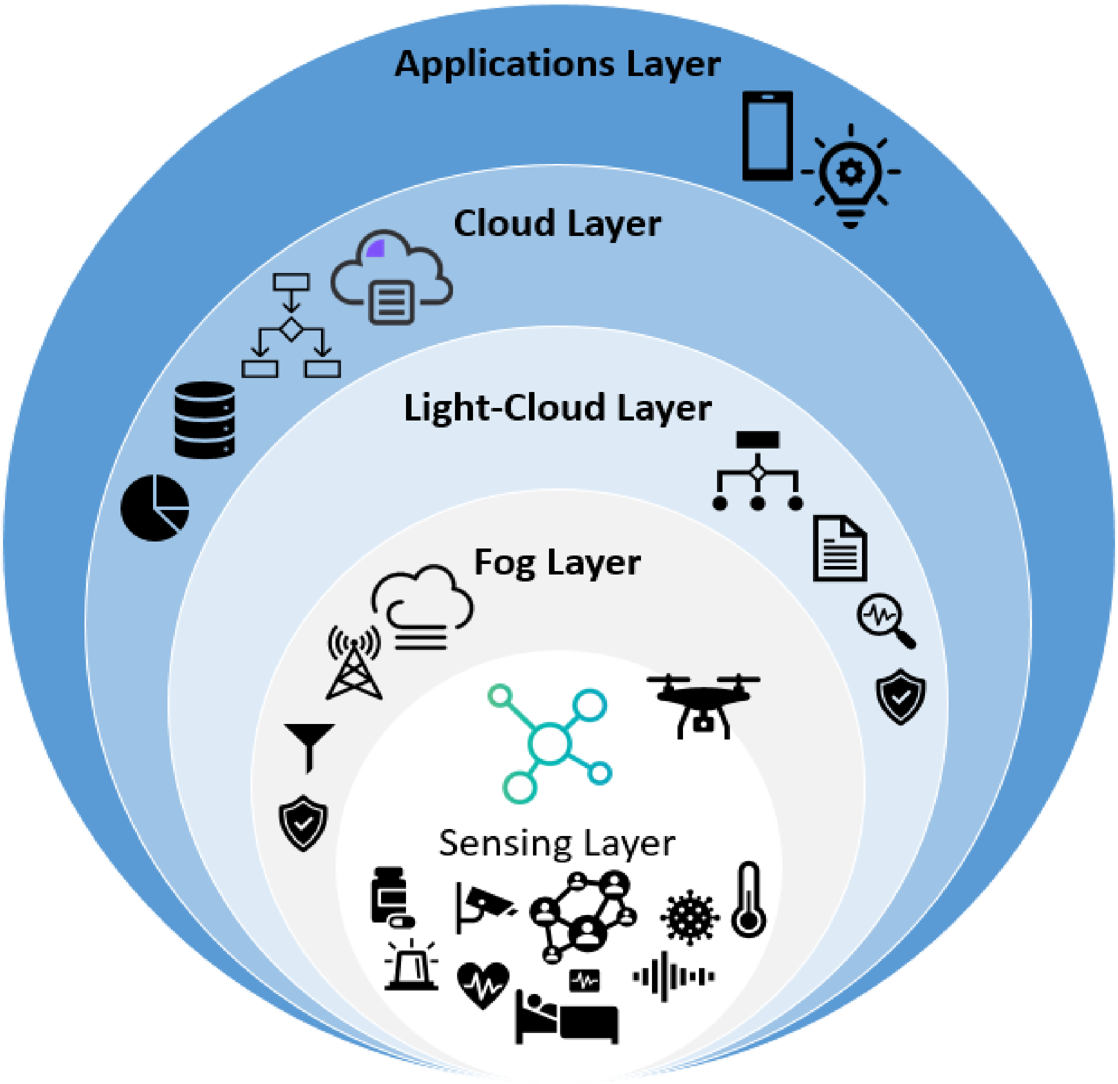


Fig 2: Proposed Framework (C-IoHT) General View

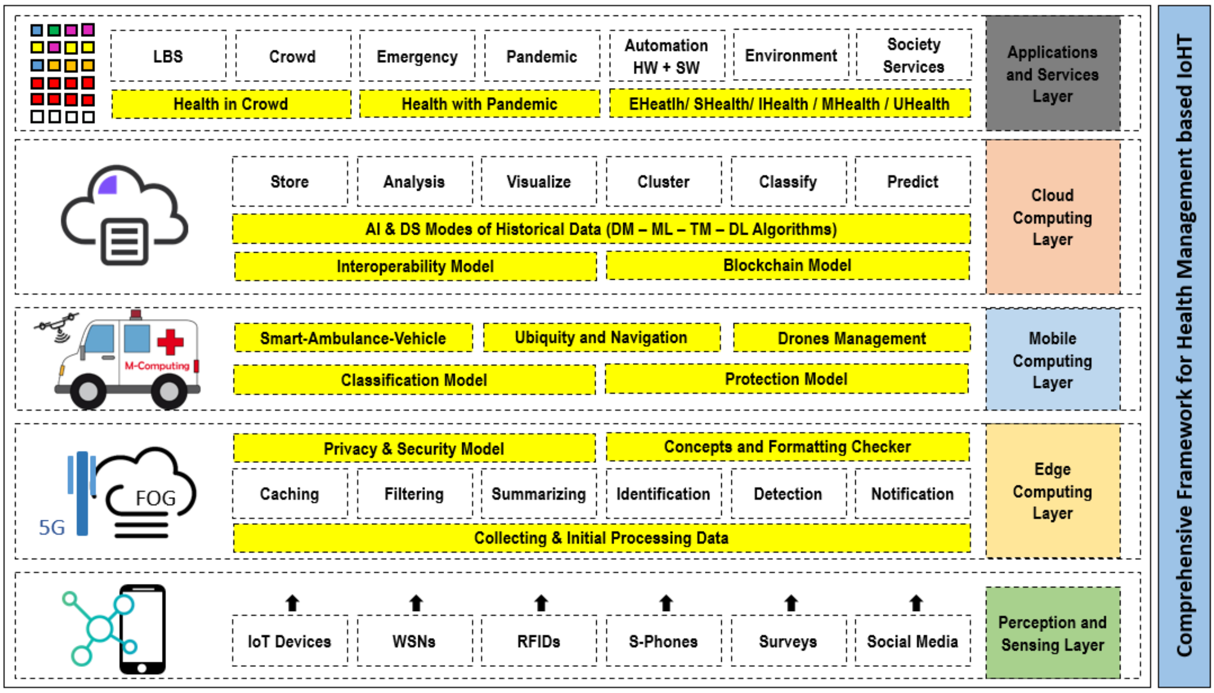


Fig 3: Proposed Framework (C-IoHT) Details View

2. Data sharing and collaboration: the framework is responsible for enabling authorized parties to access and share healthcare data for various purposes, such as clinical research and public health surveillance. The layer includes technologies such as smart contracts, federated learning, and data anonymization to ensure privacy and secure data sharing.
3. Data storage and security: the framework is responsible for securely storing the collected data and ensuring its integrity and confidentiality. The layer includes technologies such as blockchain, encryption, and access control to protect the data from unauthorized access and manipulation.
4. Governance and policy: the framework is responsible for defining and enforcing policies and regulations that govern the collection, storage, sharing, and use of healthcare data. The layer includes stakeholders such as government agencies, healthcare providers, patients, and researchers, and requires a collaborative approach to develop and implement effective policies and regulations.
5. Applications and services: the framework is responsible for providing various applications and services that can leverage the collected and shared healthcare data to improve patient care, public health, and medical research. The layer includes applications such as telemedicine, patient engagement, and disease management

In summary, the proposed C-IoHT framework aims to address the challenges in the healthcare sector by leveraging the potential of medical IoT, computing, and blockchain technologies to create a secure, reliable, and privacy-preserving healthcare system. The framework can provide numerous benefits, such as faster and more accurate diagnosis, personalized treatment, and timely public health interventions, which can ultimately improve patient outcomes and population health. To better understand the entire system, it is mandatory to describe each layer, its specific functions, and the challenges it addresses.

Monitoring and Sensing Layer

The proposed C-IoHT framework offers numerous benefits and advantages. It integrates various data sources to provide a more comprehensive view of an individual's health and well-being, which can enhance the accuracy of diagnosis and treatment. Additionally, it enables remote monitoring and telemedicine, thereby offering more convenient and accessible healthcare options, particularly for those residing in remote or underserved areas. Furthermore, the framework can facilitate early detection and prediction of health issues and disease outbreaks, which is particularly crucial during pandemics or epidemics, by monitoring data from various sources such as social media, environmental sensors, and wearable devices.

In addition, the C-IoHT framework can promote data-driven research and development in healthcare, allowing for the analysis of large and diverse datasets to uncover insights and improve healthcare outcomes. It can also enhance collaboration between healthcare providers and organizations by promoting interoperability and standardization of data. Overall, the proposed IoHT framework can significantly transform healthcare by harnessing the power of IoT, big data analytics, and AI technologies to improve the quality, accessibility, and efficiency of healthcare services.

We have undertaken the task of categorizing data sources into six primary categories, each with a distinct format for the data that they produce.

- The first category includes Smart IoT devices, such as smartphones and smart cars, which send data in the form of queries or vectors of values. This data format is typically used to provide real-time or near-real-time data that can be used for monitoring or decision-making.
- The second category is WSNs, or wireless sensor networks, which may be wearable or distributed in the surrounding environment, such as in homes or on roads. WSNs are responsible for measurements of vital signs such as body temperature, blood pressure, heart rate, respiration, as well as gas and pollution sensors, among others. These sensors use a key-value format for data storage, which allows for the collection of large amounts of data from a wide variety of sources. WSNs can also enable the collection of data from hard-to-reach populations, such as those in rural or remote areas.
- The third category is RFID tags, which are used to identify and track objects by assigning them a unique identifier. This can be used for monitoring or tracking their location, which reduces the need for physical data collection and saves time and resources.
- The fourth category is mobile applications, particularly in the medical field, which allow users to collect and contribute data via crowdsourcing. These apps use databases to store the collected data, enabling remote data collection and reducing the cost of data collection and analysis compared to traditional methods.
- The fifth category is surveys and polls, which are traditional methods for data collection that are still commonly used to gather information on a specific topic or from a certain group or sample. The data collected is often stored in Excel sheets, which allows for easy analysis and visualization.
- The sixth and final category is social media platforms, particularly Twitter, which have become the largest and fastest source of news and information. However, the data collected from these platforms is often unstructured text and requires processing to become useful. Social media platforms allow for the collection of large amounts of data from a wide variety of sources, which can provide insights that would be difficult to obtain through other means.

The C-IoHT framework aims to address various challenges related to data integration, heterogeneity, performance, security, and privacy through its multiple layers. Additionally, the framework can overcome common challenges related to real-time data provision, remote data collection, large-scale data aggregation from diverse sources, data collection from hard-to-reach populations, and cost-effectiveness of data collection and analysis compared to conventional methods.

Edge Computing (Fog) Layer

The Edge Computing (Fog) layer plays a vital role in the healthcare industry, facilitating rapid response and data processing without latency. This layer takes various forms, such as mobile devices, drones, road units, traffic lights, default gateways, and others, with each dedicated to managing a specific area or building and performing specific functions. In the proposed framework, the Fog layer performs additional functions to overcome the limitations of interoperation, privacy, and data security while improving data processing performance and emergency response times.

To begin with, the Fog node receives data from the six sources at the Sensing layer, and then processes the data by removing duplicates, summarizing data, isolating outliers, and converting some images to textual values to minimize the amount of data transmitted to the cloud. The Fog node also identifies emergency situations and responds promptly. Secondly, the Fog node standardizes all data representation methods by converting them to JSON format to enable greater interoperability and integration between systems and resources. This is called the Syntax Interoperability Solution. Additionally, the Fog node verifies the use of the concepts present in the proposed ontology to ensure semantic interoperability, which is crucial for interoperation. Thirdly, the Fog node applies specific data policies, such as removing personal information, replacing identity with a pseudonym (hash code), blurring the precise location by a percentage that does not affect the quality of the main medical service, and encrypting sensitive data before transmitting the data to the Light-Cloud. The Fog node also utilizes blockchain to ensure data transparency, reliability, and non-repudiation. Finally, the Fog node identifies and prevents anomalous data sources, such as malfunctioning or malicious sensors that send significantly different data than other sources. This is achieved through machine learning algorithms that can recognize patterns and deviations from the norm. Overall, the Fog layer provides critical support for healthcare services by enhancing response times, data processing efficiency, and privacy and security measures.

Light-Cloud Computing Layer

It is a key component of the proposed comprehensive platform for medical IoT. This layer is designed to sit between the Fog and the Cloud, providing faster data processing capabilities compared to the Cloud and more computing power than the Fog. This middle layer will play an important role in situations where we need to isolate certain areas or cluster their data and process it independently and more quickly than the Cloud and with greater capacity than the Fog. Each node in this layer will oversee a cluster or group of Fog nodes that serve a large geographical area (e.g., a neighborhood or an entire sector). This layer will also play a significant role in enhancing interoperation, data security, and privacy. The layer will ensure that data is correctly described in accordance with the proposed unified ontology stored in the cloud, thereby significantly reducing the burden on the Cloud and service providers, facilitating integration and collaboration between services, and adding a layer of identity obfuscation and data masking to the data responsible for the region, thus enhancing user data privacy and security.

Moreover, the nodes in this layer will serve as master nodes for the proposed blockchain-based data management system that ensures the reliability, transparency, and responsibility of shared data between medical centers in different regions, in addition to guaranteeing data availability and immutability. Finally, this layer introduces the idea of mobile medical services, such as an integrated medical vehicle for collecting samples from patients in their homes without the need to visit medical centers, especially during epidemics, to relieve the burden on medical centers and reduce the risk of infection.

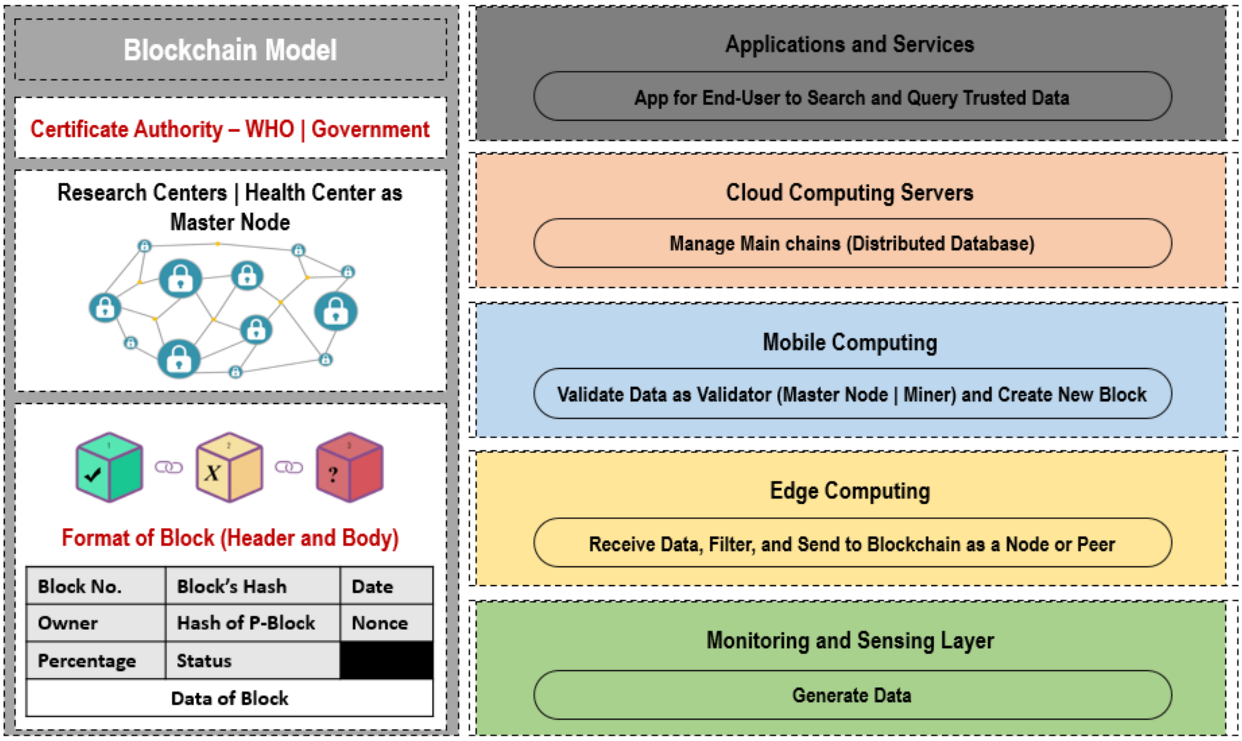

Blockchain Model
Certificate Authority – WHO | Government
Research Centers | Health Center as Master Node
Format of Block (Header and Body)
Block No.
Block's Hash
Date
Owner
Hash of P-Block
Nonce
Percentage
Status
Data of Block
Applications and Services
App for End-User to Search and Query Trusted Data
Cloud Computing Servers
Manage Main chains (Distributed Database)
Mobile Computing
Validate Data as Validator (Master Node | Miner) and Create New Block
Edge Computing
Receive Data, Filter, and Send to Blockchain as a Node or Peer
Monitoring and Sensing Layer
Generate Data

Fig 4: Blockchain Structure in the C-IoHT

This layer will also be responsible for drone stations and the proposed smart boxes that could serve as a means of delivering medicine or collecting samples from hard-to-reach locations due to the spread of infection, as well as reading certain sensor values, thereby reducing direct contact.

Figure 4 shows the proposed architecture for employing blockchain among accredited medical centers. In the proposed blockchain architecture, the fog node will be the Peer that sends information, and the intermediate nodes in the Light-Cloud layer, which represent health centers, will form a block with data that has been discovered and studied. And when a master node is sent to a new block, we will adopt a special consensus algorithm (Min-Max). The master node will verify any block before it is accepted into the chain, and if the approval value exceeds the Min threshold, a positive vote will install the block in the name of the node that sent it, provided that the number of opponents does not exceed the Max threshold value.

In summary, the Light-Cloud Computing Layer will play a vital role in enhancing the functionality and efficiency of the proposed comprehensive platform for medical IoT, ensuring data privacy and security, facilitating integration and collaboration between services, and enabling mobile medical services and drone stations to provide improved healthcare access in hard-to-reach areas.

Cloud Layer

The cloud layer is an essential part of the proposed framework. It serves as a central repository for all the data collected from the previous layers. The cloud layer provides a platform for data storage and management. The data stored in the cloud is permanent and can be accessed from anywhere and at any time. To make the most of the data stored in the cloud, AI and data science algorithms must be applied. These algorithms are used to extract insights and new knowledge from data. Statistical operations and various algorithms such as Text Mining (TM), Data Mining (DM), Machine Learning (ML), and Deep Learning (DL) are used to identify patterns, trends, and relationships within the data. These insights are important for decision-making, especially in times of pandemics or health crises.

Another important role of the cloud layer is to manage and enable interoperability. The cloud layer also plays a vital role in managing the ontology of concepts, terms, and medical data proposed in the research (see Figure 5). Ontology management involves organizing and categorizing the data in a way that makes it easier to understand and use. This is important for efficient data management and analysis. The cloud layer also provides privacy and security for the stored data. Data is encrypted to increase privacy and security, and it is divided into multiple servers to enhance availability and reliability. This ensures that the data is protected against unauthorized access, hacking, or any other security threats.

In times of pandemics, data collection is crucial, but equally important is the efficient use of this data. To this end, an algorithm has been proposed that operates in real-time to assist in the early detection of individuals with mild symptoms. This algorithm relies on a dataset containing demographic information, as well as vital indicators and measurements, such as age, gender, weight, occupation, medical history, marital status, region, number of contacts, and other relevant data. To improve the accuracy of the classification and early warning in the proposed algorithm, five important ideas have been incorporated:

- Data segmentation into two groups: healthy individuals and those with chronic diseases or elderly individuals. This reduces the impact of numerous variables and significant differences between the characteristics of the two groups, thereby mitigating the model's dispersion. Additionally, different thresholds can be used in the classification process.
- Data segmentation at the regional level to reduce the burden on the cloud and activate the role of the new Light-Cloud computing layer.
- Merging columns of data into main ones in the initial classification, and then working on all merged columns if there is a relationship with the main column. For example, for respiratory diseases, the classification can rely in beginning on a single column indicating whether the user has a respiratory disease or not, rather than asking about shortness of breath, pneumonia, asthma, and other related conditions, leading to better accuracy. We grouped the symptoms in 11 system in the human body cleared in the Figure 7 (Proposed Classification Algorithm)
- Continuous testing and classification to enable early detection and statistics by employing the fog contract instead of cloud-based predictions.
- Adopting three machine learning models that provide the highest accuracy during the training phase, followed by taking the majority principle in the testing phase.

Figure 6 illustrates the proposed classification algorithm's procedural sequence. Upon initial diagnosis (positive classification), a mobile ambulance or drone can deliver samples to the hospital instead of the patient coming to the health center in person, increasing their exposure to infection or exposing others to the virus.

The Services and Applications Layer

The Services and Applications Layer plays a crucial role in managing and aggregating all relevant services in one place for pandemic management. Service providers are responsible for registering their new services, testing them, ensuring their trustworthiness, and ensuring their compliance with proposed ontological concepts and standards. This layer helps achieve comprehensive management for health issues by integrating the following proposed and important services in pandemics.

One of the most important services that must be achieved for everyone is Electronic Health Record (EHR). It improves the chances of disease detection in case of infection and improves the chances of providing appropriate treatment and testing. Another service is Monitor and Tracking, where people can be monitored, and their data can be stored locally for several days. In case of a person's confirmed infection, it is possible to refer to the points of interest where the person has been during the previous days to detect information about the spread of the infection.

Various services are proposed and deemed important for pandemic management which are:

- Monitor and Tracking: This service allows people to be monitored and their data to be stored locally for several days. In case of a person's confirmed infection, it is possible to refer to the points of interest where the person has been during the previous days to detect information about the spread of the infection. If the person is not infected, the data can be deleted and replaced with data from other days.

- Medicine and Samples: A service to request medication or deliver samples through drones, but it requires the presence of smart boxes with unique numbers at each home so that delivery and receipt can be based on the box ID.
- Crowd Monitoring: This service uses machine learning algorithms and image processing techniques to automatically detect violators among the crowds and monitor the degree of compliance with precautions and measures.
- Navigation: Navigation is important for choosing the best route in emergency situations, especially with closures in some areas.
- First Aid: This service explains to people what they should do for first aid during pandemics while waiting for ambulances, using images, instructions, and some videos.

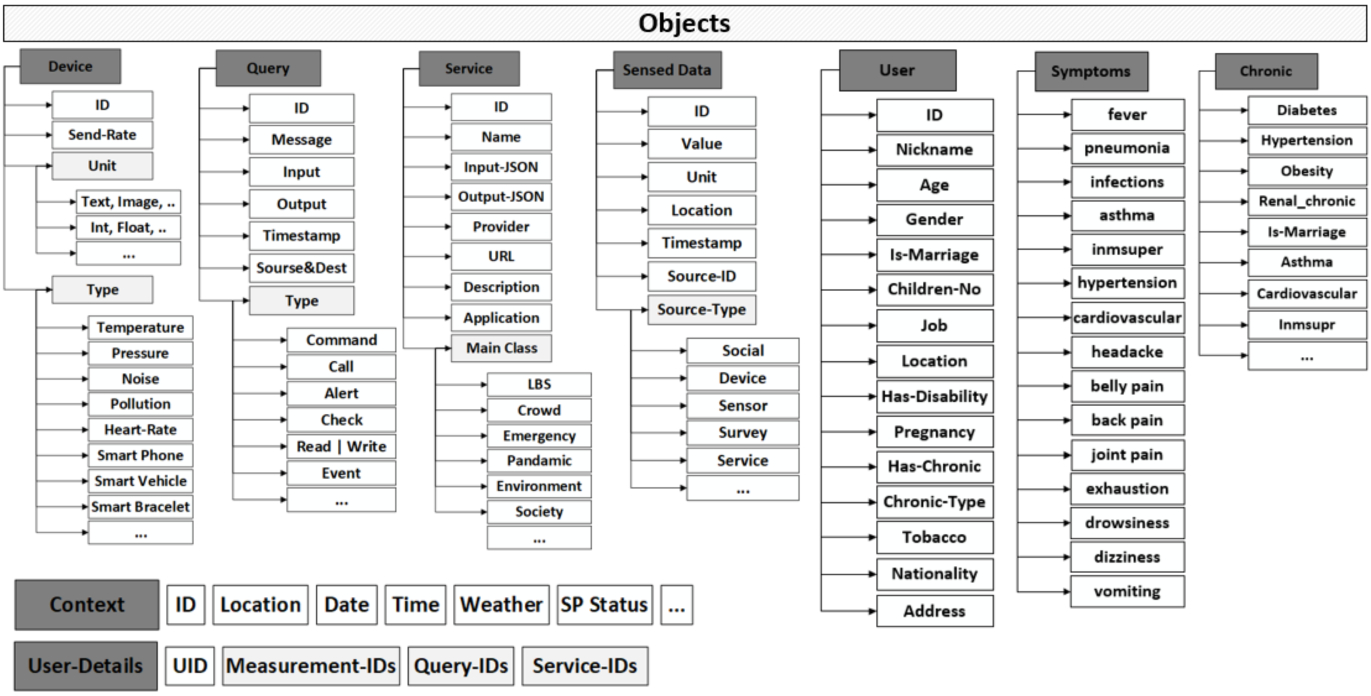


Fig 5: Proposed Ontology for Health Domain

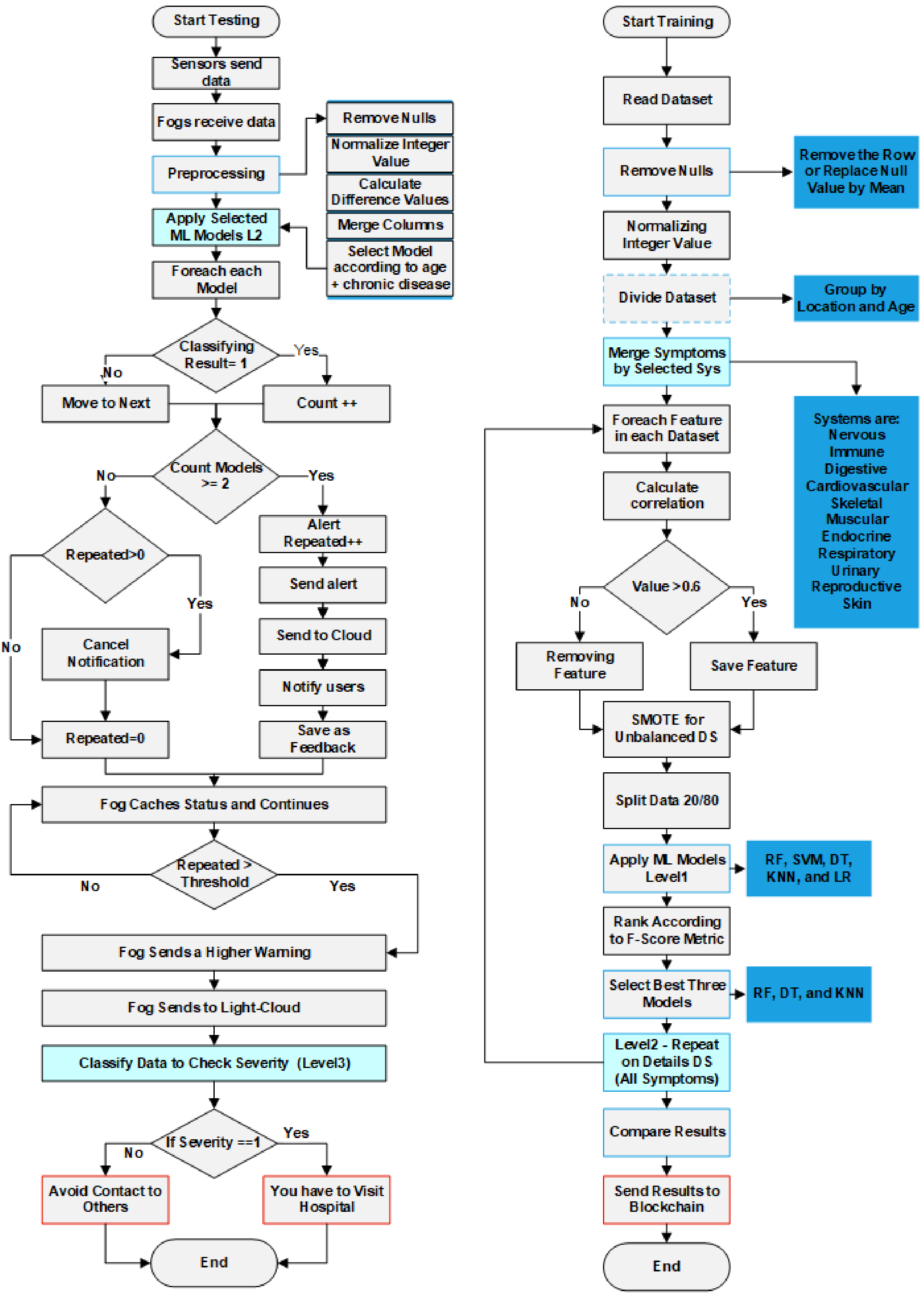


Fig 6: Proposed Classification Algorithm for Early Notification

- Social: This service uses NLP for early detection of alerts received from crowdsourcing about the spread of a certain disease or the occurrence of an emergency in a particular area.
- Awareness: This service sends health information and advice to users to raise their health awareness, prevent infection, and avoid false rumors.
- E-Consultation: This service allows for electronic consultations with healthcare providers.

- Contact Tracing: This service allows tracking the contacts of an infected person to identify potential exposures and notify them to take appropriate measures. This can be achieved through a mobile application that uses Bluetooth or GPS to trace the contacts.
- Remote Patient Monitoring: This service enables healthcare professionals to monitor the health status of patients remotely. This service can use wearable devices or sensors to collect health data and transmit it to healthcare providers in real-time.
- Mental Health Support: This service provides mental health support to people during pandemics. This service can include chatbots, virtual support groups, and teletherapy sessions to provide counseling and support to people experiencing stress and anxiety.
- Vaccine Management: This service helps manage the distribution and administration of vaccines during pandemics. This service can include a centralized vaccine registry, vaccine scheduling and appointment management, and vaccine inventory management.
- Emergency Response: This service provides emergency response services during pandemics. This service can include ambulance dispatch, emergency medical services, and emergency supplies management.
- Telemedicine: This service provides healthcare services remotely through telecommunication technologies. This service can include video consultations, remote diagnosis, and remote patient monitoring.
- Public Health Surveillance: This service monitors and tracks the spread of pandemics at a population level. This service can include real-time disease surveillance, outbreak detection and response, and data analysis and visualization.
- Data Analytics and Artificial Intelligence: This service uses data analytics and artificial intelligence to identify patterns and trends in pandemics and provide insights for decision-making. This service can include predictive modeling, data visualization, and automated decision-making.
- The electronic prescription service allows for dispensing or requesting certain medications that require a prescription, eliminating the need for a paper prescription.
- The robotics and automation service involves the use of automated robots for patient care in intensive care or isolation rooms, minimizing direct contact during medication distribution and vital signs monitoring.
- The alternative medicine and herbal medicine service provides information about herbs that have immune-boosting properties.
- Special services catering to the elderly, disabled, and chronically ill must be available at all times, even during pandemics, to meet their ongoing medical and other needs.

The unified ontology will help integrate services provided by different service providers. Moreover, the same service can also be provided by multiple entities, which will improve the quality of services and enable the user to choose the best or most suitable service based on their current context. Moreover, by integrating these domains, comprehensive management for health issues can be achieved during pandemics. The Services and Applications Layer can help streamline and manage these services, making pandemic management more effective and efficient.

Case Study - Coronavirus

In the following, we present two scenarios for using the proposed framework. The first scenario shows the working condition of the classes in a normal situation, while the second explains how the classes work during pandemics.

First general scenario - A normal situation

The first layer will collect data from users at a certain rate and send this data to the nearest fog node. The fog node cleans and summarizes the data, in addition to matching the variables and concepts used in describing the data with the unified ontology. The fog node re-encapsulates the abstracted data in a unified JSON or XML representation before sending it to the next layer (Light-Cloud). Further, the fog node will compare the user's vital values with the normal values for these values. In the event of a significant change in the values, an alert will be sent to the user through an application or a bracelet and to Light-Cloud.

The Light-Cloud layer compares the rate of change in biometrics for each user with the previous one (the rate of change for each user is computed and updated periodically in the cloud based on the user's EHR and then sent to Light-Cloud). If there is no significant change, the summarized data will be sent to the cloud as a new block when it is completed (according to data volume or time rate) to save the data from modification. Light-Cloud also measures the rate of change in an entire region. So that if the number of alerts detected or coming from fog nodes exceeds a certain threshold, an urgent alert is sent to the cloud.

The cloud creates a standardized EHR for each user and sends an update about each user's normal rate of change to the Light-Cloud layer. The cloud also tests the alerts coming from the previous layer. If there are alerts in many areas greater than a certain limit, it will go directly to work on the exceptional situation scenario.

Second scenario - the exceptional situation

When the cloud sends an alert to move to this mode, the layers will perform the same tasks as in the first scenario faster. Fog nodes receive sensor data at RT and send it to the Light-Cloud layer at a shorter rate. Light-Cloud also reduces its transmission time to the cloud. Also, the applications layer will activate many services during pandemics (such as health news, health awareness, general prevention methods, first aid, and mobile services for medical centers, etc.). Finally, a new blockchain will be formed to capture pandemic data or exceptional cases.

Fog nodes will initially warn users who have a difference from normal rates to take precautions and avoid contact with others. As for the Light-Cloud layer, it will do a very important job related to the implementation of the proposed ML-Classification Algorithm. Classification will be applied in stages or levels.

- At the first general level, the symptoms of a particular part of the body are grouped into their system. For example, if there is a cough, shortness of breath, runny nose, congestion, etc., it will indicate a problem in the respiratory system, and so on for the other major systems in the body. Then the machine is trained on this data for people who have a noticeable change in addition to the data of healthy people. Then test the accuracy of the classifier, and if it exceeds a certain accuracy threshold, the three best classification models are selected and added as a block within the new blockchain. Other nodes in the Light Cloud will test what the block-originating node has learned and confirm with approval or rejection. If approval exceeds a certain limit, Min, and rejection is less than a certain limit, Max, the block will be approved within the chain, work on its results, and move to the second level. Important note: The algorithm will always be implemented on two categories of data, the elderly and people with chronic diseases, and the category of normal people.

- Based on the previous results, a relationship between one or more organs will be discovered in the new disease spread, then the level of detailed training (level two) will begin. At this level, all symptoms related to the organs are taken. These symptoms are taken in detail within the training process of the classification algorithm to accurately detect symptoms associated with the pandemic. The results are sent to the cloud to be compared with the results of all other regions and to detect whether or not there is a relationship to the place in the spread of the disease. If there is a relationship, some areas will be isolated and some services in the application layer will be activated to satisfy these areas. Also, the three most accurate classification models are sent to the fog nodes to test the data of each user at RT. The status of each user is monitored and classified as to whether they are infected or not.

- In the last stage, and based on the continuous data, and in the event of an increase in the number of infected people, and a different level of vulnerability to the infected, the previous classification algorithm will be retrained on the injured only, to know the degree of severity based on the symptoms and data of the user (age group, gender, location, suffering from chronic diseases, ...). Thus, the fog node will always perform two tests on the data, a test to classify the user as to whether he is infected or not, and if he is infected, the severity of the injury will be tested. Based on the classification of the user's condition, the appropriate alert will be sent of the need to isolate only or the need to communicate with a medical center. The classifier will help to warn the user early and thus prevent his condition from deteriorating for the worse.

At the same time, the research medical centers will work on the collected data and analyze it to discover a quick treatment, and any discovery will be added to the new blockchain in the same way as before and tested by other centers. Meaning, medical centers will collaborate to test treatments. Actually, the results of the proposed classification algorithm are tested on actual data (Corona virus data set) in the next section, in addition to the results of the speed rate simulation in the analysis, the data processing of the three computing layers, the effect of the added Light-Cloud layer, and finally the images of the proposed new blockchain realization.

Results and Simulation

To validate the effectiveness of the proposed framework, multiple experiments and tests were conducted. The tesbeds are performed by using Visual Studio .Net 2019 environment.

First Experiment

The aim of the experiment is to demonstrate the performance enhancement achievable through the use of each layer. In order to carry our it, a simulator was developed to demonstrate the extent of performance enhancement achievable through the use of the new Light-Cloud computing layer. The computing layers - Fog, Light-Cloud, and Cloud - were equipped with variables for the number of processors or Nodes, the processing time required for a single task, task size, packet size, and connection time required for each layer. The performance of each layer was evaluated based on the total time required to transmit and process a considerable amount of data, which was tested across a range of sizes ranging from 1GB to 100 GB.

Figure 7 depicts the values inputted for the variables within the simulator and the results presented in tabular format, showcasing the requisite times in each layer for every data size. A graphical chart was also incorporated, with the X-axis denoting the data size and the Y-axis illustrating the delay time in milliseconds (i.e., the total time required). The experiment demonstrated that Light-Cloud outperformed both Fog and Cloud in terms of performance, achieving the lowest latency in most cases. These results validate the efficacy of incorporating the new layer between the Fog and Cloud layers for enhanced organizational performance. Figure 8 showcases the outcomes of the experiment in bar chart form.

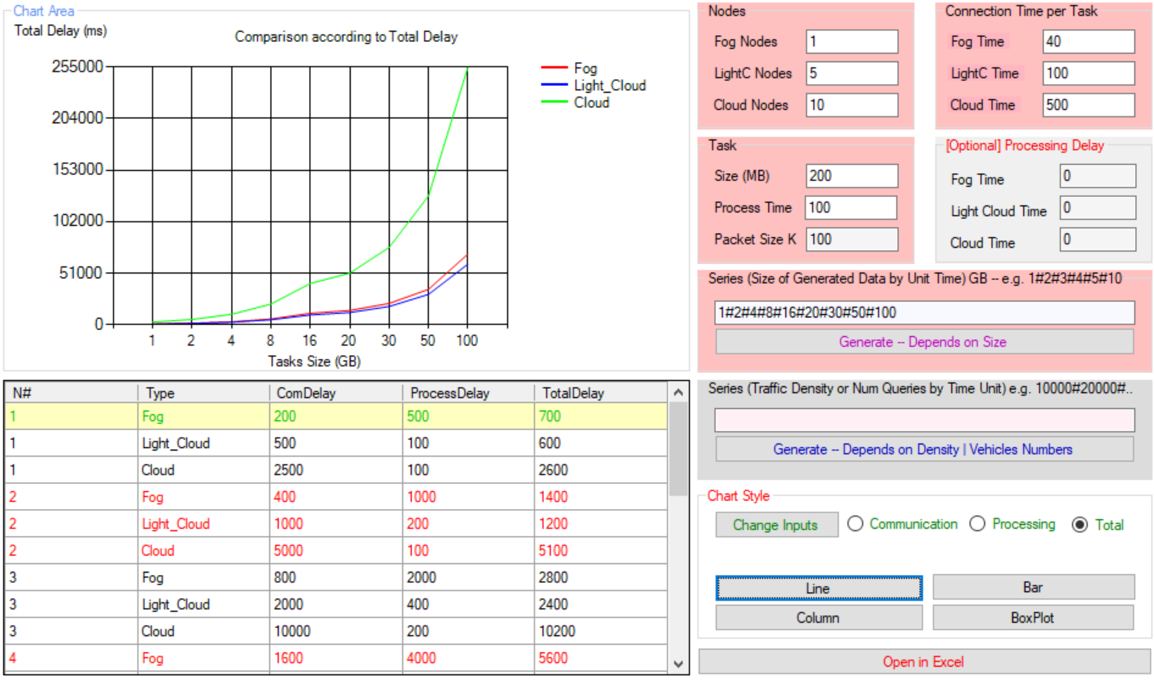
Second Experment

The objective of the second experiment was to demonstrate the potential of using blockchain technology within the proposed C-IoHT framework. The second experiment involves the creation of a Blockchain simulator to illustrate the mechanism of utilizing this technology within the C-IoHT framework. The block body in this simulator contains medical information, while the block header includes a unique identifier number, creation date, random number, and the Hash code of the previous block. An active block has been accepted by the Min+1 node in Light-Cloud and has not been rejected by the Max+1 node. It is represented in green to indicate its validity. If any changes are made to the data of a saved block in the chain, it becomes Invalid and appears in a different color, along with all subsequent blocks.

Figure 9 presents an example of a string within the emulator where one of the blocks has been modified. This experiment aimed to underscore the flexibility, importance, and applicability of blockchain technology within the proposed framework.

Third Experiment

The main goal of this experiment is to test a proposed classification algorithm on real COVID-19 data, and to investigate the relationship between respiratory system symptoms and the severity of the infection. The third experiment was conducted using a Python environment on Google Colab to test a proposed classification algorithm on real data.



Nodes

Fog Nodes: 1
LightC Nodes: 5
Cloud Nodes: 10

Connection Time per Task

Fog Time: 40
LightC Time: 100
Cloud Time: 500

Task

Size (MB): 200
Process Time: 100
Packet Size K: 100

[Optional] Processing Delay

Fog Time: 0
Light Cloud Time: 0
Cloud Time: 0

Series (Size of Generated Data by Unit Time) GB – e.g. 1#2#3#4#5#10

1#2#4#8#16#20#30#50#100

Generate -- Depends on Size

Series (Traffic Density or Num Queries by Time Unit) e.g. 10000#20000#..

Generate -- Depends on Density | Vehicles Numbers

Chart Style

Change Inputs ○ Communication ○ Processing ● Total

Line | Bar | Column | BoxPlot

Open in Excel

N#	Type	ComDelay	ProcessDelay	TotalDelay
1	Fog	200	500	700
1	Light_Cloud	500	100	600
1	Cloud	2500	100	2600
2	Fog	400	1000	1400
2	Light_Cloud	1000	200	1200
2	Cloud	5000	100	5100
3	Fog	800	2000	2800
3	Light_Cloud	2000	400	2400
3	Cloud	10000	200	10200
4	Fog	1600	4000	5600

Fig 7: Comparison between Computing Models

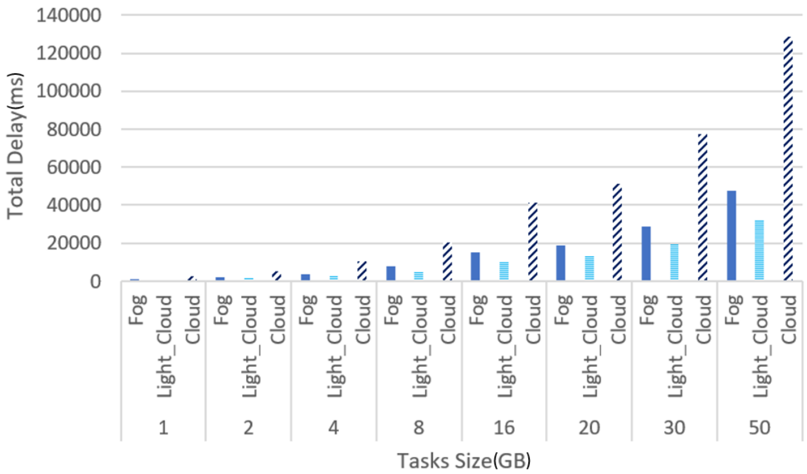
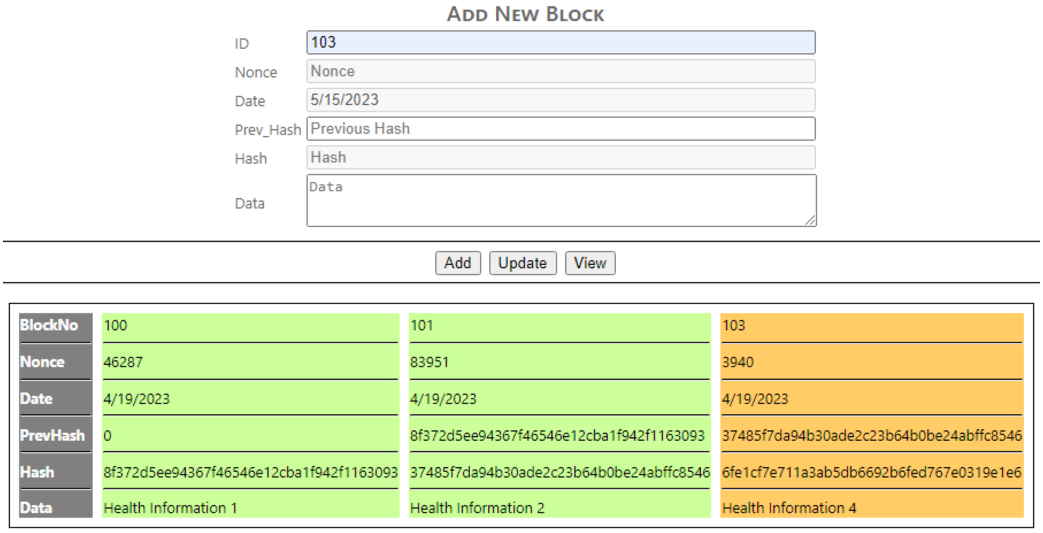


Fig 8: Performance of Computing Models According to Different Size of Data



Add New Block

ID: 103
Nonce: Nonce
Date: 5/15/2023
Prev_Hash: Previous Hash
Hash: Hash
Data: Data

Add | Update | View

BlockNo	100	101	103
Nonce	46287	83951	3940
Date	4/19/2023	4/19/2023	4/19/2023
PrevHash	0	8f372d5ee94367f46546e12cba1f942f1163093	37485f7da94b30ade2c23b64b0be24abffc8546
Hash	8f372d5ee94367f46546e12cba1f942f1163093	37485f7da94b30ade2c23b64b0be24abffc8546	6fe1cf7e711a3ab5db6692b6fed767e0319e1e6
Data	Health Information 1	Health Information 2	Health Information 4

Fig 9: Blockchain Simulation (Valid and Invalid Blocks)

The data used consisted of six previous datasets related to Covid-19, containing information on 200,000 infected individuals from various countries during the pandemic. The study focused on a single province in China, which contained approximately 12,000 records with 22 variables each, including demographic information, symptoms, and severity classification.

The data were divided into two parts, one for the elderly and the other for other groups, and two classification experiments were conducted. The first experiment involved collecting respiratory system symptoms, adding variables representing the systems' state, and measuring the correlation rate. The second experiment compared the results of five popular machine learning models (Decision Tree DT, K-Nearest Neighbor KNN, Random Forest RF, Support Vector Machine SVM, and Logistic Regression LR) based on four well-known criteria (Precision, Recall, F1-Score, and Accuracy). The RF and DT models showed the best performance, followed by the SVM, since the data entered were semi-categorical rather than numeric. Trees tend to perform better in such cases, and random forests provide proof of model stability in actual environments later. These findings are presented in Figure 10. Figure 11 and Figure 12 which compares the learning curves for KNN and RF classifiers, respectively. The graph clearly depicts the superior performance of the RF model, which achieved an accuracy greater than 0.991. Similarly, Figure 13 illustrates the accuracy of the classification algorithm before and after isolating the elderly and individuals with chronic diseases from the remaining population. The results demonstrate an improvement in accuracy of more than 6%.

Figure 14 depicts a proposed decision support dashboard for the entire city, providing real-time updates on the number of infected, recovered, and critical cases in each region, as well as the total numbers and recurrence rates of symptoms among infected cases.

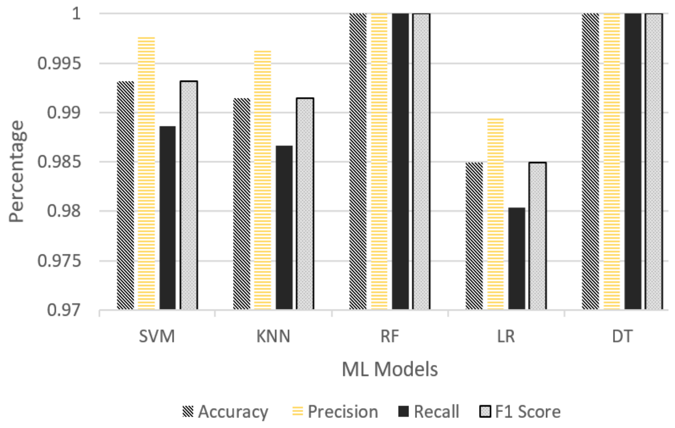


Fig 10: Comparison between Different ML Model According to Common Metric

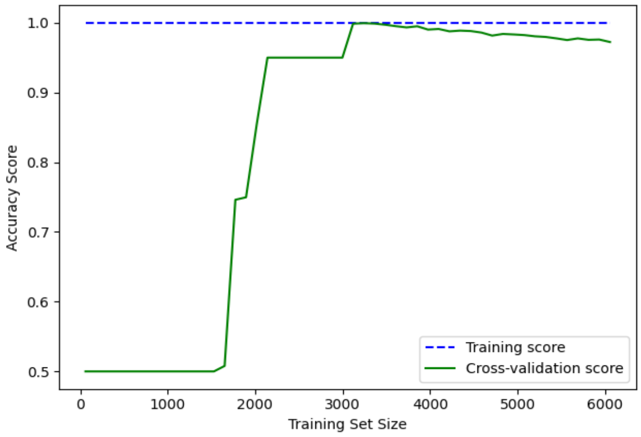


Fig 11: Learning curve for KNN model

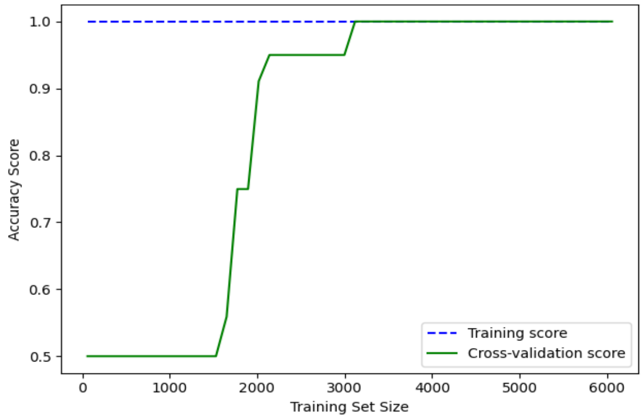


Fig 12: Learning curve for RF model

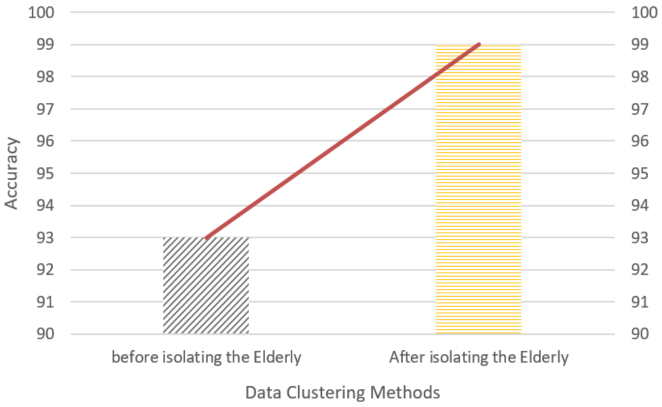


Fig 13: Accuracy Enhancement of Classification Algorithm After Our Isolating Method

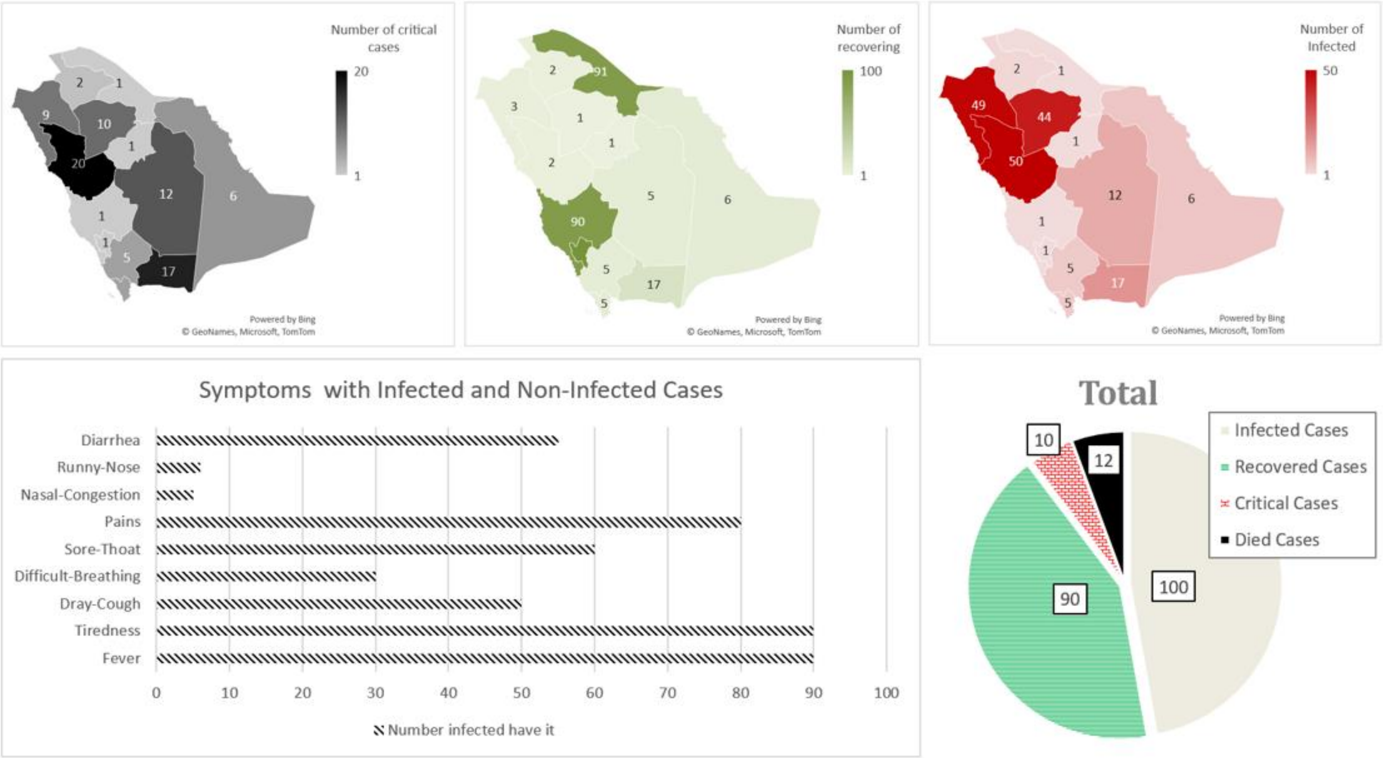


Fig 14: Dashboard of in Cloud for Decision Support

Conclusion and Future Work

In conclusion, the proposed platform aims to address several critical challenges in the healthcare industry, including improving performance and response times, standardizing medical concepts and ontologies, and enhancing privacy and security. The platform's Light-Cloud architecture with cloud and fog computing layers enhances performance and enables smooth management, while its blockchain-based architecture provides a secure and trusted environment for data sharing and processing. Additionally, the services and applications layer helps aggregate and manage relevant healthcare services, including electronic health records, contact tracing, remote patient monitoring, mental health support, vaccine management, emergency response, and more. The proposed ontology for medical concepts standardizes data representation and processing to support natural language processing algorithms, with promising results shown in the simulation of the proposed framework and algorithm to improve overall healthcare delivery quality.

Moving forward, future development areas include optimizing performance and response times, enhancing the accuracy and reliability of natural language processing algorithms, and expanding the services and applications layer's scope. Furthermore, ongoing collaboration with healthcare providers and stakeholders will be necessary to ensure that the platform continues to meet the evolving needs of the healthcare industry. There is also a need for algorithm development in several areas, including processing textual data to extract knowledge, classifying data based on healthcare ontology, machine learning for anomaly detection in medical data sources, dynamic service selection based on user characteristics and context, and image processing algorithms based on medical staff requirements.

References

[1] Habibzadeh, H., Dinesh, K., Shishvan, O. R., Boggio-Dandry, A., Sharma, G., & Soyata, T. (2019). A survey of healthcare Internet of Things (HIoT): A clinical perspective. *IEEE Internet of Things Journal*, *7*(1), 53-71.

[2] Laghari, A. A., Wu, K., Laghari, R. A., Ali, M., & Khan, A. A. (2021). A review and state of art of Internet of Things (IoT). *Archives of Computational Methods in Engineering*, 1-19.

[3] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: an up-to-date survey. *Applied System Innovation*, *3*(1), 14.

[4] Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors*, *20*(9), 2495.

[5] Bhambri, P., Rani, S., Gupta, G., & Khang, A. (Eds.). (2022). *Cloud and fog computing platforms for internet of things*. CRC Press.

[6] Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). Emerging wireless technologies in the internet of things: a comparative study. *arXiv preprint arXiv:1611.00861*.

[7] Devalal, S., & Karthikeyan, A. (2018, March). LoRa technology-an overview. In *2018 second international conference on electronics, communication and aerospace technology (ICECA)* (pp. 284-290). IEEE.

[8] Ketu, S., & Mishra, P. K. (2021). Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications*, *192*, 103179.

[9] Bahbouh, N. M., Compte, S. S., Valdes, J. V., & Sen, A. A. A. (2023). An empirical investigation into the altering health perspectives in the internet of health things. *International Journal of Information Technology*, *15*(1), 67-77.

[10] Bharati, S., & Mondal, M. H. (2021). 12 Applications and challenges of AI-driven IoHT for combating pandemics: a review. *Computational Intelligence for Managing Pandemics*, 213-230.

[11] Rehman, A.; Saba, T.; Haseeb, K.; Alam, T.; Lloret, J. (2022) Sustainability Model for the Internet of Health Things (IoHT) Using Reinforcement Learning with Mobile Edge Secured Services. *Sustainability 14*, 12185.

[12] Dang, V. A., Vu Khanh, Q., Nguyen, V. H., Nguyen, T., & Nguyen, D. C. (2023). Intelligent Healthcare: Integration of Emerging Technologies and Internet of Things for Humanity. *Sensors*, *23*(9), 4200.

[13] Rghioui, A., S Sendra, J Lloret, A Oumnad, Internet of things for measuring human activities in ambient assisted living and e-health, Network Protocols and Algorithms 8 (3), 15-28. 2016

[14] Yassein, M. B., Hmeidi, I., Al-Harbi, M., Mrayan, L., Mardini, W., & Khamayseh, Y. (2019, December). IoT-based healthcare systems: A survey. In *Proceedings of the second international conference on data science, E-learning and information systems* (pp. 1-9).

[15] Rghioui, A., Lloret, J., Sendra, S., Oumnad, A. (2020. A smart architecture for diabetic patient monitoring using machine learning algorithms. *Healthcare* 8(3), p. 348).

[16] Sher, L. (2020). The impact of the COVID-19 pandemic on suicide rates. *QJM: An International Journal of Medicine*, *113*(10), 707-712.

[17] Ciotti, M., Ciccozzi, M., Terrinoni, A., Jiang, W. C., Wang, C. B., & Bernardini, S. (2020). The COVID-19 pandemic. *Critical reviews in clinical laboratory sciences*, *57*(6), 365-388.

[18] Yamin, M. (2020). Counting the cost of COVID-19. *International journal of information technology*, *12*(2), 311-317.

[19] Apuke, O. D., & Omar, B. (2021). Fake news and COVID-19: modelling the predictors of fake news sharing among social media users. *Telematics and Informatics*, *56*, 101475.

[20] Alazab, M., Awajan, A., Mesleh, A., Abraham, A., Jatana, V., & Alhyari, S. (2020). COVID-19 prediction and detection using deep learning. *International Journal of Computer Information Systems and Industrial Management Applications*, *12*(June), 168-181.

[21] Le, T. T., Cramer, J. P., Chen, R., & Mayhew, S. (2020). Evolution of the COVID-19 vaccine development landscape. *Nat Rev Drug Discov*, *19*(10), 667-668.

[22] Amini Pouya, M., Afshani, S. M., Maghsoudi, A. S., Hassani, S., & Mirnia, K. (2020). Classification of the present pharmaceutical agents based on the possible effective mechanism on the COVID-19 infection. *Daru Journal of Pharmaceutical Sciences*, *28*, 745-764.

[23] Vaishya, R., Javaid, M., Khan, I. H., & Haleem, A. (2020). Artificial Intelligence (AI) applications for COVID-19 pandemic. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews*, *14*(4), 337-339.

[24] Khubchandani, J., Jordan, T. R., & Yang, Y. T. (2020). Ebola, Zika, Corona… what is next for our world?. *International journal of environmental research and public health*, *17*(9), 3171.

[25] Mackenzie, J. S., Drury, P., Arthur, R. R., Ryan, M. J., Grein, T., Slattery, R., ... & Bejtullahu, A. (2014). The global outbreak alert and response network. *Global public health*, *9*(9), 1023-1039.

[26] Cox, N. J., Trock, S. C., & Burke, S. A. (2014). Pandemic preparedness and the influenza risk assessment tool (IRAT). *Influenza pathogenesis and control-volume I*, 119-136.

[27] Huron, N. A., Behm, J. E., & Helmus, M. R. (2022). Paninvasion severity assessment of a US grape pest to disrupt the global wine market. *Communications Biology*, *5*(1), 655.

[28] Wolfe, C. M., Hamblion, E. L., Dzotsi, E. K., Mboussou, F., Eckerle, I., Flahault, A., ... & Impouma, B. (2021). Systematic review of Integrated Disease Surveillance and Response (IDSR) implementation in the African region. *PLoS One*, *16*(2), e0245457.

[29] Firda, A. A., & Haksama, S. (2020). Building health system resilience during Covid-19 crisis. *Jurnal Administrasi Kesehatan Indonesia*, *8*(1).

[30] Turenne, C. P., Gautier, L., Degroote, S., Guillard, E., Chabrol, F., & Ridde, V. (2019). Conceptual analysis of health systems resilience: a scoping review. *Social Science & Medicine*, *232*, 168-180.

[31] Wood, J. L., Leach, M., Waldman, L., MacGregor, H., Fooks, A. R., Jones, K. E., ... & Cunningham, A. A. (2012). A framework for the study of zoonotic disease emergence and its drivers: spillover of bat pathogens as a case study. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *367*(1604), 2881-98.

[32] Zisook, R. E., Monnot, A., Parker, J., Gaffney, S., Dotson, S., & Unice, K. (2020). Assessing and managing the risks of COVID-19 in the workplace: Applying industrial hygiene (IH)/occupational and environmental health and safety (OEHS) frameworks. *Toxicology and Industrial Health*, *36*(9), 607-618.

[33] Azzopardi-Muscat, N., Cloutier-Fisher, D., Kutzin, J., Doyle, Y., & Rothgang, H. (2014). A framework for pandemic risk management. Bulletin of the World Health Organization, 92(2), 135-142

[34] World Health Organization. (2021). Pandemic influenza preparedness framework for the sharing of influenza viruses and access to vaccines and other benefits.

[35] Sharma, A., Jaiswal, P., Kerakhan, Y., Saravanan, L., Murtaza, Z., Zergham, A., ... & Malik, P. (2021). Liver disease and outcomes among COVID-19 hospitalized patients–a systematic review and meta-analysis. *Annals of hepatology*, *21*, 100273.

[36] Islam, M. S., Rahman, M. S., & Islam, M. A. (2021). An Integrated Pandemic Monitoring and Management System: A Technological Approach. Journal of Healthcare Engineering, 2021, 1-12. doi:10.1155/2021/6623805

[37] Philippe, T. J., Sikder, N., Jackson, A., Koblanski, M. E., Liow, E., Pilarinos, A., & Vasarhelyi, K. (2022). Digital health interventions for delivery of mental health care: Systematic and comprehensive meta-review. *JMIR mental health*, *9*(5), e35159.

[38] Moss, R., Price, D. J., Golding, N., Dawson, P., McVernon, J., Hyndman, R. J., ... & McCaw, J. M. (2022). Forecasting COVID-19 activity in Australia to support pandemic response: May to October 2020. *MedRxiv*, 2022-08.

[39] Knauer, N. J. (2022). The Federal Response to COVID-19: Lessons from the Pandemic. *Hastings LJ*, *73*, 49.

[40] Albouq, S. S., Abi Sen, A. A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. M. (2022). A survey of interoperability challenges and solutions for dealing with them in IoT environment. *IEEE Access*, *10*, 36416-36428.

[41] de Mello, B. H., Rigo, S. J., da Costa, C. A., da Rosa Righi, R., Donida, B., Bez, M. R., & Schunke, L. C. (2022). Semantic interoperability in health records standards: a systematic literature review. *Health and Technology*, *12*(2), 255-272.

[42] Galetsi, P., Katsaliaki, K., & Kumar, S. (2019). Values, challenges and future directions of big data analytics in healthcare: A systematic review. *Social science & medicine*, *241*, 112533.

[43] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied Sciences*, *12*(4), 1927.

[44] Gerke, S., Minssen, T., & Cohen, G. (2020). Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

[45] Benson, T., & Grieve, G. (2021). Principles of Health Interoperability. *Cham: Springer International*, 21-40.

[46] Braunstein, M. L. (2019). Healthcare in the Age of Interoperability: Part 3. *IEEE pulse*, *10*(1), 26-29.

[47] Arzt, N. H. (2020). Application Programming Interface (API) for Immunization Information Interoperability. *Medical Research Archives*, *8*(11).

[48] Buchinger, M., Kuhn, P., Kalogeropoulos, A., & Balta, D. (2021). Towards interoperability of smart city data platforms. *Proc. Annu. Hawaii Int. Conf. Syst. Sci*., 2021, p. 2454.

[49] Jaleel, A., Mahmood, T., Hassan, M. A., Bano, G., & Khurshid, S. K. (2020). Towards medical data interoperability through collaboration of healthcare devices. *IEEE Access*, *8*, 132302-132319.

[50] Costin, A., & Eastman, C. (2019). Need for interoperability to enable seamless information exchanges in smart and sustainable urban systems. *Journal of Computing in Civil Engineering*, *33*(3), 04019008.

[51] Pradhan, M., & Devaramani, S. (2019, November). Enabling interoperability for ROS-based robotic devices for smart city HADR operations. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 1-6). IEEE.

[52] Sharma, A., Acharya, S., Rajaraman, V., Ramesh, R., Babu, A., & Amrutur, B. (2017, November). Schemas for IoT interoperability for smart cities. In *Proceedings of the 4th ACM international conference on systems for energy-efficient built environments* (pp. 1-2).

[53] Uviase, O., & Kotonya, G. (2018). IoT architectural framework: connection and integration framework for IoT systems. *arXiv preprint arXiv:1803.04780*.

[54] Gyrard, A., Zimmermann, A., & Sheth, A. (2018). Building IoT-based applications for smart cities: How can ontology catalogs help?. *IEEE Internet of Things Journal*, *5*(5), 3978-3990.

[55] Bröring, A., Schmid, S., Schindhelm, C. K., Khelil, A., Käbisch, S., Kramer, D., ... & Teniente, E. (2017). Enabling IoT ecosystems through platform interoperability. *IEEE software*, *34*(1), 54-61.

[56] Robert, J., Kubler, S., Kolbe, N., Cerioni, A., Gastaud, E., & Främling, K. (2017). Open IoT ecosystem for enhanced interoperability in smart cities—example of Métropole De Lyon. *Sensors*, *17*(12), 2849.

[57] Reda, R., Piccinini, F., Martinelli, G., & Carbonaro, A. (2022). Heterogeneous self-tracked health and fitness data integration and sharing according to a linked open data approach. *Computing*, *104*(4), 835-857.

[58] Yang, S., & Wei, R. (2020). Semantic interoperability through a novel cross-context tabular document representation approach for smart cities. *IEEE Access*, *8*, 70676-70692.

[59] Park, H. A., Yu, S. J., & Jung, H. (2021). Strategies for adopting and implementing SNOMED CT in Korea. *Healthcare Informatics Research*, *27*(1), 3-10.

[60] Hassan, M. K., El Desouky, A. I., Elghamrawy, S. M., & Sarhan, A. M. (2019). Big data challenges and opportunities in healthcare informatics and smart hospitals. *Security in smart cities: Models, applications, and challenges*, 3-26.

[61] Alam, T. (2020). Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *1*(2), 108-115.

[62] Sabireen, H., & Neelanarayanan, V. J. I. E. (2021). A review on fog computing: architecture, fog with IoT, algorithms and research challenges. *Ict Express*, *7*(2), 162-176.

[63] Pareek, K., Tiwari, P. K., & Bhatnagar, V. (2021, March). Fog computing in healthcare: A review. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1099, No. 1, p. 012025). IOP Publishing.

[64] Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. *International Journal of Information Technology*, *13*, 829-837.

[65] Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*, *7*, 74361-74382.

[66] Ferrag, M. A., Maglaras, L., & Janicke, H. (2019). Blockchain and its role in the internet of things. In *Strategic Innovative Marketing and Tourism: 7th ICSIMAT, Athenian Riviera, Greece, 2018* (pp. 1029-1038). Springer International Publishing.

[67] Ng, W. Y., Tan, T. E., Movva, P. V., Fang, A. H. S., Yeo, K. K., Ho, D., ... & Ting, D. S. W. (2021). Blockchain applications in health care for COVID-19 and beyond: a systematic review. *The Lancet Digital Health*, *3*(12), e819-e829.

[68] Bahbouh, N., Basahel, A., Sendra, S., Sen, A., & Ahmed, A. (2023). Tokens Shuffling Approach for Privacy, Security, and Reliability in IoHT under a Pandemic. *Applied Sciences*, *13*(1), 114.

[69] Chatterjee, S. (2020). AI strategy of India: policy framework, adoption challenges and actions for government. *Transforming Government: People, Process and Policy*, *14*(5), 757-775.

[70] Lee, T. F., Chang, I. P., & Su, G. J. (2023). Compliance with HIPAA and GDPR in Certificateless-Based Authenticated Key Agreement Using Extended Chaotic Maps. *Electronics*, *12*(5), 1108.

Tokens Shuffling Approach for Privacy, Security, and Reliability in IoHT under a Pandemic

Bahbouh, N., Basahel, A., Sendra, S., & Abi Sen, A. A. (2022). Tokens shuffling approach for privacy, security, and reliability in IoHT under a pandemic. Applied Sciences, 13(1), 114.

Abstract

The greatest challenge in the future of smart health services and systems is the privacy and security challenges. Several approaches for preserving privacy had provided in IoHT applications. But with the appearance of coronavirus the health care centers needed to track, collect, and share more special data like the places of corona infected and monitoring the social distance. Unfortunately, the traditional preserving approaches failed in dealing effectively with exceptional circumstances. This research introduces a new approach called Tokens Shuffling TSA to preserve the privacy, security, and reliability of collected data in the pandemics, without the need to trust a third party or services providers. TSA depends on a smartphone application and proposed protocol to manage to collect and share data reliably and safely. TSA depends on swapping the identities temporarily between cooperated users, then hiding the identities by employing fog nodes. The fog node manages the cooperation process between users in a specific area to improve the system performance. Finally, TSA uses the Blockchain structure to save data reliability, ensure the integrity of data, and facilitate access to it. By simulation, we prove the superiority of the TSA over traditional approaches like the dummy and confusion in terms of the data privacy and performance level, in addition to the adaptability to exceptional circumstances. Moreover, TSA did not affect the accuracy of the collected data, or the statistics related to it. In other meaning, the TSA will not affect the quality of the main healthcare services .

Introduction

IoHT promises a lot for a better healthy life for all, especially for people with special needs like elders, disabled, or chronic diseases [1]. IoHT provided a lot of services, technics, and smart devices to introduce a better future for users. The health applications collect a lot of personal data about users for more adaptive services [2].

Usually, these applications depend on integration between fog computing and cloud computing to support computing resources [3], provide an environment to collect and process big data, provide quick response for emergencies, and increase the availability and accessibility level of the introduced services [4]. But, despite the big development in the health sector, the corona pandemic showed that we still need more and more work in developing this sector and provide smarter services able to deal with pandemics [5]**.**

Coronavirus, or Covid-19 [6, 7], has become a global epidemic, according to the World Health Organization [8]. Covid-19 has affected all majors and domains and changed many of the tasks and priorities of our life. All official reports confirm the seriousness of this virus and the speed of its spread, so it was necessary to take real precautionary measures to relax this disaster [9]. All the states of the world have applied restrictions and measures to reduce friction between people, which is the main factor in the transmission of infection to reduce the spread of the virus [10 - 12]. Undoubtedly, modern technologies have a major role in facing the great challenges of the virus [13]. The most effective solutions in a virus situation are maintaining the social distance, tracking the infected, real-time monitoring, depending on online services to reduce human mixing, observing the adherence of people [14], etc. In addition to the medical research that focuses on understanding the virus itself and its properties.

However, new technologies have a dark side too, which is related to the security and privacy of users' data. It is a critical challenge that faces the future of these technologies [15]. Unfortunately, the most of research about Covid-19 did not care about this issue (privacy and security of data) due to the exceptional circumstance. Where, collecting data and finding functional services or applications were the main goals for facing the pandemic [16]. Moreover, the most of provided solutions and applications rely on location-based services (LBS) [17]. So, an attacker or malicious third party can collect the spatial data, then analyze it to detect a lot of sensitive and personal data for each user like his behavior, job, home, religion, average income, and ethics, to name a few [18].

Unfortunately, the current approaches and methods of preserving privacy and security of data are not suitable for exceptional cases (pandemic situations). Because, they affect the quality of the main service (QoS of Health) affecting the accuracy of data and performance of service. In addition, some protection techniques do not provide enough level of protection and most of them don't care about the reliability of data which is critical in the health domain [19]. So, we proposed a novel approach for ensuring the main triple (privacy, security, and reliability) of user data in abnormal or pandemic cases like Covid-19. Our solution will not affect the results and accuracy of the applications, especially in the health domain. The proposed solution will pave the road for other researchers to new ideas on the privacy issue during a pandemic.

So, the contributions of this work are:

- Review the common privacy approaches with their disadvantages in the IoT environment.
- Propose a new approach for preserving privacy in IoHT during the pandemic situation, especially for LBS.
- Enhance the security and maintain the reliability of data
- The proposed approach will not affect on the accuracy of the main services like health services
- Enhance the performance by depending on fog computing and users' devices computing (Dew computing)
- Utilize the blockchain for ensuring the integrity of saved data
- Present case study for applying the proposed solution in Saudi Arabia
- Provide simulation and comparison to prove the superiority of the proposed approach over the current ones.

In the remaining sections, the research presented a literature review of previous privacy approaches and methods, and then it explained the proposed approach TSA and its advantages. After that, it discussed a case study in Saudi Arabia, and the results and comparison. Finally, it put a conclusion and future trends.

Literature Review

All new and smart technologies depend mainly on data, which has become the real wealth in this era [20]. But, on the dark side of these technologies, collecting a lot about our data, our lives, and our surroundings, storing and analyzing them make these technologies able to discover a lot of sensitive information about each person, and may also discover information that the person does not know about his behavior, habits, and character [21]. Thus, the development in the level of these technologies and the level of smart services has accompanied the emergence of a new challenge related to the issue of protecting the security and privacy of this data. No one of the users satisfy to disclose his data (for example, his medical data) to the public, where this data may be exploited maliciously and greatly affect the user and his life as well. The most dangerous is dealing with a malicious or hacked service provider, and thus this server may exploit its data to reveal information outside the scope of the announced service, which is called a privacy violation [22].

In general, privacy can be defined as a person's right to determine who, when, how, why, and where the user's data will be used. As well as his right to access and manage this data completely while ensuring that his identity is not revealed to others and does not make a profile for him to link anything he does to his identity and finally not to be tracked [23]. As for security, it is an older concept than privacy and it is imperative to protect the confidentiality and integrity of data (not to modify it), and finally its availability and non-stop service. The following figure illustrates the most important concerns about data privacy and data security, to clarify the basic difference between privacy and security, and for more details, see [24]. The best solution is the one that provides both.

Many techniques and methods have been introduced to protect privacy and security, but they still suffer from open problems. Moreover, there is no effective approach that can be used during a pandemic where the accuracy of data is a critical issue in addition to performance and reliability. the next points discuss the most common protection approaches and their drawbacks, in addition to why they are not suitable for Covid-19 scenarios and duration.

Processing data approach [25]: this approach depends on summarizing or analyzing the data and finding the knowledge by using statistics methods or data mining before sending it to the service provider. It is valid for specific applications but not valid for medical applications, because it modifies the data, especially in pandemics where we need true data, and not summarized or modified.

access permission approach [26]: it is related to user awareness, enables him to access his data, ensuring service provider compliance with privacy laws like GDPR, which enable the data owner to grant access permission to his data. So, the service provider must get data access permission before using or sharing this data. This approach is not enough to deal with the malicious server or external attacker and does not compatible with the Blockchain which prevents any modification on data after saving it, and thus it does not suitable for medical applications.

Encryption and Authentication [27]: Encryption is adopted in many services to ensure the protection and confidentiality of data. but it does not preserve the data privacy from service providers themselves. Because the service provider can collect a lot of data, create a profile for each user, and reveal a lot of sensitive information that is not authorized. Thus, it is not suitable alone in health systems and services. Authentication also ensures the reliability of users and avoids counterfeiters or unauthorized to access a service. That may affect the accuracy of collected data. Particular, this approach focuses on data security more than privacy.

Blockchain [28]: many medical systems started depending on blockchain, which provides a reliable environment for saving, integrating, and preventing repetition and modification. But the blockchain does not achieve privacy from the side of the service provider (cooperated node). thus, the blockchain is considered a good choice to save data in the case of hiding the user’s identity.

Obfuscation approach [29]: Obfuscation approach: used to protect privacy, especially for the user's location, as it replaces the user's real location with a fake nearby location or hides it within a large area before sending the user's data to the service provider. It is also considered unsuitable for medical applications that require accurate data, especially in pandemics, where the location is considered one of the most important data that is used to determine statistics and places of epidemic or infection spread. Also, this approach is not concerned with the confidentiality or integrity of the data.

Dummy approach [30]: it is used to preserve privacy by sending a lot of dummy data with the user queries and data, thus it is not suitable for medical applications which need accurate sent data. Also, it does not interest in data confidentiality and integrity. In addition, it affects adversely on the performance.

Anonymization using a pseudonym [31]: It is a simple approach to protect privacy in which the user uses a pseudonym instead of his real name, but it is not effective if the user sends a lot of data or more than one query to the service provider. Also, this service does not care about the confidentiality and reliability of data coming from unknown users. Therefore, it is not suitable for pandemics. This approach was developed with a different Mix-Zone approach where the pseudonym is changed periodically but is not considered a robust privacy protection approach and suffers from the same drawbacks as the traditional anonymization approach for health systems.

Trusted Third-Party approach (TTP) [32]: it is a good approach used to ensure privacy and security of data in addition to reliability, but if the third party is malicious, the same problem will be repeated for the malicious service provider, so it is not considered a sufficient solution or a guarantor alone, but it can be utilized in other ways as we will see in the proposed approach.

Cloak area approach [33]: used to protect the privacy of the user's site. It divides the area into cells so that in each cell there is a manager known as an anonymizer that hides the identity of all users in his area from the service provider and replaces their exact locations with his cell coordinates. Thus, this approach is not appropriate for health services in a pandemic for the same reasons as the obfuscation or dummy approaches.

PIR approach [34]: It is used to protect the privacy and security of the data that reaches the user from the service provider and not the opposite, where the user requests huge information from the service provider and then works on it alone, which is therefore not suitable for the goals of health services in the pandemic.

Cache approach [35]: It is a pro-privacy approach and is not considered sufficient when used independently, usually used to reduce the number of connections with the service provider and improve performance.

Hybrid approach [36]: Many methods can combine to create a new approach with higher level of privacy protection, but these approaches will not be valid in dealing with health services which based on location. Because they do not modify the mechanism of the main integrated methods which basically are not suitable for health services as we referred before. So, the hybrid approaches do not provide solution for the main goal in this research (preserving privacy in under pandemic conditions without affecting on QoS).

Thus, we note that there is a real need for a new approach capable of dealing with location-based services during pandemics, especially those related to the medical aspect, which is presented by this research through the TSA approach, which presents a new scenario that uses concepts that were used in the current approaches, but in a different way to benefit from them while avoiding their negatives that limited its effectiveness during the Covid pandemic.

The proposed approach TSA

The main idea of the TSA approach is to rely on the local storage of data in normal situations, distribute the main service stages across multiple service providers, collaborate between users to protect their privacy and mislead the service provider, employ fog nodes to facilitate collaboration and to act as the anonymizer, and use encryption and blockchain to improve security and reliability.

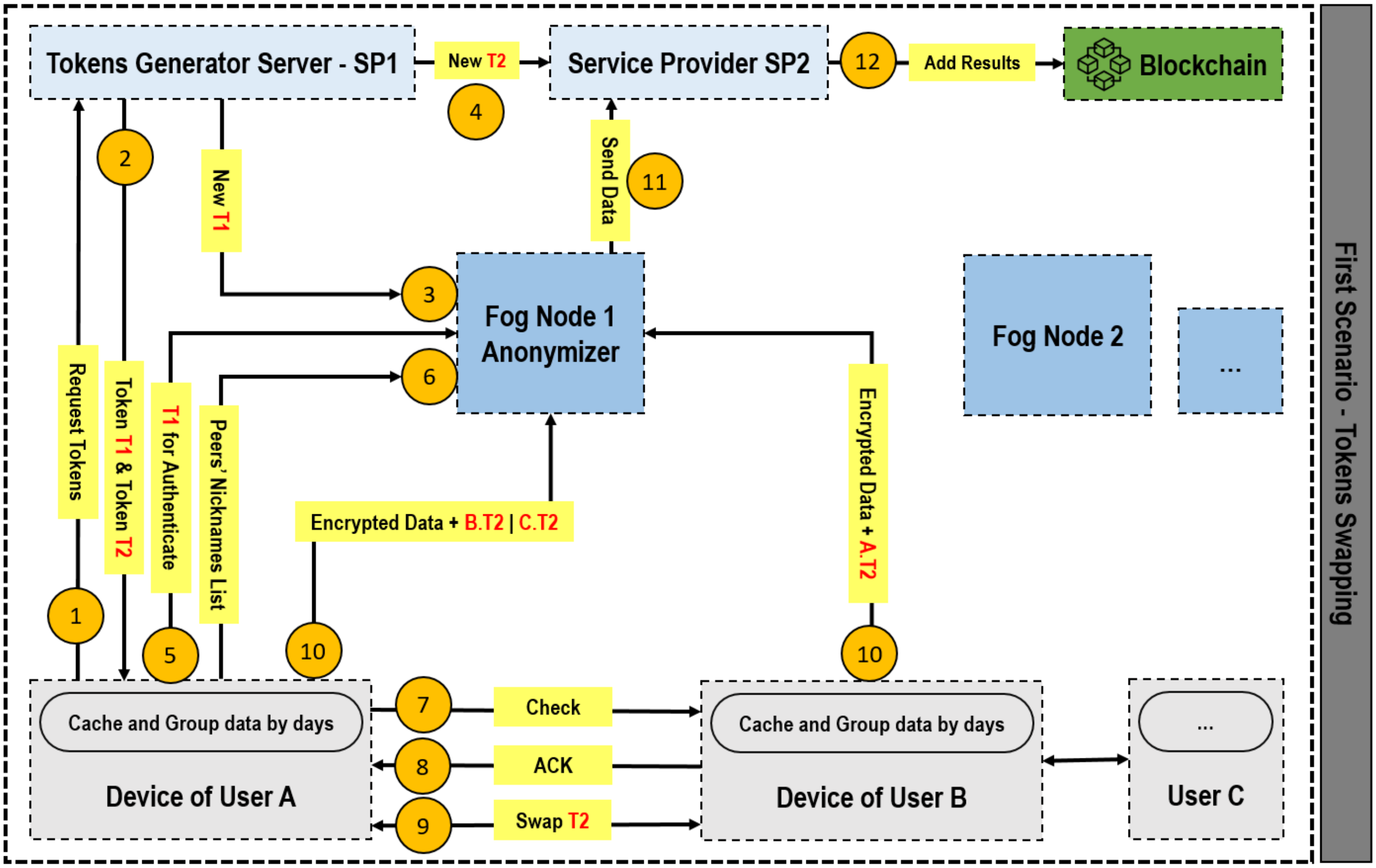


Figure 1. First Scenario of TSA

The proposed approach depends on several stages to achieve the enough preserving privacy, security, reliability of users' data, with ensuring non effecting on the quality of the main service.

In the following, the sequence of steps with description for their importance and how they work :

1- Collect the spatial data for the user and save it locally on the user's phone by proposed application to manage these data. The application will save the spatial data for the last 14 days (this period related to the Incubation period without symptoms). The application enables the user to determine a blind point (like his house), the data in this point is not saved. The importance of this step is summarized in two points, the first is reducing the effort on the service providers, especially in the exceptional circumstances, so we needn't connect, track, or save data of millions of users who are not infected. Instead of that, TSA uses the computing power of the user's device in saving data (that is called Dew computing). The second is saving data locally which reduces the connecting costs and enhances the user privacy.

2- In the case that the user is proven to have an infection, we will rely on server SP1 independent of medical services providers to verify the infection and manage the generating of tokens and send them to service providers like (SP2), whether the service is a medical or tracing one during the pandemic. Two unique tokens are generated (T1, T2) by SP1 for each infected person where the validity of the tokens is one day. T1 will be sent to the fog node which is manager for the user's area. While T2 will be sent to the SP2 which is can be medical service monitors and tracks the places of the spread of disease. SP1 does not send data about user identity, or his name to the fog node or SP2, also SP1 does not have and data about locations of user.

   By using a special server to manage tokens, the load will distribute between service providers, and the level of privacy and reliability of user data will enhance. So, no data will be accepted without verifying that the user has an effective token. In other words, closing the ports in front of frivolous or fake users who may send false and unreal data to service providers to affect the quality of services or statistics, etc. Moreover, sending a different token to SP2 than the fog node will enhance the level of privacy, and prevent the fog node from reveal the user's data to SP2.

3- After proving the infection and generating the tokens, the user must share his saved data with SP2 that are interested in tracking the places of infection spread and some important statistics during pandemics. We have presented two different scenarios to ensure the security and privacy of this data and its users:

   First Scenario (Figure 1): Infected user A communicates with his area's fog node with an alias in addition to his T1. The fog node verifies the validity of a user's token. Then it sends the user a list of all aliases of users connected with the fog node (i.e. in the same area managed by that fog node). Then, through the proposed application, users communicate with each other and exchange T2 among themselves. For example, A exchanges A with B and C. Then A encrypts the data for the first seven days with B.T2 added within it as a reliability identifier. Then A repeats the same process over the second seven days with C.T2 (to create 14 days). Note, that encryption will be done using the SP2 public key. Then each user sends their data to the fog node, which will not be able to see this data because it is encrypted. The fog node collects the data of several users and then sends it as a single block to SP2 to provide protection for users' privacy K-Anonymity where K is the number of anonymized users whose data is being sent.

   Second Scenario (Figure 2): Instead of exchanging the token, the users will exchange the data encrypted with the SP2 public key, but this time without the token, and then each user (e.g., A) sends their new collected data to the fog node with the addition of encryption for his token (A.T2) as well.

   Note: The difference between the two previous scenarios is that the first scenario is faster, but it can be hacked in the event of cooperation between the fog node and SP2, although it is a rare and illogical scenario because the service provider needs many malicious fog nodes to achieve its goal. The second scenario achieves a better level of protection, but it takes more time to exchange data between users and is less reliable of ensuring that no part of the data is lost.

4- SP2 receives the coming data with tokens of users (T2) from a fog node. This data has been greatly confused among anonymous users. SP2 checks the validity of all received T2 after decrypting it, then decrypts, processes, and makes calculations and statistics on the data. SP2 will not be able to identify the data of a particular user or form a valid user profile. If the service provider is malicious, it will have misleading information about users. After the data processing is completed, SP2 adds the results and statistics within distributed databases based on Blockchain technology to ensure that the data and results are not lost or tampered with, such as the areas or places most vulnerable to the spread of infection due to the presence of incubators of the disease in the previous period.

5- Non-infected users can download part of the data for a specific region through the application and match it with the data they have stored locally. And in the event of intersections, this can give the user an indication of the need to conduct an examination, pay attention to symptoms, or reduce meeting people in the following days, thus enhancing the level of protection. Also, the generated information is useful in discovering the places that should avoid visiting it or taking greater precautions within them.

Strengths of TSA's Approach

- ❖ TSA did not use fake data protection techniques such as the Dummy approach or data obfuscation, thus maintaining the quality of service and not affecting the accuracy of its results.
- ❖ The user in TSA does not need to trust completely any of the cooperating parties, whether service providers, fog nodes, or even cooperating users
- ❖ By saving the data locally for people who have not been proven to be infected, the load on service providers has been reduced and the privacy and security of users' data have been enhanced.
- ❖ The data sent by each user represents Dummy data for the sending user, which will enhance his privacy and encourage him to cooperate with others
- ❖ The fog node reduces the load on the user in communicating with service providers on the one hand, and on the other hand, enhances the privacy of users by not having to communicate directly with service providers.
- ❖ The use of the token greatly reduces the chances of fake users who want to tamper with the results and statistics of medical centers and service providers.
- ❖ The use of encryption and blockchain enhances data security, integrity, and reliability

Challenges of the TSA approach

- Damage to the user's device causes the loss of data that is saved locally, but it is rare
- In the event of cooperation between a malicious fog node and a malicious SP2, user data can be exposed in the first scenario and the problem has been resolved in the second scenario
  Note: the malicious here is not in carrying out behaviors different from the declared service, but rather in trying to exploit the data of users of the service.
- The approach is based on the idea of having more than one user in the same area which makes sense in pandemic situations, but if there is only one user, the TSA in the worst case, achieves what the Blind Third Part BTP approach achieves where the user encrypts their data with an SP2 key and sends it via Fog knot.

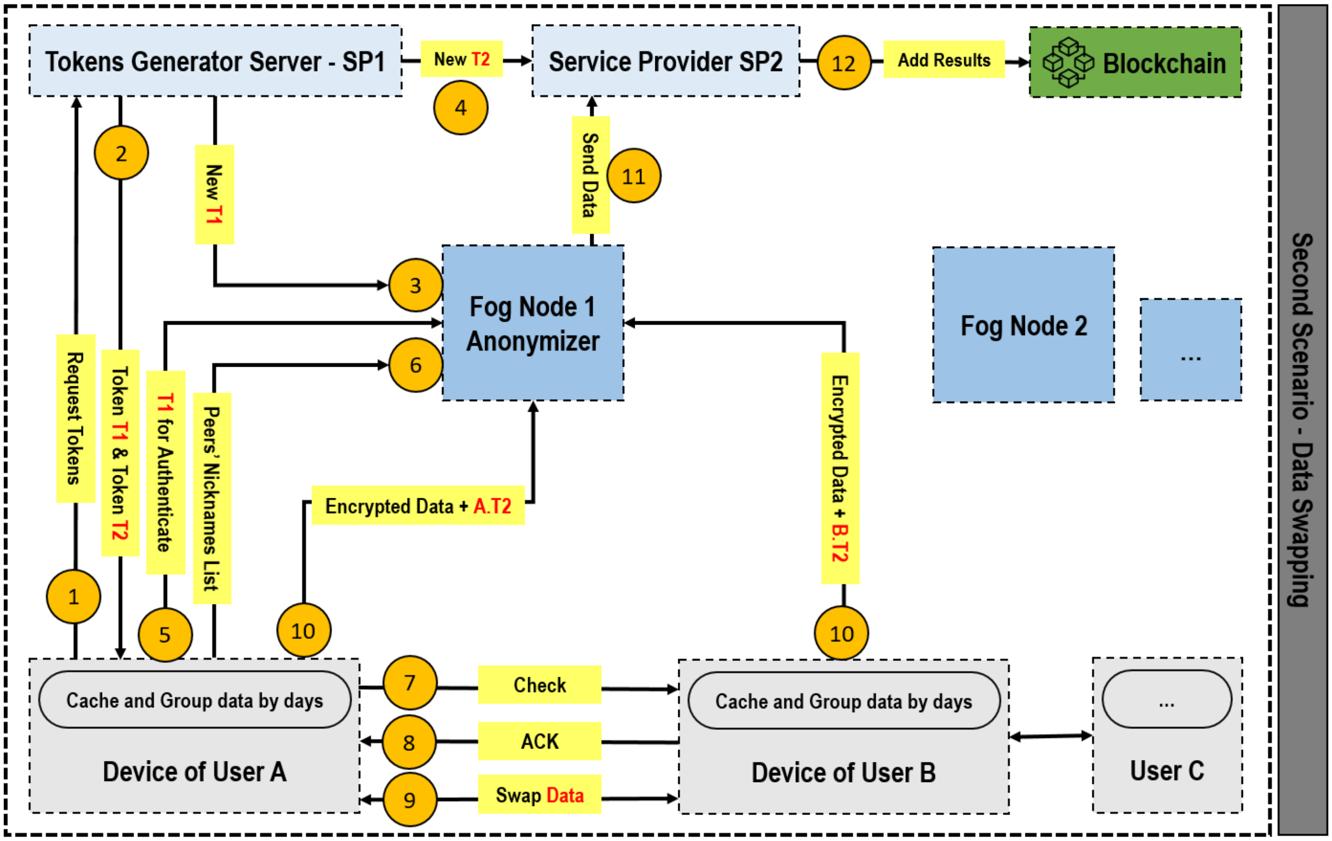


Figure 2. Second Scenario of TSA

Algorithm of Proposed Method TSA

```
Function bool AddNewData (Location1, PoI1, Date1, Time1)
Begin
        For (i=0; i< LocalCache.Items.Count; i++)
                TimeSpan = Date1 - LocalCache.Items[i].Date;
                If (TimeSpan.Days>14 )
                        LocalCache.Items[i].Remove();
                else
                        Break;
                End If
        End For
        LocalCache.Items.Add(Location1, PoI1, Date1, Time1);
        Return true;
End Function
Function Tokens CheckStatus (UserID)
Begin
        Tokens = null;
        If (ServerProvider1.check(UserID) == True) // infected
                T1 = GenerateToken1 (UserID,CurrentDateTime); // Random and Unique Token
                T2 = GenerateToken1 (UserID,CurrentDateTime); // Random and Unique Token
                Send (T1, ServerProvider2);
                Broadcast (T2, FogNodes);
                Tokens.Add(T1);
                Tokens.Add(T2);
        End If
        Return Tokens; // Note tokens will be valid for 1 day only.
End Function
```

```
Function Void ProtectAndShareData ()
Begin
    X = FogAuthentication( UserA.T1 );
    If (X)
        ListPeers = FogGetPeers ();
        For (i=0; i<ListPeers.Count; i++)
            Res = AskCooperation (ListPeers[i]);
            If (Res == Ack)
                Break;
            End If
        End For
        EncryptData = Encrypt ( ServerProvider2.PublicKey, UserA.LocalCache.Items )
        If (Scenario1.IsActive())
            B_T1 = SwapTokens (UserA.T1, UserB);
            Send (ServerPorvider2, EncryptData, B_T1) // Error Token
        Else // Scenario2.Active
            B_EncryptData = EnUserA.SwapData (EncryptData, UserB);
            Send (ServerPorvider2, B_EncryptData, UserA.T1) // Error Data
        End If
    End If
End Function
Function bool CheckPath ()
Begin
    List1 = GetAllPoI (CellID);
    Num = FindMatch (LocalCache.Items, List1);
    Percentage = 100*Num / (List1.Count + LocalCacheItems.Count);
    If (Percentage > Threshold)
        Return true; // There is large potential to be infected … Do test
    Else
        Return false;
End Function
```

Simulation and Results

Discuss the superiority of the proposed approach

In this section, we compare the proposed work with the four most common and basic approaches to privacy and security: Dummy enhance-CaDSA [30], DOA obfuscation [29], BTP [32], and SPF collaboration [36], noting that a recent scientific paper was selected for each of them. Although it was mentioned in the previous sections that these methods will not be suitable in times of pandemics because of their negative impact on data accuracy as in dummy and DOA, or because of overload or the possibility of breaking it as in BTP and SPF. But here we will ignore this feature of the proposed approach (its applicability during pandemics), and we will focus on the comparison according to standard criteria in the evaluation of the different methods of protection.

The criteria used for comparison

There are measures related to the level of privacy, the most famous of which are Entropy, K-Anonymity, and Estimate Error, and on the other hand, there are measures related to performance, the most important of which are Number of Sent Queries, Size of Sent Data or Results, Need to Processing Data, and Ratio of utilizing the cache. All the previous metrics can be measured or calculated if the necessary variables associated with each query sent from the user to the service provider are provided, and therefore they are considered quantitative metrics. There are also non-quantitative metrics such as, does the security method affect the accuracy of the main service results? does the security method need to trust a particular party such as a Peer, Fog, or SP service provider? Finally, does the method of protection protect data security as well, or only care about privacy? Generally, quantitative measures can be calculated through the following equations [25, 37]:

- K-Anonymity, which refers to the percentage of queries that belong to the user out of all the queries he sent to the service provider. Whenever this value approaches zero, this means better protection.

$$\textbf{K-Anonymity} = \mathbf{1 / (1+K)} \qquad \textbf{… (1)}$$

Where K is number of dummies of fake queries.

- Entropy (E) refers to the amount of valid data that an attacker can collect about a user, i.e. that the attacker is certain of belongs to a particular user. Usually, the value of E is between 0 and 1 where in our example 1 represents absolute uncertainty (the highest privacy protection) and 0 represents no protection, and the entropy is calculated by the following equation:

$$\mathbf{E = -\sum_{i=0}^{k} Pi * Log2(Pi)} \qquad \textbf{…(2)}$$

Where Pi is the probability that query (i) belongs to a selected user. Max (E) = 1 means the best protection for privacy where the Attacker does not have any right information about the user linked to him.

- Estimate Error (EE) It indicates the percentage of false guesses an attacker can fall on about user data and is usually calculated after calculating the entropy with the following equation

$$\mathbf{EE = E * 100\%} \qquad \textbf{…(3)}$$

- The performance rate relating to the number of queries sent and is represented by the total number in Nq
- The performance rate relating to the amount of data sent, the total is represented by S, and the data volume for a single query will be represented by Sq
- The performance rate relating to the total time T is given by calculating the time of sending the user's queries to the service provider

$$\mathbf{T = Nq*Sq*T_{Send} + Nq*Sq*T_{Process}} \qquad \textbf{… (4)}$$

- The performance rate relating to the cache and is usually given by the expected hit percentage in the cache H

$$\textbf{H = Number q are answered by Cache / Nq} \qquad \textbf{…(5)}$$

Suggested Hypotheses

To compare the previous approaches with the proposed approach in addition to the case of not using a protection technique, we ran a simulation based on some assumptions similar to what were in [29, 30, 32, 36]. These hypotheses are:

- The study is carried out on a specific area divided into sectors(cells) of almost equal size, and we symbolize the cell with the C.
- In each C cell there is a Fog Node, standing for FN, which is responsible for managing the operations of Queries, Peers, and Cache within the Null.
- Users query or visit different PoIs, (assuming 100) randomly distributing over cells, knowing that the same type can be repeated in more than one cell.
- We assume that there are 1,000 U-users scattered and moving randomly within the region during the study.

- The study period will be 2 hours, but we will consider that the system has been working since the beginning of the pandemic.
- The size of the data for one query is Sq and we will assume that Sq=1kb and therefore the total volume S can be calculated by

$$\mathbf{S = \sum_{i=1}^{k} Sqi}$$

- In the case of using noise, the size of the noise area will be denoted by the symbol SO, and therefore the size of the query will be SOq, which is greater than Sq
- Assume that the approximate average transmission time of one query to the service provider and through a 4G connection is Tsp=10ms
- Assume the approximate average transmission time of a single query to a fog node and through a WiFi connection is Tfn=2ms
- Assume that the approximate average transmission time of one query to another user Peer through a WiFi connection is Tpeer = 4ms including the period of obtaining the list of users in the same cell.

Simulation results on the Dummy approach

- The level of privacy is related to the number of dummies used by the user K, where the privacy increases with the increase in the value of K and this is clear for Equation No. 1, but according to Equation 2, the value of entropy E will never reach the maximum value of 1 because the user sends his query within the fake queries, therefore there is a real amount of information will be formed by the attacker or the malicious service provider with each transmission, and therefore it is certain that the error rate will not be 100% for the attacker based on equation No. 3.
- The level of performance will be negatively affected by the increase in the level of protection associated with K, the total number of queries Nq= 1 + K for each query. Thus, the total transmission time T will be greater according to equation 4 based on the new value of Nq.

$$\mathbf{T\_Dummy = Tsp*(Nq + Nq*K) + Tprocess*(Nq+Nq*K) \quad \ldots (6)}$$

- This approach will affect the accuracy of the results because of its effect on the total Nq and because the service provider stores wrong data about all the users.
- The Dummy approach is not effective with the use of cache, as the hit rate in cache H (Equation 5) will inevitably be lower than if only real queries are stored in the cache, based on the hypothesis proven in [A] that users in a particular region usually send similar queries .
- This approach does not require the user to trust any party, whether Peer, Fog, or SP
- This approach does not protect data security and is only concerned with data privacy.

Obfuscation approach simulation results

- The level of privacy is related to the size of the obfuscation zone SO, but it also will not reach Max(E) because the user is at the end of the zone, that is, there is a part of the zone data associated with the user and this part will reach the attacker.
- The level of performance will also be negatively affected by the increase in the level of specificity associated with SO, and since SOq > Sq, S will increase, and this will affect the transmission time and the total processing time T inevitably.

$$\mathbf{T\_Obfuscation = Tsp*Nq*\,S_{Oq} + Tprocess*Nq*S_{Oq} \quad \ldots (7)}$$

- This approach will affect the accuracy of the results also because of its effect on Sq and increase the noise on the data sent to the service provider.

- The obfuscation approach is not effective with the cache, as the hit rate in the cache will be lower due to the obfuscation of the real user's location within a random area that is difficult to replicate.
- The obfuscation approach also does not require trusting a third party, whether Peer, Fog, or SP
- This approach does not protect data security but only its privacy

Peer Cooperation approach simulation results

- The level of protection in the traditional approach to cooperation is related to the number of Peers collaborating, and the value of E increases with the number of Peers, but it will not reach the value of Max(E). In the case of the developed SPF approach, it uses the exchange method between users and therefore each user sends someone else's query and then it will be E=1 because the service provider will not have any real information about the user.
- The level of performance is also related to the number of cooperative Peers, as it affects the size of the collecting area for them and the number of their different queries, meaning that both Sq and Nq will be affected by the increase, and this will affect T negatively with the increase as well. But in the developed SPF the situation will become better due to the cooperation with one Peer and therefore the value of T

$$\mathbf{T\_Cooperation = Tsp*Nq + Tprocess*Nq + Tpeer*Nq \quad \ldots (8)}$$

- In systems that depend on non-correlated static queries, the SPF approach will not affect the accuracy of the queries, but in the case of dynamic queries that require the service provider to collect all user queries in a certain period (such as medical systems), it affects the accuracy of the results of this process significantly negatively.
- This approach is effective with the cache because only actual queries are stored in the cache
- This approach requires the user to trust Peer and does not require trust with Fog or SP
- This approach is concerned with protecting the privacy.

BTP approach simulation results

- Provides a maximum protection level E=1 because the user does not communicate with the service provider directly, but through the fog node, and it hides the information from the fog node through encryption with the service provider's public key.
- Performance level. This approach negatively affects the processing time of each query as encoding and decoding time will be added at each Tenc_dec end as well as an increase in transmission time to the fog node as an extra step. There is also a slight increase in query size due to the addition of a session key in each query to encrypt the returned results.

$$\mathbf{T\_BTP = Tsp*Nq+ Tprocess*Nq*Tenc\_dec + Tfog*Nq \quad \ldots (9)}$$

- It will not affect the accuracy of the queries
- It is considered unsuitable for the cache in its basic form because the fog node cannot read the encrypted data
- It does not require trust in Peer, Fog, or SP, but the fog node may cooperate with the SP to breach privacy, and the fog node in case it is malicious can send a fake query to tamper with the accuracy of the data of the service provider.
- Provides data security and privacy

Suggested approach

- Provides a maximum level of protection E=1 because the user does not send his data to the service provider himself, but through another user. It hides information from the cooperating user through encryption.

- The performance level will be greatly improved, although encryption is used with more time to deal with the fog node and then Peer, this only happens once (N=1) for an aggregated set of queries or data when there is a need to share it. In the normal case, all data is stored with the user himself and is not sent to the service provider, and this will save a lot of time and processing and improve performance and privacy.

$$\mathbf{T\_New = Tsp*1q + Tprocess*Nq + Tfog*1q + Tpeer*1q \quad \ldots (10)}$$

- It will not affect the accuracy of the queries at all, even the dynamic ones, as he sends an aggregated set of queries at once.
- It employs the cache in the user's device perfectly to improve performance and privacy together.
- It does not require trust in any party (Peer, Fog, and SP), and it makes the process of cooperation between more than one malicious party a complicated process.
- Provides data security and privacy and ensures data integrity from tampering.

Results and discussion

Figure 3 shows a comparison between the previous approaches in terms of E, which can also represent EE, and Figures 4 and 5 show the comparison in terms of performance, where the first is compared in terms of the number of queries sent, and the second is compared in terms of time.

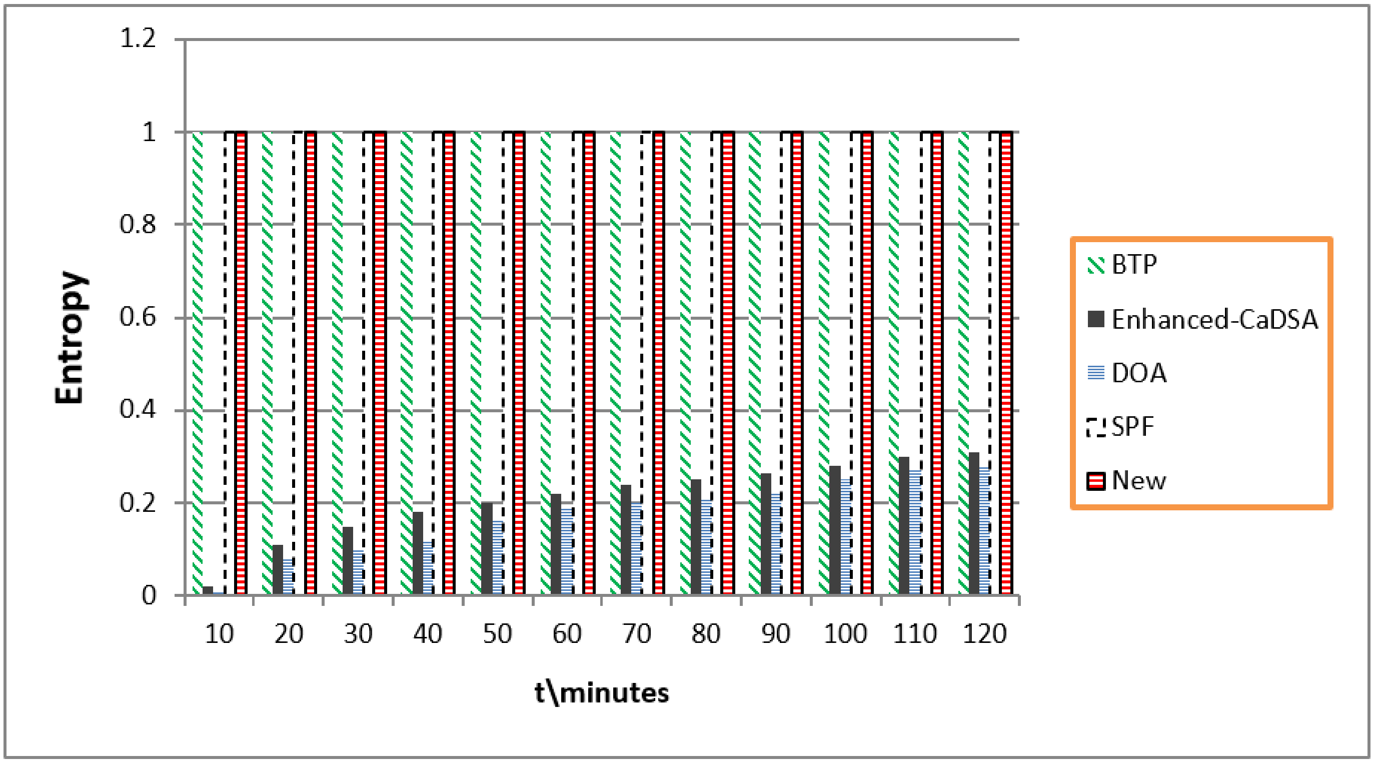


Figure 3. Privacy Level Comparison based on Entropy Metric

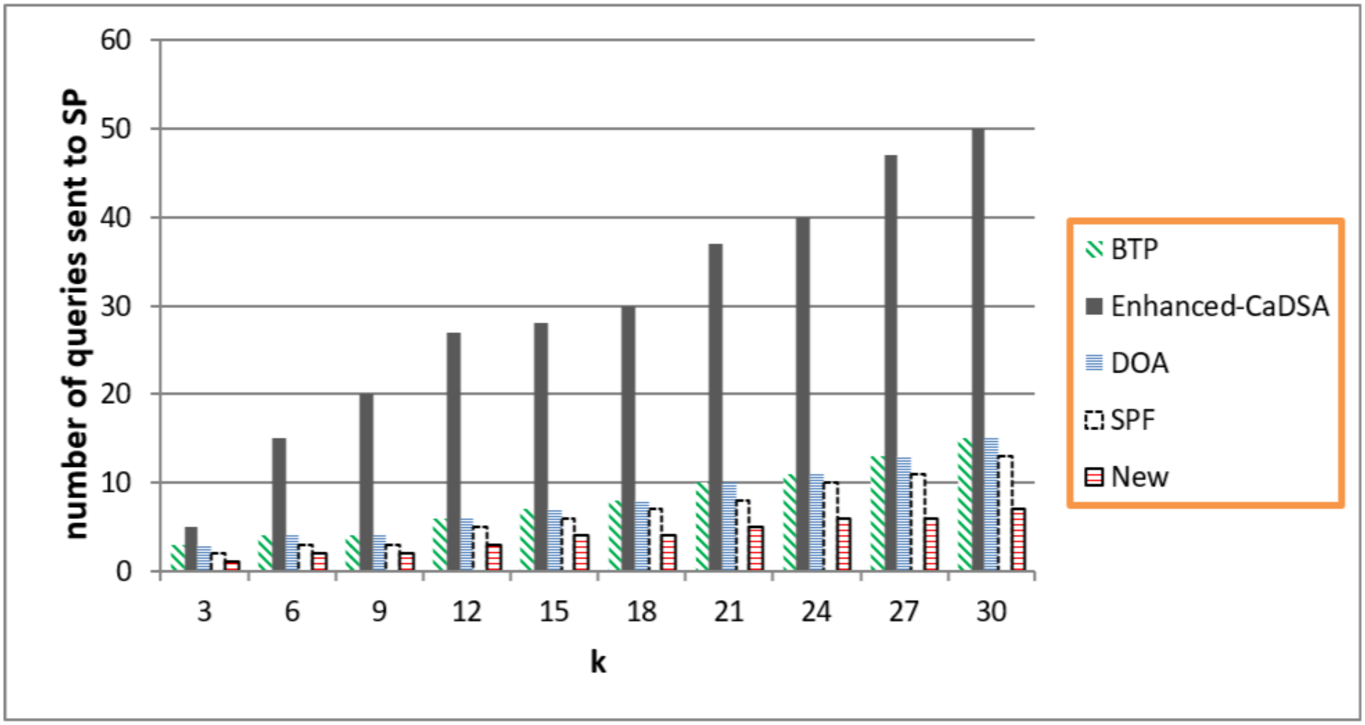


Figure 4. Performance Level Comparison based on Number of Sent Query

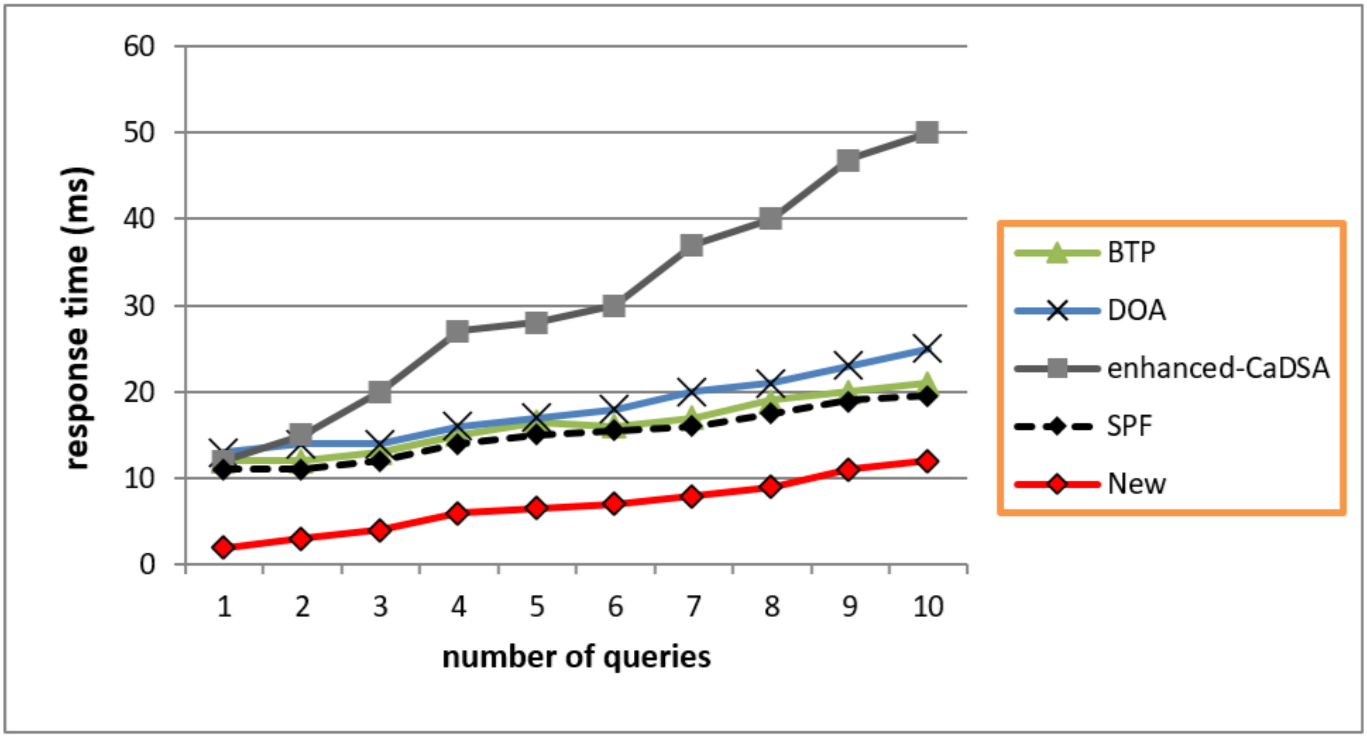


Figure 5. Performance Level Comparison based on Time

The second figure 4 considered the presence of CASH in each approach with a convergent H hit rate. The proposed approach is superior to all other methods because the user does not send every time to the service provider, but rather collects his information in the local cache and sends only at a certain event. We note that the

Dummy approach causes an increase in the number of sent queries, while the obfuscation approach and the encryption approach do not affect the number of sent in the worst case. The SPF approach is also good because it relies on real queries and on cache within the fog node, as well as on Peer.

We note that the proposed approach achieves Max(E) which is like BTP and SPF approaches when the user does not send his own query to the service provider. As for the dummy or obfuscation approach, the level of protection is lower because the user still sends part of his real information to the service provider (note: DOA here refers to relying on obfuscation only without using another approach with obfuscation). Of course, the entropy value here refers to the level of protection from the external attacker or from the service provider in case it is a malicious party. As for the level of protection from the cooperating fog node or the cooperating peer, it varies according to the level of trust that was indicated in the previous analysis for each approach.

The third figure 5 also shows the superiority of the proposed approach in terms of transmission and processing time for queries, where the dummy causes a high transmission time due to the number of extra queries, as well as the obfuscation approach causes a high time due to the size of the area and the need for additional processing. The SPF approach, even though it uses a fog node, is superior to a BTP approach that only depends on a fog node because BTP also uses encryption at every step which affects processing time. As for the proposed approach, despite its use of encryption for a group of queries, the low number of communications with the service provider significantly reduced the time and achieved superiority over the other approaches. But as we mentioned that this superiority is conditional in certain applications in which the user can not send his data with each new update in it, except in the event of an emergency.

Comparison summary and disadvantages of TSA

We note from the above, that the proposed approach outperforms the common approaches in protecting data privacy and security, in terms of privacy level and performance level without affecting the accuracy of the results, in addition to supporting dynamic queries and easing the burden on the system and the service provider, by employing the cache in the user's device. But on the other hand, there is no approach without flaws. The proposed approach is ideal for applications to protect privacy in pandemic situations, especially location-based medical services to prevent the spread of infection but may not be the best option in many applications that require the user to constantly communicate with the service provider. On the other hand, the user's dependence on storing data on his device may sometimes lead to the loss of this data, but with the development of cloud services, the user can store this data in an encrypted form within his own cloud to protect it and to provide it when needed.

Case Study – Saudi Arabia

The new solutions have depended on IoT tools and AI techniques, for example, tracking people and determining the most candidate to have infection according to the rate of intersection with infected persons (by temporal and spatial data resulted by Google-MAP or TWAKALNA “توكلنا”). The algorithms will use the previous information besides medical centers' data to predict the number of potential infected. In addition, it is very important to track the exact sites visited by the infected during their incubation period before their quarantine. We could predict people could carry the Coronavirus, where, If the person has multi-interaction with the infected, that means he is a strong candidate to be infected. Figure 6 depicts the mechanism of action for some medical systems during the Covid-19.

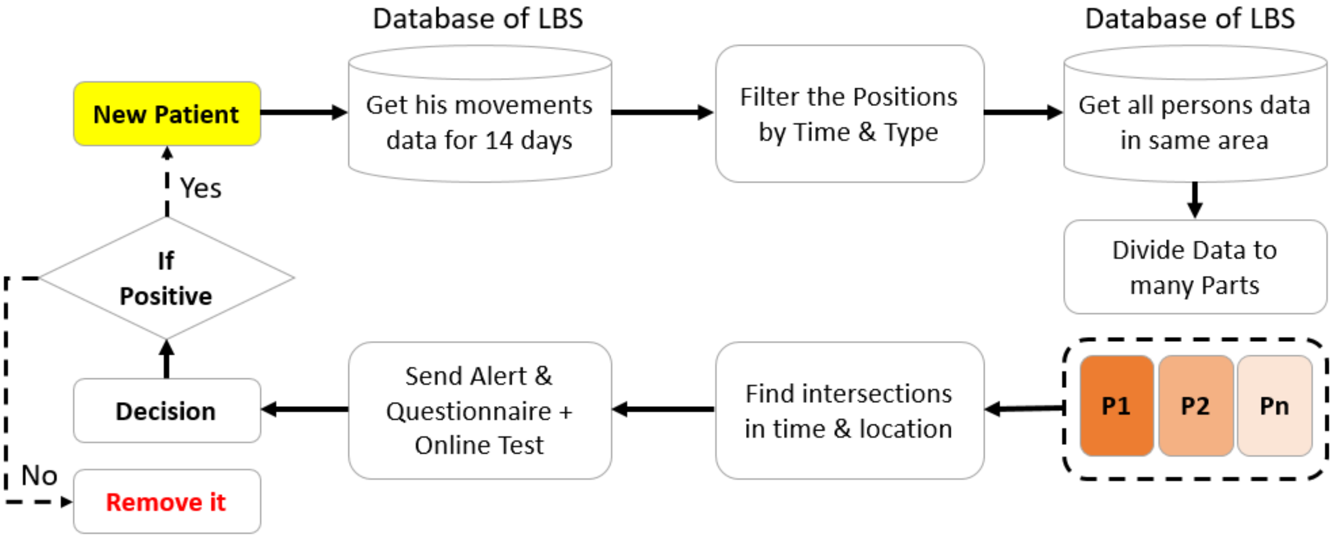

Database of LBS
Database of LBS
New Patient
Get his movements data for 14 days
Filter the Positions by Time & Type
Get all persons data in same area
Divide Data to many Parts
P1
P2
Pn
Find intersections in time & location
Send Alert & Questionnaire + Online Test
Decision
If Positive
Yes
No
Remove it

Figure 6. Scenario for Dealing with Pandemic before Applying STA for Protection

Conclusion

This work introduced an effective new TSA approach to protecting the security, privacy, and reliability of data collected during pandemics. It also presented a method of collecting data in such circumstances. The approach provided a solution to most of the drawbacks experienced by traditional protection methods associated with the impact on the main service quality or level of performance. Through simulation and discussion, we have demonstrated the superiority of the TSA over common and basic approaches to protecting data privacy and security. In the next stage, we will work on developing a standard medical protocol to work during pandemics to improve the performance of medical systems in crises with full respect for the privacy and security of users' data. We will also develop a security protocol for IoT devices and their various applications. This protocol works dynamically by machine learning algoritm to choose the best protection technology**.**

References

[1]. Bahbouh, N.M.; Compte, S.S.; Valdes, J.V.; Sen, A.A.A. An empirical investigation into the altering health perspectives in the internet of health things. *Int. J. Inf. Technol.* **2022**,1, 1–11.

[2]. Shahid, J.; Ahmad, R.; Kiani, A.K.; Ahmad, T.; Saeed, S.; Almuhaideb, A.M. Data protection and privacy of the internet of healthcare things (IoHTs). *Appl. Sci.* **2022**, *12*, 1927.

[3]. Aazam, M.; Zeadally, S.; Harras, K.A. Fog computing architecture, evaluation, and future research directions. *IEEE Commun. Mag.* **2018**, *56*, 46–52.

[4]. Abdali, T.A.N.; Hassan, R.; Aman, A.H.M.; Nguyen, Q.N. Fog computing advancement: Concept, architecture, applications, advantages, and open issues. *IEEE Access* **2021**, *9*, 75961–75980.

[5]. Bambra, C.; Riordan, R.; Ford, J.; Matthews, F. The COVID-19 pandemic and health inequalities. *J. Epidemiol. Community Health* **2020**, *74*, 964–968.

[6]. Zhang, H.; Wang, X.; Fu, Z.; Luo, M.; Zhang, Z.; Zhang, K.; He, Y.; Wan, D.; Zhang, L.; Wang, J. Potential Factors for Prediction of Disease Severity of COVID-19 Patients. *MedRxiv* **2020**,v1,1-8.

[7]. Zhao, W.; Zhong, Z.; Xie, X.; Yu, Q.; Liu, J. Relation between chest CT findings and clinical conditions of COVID-19 disease (COVID-19) pneumonia: A multicenter study. *Am. J. Roentgenol.* **2020**, *214*, 1072–1077.

[8]. World Health Organization. *COVID-19 Disease 2019 (COVID-19): Situation Report*; World Health Organization: Geneva, Switzerland, 2020; Volume 61.

[9]. Wu, Z.; McGoogan, J.M. Characteristics of and important lessons from the COVID-19 disease 2019 (COVID-19) outbreak in China: Summary of a report of 72 314 cases from the Chinese Center for Disease Control and Prevention. *JAMA* **2020**, *323*, 1239–1242.

[10]. Wang, Y.; Wang, Y.; Chen, Y.; Qin, Q. Unique epidemiological and clinical features of the emerging 2019 novel COVID-19 pneumonia (COVID-19) implicate special control measures. *J. Med. Virol.* **2020**, *92*, 568–576.

[11]. Wang, J.; Luo, Q.; Chen, R.; Chen, T.; Li, J. Susceptibility Analysis of COVID-19 in Smokers Based on ACE2, 2020.Article, DOI: 10.20944/preprints202003.0078.v1.

[12]. Naudé, W. Artificial Intelligence against COVID-19: An early review, 2020. IZA Discussion Paper No. 13110, Available at SSRN: https://ssrn.com/abstract=3568314 or http://dx.doi.org/10.2139/ssrn.3568314

[13]. Jia, L.; Li, K.; Jiang, Y.; Guo, X. Prediction and analysis of COVID-19 Disease. *arXiv* **2019**, arXiv:2003.05447.

[14]. Warren, M.S.; Skillman, S.W. Mobility changes in response to COVID-19. *arXiv* **2020**, arXiv:2003.14228.

[15]. Atlam, H.F.; Wills, G.B. IoT security, privacy, safety and ethics. In *Digital Twin Technologies and Smart Cities*; Springer: Cham, Switzerland, 2020; pp. 123–149.

[16]. Sowmiya, B.; Abhijith, V.S.; Sudersan, S.; Sakthi Jaya Sundar, R.; Thangavel, M.; Varalakshmi, P. A survey on security and privacy issues in contact tracing application of COVID-19. *SN Comput. Sci.* **2021**, *2*, 136.

[17]. Huang, H.; Gartner, G.; Krisp, J.M.; Raubal, M.; Van de Weghe, N. Location based services: Ongoing evolution and research agenda. *J. Locat. Based Serv.* **2018**, *12*, 63–93.

[18]. Jiang, H.; Li, J.; Zhao, P.; Zeng, F.; Xiao, Z.; Iyengar, A. Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36.

[19]. Aboelfotoh, R.M.A. Quality of Service and Privacy in Internet of Things Dedicated to Healthcare. Doctoral Dissertation, Université d'Avignon, Cairo, IL, USA, 2021.

[20]. Oussous, A.; Benjelloun, F.Z.; Lahcen, A.A.; Belfkih, S. Big Data technologies: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2018**, *30*, 431–448.

[21]. Ribeiro-Navarrete, S.; Saura, J.R.; Palacios-Marqués, D. Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. *Technol. Forecast. Soc. Chang.* **2021**, *167*, 120681.

[22]. Wang, Z.; Hu, J.; Lv, R.; Wei, J.; Wang, Q.; Yang, D.; Qi, H. Personalized privacy-preserving task allocation for mobile crowdsensing. *IEEE Trans. Mob. Comput.* **2018**, *18*, 1330–1341.

[23]. Yang, P.; Xiong, N.; Ren, J. Data security and privacy protection for cloud storage: A survey. *IEEE Access* **2020**, *8*, 131723–131740.

[24]. Ogonji, M.M.; Okeyo, G.; Wafula, J.M. A survey on privacy and security of Internet of Things. *Comput. Sci. Rev.* **2020**, *38*, 100312.

[25]. Sen, A.; Ahmed, A.; Eassa, F.A.; Jambi, K.; Yamin, M. Preserving privacy in internet of things: A survey. *Int. J. Inf. Technol.* **2018**, *10*, 189–200.

[26]. Davari, M.; Bertino, E. Access control model extensions to support data privacy protection based on GDPR. In Proceedings of the 2019 IEEE International Conference on Big Data (Big Data), Los Angeles, CA, USA, 9–12 December 2019; pp. 4017–4024.

[27]. Ma, J.; Naas, S.A.; Sigg, S.; Lyu, X. Privacy-preserving federated learning based on multi-key homomorphic encryption. *Int. J. Intell. Syst.* **2022**, *37*, 5880–5901.

[28]. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–34.

[29]. Albouq, S.S.; Abi Sen, A.A.; Namoun, A.; Bahbouh, N.M.; Alkhodre, A.B.; Alshanqiti, A. A double obfuscation approach for protecting the privacy of IoT location based applications. *IEEE Access* **2020**, *8*, 129415–129431.

[30]. Niu, B.; Li, Q.; Zhu, X.; Cao, G.; Li, H. Enhancing privacy through caching in location-based services. In Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, 26 April–1 May 2015; pp. 1017–1025.

[31]. Babaghayou, M.; Labraoui, N.; Ari, A.A.A.; Lagraa, N.; Ferrag, M.A. Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *J. Inf. Secur. Appl.* **2020**, *55*, 102618.

[32]. Yamin, M.; Alsaawy, Y.; B. Alkhodre, A.; Abi Sen, A.A. An innovative method for preserving privacy in Internet of Things. *Sensors* **2019**, *19*, 3355.

[33]. Alamri, S. Anonymous Trajectory Method for Indoor Users for Privacy Protection. In *International Conference on Computational Science and Its Applications*; Springer: Cham, Switzerland, 2022; pp. 104–112.

[34]. El-Ansari, A.; Beni-Hssane, A.; Saadi, M.; El Fissaoui, M. PAPIR: Privacy-aware personalized information retrieval. *J. Ambient. Intell. Humaniz. Comput.* **2021**, *12*, 9891–9907.

[35]. Agrawal, R.; Faujdar, N.; Kumar, P.; Kumar, A. Security and Privacy of Blockchain-Based Single-Bit Cache Memory Architecture for IoT Systems. *IEEE Access* **2022**, *10*, 35273–35286.

[36]. Yamin, M.; Abi Sen, A.A. A new method with swapping of peers and fogs to protect user privacy in IoT applications. *IEEE Access* **2020**, *8*, 210206–210224.

[37]. Zhao, Y.; Chen, J. A survey on differential privacy for unstructured data content. *ACM Comput. Surv. (CSUR)* **2022**, *54*, 1–28.

[38]. Ren, Y.; Zhu, F.; Sharma, P.K.; Wang, T.; Wang, J.; Alfarraj, O.; Tolba, A. Data query mechanism based on hash computing power of blockchain in internet of things. *Sensors* **2019**, *20*, 207.

A Comprehensive Intelligent Model Based on Crowdsourcing for Early Warning During Disaster Situation

Not published yet

Abstract

Disaster management is one of the most important systems of smart cities, as disaster management is directly linked to people's lives and is integrated with many different systems such as health, transportation, security, and safety, among others. The most significant challenge facing disaster management systems are the early detecting to disaster and alerting the population when a specific threat is predicted. Traditional alerts, such as general non-customized messages or un-related warning bulletins, have affected the credibility of these methods. This research presents a comprehensive model for managing intelligent alerts during flooding. This model employs an early flooding detection module as an entry point and incentive to start the alert phase. The detection module uses proposed algorithms of machine learning and text mining to process the data of Internet of Things (IoT) and Crowdsourcing. The comprehensive model integrates cutting-edge technologies to enable proactive communication and precise alert initiation. Then, the distributed fog contract throughout the city directs specialized alerts according to the context associated with the location, time, risk level, type of alert, and the nature of the user himself. Additionally, the model provides a set of important services in the form of a smartphone application to activate integration with other systems. Furthermore, the model suggests a centralized control panel for managing civil defense teams, enabling them to make sound decisions promptly and manage support services effectively. For testing and implementation, we present the design of the proposed model, as well as the necessary services, technologies, and tools for the success of intelligent alerts. Additionally, we implement a prototype of bracelet in addition to develop the smartphone application and the dash-board of the centralized control.

Keywords: Alert, Notification, Crowdsourcing**,** Internet of Things, Fog computing, Machine Learning, Flood Risk Prediction.

Introduction

Managing disaster risks is a pressing concern, intimately tied to weather patterns, climate shifts, and the planet's water resources. However, there's a gap in understanding the connection between the increasing threat of climate change and the more frequent natural disasters within the field of disaster risk management [1]. Floods stand out as immensely catastrophic events, causing widespread devastation. According to Tomar et al. [2], floods accounted for a significant 39.26% of global natural disasters between 2000 and 2014, resulting in a staggering USD 397.3 billion in damages. Reports from EM-DAT highlight Asia as the region most affected by floods and storms [3]. These damages are often attributed to various human activities such as deforestation, urbanization, and poorly planned developments [2] [3]. Additionally, the observable changes in climate, leading to extreme rainfall, have worsened the impact of flooding.

Even though floods result in considerable losses, flood management has consistently proven to be costly [4]. For instance, reports indicate that flood management efforts have incurred expenses of USD 1.5 billion to address damages valued at USD 5 billion.

The impact of floods on the environment is multifaceted and profound. Primarily, the immediate consequences encompass the loss of both property and human lives. These events result in the tragic loss of human life and livestock, widespread destruction of crops, and an upsurge in waterborne diseases [31]. Secondly, floods significantly impede economic growth and development due to the high costs associated with relief and recovery efforts. This situation can detrimentally affect investments in infrastructure and other developmental initiatives within the affected regions, potentially crippling the overall regional economy [5]. Thus, the necessity for appropriate interventions to mitigate these negative impacts becomes imperative.

An accurate assessment of flood hazard zones requires consideration of various elements, including elevation, rainfall patterns, land use, flow accumulation, and slope. The intricate interplay among these factors shapes the landscape of risk. While conventional and machine learning algorithms aid in prediction, the regional diversity necessitates tailored responses.

Identifying the most vulnerable flood-hazard areas involves the recognition of five pivotal factors: elevation, rainfall intensity, land use, flow accumulation, and slope. These factors operate in synergy, collectively contributing to the characterization of flood hazard zones. Comprehensive mapping of total flood-prone areas demands the integration of all these factors, given their differential impacts on hazard locations. Figure 1 visually depicts the interaction among these five critical factors [6].

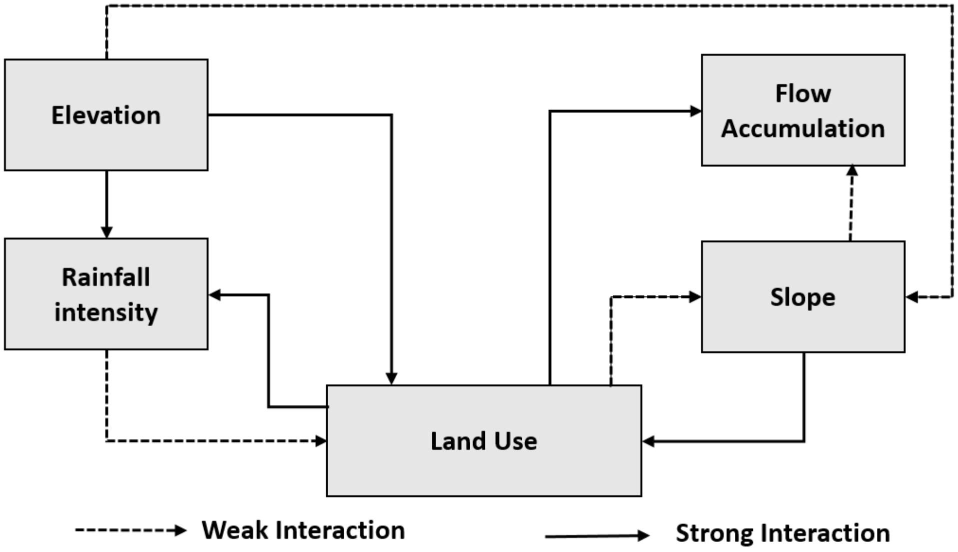


Figure 1. Interaction between Five Factors

Most of the methodologies employed by researchers in the realm of flood risk management entailed prognostications grounded in traditional physical techniques and ma-chine learning. In our preceding endeavor [19], we introduced an innovative approach that instantaneously categorizes the severity level by harnessing the power of IoT [33], fog computing [34], and Machine Learning (ML) [35]. However, the predicament with all methods lies in their inherent imprecision, as it must be borne in mind that susceptibility to flooding diverges from one region to another and even within neighborhoods, contingent upon the geographical characteristics of the area. Thus, it is conceivable that areas within the same city may exhibit dissimilar levels of vulnerability to calamities, such as floods. For instance, low-lying regions and densely populated areas are more susceptible to risks and subsequent losses [28].

Refining the accuracy of algorithms used in threat prediction and classification necessitates tapping into a variety of data sources. The accuracy and reliability of the data stand as the foremost determinant for the success of intelligent models.

In order to control floods effectively, accurate data is required. Real-time insights are provided mainly through IoT. However, the crowdsourcing data, which are fueled by mobile de-vices and social media, can play vital role to enhance the accuracy. Data accuracy in the crowdsourcing is ensured by human intervention, particularly for dynamic occurrences like floods. These models add extensive, fast data to flood prediction and response systems [29].

The interest in Crowdsourcing models has significantly increased in recent years. The prominence of these models as primary data sources has escalated, particularly given the extensive capabilities of smartphones compared to the conventional IoT components like sensors and radio identifiers [29]. The substantial volume of data generated by these models, notably through platforms like social media, has positioned them as swift and crucial sources of contemporary news. Consequently, directing attention toward harnessing and leveraging this data has become an imperative pursuit [30].

Models that use crowdsourcing have many advantages. The most unique advantage is the harnessing human senses, perception, and intelligence in preprocessing data before transmission. In other words, it is challenging to automatically analyze data coming from cameras and then send it to a human element for verification, compared to the alternative approach of sending a description of the data after human inspection and then allowing the machine to analyze this description and extract knowledge from it. The latter approach would be more accurate, especially in applications where crowds are available, such as traffic applications, or in applications that encourage crowds to participate in describing what they observe, such as sports, culture, scientific events, or in the presence of disasters like floods or fires [31].

In a prior study [19], an automated model was developed for early disaster detection, particularly focusing on events like floods. This model harnessed IoT's infrastructure only and utilized classification algorithms for data analysis as Figure 2 demonstrates. This work seeks to enhance the accuracy by integrating modern data models, specifically incorporating crowdsourcing ones. Beside the accuracy, the integration aims to deepen the understanding of disaster impacts based on text-mining algorithms and natural language processing (NLP) [36-37].

In this paper, we introduce an enhanced model aimed at constructing a comprehensive detection framework, emphasizing heightened reliability and facilitating automated classification. The model leverages IoT technologies and crowdsourcing as primary data sources. Within this framework, a dedicated machine learning module is employed for automated classification, while a distinct module specializes in handling textual data. The contributions of this work encompass the following:

- Developing a comprehensive flood detection model with real-time smart notifications.
- Leveraging Crowdsourcing models to incorporate social media, smartphone data, and human perception, enhancing model accuracy based on proposed text-mining algorithm.
- Developing essential smart services in the application for use during disasters, including Smart Notifications, Emergency Assistance, and aid requests, in addition to foster collaboration among crowds, volunteers, and civil defense teams.
- Designing a dashboard information panel providing crucial data and KPIs to defense teams, aiding informed decision-making during rescue operations.

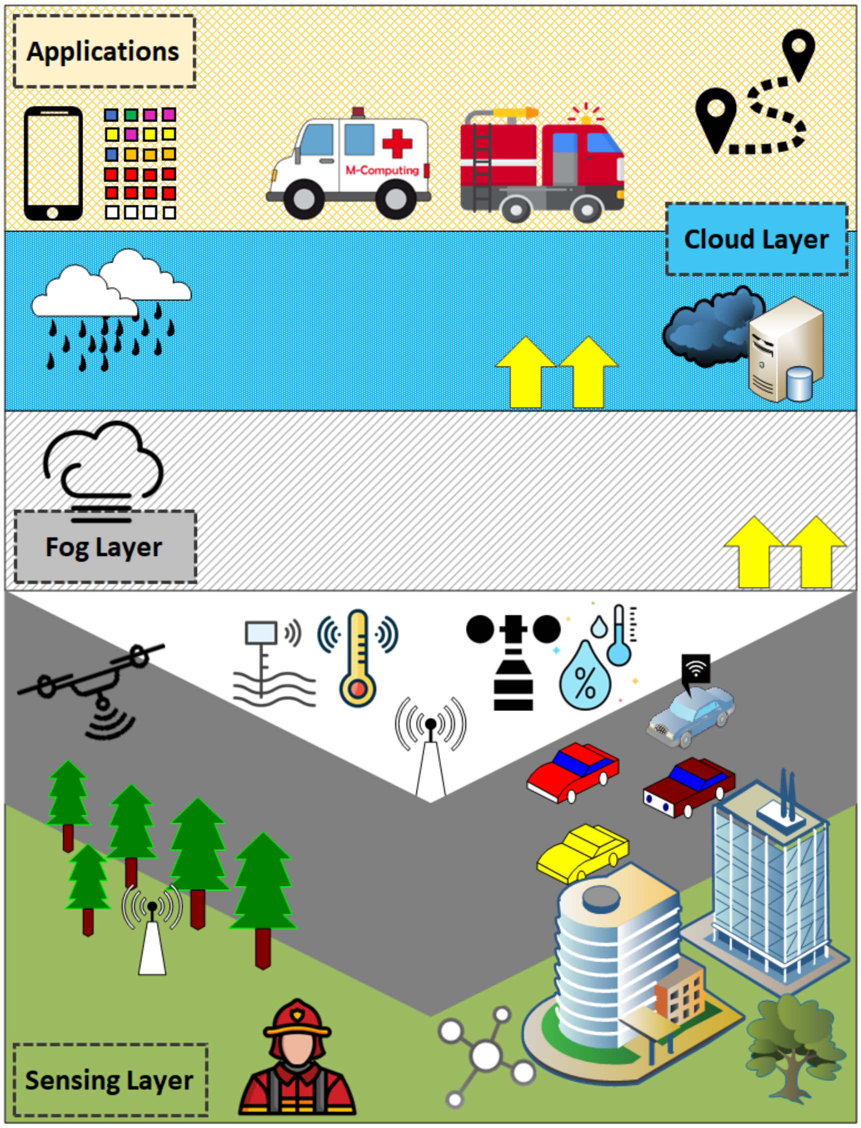


Figure 2. General view of the classification framework

The rest of the paper is structured as follows: Section 2 provides a comprehensive review of related works within disaster management, consolidating existing knowledge in this domain. In Section 3, the proposed approach is meticulously outlined, discussing the refined framework, tools employed, and a detailed exposition of the proposed algorithm. Section 4 presents empirical findings and insights derived from implementing the proposed algorithm. Finally, Section 5 serves as a conclusive summary, encapsulating key findings and implications while synthesizing the study's contributions.

Related Work

Within this section, an extensive exploration of literature pertaining to flood risk management models is undertaken. Specifically, this encompasses a detailed examination of two primary models: The Smart model and the Physical model. The discussion delves into the intricacies and applications of these models within the context of flood risk management. Furthermore, an analysis of tweets as a novel approach to understanding and evaluating flooding risk will be presented, elucidating the significance and potential insights gleaned from social media data in this domain.

2.1. *Models used in flood risk management*

Floods pose immense threats to lives and property, impacting the environment, social fabric, and economies globally. Recent years have underscored an urgent demand for precise flood modeling to aid decision-makers and communities in responding to, managing, and alleviating flood impacts [15]. Among the most formidable obstacles encountered by experts is the intricate task of forecasting floods accurately. The precision of predictions plays a pivotal role in devising effective strategies to mitigate the severity of floods and minimize their potential devastation on lives and properties [16].

The most widely used models in flood risk management are physical modeling and intelligent data-based modeling. The physical modeling is based on hydraulic experiments, through which predictive maps are generated showing areas that may be flood-ed. On the other hand, machine learning approaches rely on data and its analysis. The table below lists some studies that used both models [22]. Table 1 summarizes methods of dealing with flooding otherwise.

Table 1. Summary of the Flooding Management Methods

The objectives	Methodology Used	Smart Model	'hysical Model	Ref
Assess and analyze flooding risk in Chongqing, China	GIS spatial statistics technique	No	Yes	[7]
To investigate the roles of IoT and wireless Sensor Networks in disaster management.	Wireless Sensor Networks with IoT	Yes	No	[8]
Studied flood risk for different land use of Surma Meghna, Bangladesh	GIS and hydraulic modeling	No	Yes	[9]
Identified Flood-prone urban areas	Hydrological Modeling	No	Yes	[10]
Demonstrating that machine learning techniques can be used to accurately map and predict flood-prone areas and to develop flood mitigation plans and policies	ANN and LR	Yes	No	[11]
Identify and map the city of Jeddah's flood zones to minimize their susceptibility and include them into flood risk prevention and mitigation methods	Spatial Analysis	No	Yes	[12]
Identify high-risk areas	RFR model	No	Yes	[13]
Determine the level of risk in each area of the city.	IoT and ML models	Yes	No	[19]
ML models can predict the occurrence of urban pluvial flooding	ML models	Yes	No	[14]

Intelligent data-driven modeling and the Physical Model have risen to prominence as leading methodologies within the realm of flood risk management. These approaches reflect various perspectives for solving the problems brought on by flood disasters. The Smart Model improves early warning systems by providing rapid and precise flood predictions using real-time data from the IoT and advanced analytics as text analysis. The Physical Model, on the other hand, depends on accurate simulations of flood scenarios, providing insightful information about hydraulic processes and assisting in the comprehension of flood behavior [51].

This section focused on the two main models (the intelligent and physical). Table 2. Presents a comparative analysis between these two ones of flood risk management with stressing their advantages, uses, drawbacks, room for development, and integration opportunities, all of which are supported by pertinent references.

Table 2. A Comparative Analysis between Intelligent and physical models

Aspect	Intelligent Model	Physical Model
Strengths	• Makes use of IoT sensors and real-time data for rapid and precise forecasts [38]. • Improves flood response times by improving early warning systems [42].	• Offers precise simulation of flood scenarios, aiding in hydraulic understanding [44]. • Valuable for flood-prone regions and riverine areas, aiding in protection measures [41].
Applications	• Effective in crowded metropolitan environments, optimizing response tactics [43]. • Quick action in managing floods, minimizing potential damage [42].	• Applied in flood protection measures and development assessment [40].
Limitations	• Has issues with cost, cost scalability, and data accuracy [39]. • Might have costs related to IoT infrastructure [39].	• Needs complex data input and depends on specialized equipment [43]. • Involves costs related to specialized equipment and experiments [43].
Improvement s	• Ongoing research into enhancing IoT data accuracy [45]. • Focus on reducing IoT implementation costs [39].	• Explore integration with data-driven approaches [38]. • Incorporate advancements in machine learning [45].
Integration	• The potential for machine learning techniques to work in harmony [8]. • The incorporation of additional IoT applications for improved functionality [7].	• Integrating in a complementary manner with data-driven models [1]. • Coordination with recent technology developments [1].

2.2. Text Analysis in Flooding Risk.

Social media data can help crisis managers and responders meet their data needs by providing valuable information on the social aspects, impacts, and flexibility of cities in the face of a natural disaster [48]. Using Twitter data for flood risk analysis is a promising new field of study. This is because Twitter data can provide real-time information about flood events, which can be used to improve early warning systems and assist emergency responders in flood event management [17]. However, some issues must be addressed, such as the need to develop more precise methods for extracting and analyzing Twitter data [18]. Text analysis entails using natural language processing techniques to extract information from Twitter posts, such as the flood's location, severity, and impact on people and infrastructure [20].

According to the findings of some studies [25, 23, and 55] in the field of tweet analytics in flood risk management, Twitter data can be used to predict the location of floods with a high degree of accuracy. Twitter data can also be used to identify flood-prone areas before they occur [21]. The text of the tweet contains helpful and trustworthy information about damaged main roads and streets. This information could help with emergency response coordination and resource allocation [46].

Crowdsourcing is a model that uses people's intelligence via online human input to achieve specific organizational goals [50]. Crowdsourcing, according to a study conducted by Tripathy et al, is a viable source of reliable information on floods and waterlogging in Mumbai. The crowdsourced data can detect hotspots and has the potential to generate real-time monitoring. This information can then be used to create a flood forecasting framework. When fine-resolution observed datasets are unavailable, crowdsourced information can be extremely useful. These data sets can be used to create a robust, modern, and decision system that will allow for more precise and effective decision-making in the event of a natural disaster [47].

Although there is interest from researchers about studies on social media- platforms-based crowdsourcing in disaster management, smartphone sensor-based crowd-sensing in disaster incidents appears is still a need for more research [50]. Table 3 summarizes the differences among the models that depend on text analysis.

Table 3. Summary of Using Text Analysis for Flooding Management

R	Objectives	Used model	Results	Limitations
[23]	This study described the flood alert situation using only Tweet messages and investigating the informative potential of such data is also demonstrated.	Naïve Bayes	Twitter messages contain valuable flood-spatial information, according to text analysis techniques.	Because of the complexity of some language structures, which contain many special characters, some languages will be difficult to implement in such an environment.
[24]	investigating accurate classification for short informal (colloquial) Arabic text that is used on Twitter.	R tools	Using Colloquial Arabic text as a dataset, investigate a variety of text classification techniques.	
[25]	Using an automatic tweet parsing system, effectively use social media in locating users asking for help during a disaster	Markov model	Develop a text mining algorithm to detect flood-related tweets in English and Hindi, as well as classification of these tweets into high and low-priority classes to identify tweets that require immediate attention.	Some tweets are misclassified by the proposed system and can be studied by researchers to determine the reasons for such misclassification.
[26]	This paper aims to present the findings of an analysis using innovative methodology and used the	Decision tree	The research presented in this paper contributes to a better understanding of the systematic use of volunteer	The inequality of geo-located tweets is a critical constraint.

	2010-2011 South East Queensland Floods as a case study to demonstrate how disaster severity can be assessed using tweets		crowdsourcing data to improve disaster management practices.	
[27]	Build a model that can categorize tweets in order to better organize rescue and relief operations and save lives.	Machine learning and Deep learning models	The paper compares several conventional machines and deep learning techniques.	For the classification task, only English-language tweets were used, whereas, during disasters, users posted several tweets in their regional languages.
[49]	Make a map that characterizes the social impacts of the major flood event in Kerala in 2018.	Manual inspection	Flood impact maps derived from Telegram and Twitter.	On Twitter, relevant data is mixed in with larger amounts of irrelevant data, which means data needs more filtering steps.

Methodology and Proposed Model

Early warning can enable people to take appropriate precautions and protect themselves and their loved ones from the risks that may threaten their lives. The importance of the early warning process is no less important than the importance of early detection.

The proposed framework relies on IoT, fog computing, and ML to adjust to various risk levels based on location. Accurate algorithms are essential since current models fail to account for regional complexity and difference between areas. Our research incorporates technology for sophisticated flood risk management, which is in line with these needs.

This work expands on the ideas presented above by utilizing crowdsourcing's re-al-time accuracy to improve flood management tactics. It strengthens current methods for anticipating and managing floods by integrating IoT and crowdsourcing. The combination of these technologies improves the accuracy of flood predictions. Moreover, this research proposes a text mining algorithm to deal with textual data during floods. This confluence enables more flexible flood management measures and strengthens catastrophe preparedness and response initiatives. In fact, an effective warning mechanism is the standard for the success of all preceding analysis, classification, and prediction processes.

In our previous work [19], we presented a new ML algorithm to real-time risk level classification by relying on the IoT only. Based on the data coming from the sensing layer, the fog node applies the classification algorithm and determines the level of risk. This process is repeated periodically, and when the risk exceeds a certain threshold, people must be alerted immediately. This model is illustrated as a functional view in Figure 3.

3.1. *The Enhanced and developed framework*

To improve the accuracy compared to the previous solutions, the enhanced framework relied on the data of crowdsourcing. The importance of this data is that it comes from people at the heart of the event, so human sense and perception can be used to analyze the data before sending it to the final classification model. On this basis, the accuracy of classification and the level of impact can be more accurately determined. In this endeavor, the research proposed text mining algorithm to processing textual data.

The 2019 statistics from Statista reveal that Saudi Arabia stood within the top ten nations globally, boasting one of the highest volumes of Twitter users [52]. Furthermore, according to the ratio between

Twitter users and populations, Saudi Arabia has the highest number of users on Twitter relative to its population [53]. In addition, studies have shown that the number of volunteers all around the world is on a constant rise. The interesting about volunteers is apparent in Saudi Arabia’s Vision 2030, where one of the goals is to increase the number of volunteers from 11,000 in 2018, to an outstanding 1 million yearly [54].

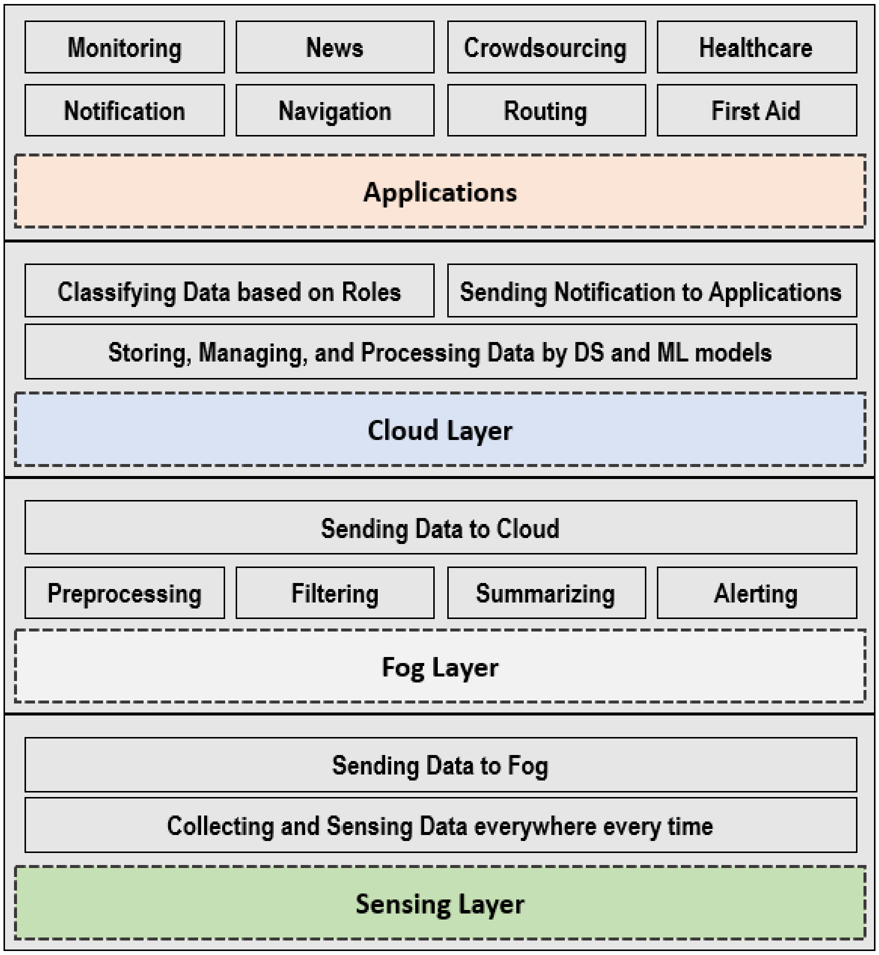


Figure 3. Proposed Model – Functional View

Additionally, this work spotted light on the alert feature by introducing a specialized smart notification component. These enhancements have rendered the proposed framework more inclusive. It is facilitating not only early flood detection but also accommodating diverse geographical locations and varying individual risk levels. The alerts will be personalized according to the severity of the threat and the recipient's profile. Furthermore, these alerts will seamlessly integrate data from disaster management agencies, civil defense units, and analysis inputs sourced from individuals through crowdsourcing, ensuring real-time data updates.

The enhanced framework receives data from the model's automatic classifier to offer personalized warnings based on individuals' temporal, spatial, and health contexts.

Figure 4 outlines the enhanced approach's general lines, consisting of nine main elements.

- Sensors: Their mission is to collect data from the actual environment (the city) and send it to the adjacent fog node
- Crowdsourcing: A service that enables users to share data with service providers.
- RT-Classifier: An automated classifier that classifies the level of risk based on the cognitive model it has, which has the data coming from 1 and 2.
- Smart-Notifier: The intelligent alert system, which is responsible for issuing appropriate alerts based on the information from the classifier and the context of each user.

- ML-Models: It is responsible for training the machine on historical data to find a cognitive model that is distributed to the fog node.
- DB-Knowledge: It contains statistical information based on the classifications of fog nodes and user data.
- GIS Systems: Geographic information systems that provide information about places and their nature, and we have paid attention to the following criteria (lev-el of depression and elevation, whether is it surrounded by mountains or not, degree of slope, the nature of the area is flat or not, the availability of water drainage places, the presence of tunnels)
- Applications: Applications and support services that will be used in the alert process and also in enabling users to participate in relief operations when needed
- D-Support: Decision support systems that rely on knowledge bases in order to support disaster management in taking the right actions.

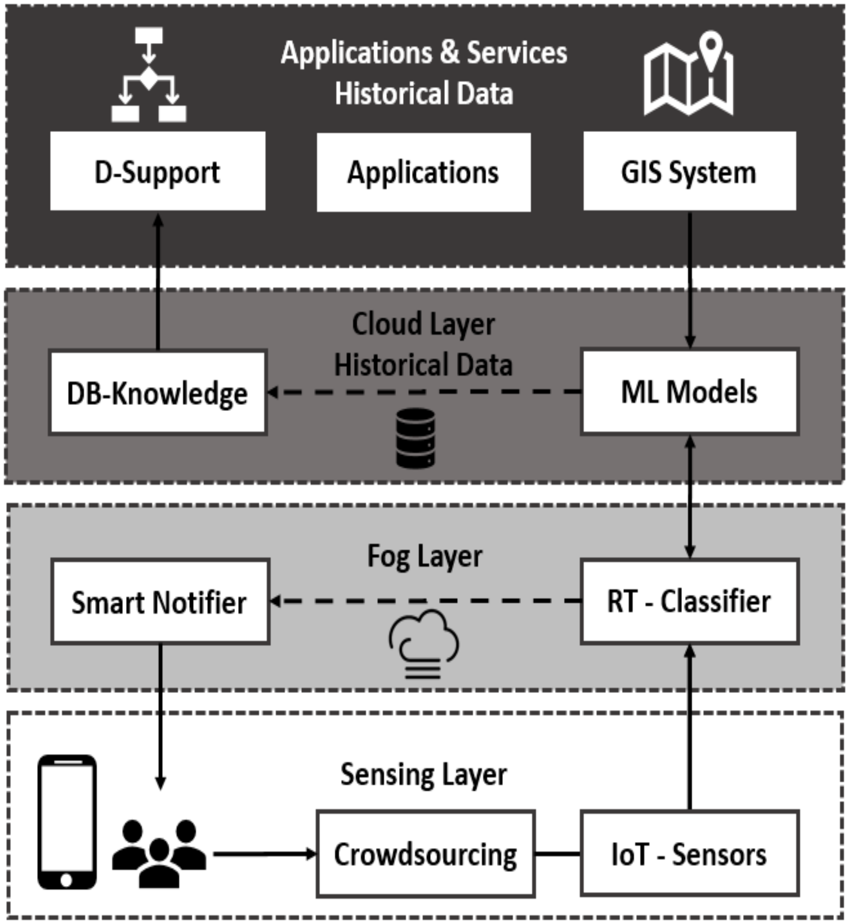


Figure 4. Proposed Model and Main Components.

The most important thing offered by the enhanced framework is the smart alert, in addition to depend on data of crowdsourcing beside the IoT one. The smart alert depends on spatial criteria on the one hand that distinguish one area from another within the city itself, and on the other hand the nature of the user himself. For example, in the case of floods, the low and sloping areas that do not contain drainage facilities will be more vulnerable than the high places or those far from tunnels.

On the other hand, the enhanced framework includes a control panel and smart phone application. To control panel summarizes information of disaster and facilitate the process of monitoring based on each area's characteristics, relief calls, and distribution locations on the map to appropriate decision. While the smart application enables both fog nodes and disaster management to communicate with users effectively and flexibly. In addition, it enables volunteer teams to support the rescue teams. Finally, the enhanced framework employs drones in some cases where access to disaster-prone areas is very difficult.

3.2. *Proposed TM Algorithm and Crowdsourcing Data*

The enhanced framework use ML to process data of Iot, and it use TM for textual data of individuals or volunteers. This combination has achieved greater comprehensiveness. Regarding the analysis of crowdsourcing data, this work adopts two methods for data acquisition:

1. Tweets of the Twitter platform due to the Twitter has become one of the fastest means of news dissemination.

2. A proposed mobile application, which allows users to send textual information and images to the SP.

The received data will be processed and analyzed by a real-time lightweight algorithm to support decision-making for disaster management and civil defense teams. The proposed algorithm is divided into two sections:

A. *Training and list preparation section*

In this section, we performed the following steps:

Step 1: Gathering Tweets
Step 2: Cleaning Data

Step 3: Tokenizing Data

Step 4: Removing Stop Words

Step 5: Stemming Words

Step 6: Building a Word Cloud

Step 7: Calculating Term Weights (TF-IDF)

Step 8: Removing Low-Weighted Words

In the data preparation phase, Algorithm collected tweets of the previous flood incidents. In the cleansing phase, the algorithm removed special characters such as (,:,., etc.,) to retain only the essential letters. This data cleansing step, known as "Cleaning," was instrumental in preparing the text for further analysis.

Next, the tokenization, it is a technique that divided the text into distinct terms using the Tokenizer process. This step broke down the text into constituent components to extract meaningful insights. Additionally, this step important to eliminating common stop words like "the," "is," and "to". The tokenization reduces data size and expedites the processing of the textual data.

Then, the stemming step, it is related to used language of tweets (Arabic or English). With Arabic the framework utilizes ISIR, while for English, the framework utilizes Porter. Both ISIR and Porter simplify words to their root forms. This standardization process ensures the consistency of analysis data.

The framework depends on the most frequent terms as a metric to create the list of important terms. Other method can be used here which is the words cloud which also re-lies on the same metric however by a visualization. The result of this step was a list of most used terms during the flood disaster which needs reviewing by a user.

In addition, the proposed algorithm implemented a quantitative measure known as TF-IDF (Term Frequency-Inverse Document Frequency) to calculate the weights of terms within the tweets. TF-IDF considered both the frequency of a word within a specific tweet and its frequency across all tweets, providing a comprehensive assessment of term importance. Consequently, the algorithm removed words with exceedingly low weights from the list, streamlining the dataset for more effective analysis.

B. Testing section:

For testing purposes, we perform the following steps, which are illustrated as flowchart in Figure 5:

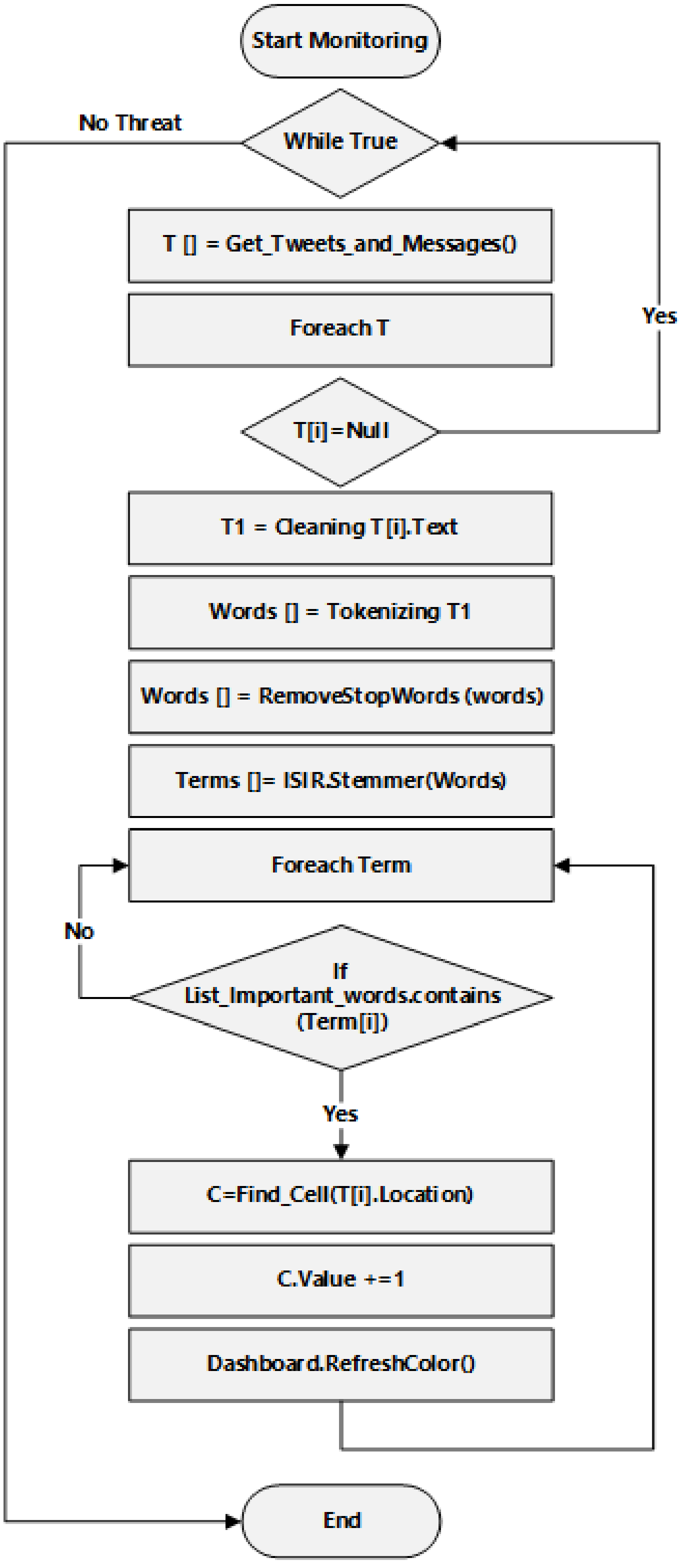

Start Monitoring
No Threat
While True
T [] = Get_Tweets_and_Messages()
Foreach T
Yes
T[i]=Null
T1 = Cleaning T[i].Text
Words [] = Tokenizing T1
Words [] = RemoveStopWords (words)
Terms []= ISIR.Stemmer(Words)
Foreach Term
No
If List_Important_words.contains (Term[i])
Yes
C=Find_Cell(T[i].Location)
C.Value +=1
Dashboard.RefreshColor()
End

Figure 5. TM Algorithm of Processing

- **Step1 Data Input**: Receiving tweets through the Twitter API+ and users' messages from the application.
- **Step 2 Data Cleaning:** Conducting data cleaning**.**
- **Step 3 Tokenization**: Tokenizing data to words based on spaces.
- **Step 4 Stop-Word Removal**: Removing stop-words.
- **Step 5 Stemming:** Specific stemming algorithm is applied to the text.
- **Step 6 Weighting Phase:** Weighting phase to remove unimportant terms.
- **Step 7 Threat Level Determination**: Matching remaining terms with the predefined lists determined by management to determine the threat level.
- **Step 8 Integration with ML Module**: Integrating the threat level with the outputs of ML module and reflecting the end results on the dashboard to facilitate tracking based on location.
- **Step 9 Dashboard Reflection**: A dashboard displays the results, including the threat level. With the help of this dashboard, data can be visualized and tracked geographically. It is a useful tool for disaster management decision-making and monitoring.

Another approach for the proposed algorithm involves using real-time tweets from users during a flood disaster. These tweets can be classified according to threat levels, and machine learning can aid in creating a model for automatic tweet classification. In future works, this model can be used to generate categorized lists based on different threat levels and topics.

3.3. Smart Alert and Smart Services

The effective alert for users is one of the most shortcomings and defects in the previous works. Moreover, the absence of an active role for the users themselves, who can be a helpful tool to provide accurate data for intelligent systems or to help rescue teams instead of being a burden on them.

Some countries employ inefficient warning methods, sending generic SMS messages to all city residents, urging caution without specifying actionable steps or hazards to avoid. This generalization overlooks geographical variations between areas, rendering these warnings inaccurate for most individuals and undermining their credibility. Other methods involve posting warnings on websites, with reliance on users actively reading these notifications, a practice that's increasingly uncommon, particularly with the prevalence of smartphones and their applications. Furthermore, existing warnings often fail to account for the requirements of individuals with specific needs.

To address these shortcomings, this work has introduced a smart application designed to deliver targeted notifications based on users' specific locations. Furthermore, beyond its core functionalities, the proposed smart application endeavors to redefine disaster preparedness and response. It aims to offer a spectrum of crucial services to users in times of emergency, thereby revolutionizing the overall approach to disaster management. Next paints show the proposed services in the application:

A. Emergency Alerts and Information Services:

Direct Alert Service: Receive location-specific alerts in real-time, ensuring that you get critical information tailored to your current location and the unique characteristics of that area. This service is essential for timely and relevant notifications during emergencies.

Awareness Service: Stay informed with periodic articles on what to do and what to avoid during disasters.

Status of Areas Service: Discover which areas are less dangerous during emergencies and how to reach them safely.

Road Condition Service: Access info about road closures due to disasters and identify available routes.

Emergency Numbers: Quickly access essential numbers like civil defense, ambulance, or police.

B. ***User Engagement and Support Services:***

Data Sharing: Play an active role by sharing real-time data from your location to help authorities assess damage accurately. Our system collects and processes this data to verify alert accuracy and refine threat level classifications.

First Aid: Gain access to vital information on how to provide first aid assistance in case of delayed arrival by ambulance crews. Learn through text and video resources on how to handle various emergency scenarios, from drowning to bleeding.

Support Bracelet: For people with special needs, we suggest using a support bracelet that provides vibration alerts.

In essence, our smart application presents a comprehensive suite of services aimed at empowering users during emergencies. Ranging from tailored alerts to instantaneous data sharing and even first aid guidance, our objective is to bolster safety measures and facilitate efficient responses during critical situations.

Next section presents the interfaces of the proposed applications and services.

Implementation and Results

This section is divided into three main sections that aim to test the proposed platform and demonstrate its feasibility and effectiveness.

4.1. Testing the Proposed TM Algorithm

This section is dedicated to testing the results of the proposed TM algorithm for classifying crowdsourcing textual data, whether tweets or comments sent by individuals themselves. A simple dataset of 1000 phrases (Tweets for real users in Saudi Arabia) has been designed and classified as a help requests or a normal condition that does not warrant concern. The algorithm has been implemented in Python by using Google Colabs platform, and the NLTK library for text processing. We used the Confusion Matrix to evaluate the proposed algorithm based on the following criteria: Accuracy, Precision, Recall, and F1-Score.

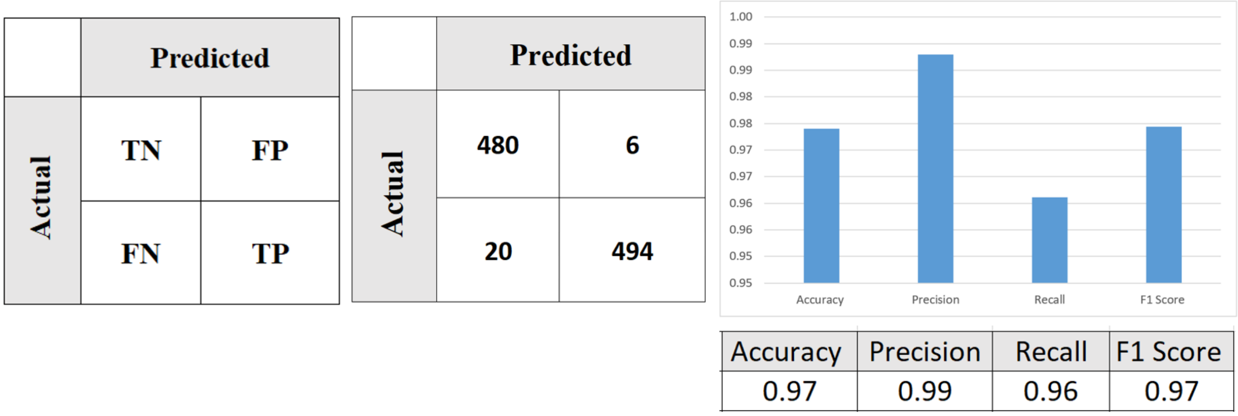
Accuracy= (TP+TN)/(TP+FP+FN+TN) **…. (1)**

Precision= TP/(TP+FP) **…. (2)**

Recall (Sensitivity)=TPR= TP/(TP+FN) **…. (3)**

F1-Score=2* (Recall*Precision) / (Recall + Precision) **…. (4)**

Figure 6 illustrates the results of the experiment on small dataset of real tweets during the last flooding in Jeddah (We collected more than 1000 tweets, we added some examples for few tweets in the index with translation to English). Results show an accuracy of 97%, knowing that the margin of error was in incorrect alerts; in other words, the algorithm system discovered all of the true alerts, which is the most important, and it misclassified some normal phrases as phrases. A request for assistance or an alert



	Predicted	
Actual	TN	FP
	FN	TP

	Predicted	
Actual	480	6
	20	494

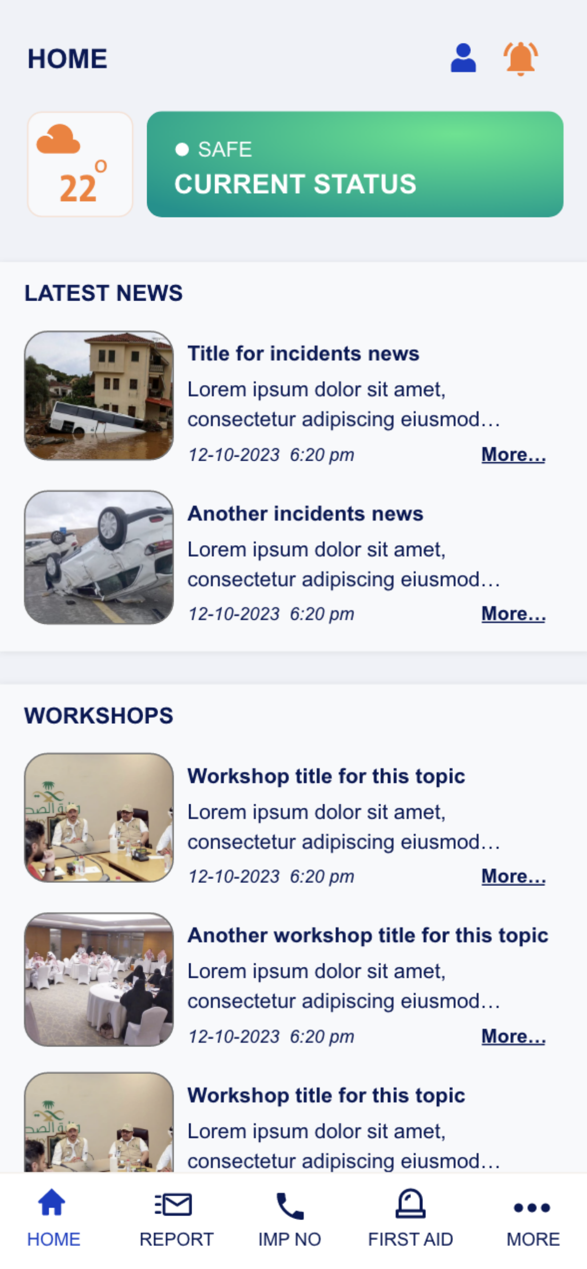
Accuracy	Precision	Recall	F1 Score
0.97	0.99	0.96	0.97

Figure 6. Confusion Matrix and the Accuracy of the Proposed Model

4.2. Implementation of the application

To facilitate the evaluation, a simplified prototype of the proposed application was developed as an Android-based system. The prototype was developed using Java for the Android application and PHP for the server-side functionality, leveraging MySQL as the database system.

Figures 7,8,9 and 10 demonstrate the main interfaces of the proposed application.



HOME

22°

● SAFE
CURRENT STATUS

LATEST NEWS

Title for incidents news
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod…
12-10-2023 6:20 pm More…

Another incidents news
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod…
12-10-2023 6:20 pm More…

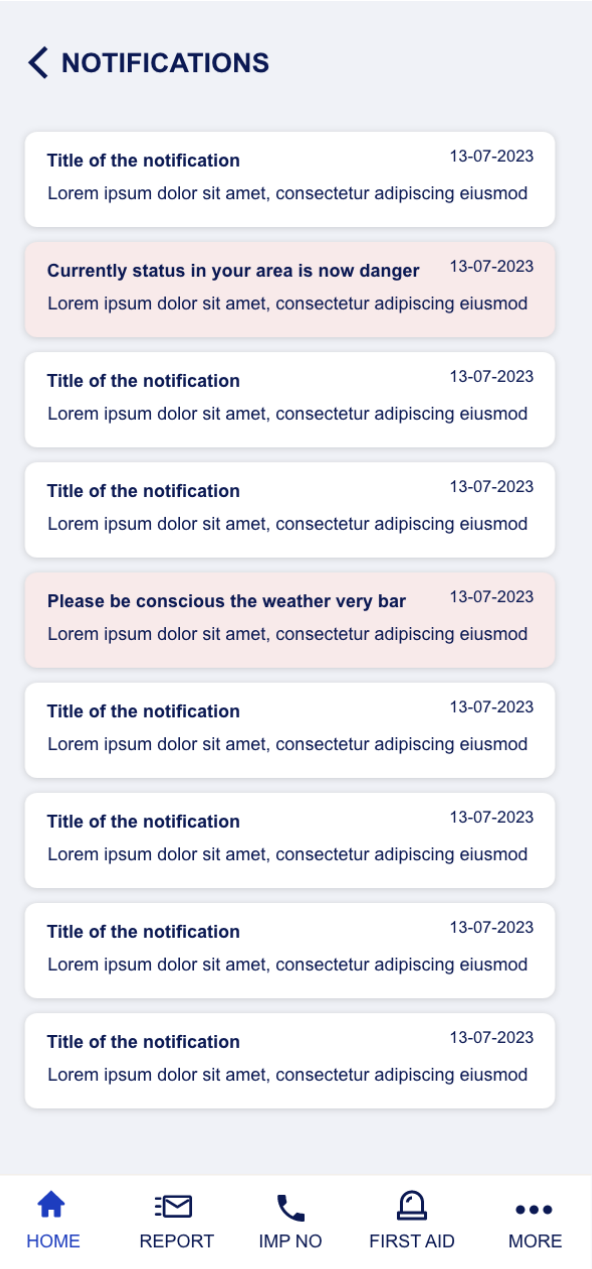
WORKSHOPS

Workshop title for this topic
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod…
12-10-2023 6:20 pm More…

Another workshop title for this topic
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod…
12-10-2023 6:20 pm More…

Workshop title for this topic
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod…

Figure 7. Home Screen



NOTIFICATIONS

Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Currently status in your area is now danger 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Please be conscious the weather very bar 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

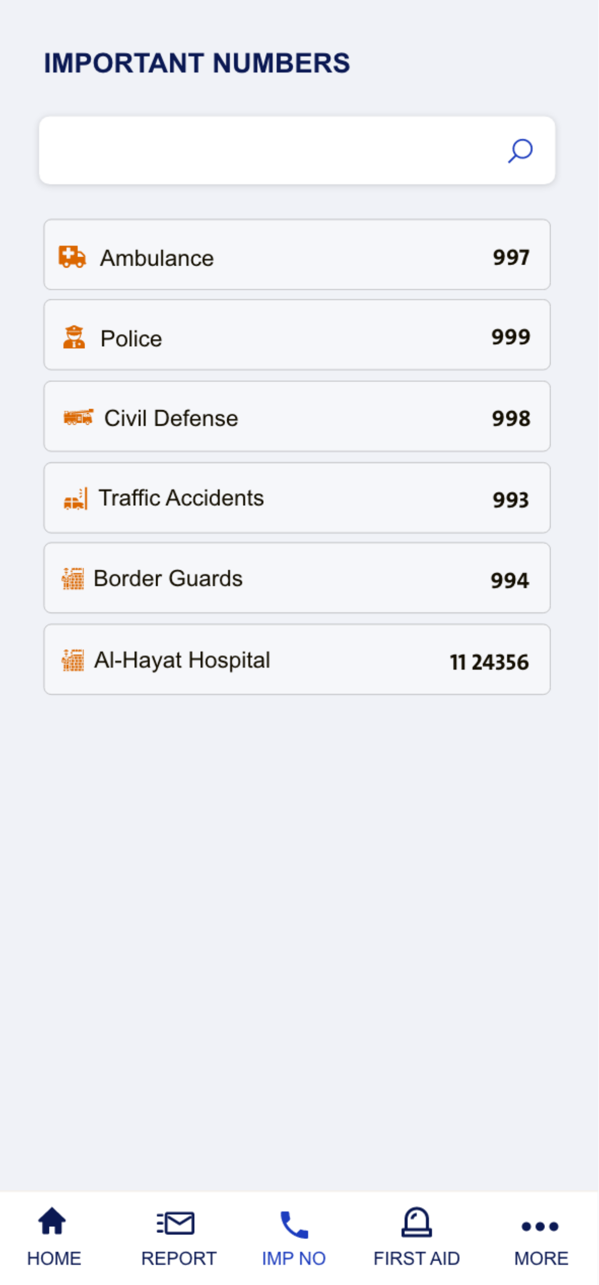
Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Title of the notification 13-07-2023
Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Figure 8. Notification Screen

Figure 7 shows the main interface of the proposed application, which comprises five distinct sections. The first section encompasses alerts, the page's title, and the user's profile information. The second section features a weather indicator, providing real-time information on the current level of danger or safety based on the user's location and the prevailing time. The third section is dedicated to disseminating crucial news updates, while the fourth section offers insights into various workshops, including first aid training, volunteering opportunities, and rescue initiatives. Lastly, the fifth section houses a range of services available within the application.

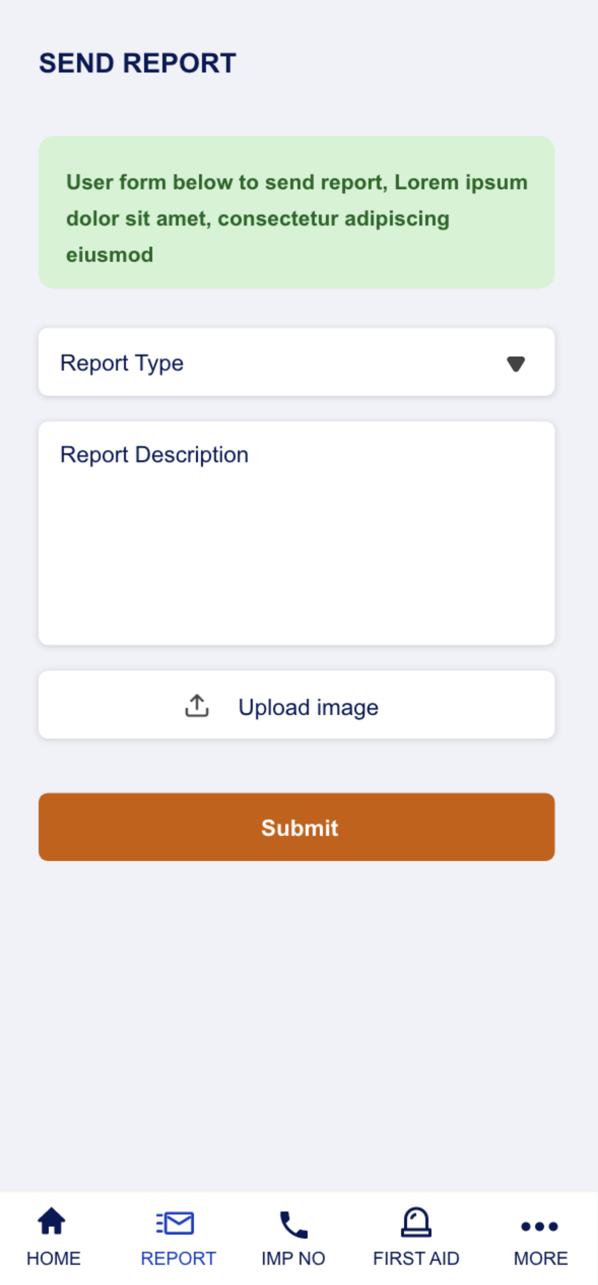
Figure 8 illustrates the alerts disseminated to users in times of emergency. Notably, the most critical alerts are distinguished by a distinct color scheme for easy identification. Additionally, these alerts seamlessly integrate with the proposed smart bracelet, ensuring individuals with special needs receive timely notifications.



IMPORTANT NUMBERS

Ambulance	997
Police	999
Civil Defense	998
Traffic Accidents	993
Border Guards	994
Al-Hayat Hospital	11 24356

Figure 9. Important Number Screen



SEND REPORT

User form below to send report, Lorem ipsum dolor sit amet, consectetur adipiscing eiusmod

Figure 10. Send Report Screen (Volunteer)

Figure 9 displays the availability of crucial contact information for users to access in urgent situations. This includes direct links to emergency services like ambulance, civil defense, and traffic management, streamlining swift responses and necessary assistance when required.

Figure 10 illustrates the report screen, purposefully designed to streamline data submissions by volunteers and registered users of the application. Volunteers have the option to select the type of disaster, incident, or situation they wish to report. They can provide a detailed description and attach a photo as needed. Additionally, the application will automatically include the location information when forwarding the report to the administration.

4.3. Alerting people with special needs

A proposed circuit was relied upon in our previous work in order to manufacture a bracelet that provides hand vibration upon receipt of an alert on the application, the bracelet will play an important role in alerting people with special needs in emergency cases. Figures 11 and 12 show the proposed circuit and the prototype of the proposed bracelet respectively. The circuit and prototype use Nano-Arduino with Bluetooth chip HC-05 and Vibration Motor, in addition to a battery. The primary benefit of the suggested bracelet lies in its affordability, as it addresses the issue of many individuals in developing countries who may be unable to afford a smartwatch.

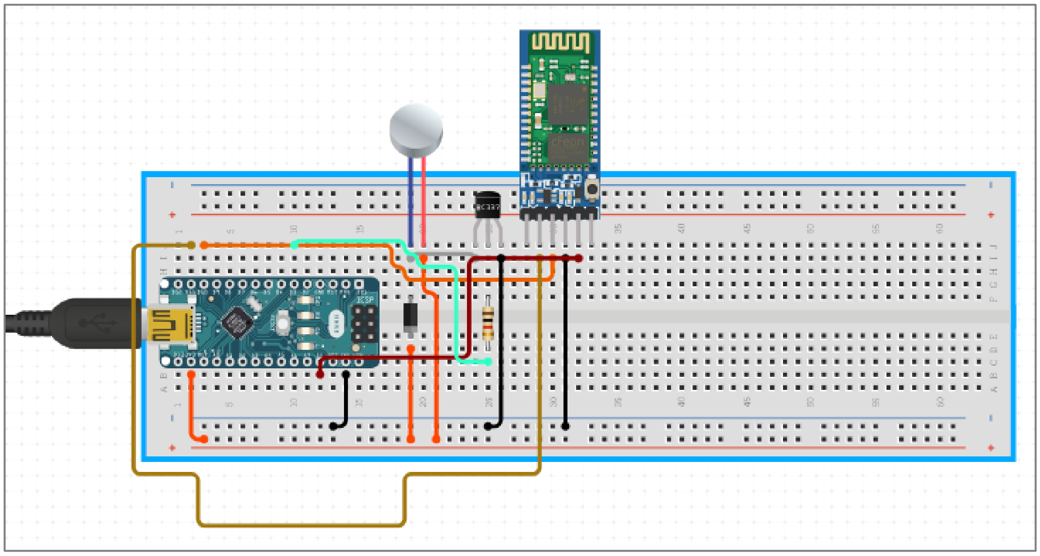


Figure 11. Proposed Circuit for the Notification Bracelet

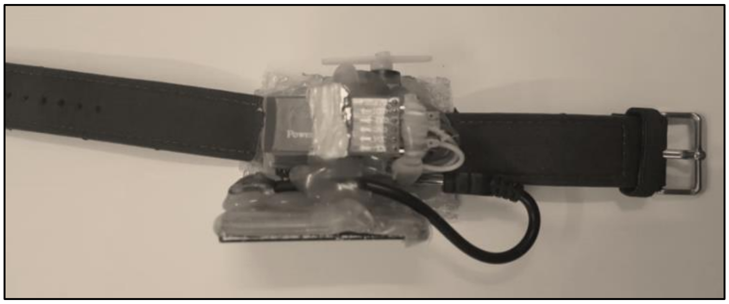


Figure 12. Prototype of Bracelet Implementation

4.4. Central Dashboard for Managing Disasters

Figure 5. Presents the steps of the proposed algorithm for refreshing the dashboard based on the processing textual data by TM. For more details about the algorithm, the source-code of implementing this part has been added in the appendix.

Figure 13 provides a simple simulated example of a disaster management dashboard that shows areas according to the degree of danger and threat, as well as according to the rates of requests for assistance by people. In addition to a map showing the distribution of ambulance and rescue teams and drones, in addition to the roads that have gone out of service. Finally, some important stats and figures. Disaster management can also send instant alert messages and directions, whether to teams or people in a specific area, just by clicking on their area and writing guidance or a message to be sent to everyone.

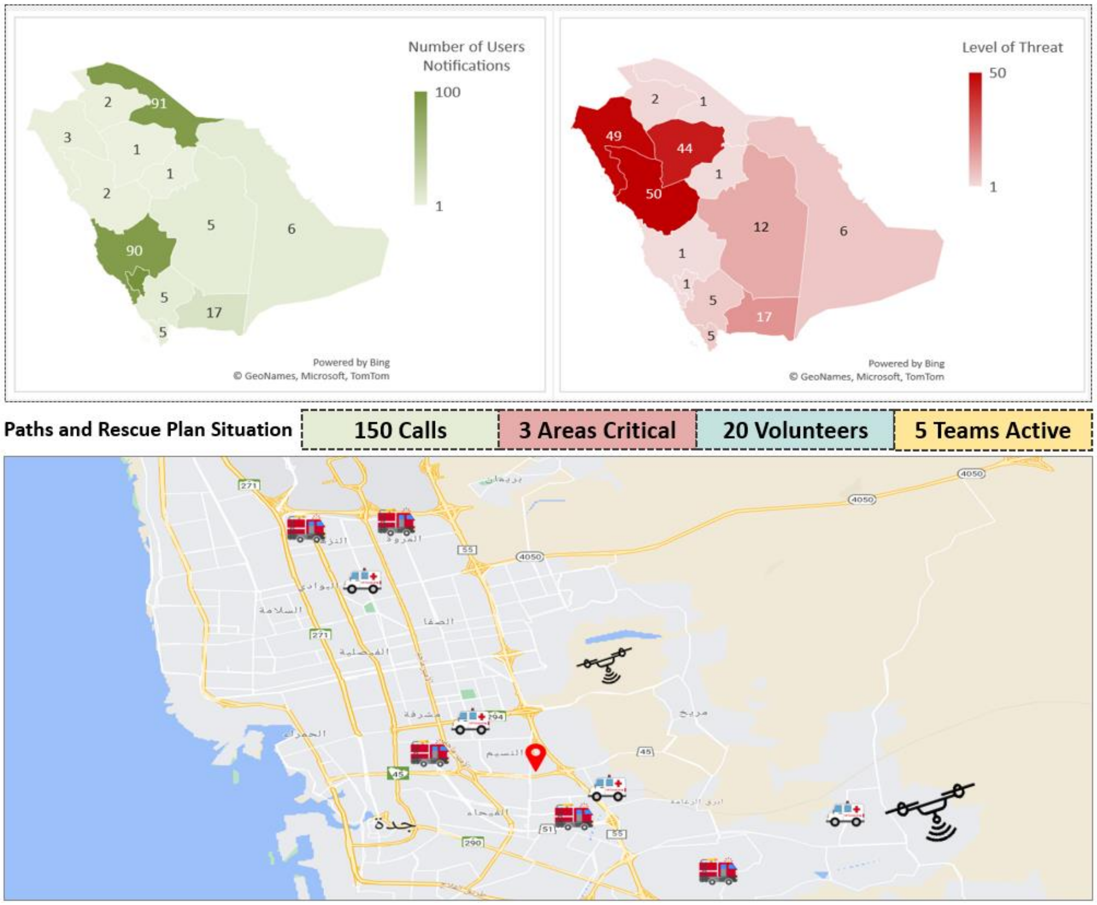


Figure 13. Demo for the Proposed Dashboard

Conclusions

This work introduces an advanced model designed for early detection of disasters, particularly focusing on floods, along with an efficient alert management system post-detection. Leveraging crowdsourcing and the Internet of Things (IoT), this research aims to enhance the precision of early threat detection through a newly proposed TM algorithm. The research also presented a new idea for providing smart alerts by employing fog computing and a smartphone application, with a suggestion of a set of supporting services. The model delivers personalized alerts tailored to the user's context, encompassing location, status, and threat level. Furthermore, the study introduced the concept of utilizing a cost-effective bracelet to alert individuals with special needs. The proposed algorithm demonstrated an impressive accuracy rate exceeding 97%. Additionally, prototypes of the phone application and the alert bracelet were successfully implemented. Future work will delve into the efficient utilization of drones during disaster scenarios, accompanied by an image analysis algorithm designed to process data captured by these drones or surveillance cameras deployed in specific locations. Addressing privacy concerns associated with crowdsourcing will also be a focal point. The forthcoming objective involves the practical application of the entire model in collaboration with relevant authorities, particularly the City Development Authority in the Kingdom of Saudi Arabia, to test the model in real-world scenarios.

References

[1] Tuzyak, Y. M. and Tuzyak, O. [2021], Risk management and advanced systems for observing, monitoring and forecasting natural disasters and events, in ‘Third EAGE Workshop on Assessment of Landslide Hazards and Impact on Communities’, Vol. 2021, European Association of Geoscientists & Engineers, pp. 1–5.

[2] Tomar, P., Singh, S. K., Kanga, S., Meraj, G., Kranjčić, N., Đurin, B. and Pattanaik, A. [2021], ‘Gis-based urban flood risk assessment and management—a case study of delhi national capital territory (nct), india’, Sustainability 13(22), 12850.

[3] Luu, C., Tran, H. X., Pham, B. T., Al-Ansari, N., Tran, T. Q., Duong, N. Q., Dao, N. H., Nguyen, L. P., Nguyen, H. D., Thu Ta, H. et al. [2020], ‘Framework of spatial flood risk assessment for a case study in quang binh province, vietnam’, Sustainability 12(7), 3058.

[4] Aid, C. [2020], ‘Counting the cost 2020: A year of climate breakdown. london, december’.

[5] Le, T., & Ngoc, T. (2020). Floods and household welfare: Evidence from Southeast Asia. Economics of Disasters and Climate Change, 4(1), 145-170. https://link.springer.com/article/10.1007/s41885-019-00055-x

[6] Ozkan, S. P. and Tarhan, C. [2016], ‘Detection of flood hazard in urban areas using gis: Izmir case’, Procedia Technology 22, 373–381.

[7] Cai, S., Fan, J. and Yang, W. [2021], ‘Flooding risk assessment and analysis based on gis and the tfn-ahp method: a case study of chongqing, china’, Atmosphere 12(5), 623.

[8] Adeel, A.; Gogate, M.; Farooq, S.; Ieracitano, C.; Dashtipour, K.; Larijani, H.; Hussain, A. A survey on the role of wireless sensor networks and IoT in disaster management. Geol. Disaster Monit. Based Sens. Netw. 2018, 3, 57–66.

[9] Baky, M. A. A., Islam, M. and Paul, S. [2020], ‘Flood hazard, vulnerability and risk assessment for different land use classes using a flow model’, Earth Systems and Environment 4(1), 225–244.

[10] Abdelkarim, A. and Gaber, A. F. [2019], ‘Flood risk assessment of the wadi nu’man basin, mecca, saudi arabia (during the period, 1988–2019) based on the integration of geomatics and hydraulic modeling: A case study’, Water 11(9), 1887.

[11] Ghile, E.H.; Shirakawa, H.; Tanikawa, H. Application of GIS and machine learning to predict flood areas in Nigeria. Sustainability 2022, 14, 5039.

[12] Daoudi, M. and Niang, A. J. [2019], ‘Flood risk and vulnerability of jeddah city, saudi arabia’, Recent Advances in Flood Risk Management pp. 634–654.

[13] Ullah, K. and Zhang, J. [2020], ‘Gis-based flood hazard mapping using relative frequency ratio method: A case study of panjkora river basin, eastern hindu kush, pakistan’, Plos one 15(3), e0229153.

[14] Ke, Q.; Tian, X.; Bricker, J.; Tian, Z.; Guan, G.; Cai, H.; Huang, X.; Yang, H.; Liu, J. Urban pluvial flooding prediction by machine learning approaches—A case study of Shenzhen city, China. Adv. Water Resour. 2020, 145, 103719.

[15] Kumar, V., Sharma, K. V., Caloiero, T., Mehta, D. J., & Singh, K. (2023). Comprehensive Overview of Flood Modeling Approaches: A Review of Recent Advances. Hydrology, 10(7), 141.

[16] Socas, R. A. M., González, M. A., Marín, Y. R., Castillo-García, C. L., Jiménez, J., da Silva, L. D. D. D. J., & González-Rodríguez, L. (2023). Simulating the Flood Limits of Urban Rivers Embedded in the Populated City of Santa Clara, Cuba. Water, 15(10), 1805.

[17] Bryan-Smith, L., Godsall, J., George, F., Egode, K., Dethlefs, N., & Parsons, D. (2023). Real-time social media sentiment analysis for rapid impact assessment of floods. Computers & Geosciences, 105405.

[18] Rodrigues, A. P., Fernandes, R., Shetty, A., Lakshmanna, K., & Shafi, R. M. (2022). Real-time twitter spam detection and sentiment analysis using machine learning and deep learning techniques. Computational Intelligence and Neuroscience, 2022.

[19] Aljohani, F. H., Abi Sen, A. A., Ramazan, M. S., Alzahrani, B., & Bahbouh, N. M. (2023). A Smart Framework for Managing Natural Disasters Based on the IoT and ML. Applied Sciences, 13(6), 3888.

[20] Yuan, F., Fan, C., Farahmand, H., Coleman, N., Esmalian, A., Lee, C. C., ... & Mostafavi, A. (2022). Smart flood resilience: Harnessing community-scale big data for predictive flood risk monitoring, rapid impact assessment, and situational awareness. Environmental Research: Infrastructure and Sustainability, 2(2), 025006.

[21] Kanth, A. K., Chitra, P., & Sowmya, G. G. (2022). Deep learning-based assessment of flood severity using social media streams. Stochastic Environmental Research and Risk Assessment, 36(2), 473-493.

[22] Hosseiny, H., Nazari, F., Smith, V., & Nataraj, C. (2020). A framework for modeling flood depth using a hybrid of hydraulics and machine learning. Scientific Reports, 10(1), 8222.

[23] Podhoranyi, M. (2021). A comprehensive social media data processing and analytics architecture by using big data platforms: a case study of twitter flood-risk messages. Earth Science Informatics, 14(2), 913-929.

[24] Alabbas, Waleed, et al. "Classification of colloquial Arabic tweets in real-time to detect high-risk floods." 2017 International Conference On Social Media, Wearable And Web Analytics (Social Media). IEEE, 2017.

[25] Singh, J. P., Dwivedi, Y. K., Rana, N. P., Kumar, A., & Kapoor, K. K. (2019). Event classification and location prediction from tweets during disasters. Annals of Operations Research, 283, 737-757.

[26] Kankanamge, N., Yigitcanlar, T., Goonetilleke, A., & Kamruzzaman, M. (2020). Determining disaster severity through social media analysis: Testing the methodology with South East Queensland Flood tweets. International journal of disaster risk reduction, 42, 101360.

[27] Kumar, A., Singh, J. P., Rana, N. P., & Dwivedi, Y. K. (2022). Multi-Channel Convolutional Neural Network for the Identification of Eyewitness Tweets of Disaster. Information Systems Frontiers, 1-16.

[28] Hu, H., Yang, H., Wen, J., Zhang, M., & Wu, Y. (2023). An Integrated Model of Pluvial Flood Risk and Adaptation Measure Evaluation in Shanghai City. Water, 15(3), 602.

[29] Esparza, M., Farahmand, H., Brody, S., & Mostafavi, A. (2023). Examining data imbalance in crowdsourced reports for improving flash flood situational awareness. International Journal of Disaster Risk Reduction, 95, 103825.

[30] Tashtoush, Y., Alrababah, B., Darwish, O., Maabreh, M., & Alsaedi, N. (2022). A deep learning framework for detection of COVID-19 fake news on social media platforms. Data, 7(5), 65.

[31] Xu, H., Wei, W., Qi, Y., & Qi, S. (2022). Blockchain-Based Crowdsourcing Makes Training Dataset of Machine Learning No Longer Be in Short Supply. Wireless Communications and Mobile Computing, 2022.

[32] Stefanidis, S., Alexandridis, V., & Theodoridou, T. (2022). Flood exposure of residential areas and infrastructure in Greece. Hydrology, 9(8), 145.

[33] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. International Journal of Information Technology, 10, 189-200.

[34] Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. International Journal of Information Technology, 13, 829-837.

[35] Mahdi, M. N., Ahmad, A. R., Qassim, Q. S., Natiq, H., Subhi, M. A., & Mahmoud, M. (2021). From 5G to 6G technology: meets energy, internet-of-things and machine learning: a survey. Applied Sciences, 11(17), 8117.

[36] Alqahtani, A., Alhakami, H., Alsubait, T., & Baz, A. (2021). A survey of text matching techniques. Engineering, Technology & Applied Science Research, 11(1), 6656-6661.

[37] Alharbi, A., Abi Sen, A. A., Yamin, M., & Bahbouh, N. M. (2023, March). A Lightweight Algorithm for Text-Classification by Text Mining. In 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 612-616). IEEE.

[38] Mohamed Saber, Tayeb Boulmaiz, Mawloud Guermoui, Karim I. Abdrabo, Sameh A. Kantoush, Tetsuya Sumi, Hamouda Boutaghane, Tomoharu Hori, Doan Van Binh, Binh Quang Nguyen, Thao T. P. Bui, Ngoc Duong Vo, Emad Habib & Emad Mabrouk (2023) Enhancing flood risk assessment through integration of ensemble learning approaches and physical-based hydrological modeling, Geomatics, Natural Hazards and Risk, 14:1, DOI: 10.1080/19475705.2023.2203798.

[39] Himanshu Rai Goyal, Kamal Kumar Ghanshala, Sachin Sharma, Post flood management system based on smart IoT devices using AI approach, Materials Today: Proceedings, Volume 46, Part 20, 2021, Pages 10411-10417, ISSN 2214-7853

[40] Cabrera, J.S.; Lee, H.S. Flood-Prone Area Assessment Using GIS-Based Multi-Criteria Analysis: A Case Study in Davao Oriental, Philippines. *Water* 2019, *11*, 2203. https://doi.org/10.3390/w11112203

[41] Sarafanov, M.; Borisova, Y.; Maslyaev, M.; Revin, I.; Maximov, G.; Nikitin, N.O. Short-Term River Flood Forecasting Using Composite Models and Automated Machine Learning: The Case Study of Lena River. *Water* 2021, *13*, 3482. https://doi.org/10.3390/w13243482

[42] Josipovic, N.; Viergutz, K. Smart Solutions for Municipal Flood Management: Overview of Literature, Trends, and Applications in German Cities. *Smart Cities* 2023, *6*, 944-964. https://doi.org/10.3390/smartcities6020046

[43] Brunner, M. I., Slater, L., Tallaksen, L. M., and Clark, M.: Challenges in modeling and predicting floods and droughts: A review, WIREs Water, 8, e1520, https://doi.org/10.1002/wat2.1520, 2021

[44] Chapter 3 Basic Principles of Open Channel Hydraulics, Editor(s): R.H. French, Developments in Water Science, Elsevier, Volume 31, 1987, Pages 82-135, ISSN 0167-5648

[45] Patrick A. Witte , Karin A. W. Snel and Stan C. M. Geertman, Less is More? Evaluating Technical Aspects and User Experiences of Smart Flood Risk Assessment Tools, Urban Planning, 2021, Volume 6, Issue 3, Pages 283–294

[46] Liu, X., Kar, B., Montiel Ishino, F. A., Zhang, C., & Williams, F. (2020). Assessing the reliability of relevant tweets and validation using manual and automatic approaches for flood risk communication. ISPRS international journal of geo-information, 9(9), 532.

[47] Tripathy, S. S., Chaudhuri, S., Murtugudde, R., Mharte, V., Parmar, D., Pinto, M., ... & Ghosh, S. (2023). Analysis of Mumbai Floods in recent Years with Crowdsourced Data. arXiv preprint arXiv:2306.09770.

[48] Karimiziarani, M., Jafarzadegan, K., Abbaszadeh, P., Shao, W., & Moradkhani, H. (2022). Hazard risk awareness and disaster management: Extracting the information content of twitter data. Sustainable Cities and Society, 77, 103577.

[49] Young, J. C., Arthur, R., Spruce, M., & Williams, H. T. (2022). Social sensing of flood impacts in India: A case study of Kerala 2018. International Journal of Disaster Risk Reduction, 74, 102908.

[50] Cicek, D., & Kantarci, B. (2023). Use of Mobile Crowdsensing in Disaster Management: A Systematic Review, Challenges, and Open Issues. Sensors, 23(3), 1699.

[51] Arabameri, A., Saha, S., Mukherjee, K., Blaschke, T., Chen, W., Ngo, P. T. T., & Band, S. S. (2020). Modeling spatial flood using novel ensemble artificial intelligence approaches in northern Iran. Remote Sensing, 12(20), 3423.

[52] Clement J. Statista. 2019 Aug 09. Leading countries based on number of Twitter users as of July 2019 (in millions) URL: https://www.statista.com/statistics/242606/number-of-active-twitter-users-in-selected-countries/ [accessed 2023-07-11]

[53] Albalawi, Y., Nikolov, N. S., & Buckley, J. (2019). Trustworthy health-related tweets on social media in Saudi Arabia: Tweet metadata analysis. Journal of medical internet research, 21(10), e14731.

[54] Talaue, G. M., Al-Turki, F. S. M., Al-Zahrani, A., Al-Aberi, M., & Al-Malki, S. (2018). Volunteerism in Saudi Arabia: Profiles, Motivations and Perceptions of Volunteer Club Members. International Journal of Civic Engagement and Social Change (IJCESC), 5(3), 1-15.

[55] Jongman, B., Wagemaker, J., Revilla Romero, B., & Coughlan de Perez, E. (2015). Early flood detection for rapid humanitarian response: harnessing near real-time satellite and Twitter signals. ISPRS International Journal of Geo-Information, 4(4), 2246-2266.

****

Chapter 4 - Addressing Interoperability Issue

This chapter extensively discusses the fourth challenge related to interoperability. Interoperability support means enabling different services, devices, and teams to work together. It ensures homogeneous data interoperability, thereby enhancing the ability to process and obtain more accurate and meaningful information. In this chapter, a research paper published in an ISI journal is reviewed, presenting a comprehensive overview of the interoperability issue and all its associated solutions. The paper also introduced a hybrid solution to effectively address this challenge.

A Survey of Interoperability Challenges and Solutions for dealing with them in IoT Environment

Albouq, S. S., Abi Sen, A. A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. M. (2022). A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access, 10, 36416-36428.

Abstract

Interoperability is a functionality that facilitates integration amongst disparate devices and systems used by applications. Integration, inter-operability, middleware, and standardization are some of the synonyms or solutions of interoperability. As such, interoperability facilitates timely, efficient, and effective completion of applications, in addition to finding new, smarter, and more adaptive services. Smart cities, like many other environments and applications, suffer from the lack of interoperability, which makes their processing very challenging. The lack of interoperability also leads to ineffectiveness, which is highly undesirable for applications that deal with emergencies or have exceptional requirements. In particular, interoperability is highly desirable in heterogeneous systems. This research presents a comprehensive review of the available methods and ways to deal with the issues related to interoperability. In addition, the article provides a classification of the available solutions to overcome the lack of interoperability. Various methods which claim to provide interoperability, are sorted out according to the domains and context in which they appear. This research has identified the advantages and limitations of the available methods for facilitating interoperability. A comprehensive framework for dealing with Interoperability in different domains is proposed. This framework provides a hybrid approach for dealing with interoperability, which could be regarded as a comprehensive and reliable solution when dealing with smart cities.

INDEX TERMS Interoperability, Smart City, Middleware, IoT, Internet of Things, Services
Integration

Introduction

The Internet of Things (IoT) has created a new world that is smarter and more adaptable to users, turning many daily activities into automated electronic tasks and devices into smart devices capable of sensing and interacting with the surrounding environment. These devices can also be accessed from anywhere, and at any time [1, 2]. So far, there is no specific standard structure for IoT, but there is a general hierarchical structure as shown in Figure 1 [3].

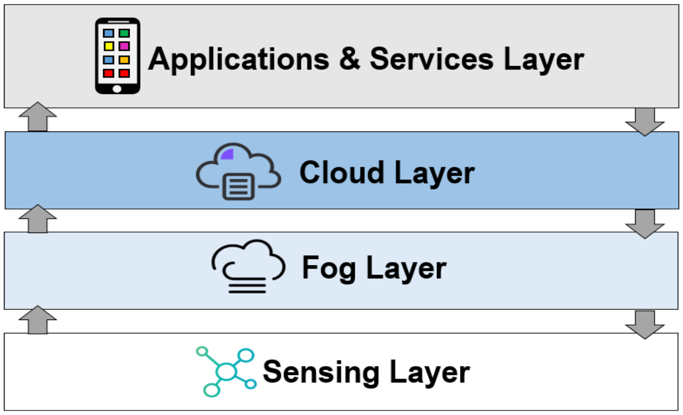


Figure 1. Common IoT Architecture

From Figure 1, we can extract the following main layers:

The first main layer (read from bottom to top) in the IoT architecture is the Perception or Sensing Layer. This layer contains millions of devices and tools that generate large streams of data from their operations. The Radio

Frequency Identification (RFID) and Wireless Sensor Networks (WSNs) form the largest percentage of these objects as RFID tags are often used to give a unique identity to objects whilst enabling their tracking. Applications involving RFID are many, including smart cards, smart locks, automatically identifying apparel, and tracking vehicles and goods.

RFID can be active or passive and provides an external tracking service with the help of the Global Positioning System (GPS). An active RFID is able to save and modify a certain amount of data. WSNs are tools that contribute to capturing the physical conditions of the surrounding environment such as movement, heat, pressure, noise, pollution, and many more. Cameras, microphones, smartphones, smartwatches, smart screens, smart vehicles, and others are examples of WSNs, which are devices with greater capabilities and resources (computing, energy, and storage) [4, 5]. RFID Tags need a reader that receives their data and sends it to the second layer. WSNs also need a virtual gateway or sink also for the same purpose. Most of these tools rely on energy-saving protocols in the communication process such as Bluetooth and ZigBee, but some use Wi-Fi. The reader or sink connects to the internet to send their data to the service provider in the cloud where any event or query is processed, stored, and answered [6].

The second layer is the Fog Computing Layer, which was found to be an intermediate layer between the tools and the cloud. The continuous process of transmitting huge amounts of data frequently to the cloud, especially with a very large number of IoT tools, greatly affects the ability of the cloud to respond quickly enough to the requests coming from users, which makes it unsuitable for many delay-sensitive applications such as medical or transportation applications. Also, continuous transmission constitutes an overload on the entire network. Moreover, communicating user data to the cloud entails the risk of detection.

Indeed, the fog node does play the role of the cloud, but only close to the edge of the network, where a group of tools in a specific area or a smart home can communicate with one of its nodes instead of the cloud. In such a case, the communication will be via Wi-Fi, which would increase the availability of services [7, 8]. Fog nodes have reasonable computing and storage capacity, which can temporarily store and process data before sending it to the cloud. For example, features can be extracted from the image and sent as text. It is also possible to collect some data and communicate it to the cloud as packet segmentation. It is possible to cancel the repetition and remove some personal data or apply some monitoring to the data such as Encryption before transmission.

All the mechanisms in the second layer improve the performance of systems and services, reduce the burden on the cloud, and improve the level of privacy and availability of services for users. Moreover, the fog node can take quick direct action in the event of any emergency or abnormal event, such as calling the nearest ambulance and specifying the location if an accident is detected. Thus, fog nodes enable IoT to respond to time-delay-sensitive applications and services as well [9, 10].

The third layer is the Cloud Layer, which provides permanent storage with high computing power to analyze data, apply some machine learning algorithms, discover knowledge from data and present it to the user in different ways or provide it to applications and services. The cloud offers three main levels of service: IaaS, PaaS, and SaaS. It allows many service providers to spread their services within it, which creates a huge number of services that deal with data coming from the first layer [11, 12].

The fourth layer is the Applications and Services Layer: This layer takes advantage of having all the data coming from the lower layers to provide a better and smarter level than traditional services. It takes advantage of past experiences and analyzes the accumulated data to reveal the user's behavior and adaptations. This is accomplished by providing services that respond to the current status of the user in real-time and alerting them of any emergency situation, as well as services that respond to the context (i.e., adapt according to the nature of the place, time, and situation in which the user is). It is impossible to limit the available services that depend on smart cities. For example, the main areas of these services and applications can be classified with some examples in each field [13, 14].

- The medical field is considered to be the most important field because it is closely related to preserving lives. Hence, we find a lot of development and interest in this field after the emergence of the IoT. Various types of wearable sensors provide continuous monitoring of the user in real-time and the formation of a comprehensive, unified medical file on the user's condition. They also provide the associated data at the desired time for medical workers. The sensors also provide alerts to the personnel in the event of any abnormal activity in their Biometrics to take the appropriate action and prevent a health disaster. The availability services of health everywhere, including remote areas, has also become possible through cooperation with smart homes, and their available tools [15, 16, 17].

- The transportation field is another important area in which IoT has made a significant impact, such as through maps, smart guidance, vehicle tracking, dynamic traffic lights, smart vehicles, and smart roads, thus providing many new and useful services in this field [18, 19, and 20].
- The energy field is also an important field. IoT has contributed to saving energy by smart and scheduled operation of devices, and continuous monitoring of their usage [21, 22].
- The environment, entertainment, business, e-governance, and education are also areas that have been greatly affected by IoT, its tools, and technologies [23, 24].

Note: All previous areas and fields are not considered independent of each other, rather are deemed to be closely connected and integrated. For example, an ambulance in the medical field needs to cooperate with special services in the transportation field; health monitoring services need cooperation with tools in the smart home; smart street lighting needs cooperation with smart energy networks; smart cars can be extremely useful in environmental monitoring and the business sector. More than that, the IoT created a new concept (M2M), which is the relationship of the machine to machine without the need for human intervention. This is a higher level of intelligence which allows machines to communicate with each other and take the appropriate action automatically [25, 26, 27].

All the aforesaid and future developments are expected to be of the higher levels of advanced systems services, capable of addressing the most significant challenges and problems. These obstacles can be easily observed because of the uncertainties and/or lack of cooperation between different technologies, devices, services, and systems due to the lack of interoperability [28]. This is a complex problem in the IoT environment, which does not contain standard protocols or standard methods for representing data and expressing services, and most of the current systems based on IoT are not opened to sharing because of their private ownership. Therefore, in the absence of this requirement, all future aspirations will remain ideas that cannot be implemented [29].

There is another challenge that is also important for the interoperability challenge, namely data privacy and security [30]. However, our research in this article focuses only on interoperability and provides a comprehensive review of the technologies and solutions that were presented during the earlier stages to support interoperability. We also present a chronological classification of the main methodologies and a workable framework for a hybrid approach that can contribute to support the interoperability of various systems and services.

Contribution and Structure of This Paper

This is a review paper. Following are the contributions of this paper. First of all, a comprehensive review of the Interoperability issues in IoT is carried out. Then the current solutions for Interoperability are classified according to their perceived effectiveness. A comprehensive framework for dealing with Interoperability in different domains is proposed. All details of the proposed framework are provided. Finally, a list of challenges and future trends, based on the review of this paper, are outlined.

Definition of Interoperability

There is no single or standard definition of interoperability, rather there are many definitions that generally attribute characteristics that refer to the importance of interoperability and the benefits that can be achieved. The following can be used to form a definition.

- Interoperability provides means to achieve connectivity, sharing, and cooperation for the transfer and exchange of data without effort from the end-user [31, 32, 33].
- Interoperability is the intermediary of connecting different platforms and creating a comprehensive database that contributes to the development of new services, reducing their costs, and providing open markets for working on data [34].
- Interoperability is the process of transmitting data in one context and receiving and interpreting it in another [35, 64].
- Interoperability refers to standardizing the form of data collected from different sensors for the purpose of exchanging and processing them in real-time (RT) while querying them in a unified manner [36].

- Interoperability is a way of creating a collaborative environment between developers that enables them to create widely acceptable systems [37, 60].
- Interoperability is an important criterion when it comes to design of a smart city which plays a critical role in reducing costs at the level of system, data, and applications [38, 59].
- Interoperability is an intermediary solution between service providers who do not want to operate on a single common platform [39, 48].
- Interoperability is policies, standard procedures, and common concepts that aid in data homogeneity and resource collaboration [40, 43].
- Interoperability is a method that enables collaboration between heterogeneous service providers and systems and allows for a data exchange process that greatly expands the ability of smart devices and systems to improve quality of life and create more sustainable services [41, 58].
- Interoperability is one of the most important challenges facing smart cities, the modern industrial revolution, and platforms in allowing heterogeneous things to work and interact with each other (hardware, systems, software, services, data) [42, 65].
- Interoperability is an open issue in the search for a solution to the problem of heterogeneity in networks and achieves cost reduction by working with open programs [43, 66].
- Interoperability is the means for different platforms to interact together by sharing knowledge and information, exchanging data, and improving the level of services [44, 47].
- Interoperability is the hope of smart cities to develop more exciting and intelligent applications through the integration of different platforms and middleware to standardize services [45, 33].
- Interoperability is the means to create standard web applications and enable integration and collaboration between them to create a better level of services [46, 67].
- Interoperability is the solution to the problem of data heterogeneity so that data can be normalized to be similar and complete and thus be processed faster and easier [47, 50].
- Interoperability is the ability of systems to exchange information with an understanding of the meaning (without ambiguity) and is a key factor in modern technology construction and development [48, 68].
- Interoperability is what allows the reuse of IoT services and the exchange of information between different applications and devices [49, 69].

A. IOT DEVELOPMENT STAGES [10, 30, 50, 69, and 70]

The following is a summary of IoT devices.

- Human beings facilitated with controls in their devices directly by radio frequencies signal or by wired connection.
- Human provided control of their devices while using internet, to create a gateway between them (user and device).
- The concept of smart device should be presented the stage where the devices are required to be e connected to the Internet directly without the getaway. More functionalities are added to these devices to increase their memory and computation ability.
- These devices start cooperation among themselves to provide smarter services without interference from human. Moreover, smart devices become relying on the cloud for storing data and enhancement of services, in addition to the availability of more advantages from the cloud properties to user provided for the applications of users.

By implementing the above functionalities, smart devices would have more abilities, in memory, computing, and power in addition they become programmable. Mobile and edge computing is used (like the Fog computing) for addressing the drawbacks of dependency on cloud only. Core Fog Nodes are used to create the recent hierarchical of IoT Structure (Dev, Fog, Core Fog, Cloud, and Apps). Many companies start working with IoT in all domains and using different protocols, data formats, languages, concepts, etc.

Properties of Interoperability

There are many properties related to interoperability such as types of data source, levels, activities, conditions, applying levels, and the context.

A. *TYPES of INTEROPERABILITY [34, 45, 51]:*

- Horizontal operation between different platforms, providers (e.g., AWS Amazon, IBM, Azure, and Google), databases, and devices.
- Vertical operation between the system, the user, and the data source. For example, the manufacture of cars that support interoperability to save M2M costs of integration protocols with open platforms.

B. *DATA SOURCE TYPES [34, 52]:*

- Open data to the public.
- Data requiring authorization to access through a third party.
- Data market between cities and other organizations.
- Static data such as the location of a place or structure.
- Real-time data, such as collected from wireless network sensors.
- Average data over a certain time range.
- Predicted future data.

C. *INTEROPERABILITY LEVELS [34, 35, 49, and 53]:*

- Foundation level: Cleaning at the level of different infrastructures.
- Functional cooperation: Technical (software and hardware) where exchanging data through portals, but without the ability to interpret this data, i.e., provide general functionality.
- Structural level: Grammar or collaboration at the level of meaningful data exchange in common formats where data structure, format, and syntax are defined.
- Semantic level: The systems understand the exact meaning of the information exchanged according to common data models.

D. *INTEROPERABILITY ACTIVITIES in the IOT [54, 60]*

- Get information about different places in cities.
- Shared resources can be accessed by using the same data-saving formats.
- Platform independence so that it can be used in different regions and different collaboration devices.
- The independence of scales, such as displayed in the form of a map.
- The services interface is unified so that the service can access different platforms, each of which provides different data and cooperates to create new services.

E. *CONDITIONS to ACHIEVE INTEROPERABILITY [49, 55]*

- Generality which provides applicability to various fields.
- Effectiveness which ensures an appropriate solution to the use cases.
- Consistency which returns the same result from the repeated use of the same application.
- Transparency which hides technical complexities.
- Scalability which supports big data analytics for all users.
- Verticality which enables working with different layers.

- Horizontality which enables working with different areas of application.
- Completeness which provides support to all use cases.
- Efficiency which enables achieving the goal in the best way.
- Finiteness which limits the number of internal steps.
- Easiness which fosters understanding of stages of education, and usage.
- Security, privacy, and trust which ensure an intrusion free, safe, and trustworthy environment.

F. *INTEROPERABILITY LEVELS IN SMART CITIES [44, 56]*

- Used protocols (ZigBee, Bluetooth, Wi-Fi, 6LoWPAN, IEEE 802.11, SigFox, GSM/GPRS, LTE, 5G)
- The most popular providers (Telefonica, Sktelecom, Nokia, Vodafone, NTT Docomo, Orange, Cisco, Telenor)
- Types of networks (WLAN, BAN, WPAN, WAN, MAN, Mobile Network)
- Used standards or platforms (IETF, 3GPP, ETSI, IEEE, OMA, OneM2M, FIWARE)
- Provided services and applications (transport, healthcare, safety, parking, waste, energy metering)
- Used devices
- Requirements (cost reduction, other services, interoperability, privacy, and security)

G. *INTEROPERABILITY CONTEXTS [53, 57]*

- The ability of the system to receive, process, and transmit clear information to another system.
- The ability of two systems or parties (machine or human) to achieve integration in the exchange of content without absence of distortion or delay.
- Collaboration between parts of distributed systems and the ability to exchange services and data.
- The exchange between information systems and services.
- Ability to combine functions and data according to their significance.
- Use tools that facilitate and coordinate work and information flow.
- The ability of systems to provide new services and accept services from others.

Motivation and Importance

The volume of software, applications, and technologies used in the industry and automation has necessitated providing a more sustainable and intelligent environment in areas such as transportation, health, infrastructure, economy, industry, and government services. But these domains have become more complex because programs and services they use have been developed in different paradigms and environments, rendering them compatible with operating systems, requiring specific data formats. Thus, creating a smart and sustainable environment is not an easy thing. It requires data to be accessed and read automatically, exchanged between applications and services, and analyzed and understood while ensuring reliability and security.

Therefore, the real integration does create a wealth of important information required for different tasks, principles, methods, and concepts to become an achievable goal [31]. Indeed, smart cities are the environment and system which provide open data platforms, create joint data centers between e-governments, and empower citizens to become sensors in a digital environment [32]. The nature of smart cities is supported by many systems that are running by public or private agents, most of which are old systems, incompatible, and non-standard. Such systems lack interoperability, which deprives smart cities of more exciting and useful applications [33].

So far, smart cities use closed systems designed for limited tasks, which cannot be integrated or extended, as there are restrictions on data exchange and accessibility [34]. Also, different areas of smart cities create additional difficulty, because they generate different and huge [35] data and need standardization and real-time processing with [36] standardized query method.

Smart cities have been developed according to a variety of commitments. They were not designed to facilitate interoperability between different systems and the ontology was missing in all areas of smart cities [37]. Instead, their main objective of them was to spread smart, safe, and sustainable services [38]. As a result, they provide fragmented services which are akin to individual ownership, rendering them impossible to work flexibly with other smart city services.

Some examples explicitly demonstrate the importance of cooperation and the need for interoperability between smart city applications and their requirements within their various systems [39]. For example, in smart cities, a disaster response must be very fast and effective. Interoperability promotes integration and cooperation between different teams and different agencies which helps to mitigate the effects of the disaster. Thus, the vehicles, sensors, medical teams, volunteers, operations management, and drones provide more accurate data in real-time and reach inaccessible places, with the ability to quickly transport small items [40].

Therefore, some view smart cities as the future to improve civilization through sensors and robots that have huge proliferation, especially in humanitarian aid and disaster management operations. However, to be able to accomplish their tasks, these robots must be able to work and exchange messages with each other as well as with the decision-support centers or leadership [41].

Another example is that of advanced health care, which requires providing monitoring everywhere, facilitated using various devices for the precision of different vital data. It is also necessary for these devices to share their data and to overcome the problem of different formats due to different development environments and manufacturers to contribute to smarter services. Electronic health records must be unified in cases of a home ambulance visit (patient and his equipment, ambulance, smart hospital, smart city, cloud), all of which must cooperate without any delay to protect the patient's life [42].

Smart healthcare is complex due to heterogeneous data and the need for collaboration between different devices and different departments and destinations [43].The same is true in the field of transportation. Smart cities need open data and open systems to enable the development of new services and applications that can address traffic congestion and air pollution issues. These applications need to integrate into the actions of smart sensors and cloud services and provide common applications (Transport, Healthcare, Safety, Parking, Waste, and Energy Metering) [44].

In the field of energy, the number of smart grids used in smart cities increases with time, and each of them (grids) belongs to a different provider, but their cooperation is an important issue [45]. For example, it is necessary for the providers to create a distributed smart digital archive that enables users and different entities to share data to provide solutions about power consumption [46]. Another case is that of data collection, which requires improved techniques of collecting data from disparate sources and processing them to increase capabilities for the needs of the smart society.

For a solution to support the interaction of different platforms, it is a requirement to have them at the same location [47]. Usually, the service providers use their sensors which are managed on different platforms, forcing them to have interoperability because some cannot work on a single common platform. Therefore, the data may be stored using the relational or non-relational format, in the form of time series, big data, or even in a cloud [48]. It is known that there is a real gap in the standard form of data on the IoT and its applications, which are often in the form of distributed systems and therefore making it difficult to process big data in real-time [49, 50, 51].

In the field of environment, which overlaps with most of the previous examples, Smart cities embrace major challenges related to climate change, especially the process of data collection, energy efficiency, and the provision of future services. All these services require integration between users, devices, facilities, and services, to create an architecture using scalable components with the support of collaborative and shared systems [52]. Even during the industrial revolution, we need to enhance compatibility amongst devices to work together within their systems, which results in saving costs [53].

Many scenarios show the need for people to be required to interact with the surrounding environment, devices, and services in the smart home, which has many other examples and applications [54]. From a more comprehensive level of smart cities, IoT is a vertical communication model that consists of a set of networks that consist of a large group of stakeholders, applications, and services that do not allow horizontal participation between them [55, 56].

The IoT has so far been able to change everything into smart things, starting from the smart home, which contains different devices connected to the Internet, designed with different standards and technologies, to the smart cities and their various applications and services [57]. The aspiration may go beyond the level of smart cities to build a unified global ecosystem of things [55]. It is not an exaggeration to say that the current biggest challenge for IoT is interoperability across heterogeneous service providers and systems. The process of restricted data access has greatly limited the capabilities of smart devices to improve the quality of life at the level of systems, services, data, and applications [58, 59].

The developers, in the IoT platforms, need to negotiate service interfaces and platforms and adapt information Application Programming Interfaces (APIs) and patterns to overcome barriers that have prevented the emergence of widely accepted systems, especially with closed commercial systems. They also need cross-platform access to resources while using the same formats for data representation. The platforms must however be metrics and otherwise independent so that they could be used in different domains without limits [60].

At the same time, many services within smart cities need to be abstract and the public should be able to achieve sustainability in all areas (monitoring and safety, cooperation and health services, daily services such as marketing, facilities management such as garages and others, transportation and traffic congestion, sustainability and environmental preservation, green services, and others) [61]. The data itself for these services must also become open to bring about new visions for smart cities. But any future solution must include not only new but also old applications and data [62], and services must be closely linked with context to improve their quality, performance, adaptability, and intelligence [63].

Historical Solutions and Approaches for Interoperability

The interest to overcome the lack of interoperability during application processing has increased greatly, especially after the spread of millions of services, applications for smartphones, devices, and systems belonging to IoT. Therefore, many attempts have been made to find a solution to this problem. In this section, we will review all the ways, methods, and suggestions that have been presented in this field so far.

A review of available research of the available methods suggests that there are many ways to support interoperability in some form, such as including in the design of applications right from the beginning of devices, but this is difficult to achieve because of the nature of ownership, API's support collaboration, middleware, or by providing dictionaries for common concepts and other methods. In the end, we will provide and review a list of branched or main approaches. In general, the methods for supporting interoperability can be summarized with the following examples:

A. *MIDDLEWARE*

Middleware is an intermediary between heterogeneous systems that converts sent messages between systems from one form to another or to a standard form that is understood by all cooperating parties. The mediator may be at the level of messages between applications or at the level of databases to support different sources. An example of Middleware is a publishing and subscription mechanism such as Broker or DDS, which is a good technique where resources are limited, and usually depend on the Message Queuing Telemetry Transport (MQTT) protocol that supports data security but does not support the discovery of new sites as in Symantec Web technologies [31, 34, 40]. The cloud is one of the proposed solutions as an intermediary for applications and services [60].

B. *MAPPING*

Mapping is the transformation of data from one form to another to enable the involved systems to work in collaboration, by mapping at the data level to create an abstraction [31]. In [42], the idea of a Mapper Code that converts from Extensible Markup Language (XML) to JavaScript Object Notation (JSON) is discussed.

C. *WRAPPER*

The wrapper works to wrap legacy systems in a layer that enables interaction with these systems by providing intermediaries between external systems and the legacy system [31].

D. *TRANSLATOR*

Translator is often used at the level of applications (between the sender and the receiver) so that the data is translated from one form to another to be understood by the receiving party, which could be a one-way or bi-way translator [31].

E. *MESSAGE EXCHANGE*

Message exchange collaboration takes place between services or applications at the level of specific data exchange by representing data in a standard way understood by both parties such as JSON and XML. This is achieved with a classification of the type of possible messages such as agreement on specific messages between different systems in emergency situations [31, 40]. Authors in [63] have presented the idea of a system to process events as messages within smart cities.

F. *DATA ADAPTER*

Data Adapter is an intermediary that enables a connection to different databases with a unified private query interface in standardized formats. This allows to create a simple web service that enables different platforms to connect to different databases and retrieve data without worrying about their heterogeneity or the diversity of their applications [48].

Researchers in [41] presented the idea of the ROS platform for robotic devices and drones to exchange messages among themselves and with the unified command center, where ROS relies on an adapter as a link for messages between the drone and the web service. In such situations, the messages were represented in an XML form containing the robot number, country, and owner, classification of the robot, device type, message type, and data.

G. BRIDGE

Bridge or external gates between applications (which is better than modification) are based on the applications themselves. Applications are built for different functions and thus the bridge translates protocols and maps data between various common formats [40]. Authors in [38] presented the idea of finding a consensus platform or bridge through three business models that support interoperability (Semantic Web, Proxy, and Standard APIs). If the criteria are different, an agent would be needed to convert the data representation between them.

H. APPLICATION PROGRAMMING INTERFACES (APIS)

Application Programming Interfaces (APIs) enable every system or application that provides public methods which can be called from other applications and systems so that these functions provide some services or data in the form required for the caller [31]. An API is usually suitable for agreeing on specific and common focal points only, and a unified standard must be relied on [34]. In [70], the necessity and importance of enabling easy data collection and sharing by providing open APIs are emphasized.

I. SERVICE-ORIENTED ARCHITECTURE (SOA)

Service-Oriented Architecture (SOA) facilitates reuse of IoT services and therefore provides an emulation of the API Gateway principle to support automation with REST, where the platform contains a description of actions and conditions, layers, an operating system for applications and services, intermediate layer, interface writing code, abstraction layer and visualize [69].

Researchers in [51] have presented a simple web service, known as “InterSensor” which provides a data integration strategy between different sensors by connecting to different platforms and their data simulations. In [67], it is confirmed that standard web applications can simplify the integration process between the data, which allows applications to collaborate and create a better level of services such as agile smart hospital by relying on the cloud and big data.

J. ONTOLOGY

Ontology provides support for catalog working to create common concepts by building a dictionary of concepts so that applications and services use them for these applications and services to cooperate, exchange, and understand data. It is often recommended to develop an old ontology instead of building one from scratch to raise the level of compatibility and support for previous systems that depended on the original ontology, and finally to prevent repetition or create different definitions of the same concept [31].

In [59], a set of examples of different famous catalogs (Ready4SmartCity, VoC, Lov4IoT, OpenSensingCity) is provided, which is based on the ontological principle of designing a smart city that supports interoperability at all levels (structure level, hardware level, systems-level, data level, applications level, services and inference level on data). Usually, the catalog focuses on information specific to a domain, time, place, measurement, etc. In [71], the need to build an ontology for smart homes, garages, health, weather, water, transportation, and environment is discussed.

K. DICTIONARY

Dictionary or Ontology adoption by developers of systems can solve the problem for new systems by using a common vocabulary. It is always preferable to rely on reusing and developing a previous ontology to support the above as much as possible. In [49], the idea of a common dictionary was presented to integrate heterogeneous data. Research in [43] emphasizes the need to develop policies, standard procedures, and common concepts that help in the homogeneity of data and the cooperation of sources.

L. SEMANTIC

Semantic refers to a way to understand the meaning of the messages by gestures or tokens, and therefore provides a higher level of cooperation during the process of exchanging data between services and applications. It implicitly relies on many techniques related to data processing and retrieval and natural language processing, in addition to its dependence on ontology [31].

Schema.org is an example of a platform that provides vocabulary and concepts common to search engines and billions of pages on the web (such as a smart object, sensor, measurement, restaurant, aviation) so that the schema can be built, developed, or shortened to a specific field or condition (such as people with needs) [60]. In [49], joint modeling was proposed using semantic web technology to link concepts, enrich content, and rely on heuristics to add new triads. The authors in [58] introduced an idea of a Resource Description Framework (RDF)-based repository which is a repository where users can search for vocabulary and then use it. In [54] semantics to improve service quality and configuration are discussed. In [72] it is suggested to use the RDF trilogy to annotate the data so that it can be understood when it is exchanged between different systems. Research in [37] also used context and ontology in order to reach common specifications and concepts within the same city or within different cities.

M. STANDARDIZING

Standardizing and profiling of data facilitate the necessary processing more rapidly. In this way, big data can be processed in real time. Standardized data also provides a simple, querying method. For data profiling, we need several stages and several techniques such as the data processing stage, context analysis stage, semantic web techniques, ontology, and finally semantic annotation to find semantics for things [36]. It should be noted that the cloud can provide several support layers (application layer, application interface layer, central services tier, virtual tier, and resource tier) [53].

In [50] the idea of normalizing the data is discussed to make it similar and complete to facilitate its processing faster and easier through several steps that include noise isolation, redundancy and treatment, increasing or changing the size, taking care of time, and put in a queue. An advancement was presented in [64], where TabDoc is a system for discovering additional knowledge from documents. These documents must be represented in a standard format (XML, Document Type Definition (DTD), or XML Schema Definition (XSD)) and may need to be integrated with an ontology approach and a specific collaboration template with certain limitations. In [56], two standards O-M1+O-DF to support interoperability are discussed in mobile applications in smart cities, especially in the field of smart transportation. This requires horizontal sharing between devices, protocols, and service providers. An idea of data exchange is deduced in terms of coordination of data to provide an understanding of the content and at the level of communication through an interface or an encoding broker.

N. OPEN DATA

The base for open or central data and information access is a platform to provide open data, available for different applications and services so that the platform becomes an e-participation center (which is very important in e-governments) [32]. However, access to data and the way of storage and coordination must be managed effectively and based on an open standard as far as possible on a specific data structure [40]. The European Union's LoV initiative to describe, allow access, and query various objects and relationships with URLs is presented in [58].

In [53], a reference is made to highlight the importance of agreement on syntax, semantics, and concepts as well as creating relationships across common interfaces, defining the required interoperability contexts, and supporting syntactic threading across standard data and message formats like XML and Symantec, semantic threading according to the meaning of the content. An example of this solution is aimed at providing a central data repository, as suggested in [42], which uses the cloud to create a unified data center. However, it suffers from delays, which may affect the quality, but this problem can be solved by relying on fog computing.

Other researchers have suggested providing central platforms for the IoT environment [35]. There is a necessity of working on a common language and common communication protocols. In [43] a central data platform is proposed which provides the ability to manage it so that it is shared between different applications (in smart cities). It plays several roles, such as:

- Central Connectivity, with a coordinating role between the different systems
- Personal Care, where each system is responsible for itself and uses the data in the central platform
- Knowledge, the central system delegates responsibilities to specific applications and systems to manage pieces of data in the central platform.

O. DISTRIBUTED DIGITAL ARCHIVE

Building a distributed intelligent digital archive is advocated in [46], which enables different users and entities to share data after modeling it in an agreed-upon or standard way. A study conducted in [48] viewed a range of popular platforms for providing specific kinds of data (ThinkSpeak, OpenSensors, The Things Network, Fiware, Weather Underground, OGC) as well as Twitter. In [58], it is emphasized that comprehensive access to data enables more sustainable systems which promise a new vision for government data in smart cities [62]. In [74], the concept of Open Government to achieve sustainability in smart cities is outlined.

P. *WEB of THINGS (WoT)*

The Web of Things (WoT) Initiative has presented a study of the advantages and challenges of open systems with an example of a smart pilot system for managing a city's climate and improving interoperability with devices, where WoT is a platform that allows users to interact with IoT via the web with open standard technologies, with an example of some of the most famous interoperability platforms (Ready4SmartCity, OpenSensingCity, Lov, Lov4IoT) [55, 73]. Federation, discussed in [40], aims to achieve integration by supporting unified interfaces, agreed standards for data models, design engineering constraints, and specific standard communication messages between parts and collaborating systems. Data is usually represented in standard ways such as XML & JSON with the use of supporting open protocols for characterization such as Representational State Transfer (REST) & Simple Object Access Protocol (SOAP).

There is great importance in using standardized standards and protocols [42]. An idea of building a federal system to unify existing systems through creating a framework for developers for an integrated project for smart cities, is presented in [49] to facilitate technical interoperability (software, hardware, and protocol), syntactic (data coordination), and semantic (terms, fields, and meanings according to context), and the organizational structure of the various infrastructures. The idea of adding a union layer at the database level is presented in [61]. This is applicable in cases where big differences in the ways of representing data between systems and then creating new APIs based on this layer appear. The idea of 'Open Data' and 'Smart City Profile' has also been suggested.

Q. *THREE LEVELS – HYBRID*

A three-level of solution as opposed to one is presented in [34], which caters for the following:

- The Foundational Level: A mechanism for exchanging data or making it accessible via Gateways or APIs but without the ability to interpret this data.
- Structural Level: Common format data exchange where the data structure, format, and syntax are defined through common languages or protocols such as MQTT, JSON, and XML standard formats.
- Semantic Level: For collaborating systems to understand the exact meaning of the exchanged information according to common data models and based on Symantec Web.

R. *PLATFORM for DEVELOPMENT*

The platform for development is used for creating a unified development platform that enables developers to adapt and create unified APIs and rely on common pattern models of information to find more compatible applications and services [60]. It provides a platform that fulfills several important criteria as outlined below:

- Create a common web interface for semantic descriptions of cloud or fog-level resources and services such as BigIoT.
- Access via shared framework to the resources using standardized formats for data representation.
- The independence of the platform so that it can be used in different regions and different collaboration devices.
- The independence for the used metrics.
- Provide a service interface so that the various services are delivered via a common application programming interface

S. *ABSTRACTION*

Abstraction is a general framework for abstracting and categorizing smart cities into infrastructure as utilities, non-financial, government and security infrastructure, activity, economic infrastructure, and living space for individuals. These are provided in addition to a central smart control that contains a full-service operator for the smart city according to its priority (monitoring, safety, cooperation Health and daily services such as marketing, utilities such as addition, parking, etc., and finally sustainability, environmental preservation, and green services) [61].

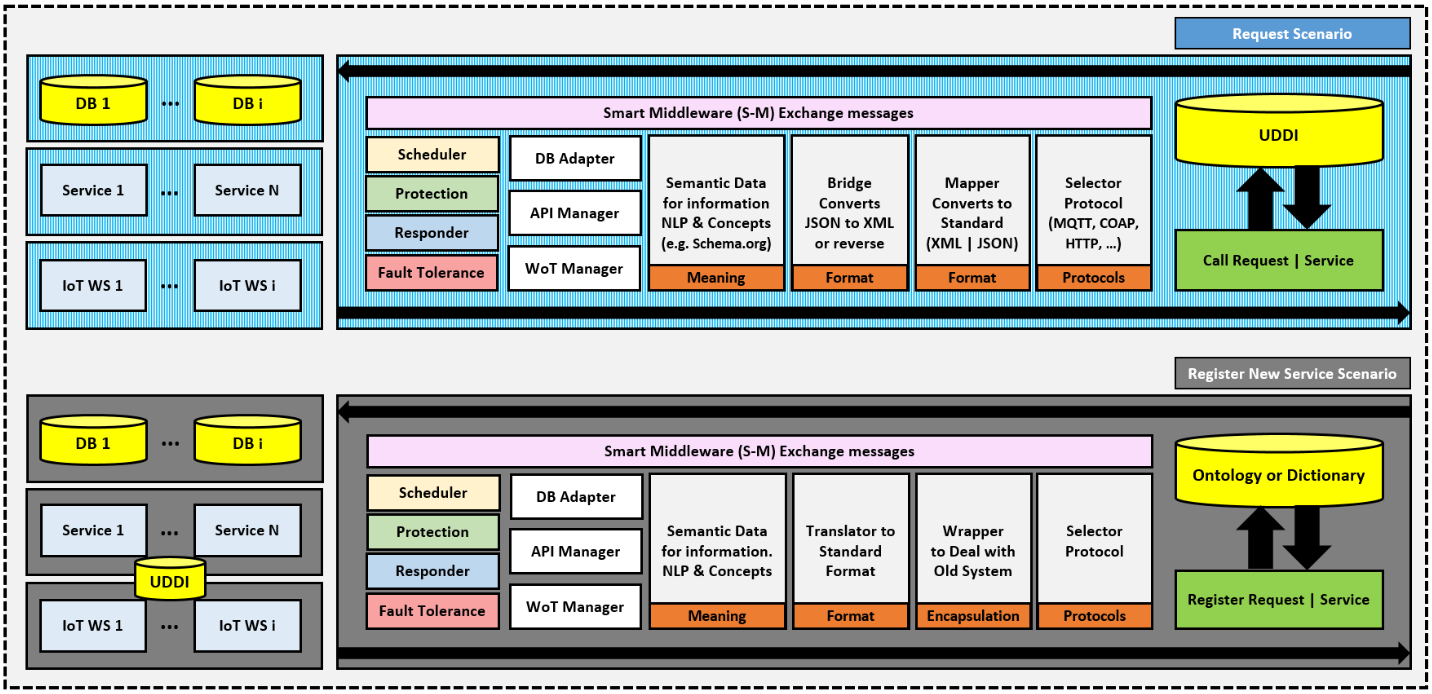
A set of common applications (e.g., GreenIoT framework) that use standard protocols, and common services in several areas is demonstrated in [44]. In [33], an SOS approach is proposed, which is a set of independent files that allow heterogeneous systems to interact together to achieve a common mission based on middleware that focuses on abstraction of smart city concepts, integration of cloud frameworks, and others that support the principle of publishing and subscription to standardize services.

T. *MARKET PLACE and PUBLISHER SYSTEM*

Econo-API has changed the way for creating applications and publishing software and services through a publisher system. It has created a marketplace for sharing data and services [55]. It consists of the following layers:

- Network Things: Anything connected to the internet.

- Access Layer: A unified protocol to enable devices and applications to challenge each other (Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (CoaP), MQTT, Extensible Messaging and Presence Protocol (XMPP)) but it does not mean understanding the meaning of the data.
- Find Layer: For providing data in a way that allows indexing and search by paying attention to the content of the message and relying on scalable semantic models.
- Share Layer: The form of data and publishing it securely through a publisher or consumer with incentives to stakeholders from service providers to participate and transparency in processing.
- Compose Layer: Provides an IDE as an integrated development environment to build compatible services and applications without the need for programming expertise.
- Integration of security management through Access control, Rules, Permission, Interfaces.



Request Scenario
DB 1
...
DB i
Service 1
Service N
IoT WS 1
IoT WS i
Smart Middleware (S-M) Exchange messages
Scheduler
Protection
Responder
Fault Tolerance
DB Adapter
API Manager
WoT Manager
Semantic Data for information NLP & Concepts (e.g. Schema.org)
Meaning
Bridge Converts JSON to XML or reverse
Format
Mapper Converts to Standard (XML | JSON)
Format
Selector Protocol (MQTT, COAP, HTTP, ...)
Protocols
UDDI
Call Request | Service
Register New Service Scenario
DB 1
DB i
Service 1
Service N
UDDI
IoT WS 1
IoT WS i
Smart Middleware (S-M) Exchange messages
Scheduler
Protection
Responder
Fault Tolerance
DB Adapter
API Manager
WoT Manager
Semantic Data for information. NLP & Concepts
Meaning
Translator to Standard Format
Format
Wrapper to Deal with Old System
Encapsulation
Selector Protocol
Protocols
Ontology or Dictionary
Register Request | Service

Figure 2. The Proposed Double Obfuscation Approach, Numbers Represent Execution Flow of Request

Proposed Comprehensive Framework for Dealing with Interoperability

According to the proposed structure of framework for the provision of the interoperability (Figure 2), we have two main phases or scenarios:

Request A Service or Data

Before calling any service, the user must know the link, parameters, and description of the service. This information can be retrieved by Universal Description Discovery and Integration (UDDI) or any public database for services. Then the user will send his request to Smart Middleware (S-M), which will manage the message exchanges between the requester and service providers.

The S-M can deal with a set of standard protocols like CoaP, SOAP, HTTP, MQTT, and XMPP. It can also make mapping for representing data by standard format (XML or JSON according to the requested service) if the request format was different. Alternatively, it will act as a bridge to convert from XML to JSON or reverse the process if required. Finally, if the service provider provides a higher level of integration, the S-Middleware will call the semantic manager, which depends on using NLP and ontology to interpret the meaning of the entities in the request.

Then S-middleware will call an adapter to provide the required DB connection with the service ID database, API manager, Web Service, or WoT. If it is a web service which deals with hardware objects like IoT. In the next stage, the scheduler makes a request (in addition to applying some policies for protection), and the responder will send back the results. A component to manage the errors to enable fault tolerance will be built in the framework.

Register A New Service or Data

SP will check the ontology or dictionary for the concepts to be used to explain its data or service. Then it will send the request to the S-M, which will determine the protocol selected by the service provider from the available list in the Selector Model. The S-M will encapsulate a service by wrapper model only if the service was built by very old technology. The S-M will then convert the data of service to the standard format and enter the phase of semantic data modeling to find the meaning of used entities, which is very critical for the SP to provide a higher level of cooperation with other services.

The DB adapter will select a suitable DB connection for the database, the API manager will create the APIs, and WOT model will create the web service to deal with IoT objects. The scheduler will track the requests, and the protection model will apply the policies to ensure security and privacy. Finally, Responder will send confirmation after recording the service, API, or data, in addition to the information in UDDI or dictionary.

Challenges

After reviewing the proposed and previous works in the field of interoperability, a set of issues and challenges that are still open in the field of interoperability can be summarized as follows:

- There is no agreed-upon definition of smart cities.
- The occasional need for human intervention.
- Energy consumption and development cost issues.
- There is no standardization for standards.
- The problem of relying on fog computing to manage some intermediate tasks.
- The issue of fault tolerance and QoS support.
- The issue of scalability, complexity, and data redundancy.
- Privacy and security issue in the open data or with cooperation
- No ontology covers all areas of smart cities and therefore it is possible to work on creating a general ontology that includes many issues (administrative areas, city objects, events, services).
- Providing global services, for example, if a person travels to another city, he can use the same application to search for car parking.
- An interest in ubiquitous computing, context-awareness.
- Configuring and collecting services in a centralized environment to create new applications.
- Processing old data, and transforming it into a useful, standardized format to enable its interaction with modern systems.

Future Trends

- Creating Open central data or distributed unified database for whole smart city, with standard formats and standard protocols.
- Provide federated services for out-of-boundaries services, or services available everywhere in the smart cities or countries.
- Provide a unified platform for developers to implement service support interoperability by default.
- Provide higher level of services' integration by using semantic web, NLP, and ontology of concepts
- Build a unified global ecosystem based on the IoT by providing a common language of understanding.
- Adding a special collaboration layer in new applications or devices which would be dynamic and programmable (Like the role of SDN in the Networks).
- Improving the quality or auto-generated services by integration of services in the health domain, and support people with special needs to interact with the surrounding environment with awareness for context.

Conclusion and Future Works

This research has discussed several issues related to interoperability in IoT. Indeed, the provision of interoperability is associated with many challenging issues when dealing with smart cities. Many opportunities for more adaptive and smarter services and applications can be achieved, only if we address this issue and provide a framework or model to enable cooperation between heterogeneous objects, devices, protocols, techniques, services, and applications. This research has reviewed most of the historical attempts to address this issue and summarized the new challenges and open issues to build comprehensive solutions that promise a lot. Finally, a hybrid comprehensive design for interoperability framework is suggested. In the future, our research would focus on the details of the proposed solution with implementation and validation on real cases of smart cities applications.

References

[1] Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243-259.

[2] Shah, S. H., & Yaqoob, I. (2016, August). A survey: Internet of Things (IOT) technologies, applications and challenges. In *2016 IEEE Smart Energy Grid Engineering (SEGE)* (pp. 381-385). IEEE.

[3] Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University-Computer and Information Sciences*, *30*(3), 291-319.

[4] Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors*, *20*(9), 2495.

[5] Campos, L. B., & Cugnasca, C. E. (2014, September). Applications of RFID and WSNs technologies to Internet of Things. In *2014 IEEE Brasil RFID* (pp. 19-21). IEEE.

[6] Yamin, M., & Ades, Y. (2009, December). Crowd management with RFID and wireless technologies. In *2009 First International Conference on Networks & Communications* (pp. 439-442). IEEE.

[7] Yi, S., Li, C., & Li, Q. (2015, June). A survey of fog computing: concepts, applications and issues. In *Proceedings of the 2015 workshop on mobile big data* (pp. 37-42).

[8] Iorga, M. , Feldman, L. , Barton, R. , Martin, M. , Goren, N. and Mahmoudi, C. (2018), Fog Computing Conceptual Model, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.500-325

[9] Mahmud, R., Kotagiri, R., & Buyya, R. (2018). Fog computing: A taxonomy, survey and future directions. In *Internet of everything* (pp. 103-130). Springer, Singapore.

[10] Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. *International Journal of Information Technology*, *13*(3), 829-837.

[11] Sadeeq, M. M., Abdulkareem, N. M., Zeebaree, S. R., Ahmed, D. M., Sami, A. S., & Zebari, R. R. (2021). IoT and Cloud computing issues, challenges and opportunities: A review. *Qubahan Academic Journal*, *1*(2), 1-7.

[12] Hosseinian-Far, A., Ramachandran, M., & Slack, C. L. (2018). Emerging trends in cloud computing, big data, fog computing, IoT and smart living. In *Technology for smart futures* (pp. 29-40). Springer, Cham.

[13] Liu, R., & Wang, J. (2017). Internet of Things: Application and prospect. In *MATEC Web of Conferences* (Vol. 100, p. 02034). EDP Sciences.

[14] Wortmann, F., & Flüchter, K. (2015). Internet of things. *Business & Information Systems Engineering*, *57*(3), 221-224.

[15] Farahani, B., Firouzi, F., & Chakrabarty, K. (2020). Healthcare iot. In *Intelligent Internet of Things* (pp. 515-545). Springer, Cham.

[16] Gandhi, D. A., & Ghosal, M. (2018, April). Intelligent healthcare using IoT: an extensive survey. In *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 800-802). IEEE.

[17] Anand, S., & Routray, S. K. (2017, March). Issues and challenges in healthcare narrowband IoT. In *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)* (pp. 486-489). IEEE.

[18] Satyakrishna, J., & Sagar, R. K. (2018, January). Analysis of smart city transportation using IoT. In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 268-273). IEEE.

[19] Saarika, P. S., Sandhya, K., & Sudha, T. (2017, August). Smart transportation system using IoT. In *2017 International Conference on Smart Technologies for Smart Nation (SmartTechCon)* (pp. 1104-1107). IEEE.

[20] Devi, Y. U., & Rukmini, M. S. S. (2016, October). IoT in connected vehicles: Challenges and issues—A review. In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)* (pp. 1864-1867). IEEE.

[21] Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the energy sector. *Energies*, *13*(2), 494.

[22] Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. (2018). Review of Internet of Things (IoT) in electric power and energy systems. *IEEE Internet of Things Journal*, *5*(2), 847-870.

[23] Alnahdi, A., & Liu, S. H. (2017, June). Mobile internet of things (miot) and its applications for smart environments: A positional overview. In *2017 IEEE International Congress on Internet of Things (ICIOT)* (pp. 151-154). IEEE.

[24] Bagheri, M., & Movahed, S. H. (2016, November). The effect of the Internet of Things (IoT) on education business model. In *2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)* (pp. 435-441). IEEE.

[25] Romaniuk, R. S. (2018). IoT–review of critical issues. *International Journal of Electronics and Telecommunications*, *64*(1), 95-102.

[26] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.

[27] Sobin, C. C. (2020). A survey on architecture, protocols and challenges in IoT. *Wireless Personal Communications*, *112*(3), 1383-1429.

[28] Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile Networks and Applications*, *24*(3), 796-809.

[29] Soultatos, O., Papoutsakis, M., Fysarakis, K., Hatzivasilis, G., Michalodimitrakis, M., Spanoudakis, G., & Ioannidis, S. (2019, September). Pattern-driven security, privacy, dependability and interoperability management of IoT environments. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1-6). IEEE.

[30] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *International Journal of Information Technology*, *10*(2), 189-200.

[31] Costin, A., & Eastman, C. (2019). Need for interoperability to enable seamless information exchanges in smart and sustainable urban systems. *Journal of Computing in Civil Engineering*, *33*(3), 04019008.

[32] Cano, J., Jimenez, C. E., & Zoughbi, S. (2015, October). A smart city model based on citizen-sensors. In *2015 IEEE First International Smart Cities Conference (ISC2)* (pp. 1-2). IEEE.

[33] Lopes, F., Loss, S., Mendes, A., Batista, T., & Lea, R. (2016, December). SoS-centric middleware services for interoperability in smart cities systems. In *Proceedings of the 2nd International Workshop on Smart* (pp. 1-6).

[34] Buchinger, M., Kuhn, P., Kalogeropoulos, A., & Balta, D. (2021, January). Towards Interoperability of Smart City Data Platforms. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 2454).

[35] Brutti, A., De Sabbata, P., Frascella, A., Gessa, N., Ianniello, R., Novelli, C., ... & Ponti, G. (2019). Smart city platform specification: A modular approach to achieve interoperability in smart cities. In *The Internet of Things for Smart Urban Ecosystems* (pp. 25-50). Springer, Cham.

[36] Balakrishna, S., Solanki, V. K., Gunjan, V. K., & Thirumaran, M. (2019, January). A survey on semantic approaches for IoT data integration in smart cities. In *International Conference on Intelligent Computing and Communication Technologies* (pp. 827-835). Springer, Singapore.

[37] Espinoza-Arias, P., Poveda-Villalón, M., García-Castro, R., & Corcho, O. (2019). Ontological representation of smart city data: From devices to cities. *Applied Sciences*, *9*(1), 32.

[38] Hwang, J., An, J., Aziz, A., Kim, J., Jeong, S., & Song, J. (2019). Interworking models of smart city with heterogeneous internet of things standards. *IEEE Communications Magazine*, *57*(6), 74-79.

[39] da Silva, W. M., Alvaro, A., Tomas, G. H., Afonso, R. A., Dias, K. L., & Garcia, V. C. (2013, March). Smart cities software architectures: a survey. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing* (pp. 1722-1727).

[40] Pradhan, M., Suri, N., Fuchs, C., Bloebaum, T. H., & Marks, M. (2018). Toward an architecture and data model to enable interoperability between federated mission networks and IoT-enabled smart city environments. *IEEE Communications Magazine*, *56*(10), 163-169.

[41] Pradhan, M., & Devaramani, S. (2019, November). Enabling Interoperability for Ros-Based Robotic Devices for Smart City HADR Operations. In *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)* (pp. 1-6). IEEE.

[42] Jaleel, A., Mahmood, T., Hassan, M. A., Bano, G., & Khurshid, S. K. (2020). Towards medical data interoperability through collaboration of healthcare devices. *IEEE Access*, *8*, 132302-132319.

[43] Liu, S., Li, W., & Liu, K. (2014, May). Pragmatic oriented data interoperability for smart healthcare information systems. In *2014 14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing* (pp. 811-818). IEEE.

[44] Ahlgren, B., Hidell, M., & Ngai, E. C. H. (2016). Internet of things for smart cities: Interoperability and open data. *IEEE Internet Computing*, *20*(6), 52-56.

[45] Ayadi, F., Colak, I., & Bayindir, R. (2019, December). Interoperability in Smart Grid. In *2019 7th International Conference on Smart Grid (icSmartGrid)* (pp. 165-169). IEEE.

[46] Brizzi, P., Bonino, D., Musetti, A., Krylovskiy, A., Patti, E., & Axling, M. (2016, July). Towards an ontology driven approach for systems interoperability and energy management in the smart city. In *2016 International Multidisciplinary Conference on Computer and Energy Science (SpliTech)* (pp. 1-7). IEEE.

[47] Jimenez, C. E., Solanas, A., & Falcone, F. (2014). E-government interoperability: Linking open and smart government. *Computer*, *47*(10), 22-24.

[48] Chaturvedi, K., & Kolbe, T. H. (2018, September). InterSensor service: establishing interoperability over heterogeneous sensor observations and platforms for smart cities. In *2018 IEEE International Smart Cities Conference (ISC2)* (pp. 1-8). IEEE.

[49] Gyrard, A., & Serrano, M. (2016, March). Connected smart cities: Interoperability with seg 3.0 for the internet of things. In *2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)* (pp. 796-802). IEEE.

[50] Babar, M., & Arif, F. (2017). Smart urban planning using Big Data analytics to contend with the interoperability in Internet of Things. *Future Generation Computer Systems*, *77*, 65-76.

[51] Chaturvedi, K., & Kolbe, T. H. (2019). Towards establishing cross-platform interoperability for sensors in smart cities. *Sensors*, *19*(3), 562.

[52] Palomar, E., Chen, X., Liu, Z., Maharjan, S., & Bowen, J. (2016). Component-based modelling for scalable smart city systems interoperability: A case study on integrating energy demand response systems. *Sensors*, *16*(11), 1810.

[53] Zeid, A., Sundaram, S., Moghaddam, M., Kamarthi, S., & Marion, T. (2019). Interoperability in smart manufacturing: Research challenges. *Machines*, *7*(2), 21.

[54] Tektonidis, D., & Koumpis, A. (2012). Accessible Internet-of-Things and Internet-of-Content Services for All in the Home or on the Move. *International Journal of Interactive Mobile Technologies*, *6*(4).

[55] Robert, J., Kubler, S., Kolbe, N., Cerioni, A., Gastaud, E., & Främling, K. (2017). Open IoT ecosystem for enhanced interoperability in smart cities—Example of Métropole De Lyon. *Sensors*, *17*(12), 2849.

[56] Karpenko, A., Kinnunen, T., Madhikermi, M., Robert, J., Främling, K., Dave, B., & Nurminen, A. (2018). Data exchange interoperability in IoT ecosystem for smart parking and EV charging. *Sensors*, *18*(12), 4404.

[57] Samuel, S. S. I. (2016, March). A review of connectivity challenges in IoT-smart home. In *2016 3rd MEC International conference on big data and smart city (ICBDSC)* (pp. 1-4). IEEE.

[58] Kolbe, N., Kubler, S., Robert, J., Le Traon, Y., & Zaslavsky, A. (2017, June). Towards semantic interoperability in an open IoT ecosystem for connected vehicle services. In *2017 Global Internet of Things Summit (GIoTS)* (pp. 1-5). IEEE.

[59] Gyrard, A., Zimmermann, A., & Sheth, A. (2018). Building IoT-based applications for smart cities: How can ontology catalogs help?. *IEEE Internet of Things Journal*, *5*(5), 3978-3990.

[60] Bröring, A., Schmid, S., Schindhelm, C. K., Khelil, A., Käbisch, S., Kramer, D., ... & Teniente, E. (2017). Enabling IoT ecosystems through platform interoperability. *IEEE software*, *34*(1), 54-61.

[61] Ahn, J. Y., Lee, J. S., Kim, H. J., & Hwang, D. J. (2016, July). Smart city interoperability framework based on city infrastructure model and service prioritization. In *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)* (pp. 337-342). IEEE.

[62] Lodato, T., French, E., & Clark, J. (2021). Open government data in the smart city: Interoperability, urban knowledge, and linking legacy systems. *Journal of Urban Affairs*, *43*(4), 586-600.

[63] Zabasta, A., Kunicina, N., Kondratjevs, K., Patlins, A., Ribickis, L., & Delsing, J. (2018, July). MQTT service broker for enabling the interoperability of smart city systems. In *2018 Energy and Sustainability for Small Developing Economies (ES2DE)* (pp. 1-6). IEEE.

[64] Yang, S., & Wei, R. (2020). Semantic Interoperability Through a Novel Cross-Context Tabular Document Representation Approach for Smart Cities. *IEEE Access*, *8*, 70676-70692.

[65] Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Communications Magazine*, *55*(9), 16-24.

[66] Avelar, E., Marques, L., dos Passos, D., Macedo, R., Dias, K., & Nogueira, M. (2015). Interoperability issues on heterogeneous wireless communication for smart cities. *Computer Communications*, *58*, 4-15.

[67] Buhalis, D., & Leung, R. (2018). Smart hospitality—Interconnectivity and interoperability towards an ecosystem. *International Journal of Hospitality Management*, *71*, 41-50.

[68] Nilsson, J., & Sandin, F. (2018, July). Semantic interoperability in industry 4.0: Survey of recent developments and outlook. In *2018 IEEE 16th international conference on industrial informatics (INDIN)* (pp. 127-132). IEEE.

[69] Uviase, O., & Kotonya, G. (2018). IoT architectural framework: connection and integration framework for IoT systems. *arXiv preprint arXiv:1803.04780*.

[70] Sharma, A., Acharya, S., Rajaraman, V., Ramesh, R., Babu, A., & Amrutur, B. (2017, November). Schemas for IoT interoperability for smart cities. In *Proceedings of the 4th ACM international conference on systems for energy-efficient built environments* (pp. 1-2).

[71] Villanueva-Rosales, N., Garnica-Chavira, L., Larios, V. M., Gómez, L., & Aceves, E. (2016, September). Semantic-enhanced living labs for better interoperability of smart cities solutions. In *2016 IEEE International Smart Cities Conference (ISC2)* (pp. 1-2). IEEE.

[72] Jabbar, S., Ullah, F., Khalid, S., Khan, M., & Han, K. (2017). Semantic interoperability in heterogeneous IoT infrastructure for healthcare. *Wireless Communications and Mobile Computing*, *2017*.

[73] Paul Murdock, Louay Bassbouss, Martin Bauer, Mahdi Ben Alaya, Rajdeep Bhowmik, et al.. Semantic interoperability for the Web of Things. PhD Thesis. Dépt. Réseaux et Service Multimédia Mobiles *(Institut Mines-Télécom-Télécom SudParis)*, 2016, pp.18. ⟨hal-01362033⟩.

[74] Jiménez, C. E., Falcone, F., Solanas, A., Puyosa, H., Zoughbi, S., & González, F. (2016). Smart government: Opportunities and challenges in smart cities development. *Civil and Environmental Engineering: Concepts, Methodologies, Tools, and Applications*, 1454-1472, P19, IGI-Global, Spain. DOI: 10.4018/978-1-4666-9619-8.ch066

****

Chapter 5 - Health and Issue in Crowd

This chapter discusses the challenge of crowd health and its associated issues. The chapter includes one research paper published in a IJIT, in addition to a draft for journal paper. The first paper presented a designed framework with protposed algorithm to ensure crowd health and safety in case of overcrowding. And, the second paper (draft under review) proposed an idea to enhance crowdsourcing by motivating crowds to contribute effectively to solutions by providing useful data. This was achieved by ensuring the privacy and data security of crowdsourced information through a dedicated approach.

Designing a Comprehensive Framework for Health Management in Crowded Events

Bahbouh, N. M., Sendra, S., & Sen, A. A. A. (2024). Designing a comprehensive framework for health management in crowded events. International Journal of Information Technology, 1-11.

Abstract

Many countries witness the organization of various events, whether sports, religious, artistic, cultural, or even political. These events gather large crowds in specific locations. A minor incident within these crowds can escalate into a disaster if not dealt with immediately and effectively. Therefore, crowd management and ensuring its safety present significant challenges to date. Preserving the safety and health of participants within crowds is one of the most sensitive issues, which becomes even more complex during pandemics. Unfortunately, there are still no effective solutions to guarantee the safety and health of crowds. The world has witnessed disasters in recent years that have led to the deaths of thousands in crowds. This research presents a classification of all challenges facing crowds. Then, it proposes a comprehensive framework to address them and enhance the health and safety of participants. The framework relies on integrating various solutions and technologies in the form of stages, tasks, and services. The research also proposes a crowd-monitoring algorithm and smart scheduling for the sanitization process, in addition to early warning and emergency procedures in case of any threat. The algorithm is based on image processing and text analysis. The algorithm has been tested on a dataset for a set of crowd images and others for tweets about various incidents, achieving an accuracy exceeding 98%. The framework will enhance the level of safety and health in crowds and pave the way for many future supporting services which can be provided via a general application for smartphones.

Keywords: Crowd, M-Healt), Internet of Things (IoT), Covid-19, Machine Learning (ML), Image Processing, Fog.

Introduction

Technology and modern communication methods, along with social media, have greatly impacted our lives in all domains. One of the most prominent effects is the proliferation of various events such as entertainment activities, celebrity gatherings, sports games, and political protests due to the ease of inviting people to gather and the rapid dissemination of news to a large number of individuals [1]. Added to these events are religious gatherings, which are considered the largest type of gatherings and crowds. Countries like India, Iraq, the Vatican, and Saudi Arabia, for example, witness massive religious events annually (See Figure 1). Saudi Arabia, in particular, is known for hosting numerous large-scale events, including sports, and entertainment festivals, as well as the largest annual gathering for performing the rituals of Hajj and Umrah [1, 2].

Fig 1. Examples of Real Crowd in Saudi Arabia (A), Iraq (B), England (C), and India (D)

Millions of people gather in a specific area to perform the Hajj, for example, as hundreds of thousands gather during the Riyadh entertainment seasons. The Kingdom aims in its Vision 2030 to increase the number of tourists to more than 30 million annually. These goals require supporting the capabilities of relevant authorities in organizing events through more effective and intelligent tools. In some previous years, such as in 2015, unexpected events occurred, leading to catastrophic results and the deaths of hundreds of participants [3]. Therefore, the increase in crowd numbers will pose a greater challenge to organizing authorities, whether increasing the likelihood of stampedes, the spread of diseases and infections, or other challenges that require integration between solutions and modern technologies [4].

Managing these crowds and ensuring their safety and health is a real challenge for everyone and a complex issue, especially when the crowds come from different cultures, ages, and nationalities. During crowds, small events or accidents can escalate into major tragedies [5]. In [6], they presented a report and compilation of all the tragic events that occurred during the past years, along with the number of casualties in each. The previous report highlights the need for an effective crowd management system. Furthermore, crowds are a source of transmission for infections and viruses, especially with limited oxygen in confined spaces, and after the 2019 coronavirus pandemic, which resulted in millions of deaths, there has been a significant increase in public health awareness.

As a result, health has been added as an additional challenge to crowds, in addition to the general safety challenges related to organizing the flow and movement of crowds and preventing stampedes. In events like the 2020 incidents in Canberra and Karbala, thousands of people died from infection due to a lack of necessary attention to health precautions [7]. Healthcare systems have suffered severe weaknesses in dealing with pandemics in general, and situations have spiraled out of control during crowds where millions of people gather in one place [8]. The impact is significantly greater on older age groups or those with chronic diseases [9]. Therefore, even advancements in the healthcare sector, including electronic health records, mobile health, and smart health, were not sufficient to meet the challenges posed by the aforementioned situations [10].

Limiting the size of crowds is not primarily an effective economic solution, and not all types of events can have their participants regulated. It is more practical to focus on crowd management starting from the planning phase of the event, by providing necessary infrastructure, civil defense teams, and regulatory measures [5, 11]. Although crowd management involves various subsystems such as transportation, accommodation, food, and others, this research primarily focuses on ensuring safety and health within crowds. This requires implementing a monitoring mechanism to proactively detect and address any threats. Therefore, contributions to this research...

1- Classifying the challenges faced by crowds and designing a framework for crowd management and addressing these challenges.
2- Proposing a lightweight algorithm for crowd monitoring based on ML and TM, along with constructing intelligent scheduling for the sanitization process, incorporating the idea of dividing into sectors and sectors into cells.
3- Suggesting an intelligent alert mechanism and a set of supporting services and technologies to support the safety and health of crowds.
4- Testing the proposed algorithm to confirm the effectiveness of the framework and identifying future challenges and points of improvement.

The following sections will discuss the aforementioned solutions and their weaknesses in facing the challenges, along with categorizing these challenges. Then, in the third section, a detailed explanation of the proposed framework and algorithm will be provided, along with supporting services and technologies. The fourth section will discuss the results of testing the proposed algorithm, along with addressing some future points. Finally, the conclusion will be presented.

Related Works

All current solutions have relied on leveraging technology such as the Internet of Things, computing, data science, and artificial intelligence to provide intelligent solutions as much as possible and to avoid health problems or challenges specific to crowds. The following is a classification of these research works into four main research areas related to crowds:

A. Relying on the IoT and mobile phones to provide necessary data

Many researches employ wearable Internet of Things devices for monitoring vital signs, enhancing digital healthcare, and providing alert and monitoring tools [4, 12]. The researchers in [12] relied on expert opinions in the healthcare field to build a context-based educational model from data coming from the Internet of Things. It emphasized the importance of promoting health awareness and health literacy.

While the researchers in [4] Presented a system for crowd monitoring based on wearable Internet of Things devices, continuously reading skin temperature, humidity, and heart rate, which are then analyzed. The system is linked to a user's mobile application to send urgent alerts when necessary. Additionally, data copies are sent to a central management system for broader case detection.

Other researches proposed the idea of turning citizens themselves into useful tools in monitoring by using wearable sensors to contribute important data to analysis systems [13]. In the [14], they leveraged the increasing capabilities of mobile phones as sensors within crowds, where these devices can collect data on a wide scale and at a low cost. This data can help track the spread of diseases and overcome barriers to accessing healthcare. However, there is a privacy challenge.

B. Relying on data science for automated crowd monitoring and preemptive threat prediction

The researchers in [15] classified crowds into congested, heavily congested, light, and natural categories using an automatic classification algorithm, then predicted the number of individuals to take appropriate preventive measures. While in the [3], the utilized deep learning CNN to detect the number of participants in the crowd, with a case study applied to Hajj where over 5000 cameras are used to monitor the crowds. Images from surveillance cameras are analyzed, and alerts are sent if the numbers exceed a certain threshold.

In the [2], they presented an algorithm to calculate the number of crowds based on the number of heads, employing various technologies to ensure crowd safety, along with suggesting a comprehensive application for services that can be beneficial to participants in large events such as Hajj. While in the [16], they monitored small crowds at various points of interest such as shopping centers through text data analysis. The research relied on user recommendations and opinions, as well as their preferences. Based on a classification algorithm, the system suggests to users the safest and nearest locations.

C. Precautionary and health measures

In the [11], they discussed the health aspect in the crowd planning stage by implementing precautionary measures and recommendations for participants to use face masks, maintain distance, and practice continuous sanitization. The research presented a framework for event reservation organization during health crises and built an automatic acceptance and rejection algorithm based on previous experiments. While in the [17] they emphasized the importance of precautionary measures such as wearing masks, and pointed out that reducing shouting and talking at events and festivals can reduce the risk of viral infection transmission among attendees.

Other researches introduced a predictive model to calculate the risk of infection in healthcare facilities during pandemics, especially in cases of contact with infected or exposed individuals [8]. The classification algorithm relies on the duration of contact, crowd density level, and average number of contacts with infected individuals, and type of protection used. The research recommended increasing clean and safe spaces to maintain social distancing. It also presented several scenarios regarding the possibility of disease spreading even in small crowds, such as gatherings in public transportation, schools, and sports team audiences.

Others presented an algorithm to monitor safe distancing between individuals unless they belong to the same family. Families are identified by staying close to each other for a duration exceeding a certain threshold [18]. They also provided a case study on processing pedestrian data at train stations in real time and generating a graphical representation. Immediate alerts can be sent when a specific distancing threshold is breached.

D. Important technologies and tools for crowd management and dealing with abnormal or emergency situations

The researchers provided a classification of several useful technologies in crowd organization [2, 19]. The most important of these technologies include:

- Internet of Things for real-time data collection from every location within the crowd and from the participants themselves.
- Wireless technologies to provide continuous fast communications.
- Computer vision for automated image processing.
- Fog, edge, and cloud computing to solve performance issues.
- Analytical tools to provide performance indicators for decision-makers.
- Mobile applications to provide remote services and constant communication with participants.
- Modeling, simulation, and virtual reality (VR) for training-specific scenarios for both participants and civil defense teams. In the [20], they proposed using the simulation for traffic movement and crowd flow by utilizing platforms such as Deepint.net to estimate and simulate pedestrian movement and congestion times. While in the [21] utilized virtual reality to simulate stampede incidents and applied them to various events. The experiments highlighted the necessity of emergency exits as an important measure to address stampede issues and distribute loads.
- Augmented reality (AR) and mixed-reality to guide crowds and enhance their knowledge about locations, points of interest, or evacuation routes. In the [22] they emphasized the importance of Meta-verse technologies in managing and monitoring crowds, and presented various scenarios for analyzing individual data during crowds to understand their behavior

In summary, the main reason for crowd disasters is the lack of sufficient event planning and the absence of prompt response to incidents primarily. Moreover, the lack of attention to the health aspect has a significant impact, especially during pandemics. Previous research has focused on specific problems and provided scattered, non-comprehensive solutions to the problem of safety and health in crowds. These solutions also suffer from problems related to cost, paying attention to the individual instead of crowding, determining the level of crowding or the number of participants, in addition to employing some modern technologies or mobile phone services. Table 1 presents a summary of previous works with the main contributions and weaknesses of each.

Table1. Previous contributions in the crowd management

Ref	Main Contributions	Disadvantages
[4][12][13]	Relying on wearable sensors for early detection of health conditions	Cost, focusing on the individual level rather than the crowd, failure to solve the problem of transmission of infection, failure to provide support services.
[14]	Using mobile phones to collect data and provide remote health consultations	No solutions were provided for safety, the problem of infection was not solved, and the possibility of delayed response in the case of large crowds
[15]	Classifying crowds according to the degree of crowding and predicting the number of people	Lack of focus on the health issue
[2][3]	Analyzing camera images to detect the numbers of participants using machine learning and deep learning	High computational cost, lack of focus on the health issue
[16]	Analyze text data and user connections to reduce congestion at points of interest	It did not care about the crowd, it did not address the health issue
[11] [17]	Establish precautionary measures and recommendations with a reservation system for events that witness crowds to control numbers, places, and times.	It didn't care about the crowd while the event was happening
[8]	Presenting a model to predict the degree of risk of infection through contact with infected people	Not applicable in large crowds
[18]	Monitoring the safe social distance between individuals and alerting when they are violated	Not applicable in large crowds, insufficient to address health and safety issues
[2][19]	Proposing the use of modern technologies to activate communications, computing, and gathering information within crowds	Helpful tools, but insufficient without their use within a unified framework and activated algorithms
[20][21]	Using simulation, virtual and augmented reality to train crowds	Inadequate, did not care about the health aspect

This research will focus on the aforementioned matters due to their connection to crowd safety, but at the same time, it will also focus on ensuring and enhancing crowd health through the proposed framework. The research has focused on the health triad, which includes prevention through planning and compliance, a list of recommendations, care through continuous monitoring and early detection with immediate response, and finally, promotion through adaptation to face challenges or emergencies and deploying various technologies. Additionally, a list of recommendations that must be achieved will be provided.

The Proposed Framework and Solutions

Successful health management during gatherings necessitates specialized protocols tailored for large crowds. This involves prioritizing prevention, followed by continuous monitoring for early threat detection and timely alerting. Additionally, activating effective communication mechanisms with medical units, civil defense, volunteers, or even the participants themselves is crucial to providing immediate response during emergencies. To achieve this, the research suggests a comprehensive framework consisting of five main layers. Each layer utilizes a set of modern technologies and tools to accomplish various tasks.

3.1 The Framework

Figure 2. illustrates the proposed framework along with its corresponding layers:

- Perception layer: Responsible for providing data through the Internet of Things such as radio frequency identification (RFID) tags or network sensors, in addition to the crowd through their smart devices, as well as data on crowd services.
- Fog layer: Divides crowd areas into sectors to facilitate data collection and real-time processing, detecting any anomalous data that may pose a threat later and responding to emergencies without delay. The fog nodes provide wireless communication with users and their devices through various communication protocols such as Bluetooth, ZigBee, LORA, Wi-Fi, etc.
- Master Fog Layer: An additional computational layer, where each master node is responsible for a cluster of fog nodes, and the layer is also responsible for mobile health services, whether drones or mobile health centers.
- Cloud layer: The central computing layer where all summarized data coming from the fog node as historical data is aggregated. Data science algorithms are applied here to discover additional knowledge, understand behavior, and improve future solutions.
- Application layer: The layer responsible for providing various health services that must be provided for crowd management such as alerts, guidance, consultations, requests for assistance, volunteer encouragement, reporting, searching for missing things, searching for points of interest, etc.

3.2 Main Tasks of the Framework

The proposed framework for crowd management focuses on key tasks which are grouped in A, B, and C:

A. Planning, Registration, and Infrastructure

- Preferably provide an electronic registration service for participants, through which verification of the availability of necessary vaccines and their immunity from infectious diseases is conducted. The registration process also helps determine the approximate size of the crowd and thus prepares for it appropriately by the responsible organizing management and support teams.
- Distribution of a special wristband (RFID Tag), which is low-cost, less than $1, but can greatly facilitate the process of tracking individuals and organizing crowds.
- Prepare the infrastructure and verify its capacity to accommodate the crowd size, in addition to providing continuous wireless communication with the crowd in all areas. Also, ensure full coverage of all areas with surveillance cameras, noting that drones can be relied upon in hard-to-reach areas.
- Upload a dedicated application by the crowd, which provides them with a continuous communication with the organizing management, volunteers, support teams, and medical services, in addition to providing many health services and useful accompanying services for the crowds (such as awareness, alerts, electronic consultations, reporting, recommendations in case of flow and guidance, volunteer registration, first aid guidance, etc.).
- Prepare sanitizing devices (spraying) and activate them in case of disease outbreaks or during pandemic periods to operate on a scheduled.

- Equip the streets with digital boards used as directional signs and guidance tools in emergencies through automated content control.

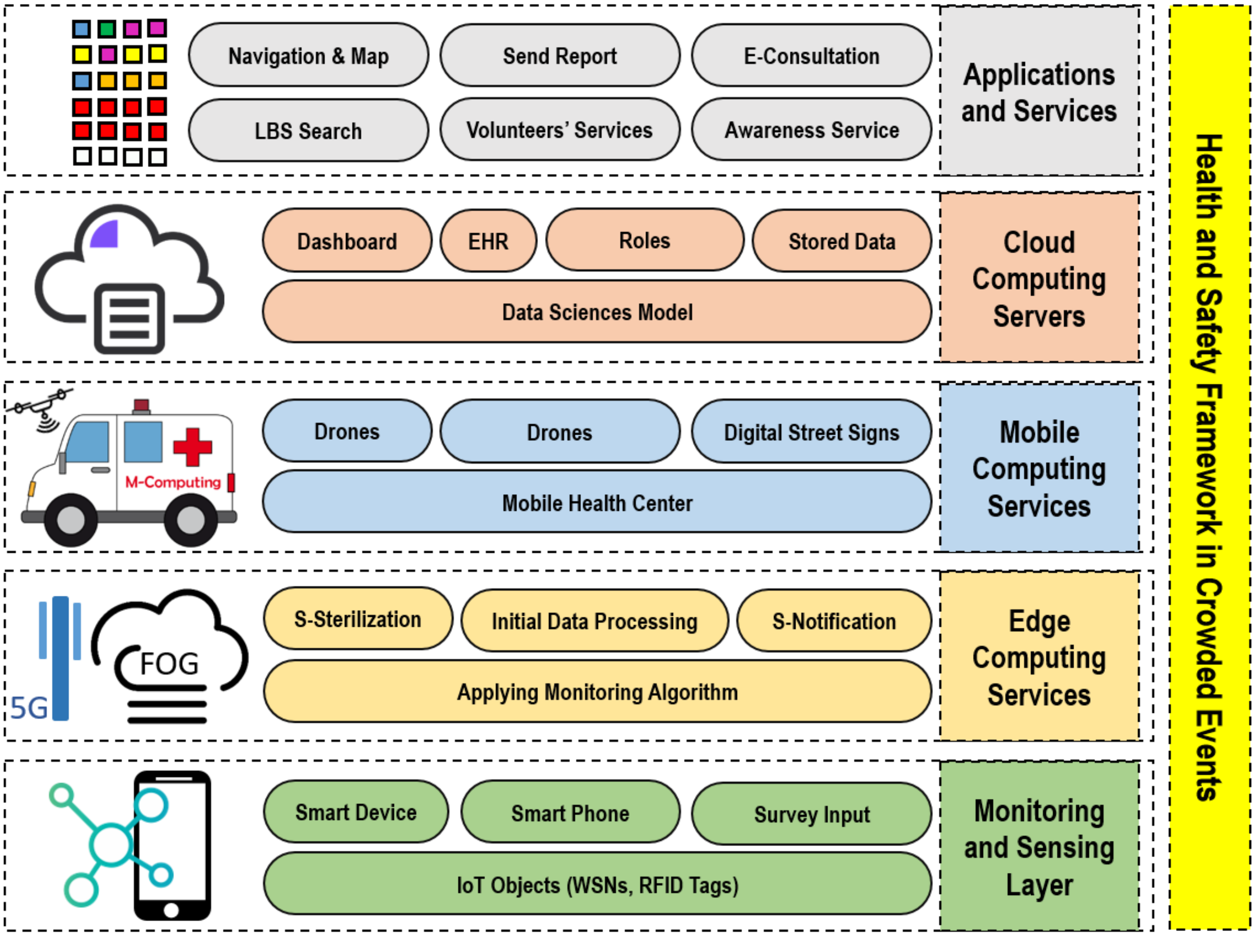


Fig 2. The Proposed Framework

B. Continuous Monitoring and Proposed Algorithm

- Proposing smart gates by dividing the area into sectors for distributing the load and controlling the number of users in each sector to prevent congestion that may lead to catastrophic stampedes or violations of distancing measures. The existing numbers in each sector will be precisely regulated through wristbands and gates without the need for machine learning algorithms or deep learning to calculate the numbers, which require high computational power.
- Proposing a lightweight algorithm (Algorithm1) for continuous and effective monitoring within each sector to monitor unauthorized gatherings, and compliance levels, and detect any threats within the sector. Figure 3 illustrates the mechanism of the proposed algorithm.

Note 1: The wristband can be enhanced by embedding some sensors for vital data. By monitoring this data, early detection of abnormal health conditions for each individual and tracking the overall health status of areas can be achieved. However, this step would increase costs, so it has been replaced by sending daily health inquiries through the proposed communication application to monitor the health status of each individual.

Note 2: An algorithm for detecting mask-wearing compliance has not been implemented because it would impact performance and require extensive camera deployment to capture faces, which would hinder movement among the crowds. Additionally, continuous facial imaging is considered a privacy violation in many cultures.

C. Alert and Emergency Management:

- Crowds are alerted via the smartphone application in case of any potential threats, with instructions sent accordingly.
- Smart gate control for the sectors surrounding the activated sector during emergencies to reduce congestion.
- Control over the sanitation schedule within the specified sector and adjustment of the timing based on the level and type of threat.
- Crowd flow control within the specified sector using the concept of digital streets and digital directional signs, along with activating additional exits.
- Dispatching alerts to support teams and volunteers in case of emergency medical situations and sending alerts to the nearest health center for the sector.
- Activating drones to deliver necessary supplies quickly upon request to a specific cell within the sector.

3.3 The Proposed Algorithm (Algorithm 1)

The proposed algorithm relies on two stages. The first stage processes the crowd images within the sector only to detect the level of compliance with social distancing. In case of suspicion of a threat above a certain threshold, the second stage is activated, which relies on processing the data generated by the crowd itself or volunteers within the sector. If the threat is confirmed and its type is identified in the second stage, immediate alerts will be sent, and crowd flow management tasks will be activated during emergencies.

Image processing relies on a simple idea in the fog node, where the fog node divides the sector's image into an equal number of small cells. First, the image is converted from RGB to HSV (Hue Saturation Value is used to separate image luminance from color information), then correlation matching is performed between each cell (Image1) and its counterpart in the image of the same area before the crowd gathers (Image2). Based on the difference ratios, the area is colored red, yellow, or green to indicate the level of congestion. If the number of red or yellow cells exceeds a certain threshold, the second stage is activated. The first stage also contributes to measuring the speed and direction of crowd movement, which are crucial pieces of information for crowd management. It also has thresholds that must not be exceeded; otherwise, it will be considered as an indicator of a potential threat.

Hint: To address the issue of potentially dividing the crowd into two cells, we have two options. Firstly, we can repeat all previous steps after changing the starting position of the division to (cell’s width/2, cell’s height/2). Alternatively, we can merge each pair of adjacent yellow cells and re-match them.

The second stage begins by focusing on the textual data coming from the crowd within the specified sector, whether through reports coming from an application on participants' phones or volunteers. (Note: Tweets issued by the crowds themselves can be processed, but they will be at the crowd level, not at the sector level). Generally, the textual data for each report or tweet is processed through the following steps:

- Data cleaning process to remove special characters and language detection, then the data is tokenized into a list of words.
- Removal of non-significant stop words based on a language-specific list.
- Applying of stemming to remove additions and unify words with different formulations.
- Calculation of word frequencies and then calculation of word weights based on the Inverse Document Frequency (IDF) function.
- Removal of less important words below a threshold, and matching important words with a list of words for each threat (lists of words are prepared for each threat to be monitored, such as a list for stampedes, a list for health issues like hard breathing or fainting, etc.).
- Based on the matching, tweets indicating a specific threat are classified, and if the number of classified tweets as a threat exceeds a certain threshold, the emergency status for the specified area will be activated.

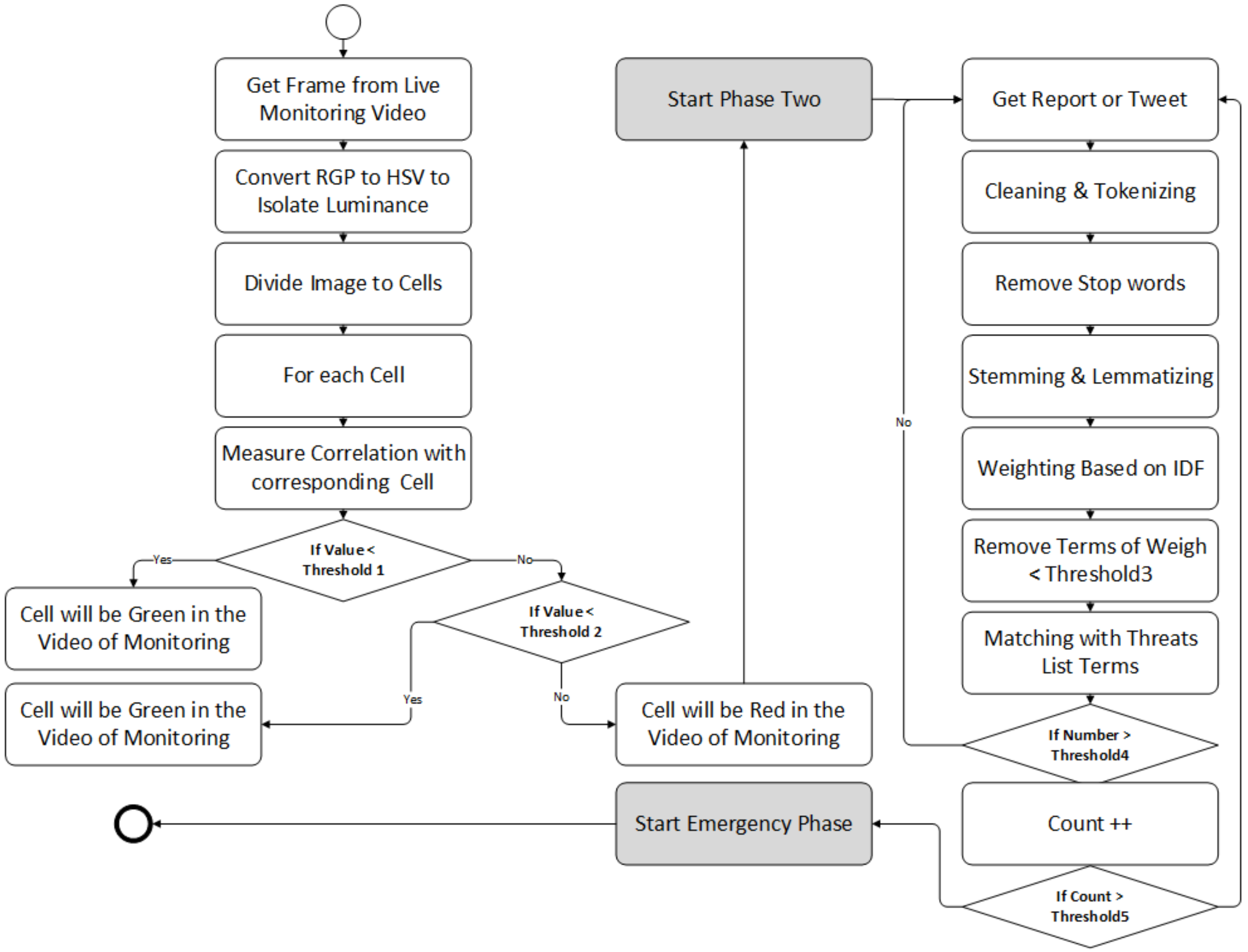

Get Frame from Live Monitoring Video
Convert RGP to HSV to Isolate Luminance
Divide Image to Cells
For each Cell
Measure Correlation with corresponding Cell
If Value < Threshold 1
Yes
No
Cell will be Green in the Video of Monitoring
If Value < Threshold 2
Yes
No
Cell will be Green in the Video of Monitoring
Cell will be Red in the Video of Monitoring
Start Phase Two
Get Report or Tweet
Cleaning & Tokenizing
Remove Stop words
Stemming & Lemmatizing
Weighting Based on IDF
Remove Terms of Weigh < Threshold3
Matching with Threats List Terms
If Number > Threshold4
No
Count ++
If Count > Threshold5
Start Emergency Phase

Fig 3. The Proposed Algorithm's Steps

Figure 3 shows the proposed algorithm and its basic steps. The algorithm starts from the moment a frame is captured from the surveillance video of the crowd area, then it is converted to the HSV color system to avoid the effect of lighting, then the stage of dividing the image into parts (cells). So that, each part is matched with its corresponding image of the same place without the crowd (the matching stage). Based on the degree of correlation, the level of crowding in the cell is determined and a color map is changed. If the crowd level is large (red color), the processing phase for upcoming crowd reports within this area begins. It goes through the stages of word processing (cleaning, removing stop words, stemming the words to their roots, and then weighing importance). Finally, match the important terms in the polarity lists of the issue to be traced. If the percentage of reports classified as a threat exceeds a certain limit, a state of emergency is activated to solve the overcrowding or health problem within the area as quickly as possible.

3.4 Novelty of the Proposed Solution

The main feature of this research is comprehensiveness, meaning the research addressed the issue of maintaining the safety and health of crowds at all stages (the preparation stage and precautionary measures, continuous monitoring and early detection of the threat, dealing with the threat and emergencies). The research presented the proposed solutions under the umbrella of a unified framework that supports the employment of many modern technologies together to achieve effectiveness, such as the Internet of Things, fog and cloud computing, drones, and machine learning algorithms. More than that, the research presented the idea of digital gates to control the size of crowd and then divided the processing at the district level to increase the level of accuracy and solve the performance problem. It also presented a lightweight algorithm that enables easy, real-time monitoring of the crowd within the cell and determining the type of emergency event if it occurs. Finally, the research proposed a set of services for crowds and paved the way for service providers to provide their services in a unified framework that makes it easier for users to access them, deal with them, and test what is best for them according to the context.

Results, Recommendations, and Future Scope

In this section, we present the results of testing the proposed algorithm on some images from the (Dense Tracking Dataset [23]) of crowds in various events. The images represent frames from three videos captured of crowd movement in real events (each video represents a sector) to monitor the change in cell status within the sector. Additionally, a test set of 1000 tweets [24] classified as expressing threats or being natural was worked on. Google Colab platform was used with Python language for the proposed algorithm. Precision and Recall were relied upon to evaluate the algorithm.

For image processing, the accuracy was close to 99%, relying on a simple principle in the matching process. As for text processing, Confusion Matrix was utilized. The accuracy was over 98%, considering that accuracy is related to the comprehensiveness level of threat word lists. The following Figure 4 presents an example of applying the image processing step within the algorithm, while Figure 5 illustrates the scatter matrix of the text data processing step test. It shows the number of true negative (TN) cases that refers to the number of negative cases which are classified correctly as negative. Others values are the true positive (TP) cases, in addition to the false negative (FN) and the false positive (FP) ones. Furthermore, the research concluded through previous studies a set of important recommendations necessary to ensure effective crowd management, in addition to some challenges that need to be addressed in future work.

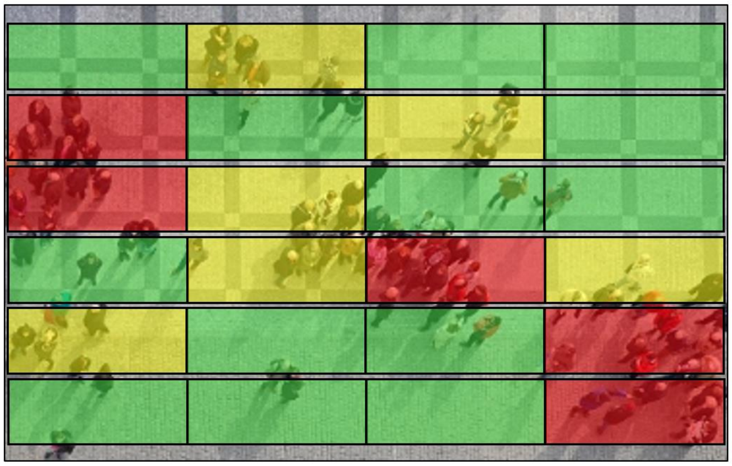


Fig 4. Example of Applying Algorithm 1 – Image Processing Phase

	Predicted	
Actual	TN	FP
	FN	TP

	Predicted	
Actual	490	10
	2	498

Accuracy	Precision	Recall	F1 Score
0.99	1.00	0.98	0.99

Fig 5. Results of Testing Algorithm 1 – Text Processing Phase

4.1 Recommendations Related to Crowd Safety and Health:

- Ensure the infrastructure of gathering places and provide easily accessible public facilities in crowded areas.
- Focus on awareness for crowds before and during gatherings.
- Implement continuous sanitization mechanisms during pandemics to reduce the risk of infection, especially in gatherings.
- Place fire extinguishers, oxygen tanks, and vents in easily accessible locations within crowds.
- Ensure uninterrupted service during gatherings and provide wireless communication means without the need for the internet [25].
- Activate cooperation between civil defense teams and participants themselves in large crowds.
- Activate services for volunteers and train them in rescue and first aid operations.
- Develop simulation scenarios for emergencies and test them.
- Provide medical teams in each sector or health centers at the central point for each group of sectors.
- Re-engineer hospitals and their infrastructure.
- Provide remote healthcare services such as electronic consultations.
- Conduct daily health surveys.
- Implement robotic services within healthcare centers to reduce contact with medical teams and the transmission of infections in case of epidemics.
- Deploy small mobile clinics to alleviate crowding in healthcare centers and provide healthcare services everywhere.
- Activate drone applications for monitoring and delivering supplies.
- Pay attention to maintaining privacy and data security within crowds [26-29].
- Establish a unified platform for crowd services to support interoperability, enhance service quality, and facilitate access, in addition to supporting automated service selection based on context and user preferences [30].
- Pay attention to people with special needs, the elderly, children, and those with chronic illnesses by providing special services for them [31].

4.2 Future Scope

There are a group of challenges that must be worked on in future trend related to crowds, the most important of which is:

- Solving the problem of privacy and security of user data within crowds
- Providing VR and AR services to train crowds at recurring events to adhere to safety and health instructions
- Building a Super Application for crowd services to facilitate access by users and improve their quality
- Building a unified ontology for crowds to support interoperability between different service providers and products
- Providing services to support people with special needs and chronic disease within crowds [32, 33]

Conclusion

The research discussed the challenge of maintaining safety and health within crowds. It proposed a framework with a series of stages and tasks starting from crowd planning, then continuous monitoring, and emergency procedures in case of threat detection, in addition to a range of supporting services through a smartphone application. The research proposed a lightweight algorithm for early threat detection through image and text processing. Finally, the research presented a set of important recommendations and challenges that need to be addressed in the future works.

References

[1]. Khan, K., Albattah, W., Khan, R. U., Qamar, A. M., & Nayab, D. (2020). Advances and trends in real time visual crowd analysis. Sensors, 20(18), 5073.

[2]. Yamin, M., Basahel, A. M., & Abi Sen, A. A. (2018). Managing crowds with wireless and mobile technologies. Wireless Communications and Mobile Computing, 2018.

[3]. Habib, S., Hussain, A., Islam, M., Khan, S., & Albattah, W. (2021, April). Towards efficient detection and crowd management for law enforcing agencies. In 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA) (pp. 62-68). IEEE.

[4]. Rojas, J. P., Rehman, M. U., Hussein, A., E'mar, A., AlRaei, Y., AlZaher, H., & Mohandes, M. (2022). Kirigami-enabled wearable health and crowd monitoring system. Arabian Journal for Science and Engineering, 47(3), 3583-3595.

[5]. Al-Qurashi, M. A. M., Al-Qahtani, A. A., Abdulaziz, S. I., & Habra, R. S. A. (2023). The Quality of Crowd Management and Its Impact on the Experience of Event Visitors in Riyadh Season. Academic Journal of Research and Scientific Publishing| Vol, 5(52).

[6]. Sharma, A., McCloskey, B., Hui, D. S., Rambia, A., Zumla, A., Traore, T., ... & Rodrigues-Morales, A. J. (2023). Global mass gathering events and deaths due to crowd surge, stampedes, crush and physical injuries-lessons from the Seoul Halloween and other disasters. Travel medicine and infectious disease, 52.

[7]. Luo, Y., & Ibrahim, R. (2022, March). Securing Crowd Management Over Patients' Behavior in Chinese Public Hospitals. In Proceedings of the 2nd International Conference on Design Industries & Creative Culture, DESIGN DECODED 2021, 24-25 August 2021, Kedah, Malaysia.

[8]. Dy, L. F., & Rabajante, J. F. (2020). A COVID-19 infection risk model for frontline health care workers. Network Modeling Analysis in Health Informatics and Bioinformatics, 9(1), 57.

[9]. Bahbouh, N. M., Abi Sen, A. A., Alsehaimi, A. A. A., & Alsuhaymi, E. A. (2022, March). A framework for supporting ambient assisted living for users of special needs. In 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 427-432). IEEE.

[10]. Bahbouh, N. M., Compte, S. S., Valdes, J. V., & Sen, A. A. A. (2023). An empirical investigation into the altering health perspectives in the internet of health things. International Journal of Information Technology, 15(1), 67-77.

[11]. Almutairi, M. M., Yamin, M., Halikias, G., & Abi Sen, A. A. (2021). A framework for crowd management during COVID-19 with artificial intelligence. Sustainability, 14(1), 303.

[12]. Nittayathammakul, V., Chatwattana, P., & Piriyasurawong, P. (2022). Crowd Context-Based Learning Process via IoT Wearable Technology to Promote Digital Health Literacy. International Education Studies, 15(6), 27-38.

[13]. Pigliautile, I., & Caratù, M. (2022, May). Application of Crowd Sensing for Sustainable Management of Smart Cities. In INTERNATIONAL SYMPOSIUM: New Metropolitan Perspectives (pp. 2800-2808). Cham: Springer International Publishing.

[14]. Zhang, E., Trujillo, R., Templeton, J. M., & Poellabauer, C. (2023). A Study on Mobile Crowd Sensing Systems for Healthcare Scenarios. IEEE Access.

[15]. Albattah, W., Khel, M. H. K., Habib, S., Islam, M., Khan, S., & Abdul Kadir, K. (2020). Hajj crowd management using CNN-based approach.

[16]. Durán-Polanco, L., & Siller, M. (2021). Crowd management COVID-19. Annual reviews in control, 52, 465-478.

[17]. Smith, J. A., Hopkins, S., Turner, C., Dack, K., Trelfa, A., Peh, J., & Monks, P. S. (2022). Public health impact of mass sporting and cultural events in a rising COVID-19 prevalence in England. Epidemiology & Infection, 150, e42.

[18]. Pouw, C. A., Toschi, F., van Schadewijk, F., & Corbetta, A. (2020). Monitoring physical distancing for crowd management: Real-time trajectory and group analysis. PloS one, 15(10), e0240963.

[19]. Felemban, E. A., Rehman, F. U., Biabani, S. A. A., Ahmad, A., Naseer, A., Majid, A. R. M. A., ... & Zanjir, F. (2020). Digital revolution for Hajj crowd management: a technology survey. IEEE Access, 8, 208583-208609.

[20]. Garcia-Retuerta, D., Chamoso, P., Hernández, G., Guzmán, A. S. R., Yigitcanlar, T., & Corchado, J. M. (2021). An efficient management platform for developing smart cities: Solution for real-time and future crowd detection. Electronics, 10(7), 765.

[21]. Zhao, H., Thrash, T., Kapadia, M., Wolff, K., Hölscher, C., Helbing, D., & Schinazi, V. R. (2020). Assessing crowd management strategies for the 2010 Love Parade disaster using computer simulations and virtual reality. Journal of the Royal Society Interface, 17(167), 20200116.

[22]. Koshnicharova, D., Mihovska, A., Koleva, P., & Poulkov, V. (2022, October). Data-driven interactive crowd management systems for Metaverse scenarios. In 2022 25th International Symposium on Wireless Personal Multimedia Communications (WPMC) (pp. 549-554). IEEE.

[23]. Nemade, N. A., & Gohokar, V. V. (2016, December). A survey of video datasets for crowd density estimation. In 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC) (pp. 389-395). IEEE.

[24]. Hamoui, B., Mars, M., & Almotairi, K. (2020, May). FloDusTA: Saudi tweets dataset for flood, dust storm, and traffic accident events. In Proceedings of the Twelfth Language Resources and Evaluation Conference (pp. 1391-1396).

[25]. Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. International Journal of Information Technology, 13, 829-837.

[26]. Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. International Journal of Information Technology, 10, 189-200.

[27]. Bahbouh, N., Basahel, A., Sendra, S., & Abi Sen, A. A. (2022). Tokens shuffling approach for privacy, security, and reliability in IoHT under a pandemic. Applied Sciences, 13(1), 114.

[28]. Abi Sen, A. A. (2022). A comprehensive privacy and security framework for dynamic protection (CPSF). International Journal of Information Technology, 14(5), 2477-2485.

[29]. Yamin, M., & Abi Sen, A. A. (2020). A new method with swapping of peers and fogs to protect user privacy in IoT applications. IEEE Access, 8, 210206-210224.

[30]. Albouq, S. S., Abi Sen, A. A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. M. (2022). A survey of interoperability challenges and solutions for dealing with them in IoT environment. IEEE Access, 10, 36416-36428.

[31]. Namoun, A., Tufail, A., Nawas, W., BenRhouma, O., & Alshanqiti, A. (2023). A Systematic Literature Review on Service Composition for People with Disabilities: Taxonomies, Solutions, and Open Research Challenges. Computational Intelligence and Neuroscience, 2023.

[32]. El-Magd, L. M. A., Dahy, G., Farrag, T. A., Darwish, A., & Hassnien, A. E. (2024). An interpretable deep learning based approach for chronic obstructive pulmonary disease using explainable artificial intelligence. International Journal of Information Technology, 1-16.

[33]. Yamin, M. (2020). Counting the cost of COVID-19. International journal of information technology, 12(2), 311-317.

Double Cloak Area Approach for Preserving privacy and Reliability of Crowdsourcing Data

Bahbouh, N. M., Alkhodre, A. B., Sendra, S., Abi Sen, A. A., Alsaawy, Y., Benaida, M., & Almoamari, H. (2024). Double Cloak Area Approach for Preserving privacy and Reliability of Crowdsourcing Data. IEEE Access.

Abstract

Crowdsourcing has become an important data source that many smart city applications rely on, such as health, traffic, security, safety, etc. The data coming from Crowdsourcing usually includes the location data of the users. Unfortunately, revealing users' locations by service providers or an external attacker exposes users to many threats, reveals a lot of private and sensitive information about their behavior, hobbies, and habits, and may sometimes expose them to real danger. Traditional techniques for protecting privacy in location-based services are no longer effective, especially with the development of attackers' techniques and capabilities. This paper presents an improved approach called Double Cloak Area (DCl-Ar) to effectively protect users' privacy and ensure data reliability in Crowdsourcing-based systems and services. The proposed approach will provide two levels of protection. The first level depends on users to create a first cloak area, while the second level depends on fog nodes to create an extended second cloak area. Moreover, the proposed approach will provide three different scenarios for managing collaboration between fog nodes to select the second anonymizer. Through simulation and comparison, we prove the superiority of the proposed approach in terms of the level of specificity without a significant effect on performance.

Keywords: Crowdsource, Protection, DCl-Ar, Anonymizer, Fog, IoT, Security, Reliability.

Introduction

The Internet of Things (IoT) has changed many concepts of our lives and made our cities smarter [1]. In achieving this, the IoT relied mainly on sensing data from everywhere through billions of wireless network sensors (WSNs) and Radio Frequency Identification (RFID) [2]. The WSNs provide information about the surrounding environment, such as temperature, pressure, noise, pollution level, etc. [Ref]. RFID Tags provide unique object identifiers that enable systems and applications to interact with and track them [4].

In general, the huge amounts of data generated by the IoT (through the layer of sensors, tags, and smart devices) were the main axis in creating systems and services that are more advanced and adapted to users [5]. Because of the weakness of the resources for the IoT, it was necessary to rely on analyzing this data within the cloud [6]. This step helps to understand the behavior of users and provide services that are more commensurate with their requirements, detect services' defects and remedy them, or reveal new knowledge and support more accurate and correct decisions [7].

The cloud was not able to meet the requirements of all types of smart systems and services on its own, especially those that are sensitive to delays, such as medical applications, traffic congestion, disaster handling, and others [8-10]. Therefore, new computing paradigms have emerged, such as edge computing or what is known as fog computing [11]. Where smart cities provide a network of fog nodes spread densely to cover most areas of the city in the form of adjacent cells. The fog node presence near IoT tools and users makes it able to conduct rapid processing in real-time and provide alerts or immediate responses in emergencies. Thus, cloud computing and fog computing integration has contributed to supporting more forms of smart applications [12]. Figure 1 shows the main layers in the IoT, the stages and processes in each layer, and the main protocols used [13].

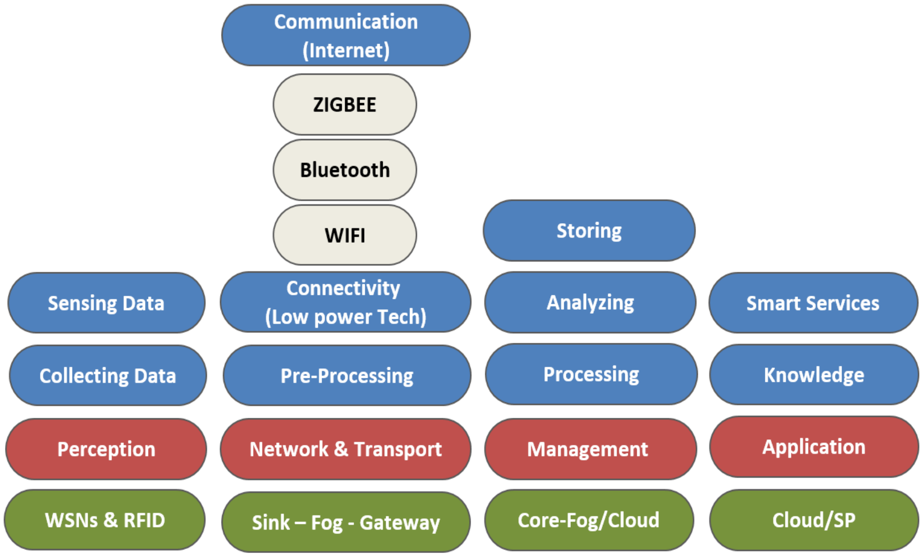


Figure 1. Main Layers and Phases of IoT

Recently, important new models such as Crowdsourcing have emerged to provide better data than the IoT [14]. Crowdsourcing integrates human perception, experiences, and evaluation with visual and auditory recognition on the one hand, in addition to the sensors and technologies in smart devices on the other hand [15]. More than that, mobile phone have become more resourceful, so the devices' resources can be used to carry out primary data processing and reduce the load on the higher computing layers [16]. Despite the importance of new models of data sources, such as Crowdsourcing, in supporting smarter and more effective services, they face challenges related to the reliability of the transmitted data, the containment of malicious and misleading data, and the challenge of the security and privacy, especially with the adoption of Crowdsourcing models on the location of users as one of the main parts of the data sent [17, 18].

In recent years, interest in protecting the privacy and security of users has increased dramatically. Most developed countries have developed privacy laws, such as the European low General Data Protection Regulation (GDPR) and the US law [19]. These laws focused specifically on managing the relationship of service providers (SPs) with their users' data. Unfortunately, most of the data coming from the IoT or Crowdsourcing models can be analyzed to reveal a lot of sensitive data about its users. It is even more dangerous when this data contains the user's location, such as where he is at certain times or what he usually visits. It is necessary that the data contain the user's location for Location Based Services (LBS) and smart systems [20].

LBS represented a sizable leap in the level and form of new services and applications, especially with the large spread of smart devices and mobile phones, in addition to the development in communication technologies [21]. But revealing users' location compounds the risk for both privacy and security. Figure 2 shows a comparison between security and privacy concerns [22].

Despite the interdependence between the concepts of privacy and security, there is a big difference in interest in each of them, or what is known as the triple interest. Firstly, data security is concerned with confidentiality and not exposing data to any unauthorized one by encrypting it. Secondly, data security is concerned with ensuring the integrity and reliability of data and not modifying it during transmission or storage over the network. Third, data security is concerned with ensuring data availability permanently, continuity of the service, and not being subjected to an attack that causes it to stop [23].

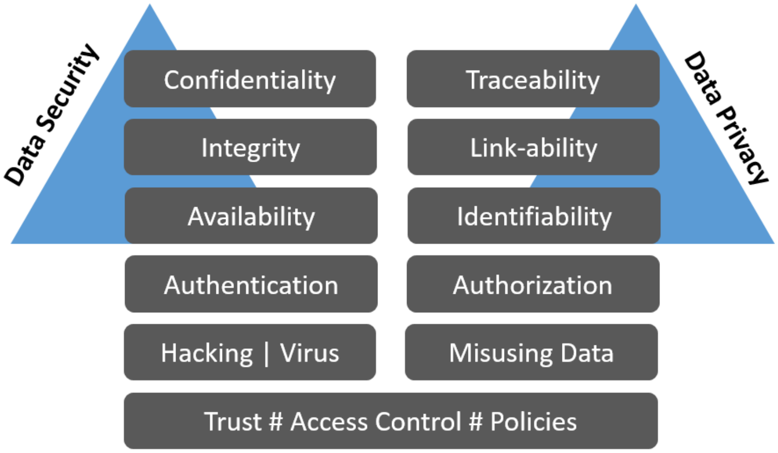


Figure 2. Security vs. Privacy

On the other hand, privacy is about users. First, privacy seeks to hide the owner's identity of transmitted or stored data over the network. More than that, privacy limits the ability of SPs to link data to users and create a profile for each user, thus revealing additional data about him. Finally, privacy is keen to prevent users from being tracked, such as knowing their locations over time [24].

The attacks that LBS can suffer can be categorized into two types of attacks, the anonymous attack and the active attack. As for the anonymous attack, the attacker seeks to steal users' data, analyze it, and reveal a lot of sensitive data about them without the user's knowledge. While in the active attack, the attacker seeks to block the service or modify the data. The first attack (anonymous) may be more dangerous than the second because the user is unaware of the problem. The first attack is also more privacy-related, especially in forms like Crowdsourcing. The single information sent by the user may not be confidential, but collecting a lot of information and linking it to the user and his location over time will cause a real threat to reveal much of the user's privacy, such as information about his habits, behavior, religion, work, social status, and others [25].

Therefore, in this research, we focus on protecting privacy within Crowdsourcing applications from the SP, knowing that the malicious SP is more dangerous than the external attacker, as it has access to all the stored data. More than that, the research will provide a mechanism to improve the reliability of the data and propose an idea to improve the level of security as well. Data privacy and security constitute the biggest challenge for users to cooperate with modern services and systems, especially those that use user data sent as a basis, such as Crowdsourcing and LBS models.

Briefly, the contributions to this research will be as follows:

- Propose an improved approach to ensure users' privacy in Crowdsourcing-based services.
- Employ collaboration between fog nodes in smart cities to improve privacy and ensure data reliability in crowdsourcing models.
- Propose three scenarios to manage the collaboration process at the peers' level and the fog nodes level.
- Present real cases of applying the proposed approach in different smart applications and services.
- Implement a simulation to prove the superiority of the proposed approach over previous privacy methods.

The second part of the research is a reference study. The third section will detail the proposed approach. The fourth section will present several cases of applying the proposed approach in different applications. The fifth section will show the results of the simulation and a comparison between the proposed approach and previous methods. Finally, a conclusion with some points for the future.

Related Work

This section provides a reference study for the most important methods of protecting privacy, specifically in LBS, such as services that use Crowdsourcing models to collect their data. Also, the section compares the previous methods and their pros and cons, in addition to identifying the part that each method protects within the user data or queries. Moreover, the section presents a table (Table 1) for speed review.

2.1 Anonymity

It is the simplest way to protect privacy, which depends on concealing the user's identity by replacing it with a pseudonym or a fictitious or specific code. So, the attacker cannot link the collected data to the user's file. That means the obtained knowledge by analyzing the data does not constitute a threat to the user. But attackers can easily break this method by monitoring the IP address or linking all data to a user's nickname. If the user's locations are always revealed as in LBS, his real identity can be inferred also [26].

2.2 Encryption

This method is used if there is trust between the user and the SP so that the two parties agree on a shared key to encrypt the data, and the malicious party cannot view it. However, as we mentioned previously, the trust between the SP and the user may not be required in many modern applications like crowdsourcing based. Moreover, the SP may be a malicious party seeking to collect data about users and breach their privacy. Generally, this method can be used when the user trusts the SP [27].

2.3 Data Summarization

This method reduces the amount of sent data to the server, which means the data is summarized. For example, sending the average consumption during a period for all devices is better than sending the rate of consumption of each electrical device in the smart house (from the privacy perspective) [28]. Therefore, the SP cannot reveal additional information about the user's life in this way. In another way, protection methods based on data summarization use Data Mining (DM) algorithms to find important information from the data before sending it, then send only the information that the SP needs without additional data to be analyzed, which causes discovering sensitive data about the user by the time [29]. But, for crowdsourcing-based services, which need as much details data in real-time as possible, this protection method is not acceptable.

2.4 Access Permission

Many SPs are now relying on this method to notify the user that they care about their privacy, where the user has the right to access his data at any time and from anywhere and the right to modify and delete the data. But what if the SP is malicious, it can easily make a copy from data in another place. Therefore this method is not enough to protect privacy from this type of attack. This method can enhance the privacy and security of an external attacker [30].

2.5 Trusted Third Party (TTP)

Sometimes the SP cannot be trusted, so a third party can be a broker between the user and the SP. The third-party isolates the users' identities from the SP, and the SP cannot obtain information about the users. But the third party may pose a threat to the privacy of the user if it is hacked or if it is malicious. If this approach is enhanced, it can be a good option for some crowdsourcing-based services [31].

2.6 Obfuscation

This approach depends on adding noise to the data before sending it to the SP or making an amendment to some data to prevent the SP from obtaining accurate information. However, some of these processes are not acceptable in crowdsourcing-based services which require accurate locations (like health or transportation services). This method is good at protecting the privacy of the user's location, which is one of the most dangerous parts of information that a malicious attacker can exploit. Some methods of obfuscation send a nearby location or a landmark in the same area instead of the user's exact location. But, in dynamic queries (frequently contacting SP), this approach can be hacked, where an attacker can draw a path for the user's movement, then predict the location of his presence in a particular area at a certain time. Moreover, If the obfuscation area is homogeneous (for example, all the buildings are related to medical activities), the attacker can obtain true information about all users in the cell without needing to accurate location. [32]

2.7 Dummy

This approach depends on sending many false queries to the SP with the real one. So the SP cannot differentiate between them. Therefore, if this data is stored with the SP side and analyzed, the SP will get misleading information about users and their interests. Thus, this method seeks to protect the privacy of transmitted data as location data. But it may not be suitable for many crowdsourcing-based services like transportation services (traffic issues), in which the number of inquiries or vehicles located in a particular area has to be accurate. Also, generating a smart dummy is difficult to be detected, especially with moving users (dynamic queries) [33-34].

2.8 Collaboration among Users

It is one of the good ways to protect privacy if the SP is a threat to users. Therefore, the goal is to reduce the amount of data that can be collected by SP. To achieve that, users exchange the results of the queries they have. For example, user A can inquire about a specific target from B or C who are in the same area instead of calling the SP. There are many other ways to collaborate. In general, this method needs to have many users in the same area to be somewhat effective, as it sometimes causes delays compared to communicating with the SP directly [35].

2.9 Cloak Area

It is the development of the TTP approach by dividing the area into many regions or cells. Each cell has an Anonymizer that protects the users' privacy from SP. Anonymizer will manage the peers inside its region only. Therefore, it will not pose a threat to the users' privacy when users deal with Anonymizer within their cells. This approach can be accomplished in another way through the cooperation of users to send all the queries at once by one of them to mislead the SP. That will prevent the SP from collecting information about each user, known as K-Anonymity [36].

2.10 Private Information Retrieval (PIR)

The user requests a large amount of data from the SP, then stores it in his memory. For future queries, the user will search in his memory without the need to contact the SP for each query. That means the SP cannot determine what the user wants. But this method requires considerable capabilities and resources for the user, which may not be available on many devices [37].

2.11 Hybrid Techniques

These methods rely on integration and merging some techniques to provide more security and privacy or better performance. For example, users can use a cache of TTP to reduce the need to contact the SP and improve system performance. Also, some methods used cooperation between users to create smart dummies. In mobile devices, manufacturing companies have started implementing many policies to enhance their users' privacy [38]. For example, in the IOS operating system, the user can review all the permissions that applications require such as permission to access contact information, messages, media, camera, or mic. Also, when using the mic or the camera, an indicator will appear to notify the user that the camera or mic is currently being used by an application, even if it is hidden usage. Also, some permissions can be given only at the time of using the application by the user [39-40]. Moreover, the user can select the option to prevent access to his accurate location if he gives the location permission to an application. All the previous options are also good and useful, but still not enough to preserve the users ' privacy from the SP like the iPhone company. Therefore, privacy still needs more effective compatible solutions with different applications.

Summarize

All previous approaches and methods of protection have drawbacks. These drawbacks prevent the previous protection techniques from being suitable for crowdsourcing-based services, which require enhanced methods. Table 1 summarizes the previous techniques and their drawbacks in addition to the attacks of each approach. Most traditional approaches do not suit crowdsourcing-based services, which require accurate data without delay. Even the anonymity approach is very weak in the protection perspective. The TTP and Cloak-Area can be enhanced to suit crowdsourcing-based services.

Previously, we have presented our hybrid approach, which depends on the doubling of protection to improve privacy and security. We presented Double Cache (DCA) [41] and Double Obfuscation (DOA) methods [42]. But, neither DCA nor DOA are not suitable for crowdsourcing-based services too, where this kind of service requires maintaining the data accuracy without large delay in processing. So, in this research, we present an enhanced approach called “Double Cloak Area” (DCL-Ar) which is suitable for crowdsourcing-based services by providing accurate information, a higher level of protection, and reliable data, without significant effect on the performance.

Table 1. Comparison of the privacy approaches

Approach	Method	Protected Part	Drawbacks	Fit Crowdsourcing	Main Attacks
Anonymity	Nickname	ID	Very Weak	No	Linking Data + Data reliability
Encryption	Cryptography	Data / Query	Trust to SP	No	Malicious SP
Data Summarize	DM and Statistics	Data / Query	Delay	No	Tracking Data
Access Permission	Authorization	Data / Query	Trust to SP	No	Malicious SP
TTP	Trusted Broker	Data / Query	Trust to TTP	Can be if updated	Malicious TTP
Obfuscation	Add noise	Data / Location	Accuracy of Result	No	Path Tracking + Homogeneity
Dummy	Send false queries	Query / Location	Accuracy of Result	No	Map Knowledge + Homogeneity
Collaboration	Peers Cooperation	Query / Location	Trust to Peers	No	Homogeneity
Cloak Area	Anonymizers	Query / Location	Trust to Anonymizer	Can be if updated	Areas Tracking
PIR	Query huge data	Query / Location	Load and Resources	No	DOS

Proposed Approach – Double Cloak Area (DCl-Ar)

The Cloak-Area approach is an approach that can be developed to be suitable for crowdsourcing applications with better security. In the traditional Cloak-area method, all users in the area send their queries to the Anonymizer. Anonymizer replaces exact queries' locations with a unified location. The Anonymizer then sends the queries on behalf of peers (users) to the SP to hide their identity. Location replacement is necessary to protect the privacy of user locations because both the cloak area and the number of users are small. Also, the section compares the previous methods and their pros and cons, in addition to identifying the part that each method protects within the user data or queries. Moreover, the section presents a table (Table 1) for speed review. In the case of dynamic queries (users are in constant motion), the malicious SP may be able to isolate the queries, track their users, and reveal their identity later. The SP can also implement a area tracking attack, and it can also implement a homogeneity attack and reveal additional information about users if all points of interest (PoI) in the cloak area are of the same nature.

Unfortunately, the process of changing users' locations causes additional weaknesses in the traditional Cloak-area approach. We can summarize them in the following points:

- Negative impact on the accuracy of the basic service. This approach will not suit precise LBS like many Crowdsourcing services.
- Anonymizer needs to re-process the data returned from the SP (in the case of queries) to map real user locations, and this negatively affects performance.
- The user may leave the region for another region before receiving the results of his query from the Anonymizer.

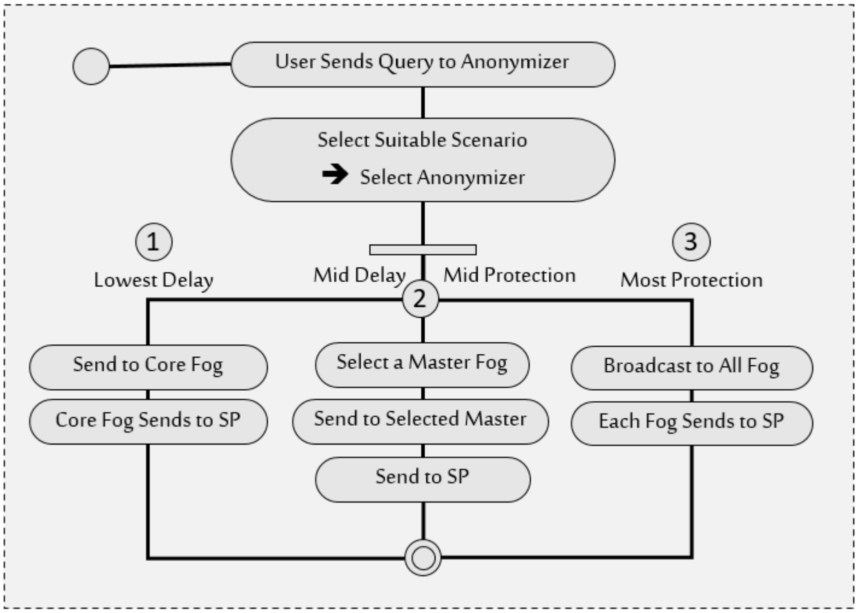


Figure 3. High Level Architecture of DCl-Ar

To solve the previous problems and challenges, we have to provide a developed approach that ensures the accuracy of data and queries' locations and ensures adequate protection for users from tracking. Therefore, we have to introduce a solution to the homogeneity in the area and the small number of users. This paper presents the idea of the "DCl-Ar" enhanced approach. The approach ensures the formation of a large cloak area with a lot of users and without overhead affecting the system's performance on the Anonymizer. Moreover, the "DCl-Ar" approach solves other challenges and weaknesses, such as when the user leaves the cloak area before receiving the result. Also, the approach supports working with crowdsourcing services that require accurate data.

The main idea of the proposed approach is to multiply create a private cloak area between peers and apply it between fog nodes (between Anonymizers) to form a larger area. In other words, the DCl-Ar will depend on two cloak regions. Cloak-area$_1$ will be peer-to-peer, and the fog node in the first area will play the role of Anonymizer$_1$. The second region, Cloak-Area$_2$, will be between adjacent fog nodes. Cloak-Area$_2$ has three different scenarios for collaboration and selection of Anonymizer$_2$. In the first scenario, the Core-Fog node will be Anonymizer$_2$ if a layer for cores nodes is available. In the second scenario, one of the cooperating Fog nodes will be selected to act as Master Anonymizer$_2$ on each communication with the SP. In the last scenario, all fog nodes will be sent to the SP together, which means that each fog node will play two roles: Anonymizer$_1$ and Anonymizer$_2$. The three scenarios help the proposed approach to be dynamic in working with the available architecture and diversity of Crowdsourcing applications and services. Figure 3 depicts the high-level architecture of the DCl-Ar.

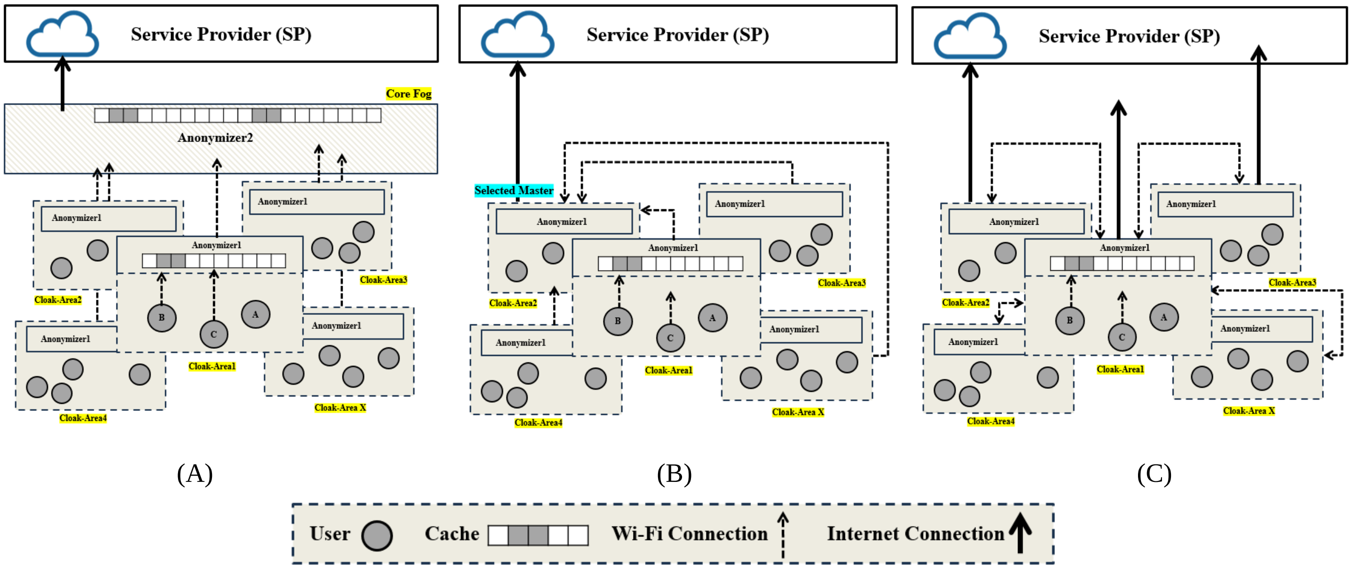


Figure 4. Scenarios of DCl-Ar Approach

The following steps describe how the proposed approach works in the first scenario (Figure 4. A):

1- Each user chooses an alias (nickname) when entering a new cell (connecting to a new fog node).
2- Each user sends data or query with location to the fog node (Anonymizer$_1$) which manages Cloak-Area$_1$.
3- In the case of sending data, the fog node can match the data to detect the existence of a data conflict and reveal the sender of unreliable data.
4- The fog node collects the received queries in the Cloak-Area$_1$ set without changing the locations of the queries.
5- The fog node sends data to Core-Fog, which represents Anonymizer$_2$.
6- The Core-Fog node sends all query sets to the SP without sending any user or fog node id.
7- The SP receives data or queries from Anonymizer$_2$ and cannot reveal any information about users or fog nodes and their areas.
8- In the case of a query, the SP returns the results to Anonymizer$_2$.
9- Anonymizer$_2$ distributes a copy of the results to each fog node.

10- Each fog node receives its results and returns them to users within the area. As for the results of queries for other areas, the fog node stores them in its cache (to answer users' queries of neighboring areas who may enter Cloak-Area$_1$ without needing to connect to the SP).

The following steps describe how the proposed approach works in the third scenario (Figure 4. B):

1- Each user chooses an alias when entering a new cell (connecting to a new fog node).

2- Each user sends data or query with location to the fog node (Anonymizer$_1$) which manages Cloak-Area$_1$.

3- In the case of sending data, the fog node can match the data to detect the existence of a data conflict and reveal the sender of unreliable data.

4- The fog node collects the received queries in the Cloak-Area$_1$ set without changing the locations of the queries.

5- The Fog node sends its data to the Master Fog node, which is rotated among all the cooperating Fog nodes.

6- The fog node, which plays the role of Anonymizer$_2$, sends all query groups to the SP.

7- The SP receives data or queries from Anonymizer$_2$ and cannot reveal any information about users or fog nodes and their areas.

8- The SP will be forced to return the results in the event of queries to the Anonymizer$_2$ that is sent to it without the ability to reveal what each cooperating fog node wants.

9- Anonymizer2 distributes a copy of the results to each fog node.

10- Each fog node receives its results and returns them to users within the area. As for the results of queries for other areas, the Fog node stores them in its cache (to answer queries of users of neighboring areas who may enter Cloak-Area$_1$ without the need to connect to SP).

The following steps describe how the proposed approach works in the second scenario (Figure 4. C):

1- Each user chooses an alias when entering a new cell (connecting to a new fog node).

2- Each user sends data or query with location to the fog node (Anonymizer$_1$) which manages Cloak-Area$_1$.

3- In the case of sending data, the fog node can match the data to detect the existence of a data conflict and reveal the sender of unreliable data.

4- The fog node collects the received queries in the Cloak-Area$_1$ set without changing the locations of the queries.

5- The fog node sends its data to all neighboring fog nodes and receives sets of queries from neighboring nodes.

6- Each fog node sends all query sets to the SP.

7- The SP receives data or queries from Anonymizers and cannot reveal any information about users or fog nodes and their areas.

8- The SP will be forced to return the results in the event of queries to all the fog nodes sent to it without the ability to detect what each fog node wants specifically.

9- Each fog node receives its results and returns them to users within the area. As for the results of queries for other areas, the Fog node stores them in its cache (to answer queries of users of neighboring areas who may enter Cloak-Area$_1$ without the need to connect to SP).

Algorithm of DCl-Ar

```
//User or Peer
Result = Send (Anonymizer1, Nickname, Location, Data);
//Anonymizer1
```

```
List_Queries1 []= null;
List_Queries2 []= null;
While (true)
        New_Query = Get_Query();
        List_Queries1.add (New_Query);
        List_Queries2.add (Anonymizer1, New_Query.Location, New_Query.Data)
Anonymizer2 = Find_Anonymizer2();
// Scenario1 for Find_ Anonymizer2
Anonymizer2 = get_Core_Fog (Anonymizer1.Location)
Results = Send ( Anonymizer2, List_Queries);
// Scenario2 for Find_ Anonymizer2
List_Fog = Get_Neighbors(Anonymizer1.Location) ;
For (int i=1; i<= List_Fog.Count; i++)
        Results = Send ( List_Fog[i]; List_Queries);
List_Queries.Clear();
// Scenario3 for Find_ Anonymizer2
Counter = Get_Next_Counter();
List_Fog = Get_Neighbors(Anonymizer1.Location) ;
Anonymizer2 = Counter mod List_Fog.Count;
Results = Send ( Anonymizer2, List_Queries);
If (Anonymizer1.ID == Anonymizer2)
        While (true)
                List_Queries [] = Get_List ();
                List_Queries2.Add ( List_Queries );
                Results = Send (SP, List_Queries2);
                List_Queries2.clear();
                Return (List_Queries.Anonymizer, Results);
For (int i=1; i<= Results.Count; i++)
        Return (List_Queries1[i].UserID, Results[i]);
End;
```

```
//Anonymizer2
While (true)
        List_Queries [] = Get_List ();
        Results = Send (SP, List_Queries);
Return Result
```

Hint, in case of sending data without waiting for results, Anonymizer will play another role to check the reliability of sending data by the user. Moreover, Anonymizer can collect data until a specific limit and then sends it to the next level instead of sending it directly like in the query case.

Real examples about Crowdsourcing Services and Privacy Threat

This section reviews some services and applications of the main areas, how these services can be exploited to penetrate the privacy of users, and then how the proposed approach can protect their privacy.

4.1 Health

Many concepts have developed after the emergence of the IoT, starting from Smart Health and Ubiquity Health to the Internet of Healthy Things (IoHT). These technologies depend mainly on providing vital measurements and data about the patient in real-time, as this data is collected from sensors, whether wearable or spread in the environment surrounding the user. This data is processed and analyzed for early detection of any serious or potential change in the user's health. Recently, with the Corona crisis, the number of digital services in the health field increased, and homes were turned into health centers based on IoT [43].

Moreover, many services and health centers have depended on crowdsourcing to get more information about users during the pandemic. Unfortunately, the malicious SPs have enabled us to collect a lot of sensitive data and violate users' privacy, for example, by tracking users’ activities and locations. Thus, the question was, how to work with medical pandemics and collect useful data, but without jeopardizing user privacy and threatening it? DCl-Ar can be used with most health services that don't require a specific identity for the user.

Moreover, DCl-Ar can utilize the anonymizer node to compare data and detect any abnormal or unreliable data [44].

4.2 Transportation and Traffic Management

Traffic systems have also evolved greatly following the IoT revolution. Smart vehicles, smart traffic lights, digital streets, street conditions, smart parking lots, as well as various LBS have appeared. Most of these services depend on crowdsourcing. Malicious parties or providers of mapping or location-based services can track a user's location for a period to discover much user data not associated with the advertised service [45]. For example, when analyzing the places that the user visits during a month, it is possible to know the nature of the user, where his home is, when he leaves the house, if he is sick and visits health centers, a visitor to luxury or popular restaurants, an active employee and arrives on time, Or often late if he has children in school or not, and many other data and sensitive data that SP is not allowed to access them. DCl-Ar does not allow SPs to link data to a specific user or create a profile for any user who uses these services.

4.3 Business

Electronic invoices and purchases online are significantly diffused, by analyzing invoices that can reveal data about user behavior, richness or spending rate and income, and when there are special occasions in his life. Moreover, the delivery services reveal the user's location and places (at home or work). Recently, many companies utilized crowdsourcing data and tools like reviews, comments, questioners, etc. to get much information about their products and customers. Unfortunately, a huge amount of the collected information is private, and users do not know about it [46]. DCL-Ar enables companies to get purposive information about their products and customers without disclosing the customers' identities

4.4 Smart Phones and social media

They are the smartest devices that have become connected to the user's life because they contain many different services and applications. Social networking applications have also become one of the main things in the user's life and have become the means for expressing opinions, displaying talents, hobbies, and discussions, and a primary source for obtaining news [47].

Smartphones and social media are the main tools for most crowdsourcing services. So, at the same time, they are a main threat to the user's privacy which can reveal his interests, behavior, hobbies, preferences, inclinations, and a lot about his private life [48]. Although smart services require more and more user data to provide continuous enhancement and better quality, privacy must be guaranteed. DCL-Ar can help in this part.

Briefly, after studying some real privacy threats and penetration, we realize the danger of modern applications and technologies that are spreading all around us like many services based on crowdsourcing. The proposed approach can play an important role in supporting these services and their future by preserving the user's privacy. The next section will discuss and prove the effectiveness of DCL-Ar in protecting privacy without a significant effect on performance.

Results and Discussion

To prove the superiority and efficiency of the proposed "DCl-Ar" approach, this section presents the results of comparison with several other methods, namely.

1. Without using any protection method.
2. Using the traditional Cloak-Area approach (Cloak Area) [36].
3. Using the obfuscation approach (DOA) [42].
4. Using the peer-to-peer approach (SPF) [49].

5. Use the dummy approach (Enhanced-CaDSA) [38].

The comparison relied on standards to measure the level of privacy and protection achieved and the level of affecting performance**.**

1- K-Anonymity [24, 49] It is expressed by dividing 1 by the number of queries sent to the SP, whether true or false.

K-Anonymity = 1/ (1+K) where K = number of false queries

2- Entropy [24, 49], which represents the amount of real information that the SP can link to the sender's user, or the percentage of the SP's certainty that the information it has is related to a specific user.

$$\boldsymbol{Entorpy = -\sum_{i=1}^{n} pi * \log_2 pi}$$

Where n is number of sent queries, and pi is probability of query i belongs to the user.

There is another standard for privacy, but it is completely related to entropy, for example, Estimation Error, which is a percentage of Entropy, and the Ubiquity standard, that is, the spread of the user everywhere within the region, which is Entropy^2.

3- Time is related from the moment the query is sent to the moment the result is received by two main factors: Send Time (ST) and Process Time (PT). Time is also affected by the data size (DS), the number of queries sent (NQ), and the Cache Hit Ratio (CHR) [24,49].

4- There are non-quantitative standards related to the level of efficiency of the proposed approach and its robustness in the face of attacks, in addition to its ability to adapt to specific applications and services such as Crowdsourcing.

Mathematical Analysis

Based on the previous criteria, each of the compared methods was analyzed.

Without Protection Method

- K-Anonymity = 1 ➔ No protection
- Entropy = Log (1) = 0 ➔ No dept, so no protection
- DS= 1KB ➔ No change
- Time = ST
- Cache can be used here.

Traditional Cloak-Area

- K-Anonymity = 1/(1+K) ➔ K is number of cooperated users in the area
- Entropy = -1/k * Log (1/k) if all dummies have same probability ➔ Entropy < 1 (Maximum)
- DS= 1KB ➔ No change for each query
- Time = ST + Sending time to Anonymizer of the area + PT of mapping result to real location of peers
- Cache can be used but will not achieve good CHR because of the changing locations of queries.
- Not suitable for Crowdsourcing applications
- Homogeneity attack and tracking area attack.

Dummy Approach (Enhanced-CaDSA)

- K-Anonymity = 1/(1+K) ➔ K is number of dummies
- Entropy = -1/k * Log (1/k) ➔ Entropy < 1 (Maximum)
- DS= (1+K)KB ➔ No change for each query
- Time = (1+K)*ST
- CHR will be affected adversely if the cache is used here, because storing for dummy queries.
- Not suitable for Crowdsourcing applications
- Tracking real query and detecting dummies attack

Obfuscation Approach (DOA)

- K-Anonymity = 1/(1+D) ➔ D is number of possible false locations in the area
- Entropy = -1/D * Log (1/D) ➔ Entropy < 1 (Maximum)
  but in enhanced obfuscation DOA Entropy =1 (Maximum) because there is no direct connection to SP by user.
- DS= 1KB + Obfuscation area range
- Time = ST + PT of mapping result to reallocation of user
- CHR will be affected adversely if the cache is used here, because changing queries' real locations.
- Not suitable for Crowdsourcing applications
- Homogeneity attack, tracking area attack, and Map Knowledge Attack.

Peers-Cooperation (SPF)

- K-Anonymity = Maximum because user sent query for another user to SP.
- Entropy = 1 (maximum) because SP has only one query ➔ E=0,
  but the query for another user➔ Entropy = Max - 0 = 1
- DS= 1KB ➔ No change
- Time = ST + Swapping Time among peers + Swapping time between peers and Fog+ Swapping time among fogs + Swapping time between fog and peers.
- CHR maximum because only real queries used, in addition there is double cache can be used here.
- Can be used with Crowdsourcing applications because no change for locations only Identities of users.
- Peer Attacks or Cooperated peer disconnected

Proposed Approach (DCl-Ar)

- K-Anonymity = Maximum because the user doesn't connect to SP at all.
- Entropy = 1 maximum because SP doesn't have any information about users themselves.
- DS= 1KB ➔ No change
- Time = ST + Sending Time to Anonymizer$_1$ + Sending Time to Anonymizer$_2$.
- CHR maximum because only real queries used, in addition there is double cache can be used here, more each cache can store data of neighbors' caches.
- Can be used with Crowdsourcing applications because no change for locations only Identities of users.
- If many fogs were malicious in the same time they can threat the users privacy, also if there is cooperation between fogs and SP, however this is not logic or very rare.

Results and Discussion

Simulations were made on the same data and assumptions used in previous papers, and then based on quantitative standards, the results shown in the following figures were plotted.

The assumptions were as follows

1- The size of a single query without protection is 1KB
2- The number of users is 10,000 users
3- The number of regions is 100 * 100
4- The size of the cache is 100KB
5- The number of points of interest is 100

We used C# with SQL Server databases on Visual Studio.Net 2019. We relied on some data from the Geo-Life dataset of 17,000 tracks of 180 collaborating users monitored over three years.

Figure 5 shows that the proposed approach, in addition to the SPF and DOA approach, achieves privacy protection with a maximum Entropy (Entropy= 1) due to the user not communicating with the SP directly, as in the proposed approach and DOA, or the user sending a query to another user, as in SPF. In the dummy approach, the SP can obtain part of the user's information within the set of dummy queries sent. Also, in the traditional Cloak-Area, the SP can detect the identity of users and reveal information about them in the case of a small area or a small number of users.

More than that, the proposed protection method (DCl-Ar) is distinguished by using two levels to hide the user's identity from the SP (Anonymizer1 and Anonymizer2), in addition to hiding the user's query and data within a large number of users and hiding his location within a large area with a large number of PoI. Thus, the proposed approach guarantees a high level of privacy. And since the achieved privacy is maximum (Entropy=1), then, both standards Ubiquity and Estimation Error will be Maximum as well, because these two standards are related to Entropy. This is logical in the DCl-Ar because users' queries are not modified, and the large users' number means that they are spread in all places within the cloak area, and thus the probability that the SP will be wrong in specifying the user's location is maximum too.

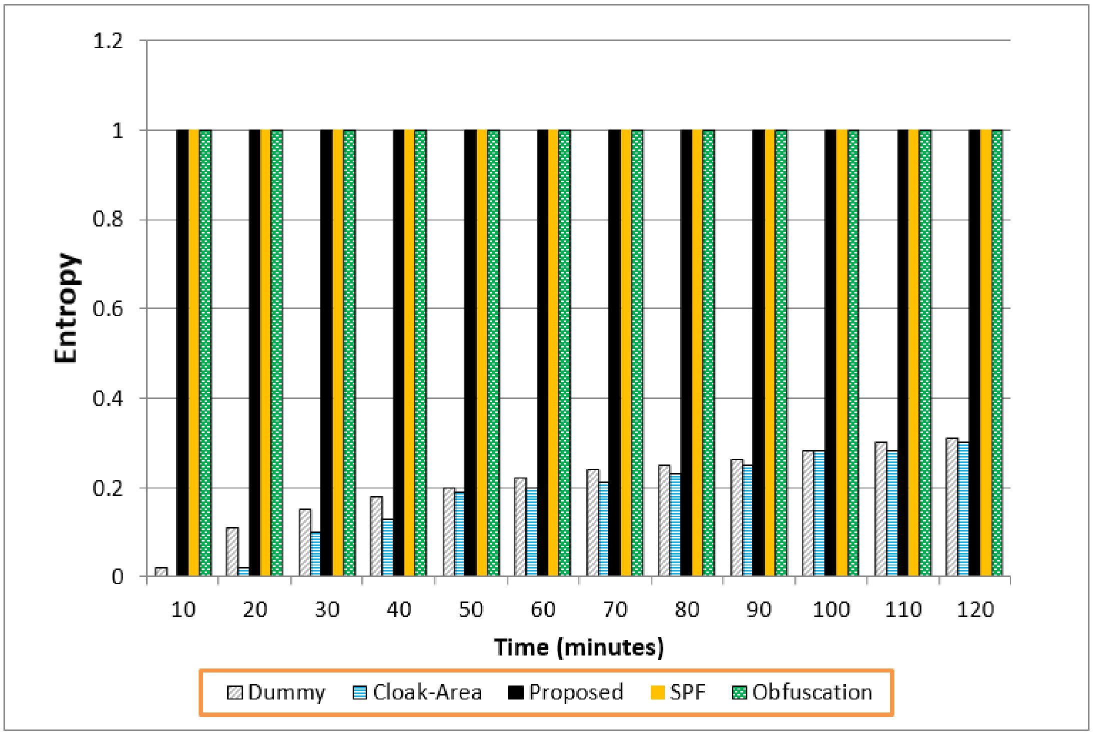


Figure 5 Comparison based on Entropy.

Figure 6 shows the number of queries sent to the server, which has a role in determining the level of system performance and the level of privacy as well. As the number of queries sent to the SP is lower, the information is less likely to be disclosed, less load on the system, and a better performance rate. In terms of the number of queries, the type of protection used plays a big role, in addition to the use of cache memory in the area where the users are located. The results show the superiority of the proposed approach DCl-Ar in addition to the SPF in achieving the lowest number of queries sent. The justification for this is that both approaches do not use dummies to increase the number of queries on the one hand, and do not modify the query location, which negatively affects the hit rate. Moreover, both the DCl-Ar approach and the SPF use two caches, which gives double the probability of a hit. What further distinguishes the DCl-Ar from SPF is that the cache in the proposed approach can store queries for a contiguous area. This will be useful in solving the problem of moving the user from one area to another before receiving his result, increasing the hit rate, and benefiting more from the cache.

The foregoing discussion is reinforced by Figure 7 which shows the superiority of DC1-Ar approach in terms of hit rate. Justify this by storing only real queries for users, in addition to not modifying the query locations. In Figure 7, we assume that the traditional Cloak Area has a cache also, but the hit rate is lower because all user queries are linked to one location, which is contrary to reality. The dummy method remains the worst because dummy queries are stored in the cache, which affects the hit rate negatively, even if these dummies are chosen intelligently.

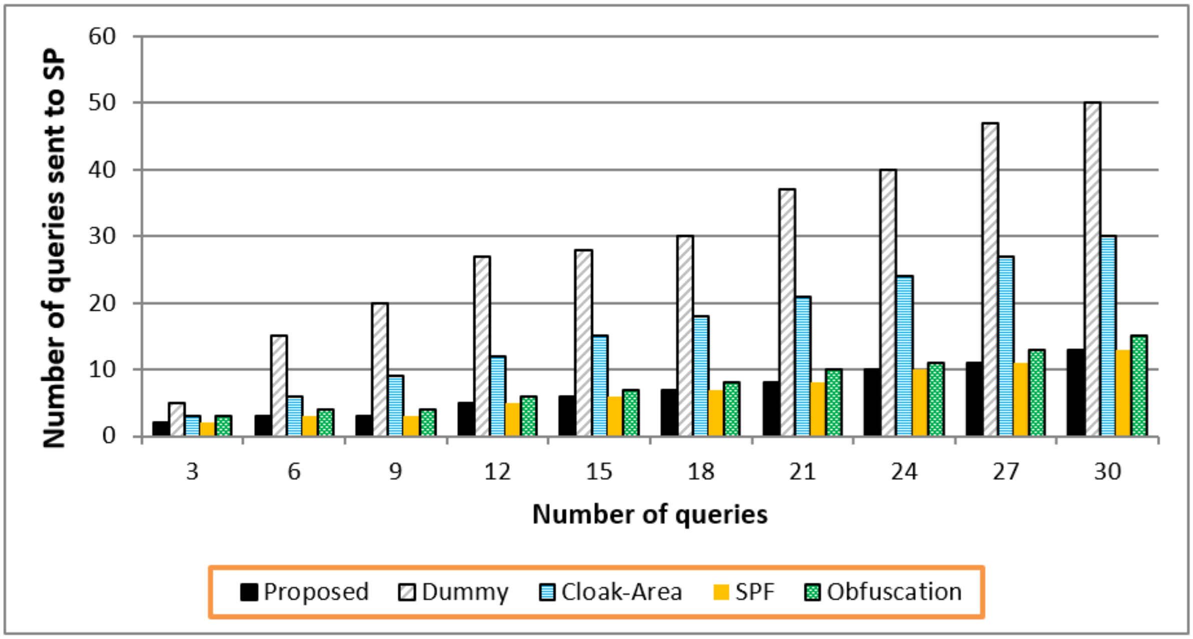


Figure 6 Comparison based on Number of Sent Queries

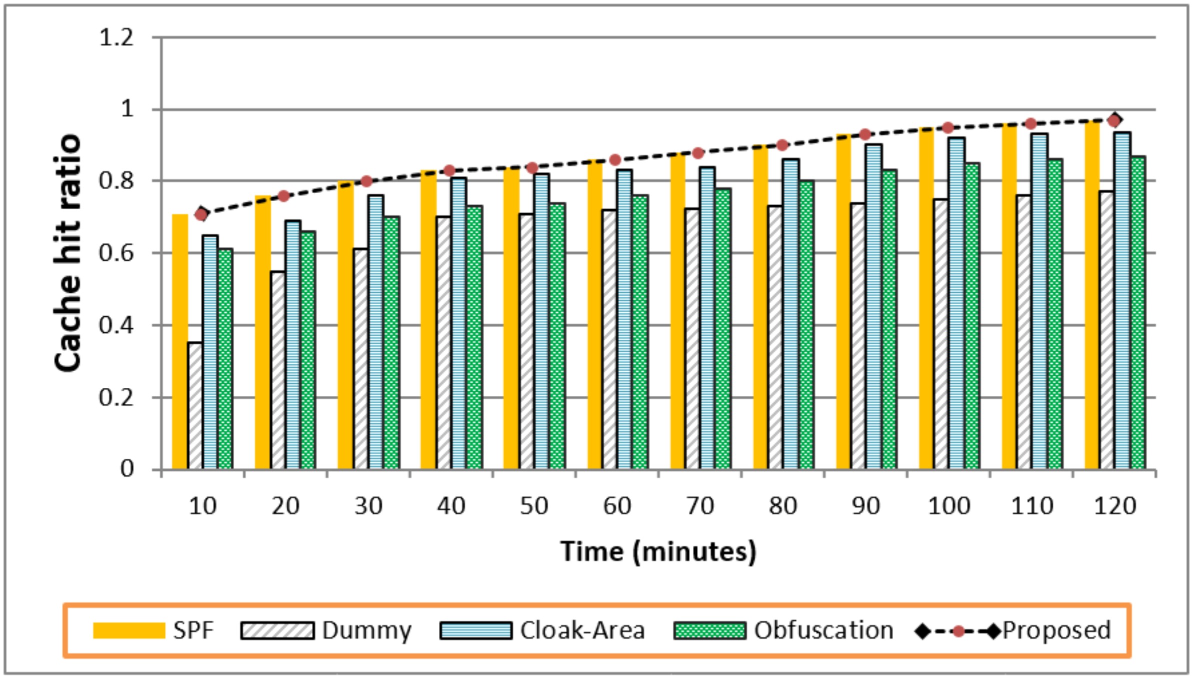


Figure 7 Comparison based on Cache Hit Ratio

Figure 8 shows the response speed standard and shows the superiority of the proposed approach DC1-Ar, followed by the SPF approach and then DOA. Cloak-Area and Dummy are the worst because of the overhead caused by dummies or the need to process the returned data in the case of the traditional Cloak-Area and mapping the results to real user's locations. The superiority of DCl-Ar is due to the lack of the need to process the returned results on the one hand, and on the other hand, the use of cache helps in the speed of the answer, especially in the case of a high infection rate. Finally, the transmission time in DC1-Ar is less than that of SPF because the proposed approach uses only two extra steps while SPF uses four steps. The additional steps are Wi-Fi connections, and therefore the transmission time is much less compared to connecting via the Internet with the SP.

Note: The ping experiment was conducted several times for an internal connection and several times for an external connection, and then calculated the averages. After that, the percentage difference in time was calculated, and it appears that the internal communication (locally) is 0.1 of the time required to contact an external SP.

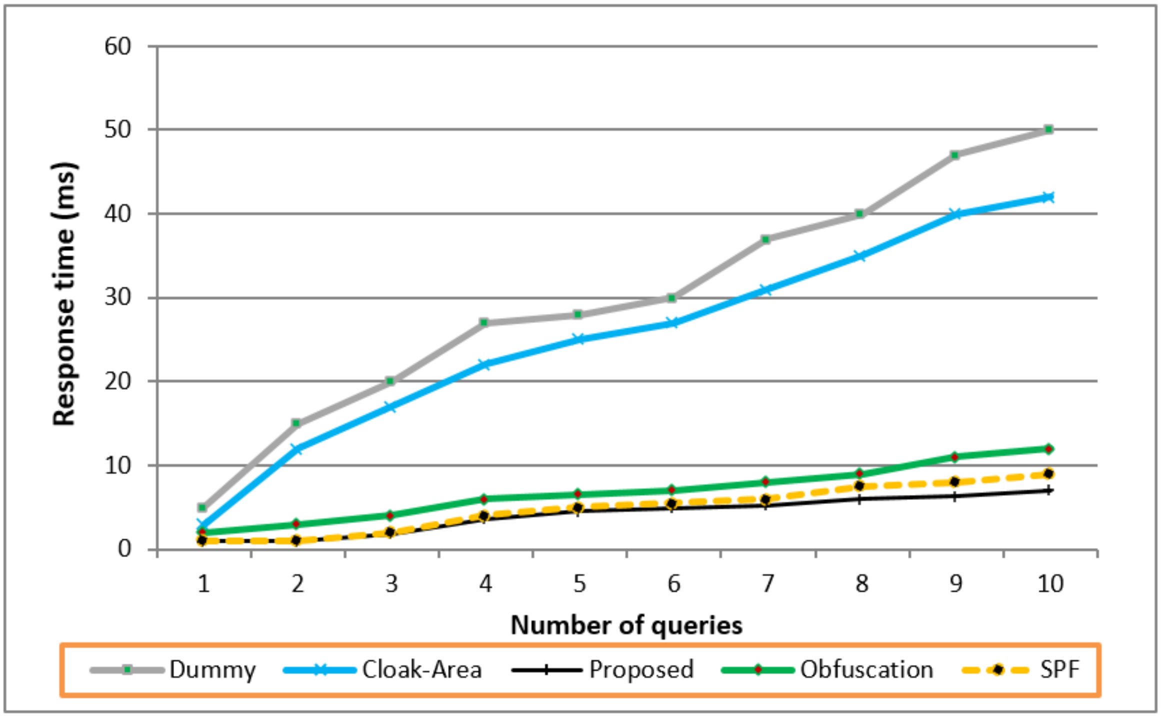


Figure 8 Comparison based on Response Time.

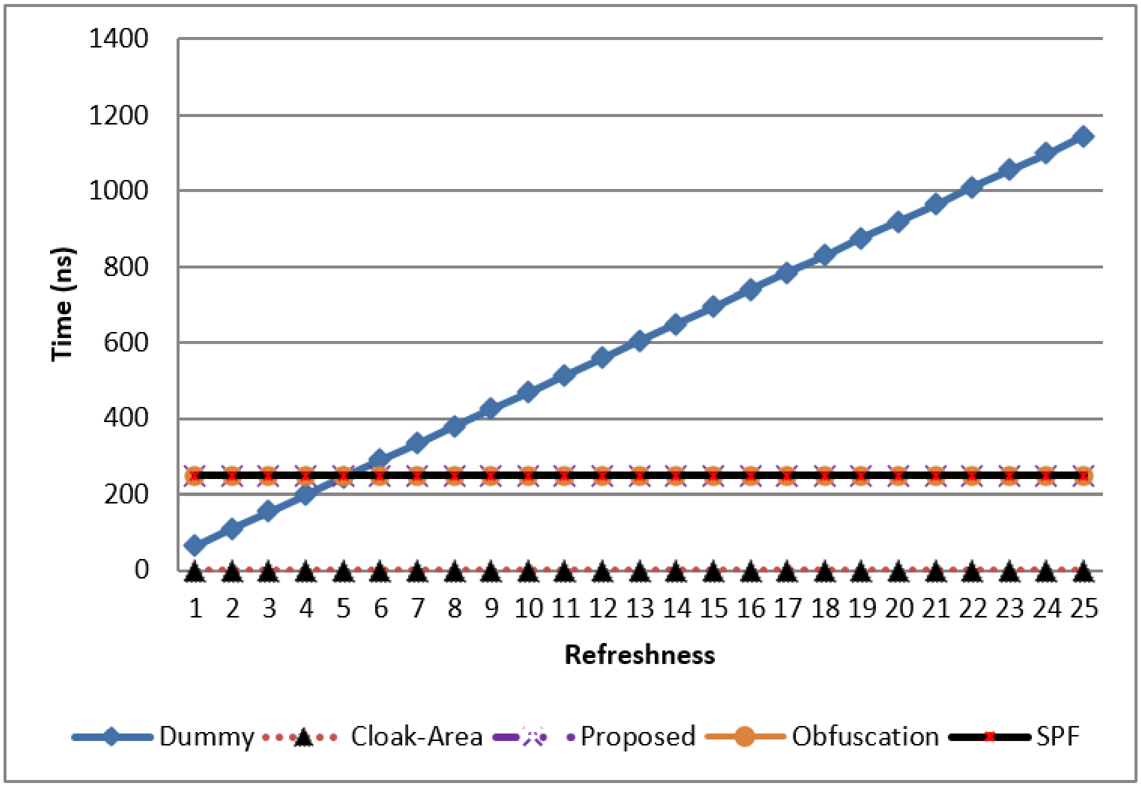


Figure 9 Comparison based on Cache Refreshness Time

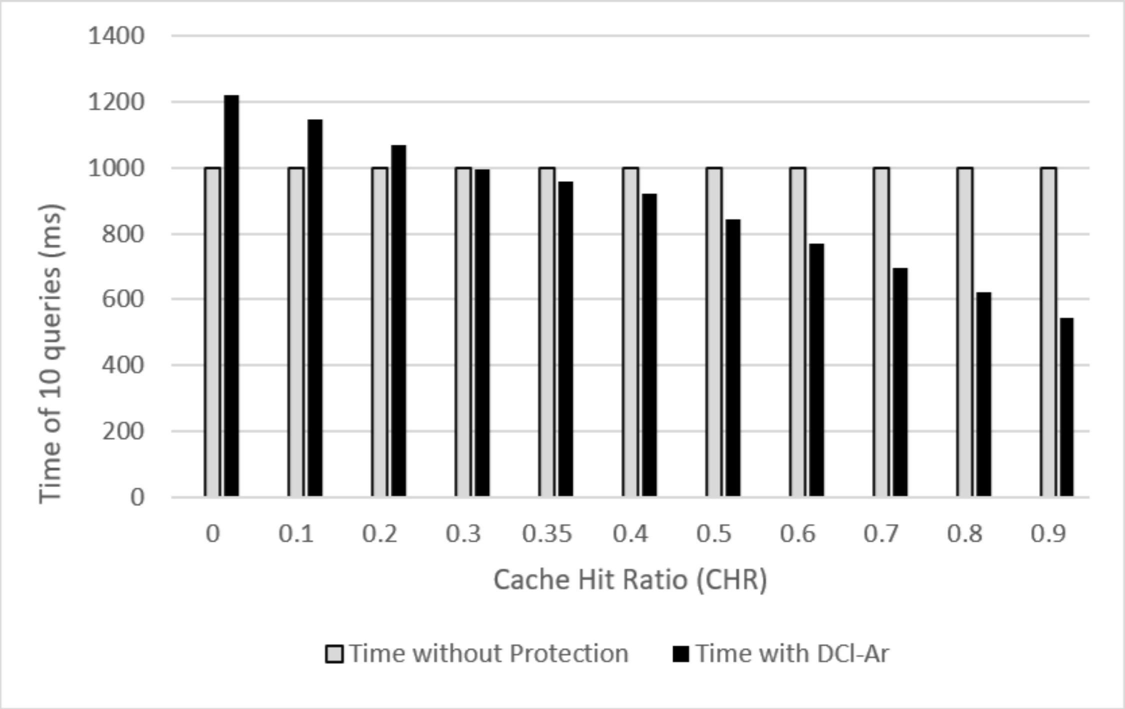


Figure 10 Comparison based on Total Time of Ten Queries

Figure 9 shows the time required to update the data in the cache. If the cache is not used as in the traditional Cloak Area, there will be no time for updating. In the proposed approach DCl-Ar, the same technique was used in SPF and developed Obfuscation DOA, where all data is constant, and only the duplicated query position is updated. But in the dummy, all elements in the cache are swapped, so the required time increases with the number of stored queries.

Figure 10 shows the difference in the needed time to respond to ten queries between using no protection and using DCl-Ar, at different cache hit rates. It is logical that in using no protection, the time will be constant, but with the protection approach that depends on cache, and if the hit rate is small, less than 3, the time will be worse (greater) due to the additional protection steps. But if the hit rate is large, the proposed approach may be better than without using protection and without using a cache. But note when not using protection and using a cache, of course, time will be much better, but there is no justification for using an additional party if protection such as Anonymizer is not used.

Disadvantages of DCl-Ar and Future trends in privacy

As an approach to protection, there is no one without drawbacks. DCl-Ar has a few drawbacks also which are:

- If the set of fog nodes (Anonymizers) are malicious they can disclose the privacy of users. However, this is very rear to hack many of fogs at the same time.
- If there is cooperation between malicious fogs and SP, this premise is also not logical.
- As any protection method there is adversely effect on the time of processing

Anyways, the multi-proposed scenarios in DCl-Ar are proposed to relax previous points according to the type of services.

Moreover, in the following points we mention some future trends in the privacy domain which we plan to work in the next:

- Create a privacy protection platform like antivirus ones in the security.
- Find special protocols to protect privacy, as are the protocols for protecting data security during transmission.
- Find a tool for analyzing the level of privacy in any application like the tools of penetration testing of security.
- Increase the awareness of users in protecting the privacy of their data and not compromising it to any party.
- Find a solution to protect privacy in pandemics, during which privacy terms and restrictions are greatly tolerated.
- Find a dynamic platform that includes many different protection methods to adapt to different IoT apps.
- Employ machine learning for smart selection the best protection technique for each service or application.
- Create a knowledge base for each kind of application and its related threats.

Conclusion

The research reviewed a developed privacy protection approach called DCl-Ar within services and applications based on Crowdsourcing models. DCl-Ar presented two levels of protection with three different scenarios according to the available architecture, level of protection, and required performance. DCl-Ar relied on fog nodes and their cooperation in creating a large cloak area with many users, which led to an increase in the level of protection without affecting the accuracy of the services. The approach employs the cache of fog nodes to lessen the impact of protection on performance. More than that, DCl-Ar provided an idea to solve the problem of data reliability coming through Crowdsourcing. Through simulations, we have demonstrated the superiority of the developed approach over the traditional Cloak-Area approach, the improved dummy approach, the obfuscation approach, and the developed collaboration approach in terms of level of protection and performance, and most importantly, that it is suitable for working with services based on Crowdsourcing.

References

[1] Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International journal of communication systems*, *25*(9), 1101.

[2] Pal, K. (2023). Challenges of Using Wireless Sensor Network-Based RFID Technology for Industrial IoT Applications. *Handbook of Research on Advancements of Contactless Technology and Service Innovation in Library and Information Science*, 80-100.

[3] Fahmy, H. M. A. (2023). WSNs applications. In *Concepts, applications, experimentation and analysis of wireless sensor networks* (pp. 67-242). Cham: Springer Nature Switzerland.

[4] Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012, April). RFID technology and its applications in Internet of Things (IoT). In *2012 2nd international conference on consumer electronics, communications and networks (CECNet)* (pp. 1282-1285). IEEE.

[5] Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review*, *39*, 100318.

[6] Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based big data storage systems in cloud computing: perspectives and challenges. *IEEE Internet of Things Journal*, *4*(1), 75-87.

[7] Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: architecture, opportunities, and open research challenges. *ieee access*, *5*, 5247-5261.

[8] Bahbouh, N. M., Compte, S. S., Valdes, J. V., & Sen, A. A. A. (2023). An empirical investigation into the altering health perspectives in the internet of health things. *International Journal of Information Technology*, *15*(1), 67-77.

[9] Alsaawy, Y., Alkhodre, A., Abi Sen, A., Alshanqiti, A., Bhat, W. A., & Bahbouh, N. M. (2022). A comprehensive and effective framework for traffic congestion problem based on the integration of IoT and data analytics. *Applied Sciences*, *12*(4), 2043.

[10] Aljohani, F. H., Abi Sen, A. A., Ramazan, M. S., Alzahrani, B., & Bahbouh, N. M. (2023). A Smart Framework for Managing Natural Disasters Based on the IoT and ML. *Applied Sciences*, *13*(6), 3888.

[11] Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. *big data and cognitive computing*, *2*(2), 10.

[12] Sen, A. A. A., & Yamin, M. (2021). Advantages of using fog in IoT applications. *International Journal of Information Technology*, *13*, 829-837.

[13] Kumar, N. M., & Mallick, P. K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia computer science*, *132*, 109-117.

[14] Garcia-Molina, H., Joglekar, M., Marcus, A., Parameswaran, A., & Verroios, V. (2016). Challenges in data crowdsourcing. *IEEE Transactions on Knowledge and Data Engineering*, *28*(4), 901-911.

[15] Pasolini, G., Guerra, A., Guidi, F., Decarli, N., & Dardari, D. (2020). Crowd-based cognitive perception of the physical world: Towards the Internet of Senses. *Sensors*, *20*(9), 2437.

[16] Zaman, S. K. U., Jehangiri, A. I., Maqsood, T., Ahmad, Z., Umar, A. I., Shuja, J., ... & Alasmary, W. (2021). Mobility-aware computational offloading in mobile edge networks: a survey. *Cluster Computing*, 1-22.

[17] Feng, W., Yan, Z., Zhang, H., Zeng, K., Xiao, Y., & Hou, Y. T. (2017). A survey on security, privacy, and trust in mobile crowdsourcing. *IEEE Internet of Things Journal*, *5*(4), 2971-2992.

[18] Sodagari, S. (2022). Trends for mobile iot crowdsourcing privacy and security in the big data era. *IEEE Transactions on Technology and Society*, *3*(3), 199-225.

[19] Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1-6.

[20] Huang, H., & Gartner, G. (2018). Current trends and challenges in location-based services. *ISPRS International Journal of Geo-Information*, *7*(6), 199.

[21] Usman, M., Asghar, M. R., Ansari, I. S., Granelli, F., & Qaraqe, K. A. (2018). Technologies and solutions for location-based services in smart cities: Past, present, and future. *IEEE Access*, *6*, 22240-22248.

[22] Abi Sen, A. A., & Basahel, A. M. (2019, March). A comparative study between security and privacy. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1282-1286). IEEE.

[23] Yee, C. K., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of Information and Communication Technology in Education*, *8*(2), 34-42.

[24] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *International Journal of Information Technology*, *10*, 189-200.

[25] Gupta, R., & Rao, U. P. (2017). A hybrid location privacy solution for mobile LBS. *Mobile Information Systems*, *2017*.

[26] Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors*, *20*(22), 6587.

[27] Ren, W., Tong, X., Du, J., Wang, N., Li, S. C., Min, G., ... & Bashir, A. K. (2021). Privacy-preserving using homomorphic encryption in Mobile IoT systems. *Computer Communications*, *165*, 105-111.

[28] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740.

[29] Kreso, I., Kapo, A., & Turulja, L. (2021). Data mining privacy preserving: Research agenda. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *11*(1), e1392.

[30] Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, *7*, 61656-61669.

[31] Yamin, M., Alsaawy, Y., B. Alkhodre, A., & Abi Sen, A. A. (2019). An innovative method for preserving privacy in Internet of Things. *Sensors*, *19*(15), 3355.

[32] Xu, H., Zhou, Y., Ming, J., & Lyu, M. (2020). Layered obfuscation: a taxonomy of software obfuscation techniques for layered security. *Cybersecurity*, *3*(1), 1-18.

[33] Diyanat, A., Khonsari, A., & Shariatpanahi, S. P. (2016). A dummy-based approach for preserving source rate privacy. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1321-1332.

[34] Siddiqie, S., Mondal, A., & Reddy, P. K. (2023). An improved dummy generation approach for infeasible regions. *Applied Intelligence*, 1-15.

[35] Shokri, R., Theodorakopoulos, G., Papadimitratos, P., Kazemi, E., & Hubaux, J. P. (2013). Hiding in the mobile crowd: Locationprivacy through collaboration. *IEEE transactions on dependable and secure computing*, *11*(3), 266-279.

[36] Zheng, J., Tan, X., Zou, C., Niu, Y., & Zhu, J. (2014, July). A cloaking-based approach to protect location privacy in location-based services. In *Proceedings of the 33rd Chinese Control Conference* (pp. 5459-5464). IEEE.

[37] Fung, E., Kellaris, G., & Papadias, D. (2015, August). Combining differential privacy and PIR for efficient strong location privacy. In *International Symposium on Spatial and Temporal Databases* (pp. 295-312). Cham: Springer International Publishing.

[38] Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2015, April). Enhancing privacy through caching in location-based services. In *2015 IEEE conference on computer communications (INFOCOM)* (pp. 1017-1025). IEEE.

[39] Kreuter, F., Haas, G. C., Keusch, F., Bähr, S., & Trappmann, M. (2020). Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. *Social Science Computer Review*, *38*(5), 533-549.

[40] Frik, A., Kim, J., Sanchez, J. R., & Ma, J. (2022, April). Users' expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-24).

[41] Sen, A. A. A., Eassa, F. B., Yamin, M., & Jambi, K. (2018). Double cache approach with wireless technology for preserving user privacy. *Wireless Communications and Mobile Computing*, *2018*.

[42] Albouq, S. S., Abi Sen, A. A., Namoun, A., Bahbouh, N. M., Alkhodre, A. B., & Alshanqiti, A. (2020). A double obfuscation approach for protecting the privacy of IoT location based applications. *IEEE Access*, *8*, 129415-129431.

[43] Adetunji, C. O., Olaniyan, O. T., Adeyomoye, O., Dare, A., Adeniyi, M. J., Alex, E., ... & Shariati, M. A. (2022). Internet of health things (IoHT) for COVID-19. *Assessing COVID-19 and Other Pandemics and Epidemics using Computational Modelling and Data Analysis*, 75-87.

[44] Sodagari, S. (2022). Trends for mobile iot crowdsourcing privacy and security in the big data era. *IEEE Transactions on Technology and Society*, *3*(3), 199-225.

[45] Zhang, C., Zhu, L., Xu, C., Du, X., & Guizani, M. (2019). A privacy-preserving traffic monitoring scheme via vehicular crowdsourcing. *Sensors*, *19*(6), 1274.

[46] da Silva, M., Viterbo, J., Bernardini, F., & Maciel, C. (2018, November). Identifying privacy functional requirements for crowdsourcing applications in smart cities. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 106-111). IEEE.

[47] Rashidi, B., Fung, C., Nguyen, A., Vu, T., & Bertino, E. (2017). Android user privacy preserving through crowdsourcing. *IEEE Transactions on Information Forensics and Security*, *13*(3), 773-787.

[48] Hassan, N. H., & Rahim, F. A. (2017). The rise of crowdsourcing using social media platforms: Security and privacy issues. *Pertanika Journal of Science & Technology*, *25*(110).

[49] Yamin, M., & Abi Sen, A. A. (2020). A new method with swapping of peers and fogs to protect user privacy in IoT applications. *IEEE Access*, *8*, 210206-210224.

****

Chapter 6 - Addressing Security, Privacy, and Reliability Issue

This chapter discusses the challenge of preserving the security and privacy of health data and ensuring its integrity. This chapter is extensive, considering that many studies consider security and privacy among the major challenges of modern technologies. It contains two draft for research papers, in addition to a conference.

The first paper (draft under review) presented a comprehensive review of blockchain, specifically consensus algorithms. It then proposed an idea for a new consensus algorithm more suitable for working with health data during pandemics, ensuring its integrity and security. The second paper (draft under review) detailed different methods of inference attacks and presented a robust approach to protecting health data within crowds, especially data from drones used during pandemics.

Finally, the chapter presented a conference paper on proposed methods for privacy protection within smart city and location-based services (LBS).

A Survey of Blockchain Consensus Algorithms with New Proposed One “PoPR”

Not published yet

Abstract

In our contemporary landscape, digital data has ascended to a paramount position, constituting the cornerstone of intelligent systems and services across diverse domains. This evolution is significantly propelled by the proliferation of smart devices, the Internet of Things (IoT), and social networking applications, engendering an unprecedented surge in data volume. Concurrently, various computing paradigms have streamlined the processing of this data, facilitating knowledge extraction and the refinement of advanced user-centric services. Amidst this digital renaissance, data grapples with a triad of pivotal challenges: security, privacy, and reliability. In response to these challenges, blockchain technology emerges as a transformative solution across a multitude of applications. This research embarks on a comprehensive exploration of blockchain, with a specific focus on consensus algorithms and their operational mechanisms. Moreover, this study introduces a novel approach grounded in historical records, designed to infer the reputation of individual nodes within the blockchain network. Through meticulous simulation and thorough discussion, we substantiate that our proposed method yields superior outcomes compared to existing alternatives, particularly in contexts reliant on crowdsourcing as a pivotal data conduit. This research thus contributes to the enriched understanding and practical advancement of blockchain technology within the realm of modern data challenges.

Keywords: Proof, Peers, Reputation, Crowdsourcing, IoT, PoW, PoS.

Introduction

The advent of blockchain technology has ushered in a formidable resolution to the multifaceted challenges of data security, privacy, and reliability. However, comprehending the mechanism through which blockchain accomplishes this feat necessitates tracing the origins of these challenges and delineating the exigency that catalyzed the inception of blockchain and its allied protective methodologies.

In the wake of exponential advancements in communication and the ubiquitous proliferation of devices and smartphones, data has ascended to the status of the quintessential bedrock upon which the functionality of smart applications across diverse domains rests. The proliferation of big data, engendered by the Internet of Things and its constellation of billions of interconnected devices, has been instrumental in deciphering user behavior and furnishing them with bespoke and adaptive services. The paradigm of smart cities harnesses an array of computing models, encompassing cloud and fog computing, to expedite the swift processing and analysis of voluminous data, thus unearthing crucial insights that embellish the quality of users' lives. Moreover, the meteoric evolution of data science, fortified by artificial intelligence algorithms, machine learning, deep learning, and data mining, has ushered in an epoch where the colossal reservoirs of stored data are meticulously harnessed to unveil a trove of user-centric information and revelations that often transcend individual knowledge itself.

At the crux of this transformative landscape lies the Internet of Things, transmuting the global milieu into an intricate interconnection of entities. Within this labyrinthine network, machinery communicates autonomously, obviating the need for human intervention. Every facet of this network is perpetually accessible from any vantage point, endowing users with the capability to control and glean real-time insights from the incessant stream of shared data. Foremost among the instrumental components of this paradigm are wireless sensor networks (WSNs), omnipresent within a myriad of smart devices. These sensors gauging the physical attributes enveloping users—ranging from temperature and pollution levels to pressure and water volume—empower this constellation with a high level of environmental awareness. Furthermore, the spectrum extends to wearable sensors, assiduously measuring vital physiological indicators, encompassing heart rate, respiration, blood pressure, body temperature, and even cerebral signals.

Additionally, radio frequency identifiers (RFID) stand as a pivotal linchpin of the Internet of Things, seamlessly integrated within smart devices or coalesced with physical entities. Furnishing objects with distinct digital identities and affording users the means to monitor, trace, and directly interact with these entities, RFID assume a cardinal role within this interconnected framework. Collectively, both WSNs and RFID imbue erstwhile inanimate entities with the quintessence of intelligence, endowing them with a unique identity, sensing ability, communicative prowess, data processing capability, and the acuity to effectuate contextually apt decisions—a manifestation akin to the multifaceted capabilities encapsulated within smartphones.

Smartphones and tablets, omnipresent in our contemporary world, stand as pivotal constituents of the Internet of Things, interwoven with network sensors and radio identifiers. These devices have orchestrated a paradigm shift, engendering a profound transformation across diverse spheres through an assortment of applications and services—exceeding billions—that pivot on data gleaned from both the Internet of Things and users via social networking and assorted electronic platforms emblematic of crowdsourcing models. Notably, the majority of these applications funnel user-generated data to cloud repositories, where it undergoes processing, knowledge extraction, behavioral scrutiny, and preemptive anomaly detection. This confluence has been instrumental in birthing an array of refined applications and nurturing the ubiquitous proliferation of intelligence across an array of domains, spanning smart health, traffic optimization, energy management, environmental stewardship, urban planning, intelligent domiciles, and myriad others.

Crowdsourcing emerges as a paradigm both ancient and contemporary, embodying the age-old dependence on user-provided data and innate human sensory perception. Concurrently, a new incarnation emerges through its fusion with data yielded by intelligent devices. This amalgamation affords crowdsourcing models a surfeit of advantages. Notably, the innovative facet resides in harnessing perceptible data, including images and sounds, to exploit analytical prowess and human evaluation capabilities—thereby endowing this phase with a gamut of automated data processing functionalities.

However, these transformative advances cast shadows, begetting challenges that pose formidable threats to the continuum of intelligent applications and services. These challenges are encapsulated within three pivotal dimensions:

Firstly, data security, a time-honored tenet whose significance has surged exponentially alongside the evolution of communication modalities and digital data. Data security is subsumed within three distinct layers of safeguarding:

1. Data Confidentiality: Shielding confidential information such as passwords, account balances, and classified military intelligence from unauthorized access.
2. Data Integrity: Preventing unauthorized alteration or tampering of data during its voyage through networks, thereby safeguarding its sanctity during transit.
3. Data Availability: Ensuring uninterrupted service provision and unfettered access to data at all times and from any location.

Secondly, data privacy, a relatively nascent construct, has evolved into an autonomous challenge. Although initially regarded as a facet of data security, the proliferation of adaptive services and the ubiquitous Internet of Things has fostered its emergence as a distinct concern. Privacy is imperiled when service providers or data custodians inadvertently or intentionally divulge sensitive personal information, surpassing the data or queries originally submitted by users. In response, several nations have enacted privacy laws—such as the European General Data Protection Regulation (GDPR), American statutes, and regulations in Saudi Arabia—to safeguard user privacy. Comparable to data security, privacy hinges upon three primary levels of safeguarding:

1. Preserving User Anonymity: For many crowdsourcing applications, preserving or abstaining from the storage of users' identities is imperative, as divulgence can facilitate malicious linkage of information to individuals, thereby compromising privacy.
2. Location Tracking: This pertains to users' geographical coordinates, particularly since an abundance of services, data, or queries engaged by users pertains to their present location. The exposure of users' whereabouts during vulnerable periods empowers attackers to glean substantial insights into user behavior, occasionally transcending mere threats to encompass physical assaults on users or their assets.
3. Profiling: This entails the compilation of comprehensive dossiers encompassing every facet of a user's existence and data, gravely jeopardizing privacy. Unauthorized access to such profiles by malicious actors lays bare an individual's private, sensitive, and confidential data.

Thirdly, data reliability, the cornerstone of smart service efficacy. The reliability is heavily required with the crowdsourcing models. Simultaneously, the susceptibility of Internet of Things entities to attacks or malfunctions engenders the generation of erroneous or manipulated data. Such discrepancies invariably impede core service performance and effectiveness, potentially exerting profound implications on user welfare. This ranges from compromised smart healthcare services to Civil Defense Department decisions in emergency scenarios predicated upon erroneous information. Consequently, data reliability attains cardinal significance, pivotal in ensuring optimal data utilization.

Conspicuously, an overarching synthesis of the preceding elements emerges, mandating a holistic integration wherein no facet can be disregarded in favor of another. Instead, priority allocation hinges on the specific application or service, as well as the user demographic. Meanwhile, disparate challenges, including data interoperability, heterogeneity, and performance, loom large in the realm of digital data. However, this study's focal point centers on the triad of data security, privacy, and reliability.

So the most important contributions of this research are

1- A reference study on Blockchain technology in protecting the triple (security, privacy, and reliability)
2- A reference study on different consensus methods and algorithms in the blockchain
3- Proposing a new consensus algorithm with a comparison table with previous algorithms according to several criteria for consensus algorithms
4- A discussion and simulation to prove the possibility of applying the proposed algorithm and a discussion of some of its special applications such as crowdsourcing with the health care during pandemics and emergencies.

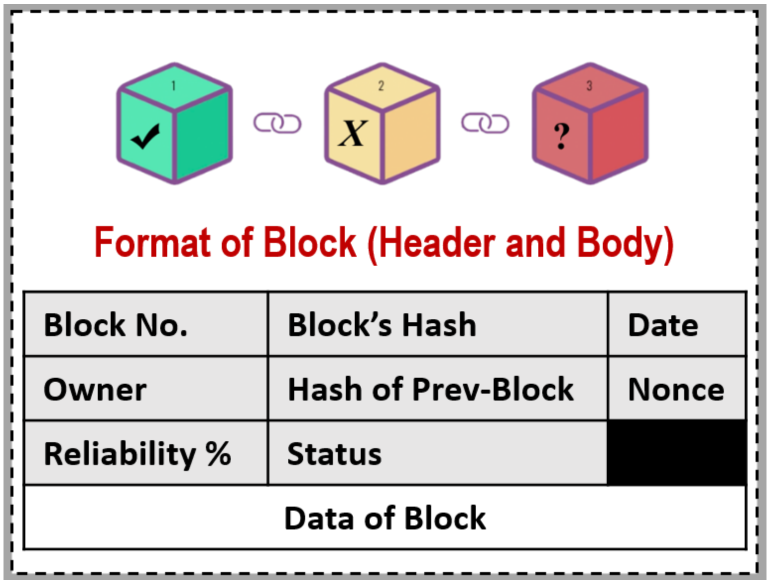
In the next section, we will discuss a brief history of the blockchain, and then in the previous works section, we will specifically discuss the different consensus algorithms in the blockchain. In the proposed algorithm section, we will discuss the proposed consensus method in detail, and in the results section, we will discuss the superiority of the proposed method over other methods in some applications, and finally a summary of what was presented during the research, in addition to some future directions.

A Brief History of Blockchain

The blockchain is a paradigm that utilizes the concept of a distributed ledger to address challenges related to the security, privacy, and reliability of data. Despite building upon previous well-known technologies such as Peer-to-Peer networks, distributed databases, and hashing functions, the concept of a chain and consensus algorithms gave birth to this new entity or model known as the blockchain. Its first true appearance was through a research paper by a Japanese researcher named Satoshi Nakamoto, who proposed an alternative digital currency and a replacement for traditional central banking. The central idea was to eliminate the need for a centralized entity, like a bank, in managing financial transfers between participants' accounts. However, what if the bank declared bankruptcy? What guarantees would exist for these individuals? Additionally, the bank levies fees on transactions between individuals, and the bank's management has access to all financial operations of each user, jeopardizing their privacy significantly. The alternative solution was simple: create a decentralized entity where all users are equal in terms of authority and power. Each participant would possess a complete copy of the database, containing the transactions or transfers between them.

No user can assault or falsely claim, as all other users have a copy of the data. The data is divided to facilitate storage, tracking, and review in blocks. A block is a set of transactions that occur over a specified time period or reach a certain size. Each block has two parts: the body, which contains operations and transactions, and the header, which holds general information about the block's content, in addition to the block number, creation date, owner, and most importantly, the Hash value of the block. This ensures that the block's data cannot be modified after its creation. To enhance security and sequence the blocks within the blockchain, the Hash of the previous block was added along with header data in each block. Thus, when calculating Hash values for a specific block, one of the inputs will be the Hash value of the previous block. This means that altering data in one block will change its Hash value, consequently affecting all subsequent block Hash values in the chain. In another sense, for an attacker to deceive users, they must first modify the value of a specific block, then alter the Hash values of all subsequent blocks in the chain. Then, they must repeat this process within a 50%+1 majority of users within the chain, ensuring that the majority of users have the same data, thus making the data they possess the correct one – a nearly impossible task. Figure 1 illustrates the form of a block and the core data present in the header, noting the addition of new information related to data reliability. Data reliability is linked to the voting percentage used in the proposed algorithm within this study (PoPR).

The blockchain also relies on the concept of the Power of Code, meaning that the distributed code held by each individual in the blockchain is what manages the chain's operations. This code is often open-source, meaning its behavior is verified by all participating users. Thus, since we depend on a distributed ledger among all nodes, any process of adding a new block to the chain, for instance, must gain acceptance from most nodes whose code validates the new block's data (Hint: usually the blockchain will be only for a specific application and processes). This is achieved through a consensus process among users. Logically, 50%+1 of the users confirm the validity of incoming data before a new block is approved. Most consensus algorithms will be outlined in the following section. If a node is not connected to the network, it becomes inactive. Upon reconnection, the node's code actively synchronizes its blockchain with the chains of adjacent nodes. (Figure 2. depicting the differences between distributed, centralized, and decentralized).



Format of Block (Header and Body)

Block No.	Block's Hash	Date
Owner	Hash of Prev-Block	Nonce
Reliability %	Status	
Data of Block		

Figure 1. Block Structure of Blockchain

Through the aforementioned characteristics and techniques of the blockchain, the blockchain has achieved the following features:

1. Decentralization and Power of Code: Each node or user within the chain possesses a copy of the database. There is no central authority that can control the data independently. Authority is equal among all participants and is managed through the application code adopted by all subscribers.
2. Transparency by Ledger: All operations are voted on, accepted, and approved by the users themselves in the chain. They are recorded in the ledger and cannot be altered except through subsequent transactions in later blocks.
3. Trust by Consensus: A new block cannot be added to the chain without majority agreement.
4. Security and Privacy by Encryption: The blockchain employs encryption to protect transmitted data. Only the code possessed by members performs decryption for verification, and non-participating users cannot access the data within the blocks on the chain.
5. Immutability by Hashing: Ensuring the absolute prevention of data modification and ensuring its integrity, as data within a block cannot be modified after approval.

Blockchain Applications

Despite the initial association of blockchain with digital currencies, its applications have extended far beyond this scope. The features of blockchain have led to the development of various applications and services that employ it to provide an enhanced level of trust and security for users. Below is a list of some of the most important blockchain applications:

1. Digital Currencies: Initial and most famous applications, such as Bitcoin, Ethereum, Dash, and others. These currencies found support from e-commerce platforms and currency exchange platforms. However, the prices of digital currencies are volatile and highly influenced by major corporate announcements or political recognition.
2. Smart Contracts: Among the most significant applications, smart contracts were the gateway for blockchain to move beyond digital currencies. They opened up applications such as property and land management, buying and selling processes, and property transfer. Business and governmental sectors

were among the primary beneficiaries of these applications. Additionally, some healthcare applications like health insurance contracts.

3. IoT Integration and Data Science: The extensive presence of Internet of Things (IoT) devices has led to many security breaches. Blockchain ensures the protection of IoT data and its various applications. Furthermore, data science requires reliable data for impactful insights. Integrating blockchain guarantees data trustworthiness and protects the results and models from alterations or breaches.
4. Secure Health Records: Blockchain ensures the protection of patient's health data, maintaining its integrity and preventing unauthorized modifications. It also facilitates controlled access to these records for both patients and authorized personnel. Sensitive services like organ donation require high-level security to prevent data tampering, a role fulfilled by blockchain.
5. Supply Chain Management: Blockchain monitors process sequences, and safeguards data integrity and its integration, particularly in specialized industries like pharmaceuticals and their supply chains.
6. Voting Systems: Simulating the consensus process, voting and polling applications prevent vote manipulation, ensuring transparency for all participants. It can also be employed in the healthcare sector for managing medical research and discoveries, especially during pandemics.
7. Governance Applications: Governments are increasingly utilizing private blockchain networks for decision-making, ensuring that influential decisions are made by multiple governmental entities. Data and decisions issued by these networks cannot be altered or manipulated.
8. Crowdsourcing: Applications such as traffic management, crowd control, disaster management, and search and rescue teams rely on the credibility of data provided by users or nodes to ensure the quality and success of the provided smart services.

However, blockchain also faces challenges that can be summarized as follows:

- **Security Attacks:** Blockchain is susceptible to specific attacks like the 51% Attack, where an entity gains control over the majority of the network and therefore its decisions. Despite the difficulty of such attacks, there have been instances of breaches, such as the breach of a currency within the Japanese Pool with over 300,000 subscribers. This led to the exploration of various consensus methods to prevent this issue. Other attack types include Selfish Attacks, Sybil Attacks, Denial-of-Service (DOS) Attacks, and Man-in-the-Middle Attacks.
- **Privacy:** Transparency is a significant advantage of blockchain, yet it can negatively affect privacy. Despite data security, all participants in the network possess accurate copies of the data, potentially compromising user privacy in some applications. Solutions have been proposed, including access control and data visibility management, but they can impact network performance. Other solutions have integrated alternative consensus methods to enhance privacy.
- **Performance:** As the blockchain size and the level of security and privacy increase, performance is negatively affected. Some large chains require significant resources that regular individuals cannot provide. Remedies like Merkle Tree representation to accelerate block number searches and multi-tiered nodes (regular nodes and master nodes) with varying resource levels have been proposed. Additionally, reducing block size and modifying consensus methods have been suggested.
- **Illicit Exploitation:** Blockchain has been exploited for illegal activities such as tax evasion and money laundering. Various consensus methods have emerged to address this problem.

From the above, it's evident that most of blockchain's challenges can be tackled through changes in consensus mechanisms or opting for different types of chains (Public, Private, Federated). Therefore, this research focuses on different consensus methods, outlining the features and drawbacks of each method or algorithm. In the following section, a comparison of different consensus methods within blockchain models will be presented.

Consensus Algorithms of the blockchain

Consensus algorithms are the collaboration and agreement of all Peers to reach a majority decision in real-time and then record it on the ledger. Consensus is, therefore, a system of validation and building trust among members, and is an important component of a blockchain to ensure its security, reliability, and resilience. Through consensus algorithms, the blockchain can provide reliability and trust between nodes, in addition to several advantages:

1. Decentralization and preventing the control of a specific entity over the network.
2. Inclusiveness of all nodes and achieving participation and cooperation between them.
3. Justice for all and equality in voting and decision-making.
4. Provide some incentives and rewards that promote good behavior and reduce malicious behavior.
5. Tolerance for errors in the event of a failure of one of the nodes or a malfunction in the network.
6. Prevent duplication and ensure that a unified decision is achieved as an outcome.
7. Ensure the security, privacy, and safety of transactions and credits.
8. Resist attacks such as 50%+1, Sybil, and Double Spending.
9. Fork challenges in the chain when there are two blocks awaiting approval at the same time.
10. Maintaining good performance even with the increase in the number of users and the number of transactions.
11. Accessibility for all network members, regardless of their hardware and computing power.
12. The type of applications compatible with the same consensus algorithm.

Due to the development of the use of the blockchain, it is used in many applications in various fields. The traditional consensus method is no longer sufficient for all these applications or different forms of blockchains (public, private, and federal). Therefore, many consensus algorithms have appeared, each with advantages and disadvantages, and each of them is more suitable for a certain type of application than other methods. The following figure 2 shows a simple visualization of the stages of the consensus process. The process begins by sending one of the nodes a request to create a new block as in A. The node begins to verify it gradually as in B, and upon completion of all active nodes, the voting percentage is calculated, and accordingly, the new block is accepted or rejected As in C.

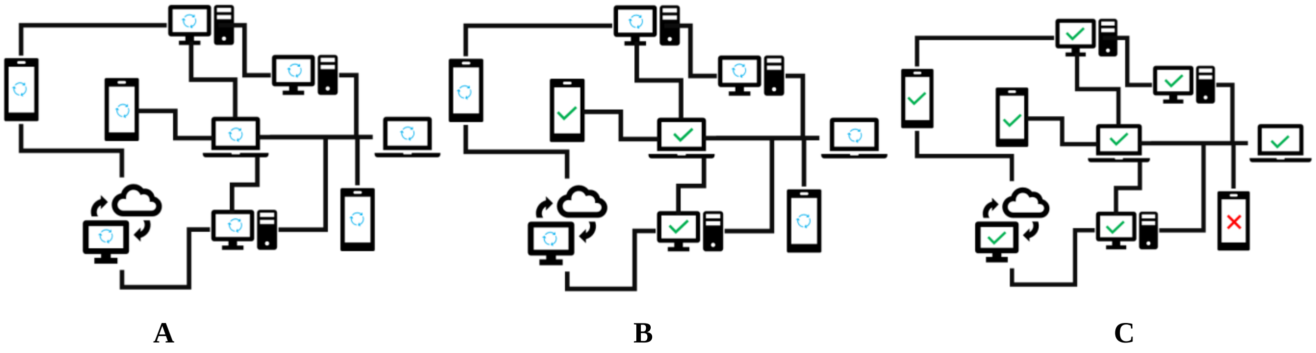


Figure 2. A general sequence of the consensus mechanism that a blockchain follows

Below is an explanation of the concept and the fundamental approach adopted by each of these consensus algorithms:

1. **Proof of Work (PoW):** PoW is the oldest consensus algorithm and was introduced with the first digital currency, Bitcoin. PoW draws its main idea from the process of mining and solving a complex mathematical puzzle that requires time and computation. The solution involves trial and error to find a random value called a Nonce composed of 16 characters. The Nonce is combined with data and the previous block's hash to create a new Hash Code. Participants in the mining process are called Miners. The fastest Miner to solve the puzzle and obtain the required Hash Code for the new block receives a reward and the block is named after them. The block is then added to the chain. This consensus process is known as Proof of Work and is commonly used in digital currency applications due to its high security, where everyone within the chain has a role in governance.
2. **Proof of Stake (PoS):** This method competes directly with PoW and is one of the most well-known alternatives. Participants are referred to as Validators instead of Miners. To become a validator, one needs to invest a certain amount of money or stake. Validators then bi a specific amount or portion of their stake (slashing) and the weight of their authentication is based on the stake. However, if a malicious block is endorsed and rejected later, a portion of the stake is deducted as a penalty. PoS is a fast consensus method that addresses PoW's challenges. Ethereum is a notable platform that has adopted this method.
3. **Delegated Proof of Stake (DPoS):** DPoS is one of the fastest consensus algorithms. It is an enhanced version of PoS that operates on the principle of delegation. A smaller number of delegates are chosen through democratic voting, similar to traditional PoS. These chosen delegates later verify the blocks.
4. **Leased Proof of Stake (LPoS):** A further enhancement of PoS. It allows nodes with limited resources to participate. Nodes with significant stakes can engage as full nodes according to the basic PoS protocol, while nodes with smaller stakes can lease their balance to the full nodes. Smaller nodes receive a portion of the rewards earned by the full nodes based on the leasing ratio.
5. **Practical Byzantine Fault Tolerance (PBFT):** Participants must agree on an effective strategy to prevent catastrophic system failures. Users confirm messages received by performing calculations and recomputing the outcome. Decisions are based on group consensus. This method features two levels of data verification (group administrators and individual voters within the group), although having administrators might not align well with public networks. Another variant focuses on tolerating a certain level of dissent to counteract a 50% + 1 attack. This involves increasing the consensus threshold to, for example, 67% + 1 instead of PoW's 50% + 1. PBFT, in its initial form, improved performance.
6. **Proof of Location (PoL):** Nodes are required to prove their authenticity by sharing their true location. This method is suitable for electronic contracts involving online stores to ensure trusted customer relationships. All nodes have equal voting power.
7. **Proof of Physical Address (PoPA):** Similar to PoL, but this time verification is based on the person's or node's credibility through their linked bank account.
8. **Proof of Importance (PoI):** A variant of PoS, where a node's importance is determined by various factors, such as contribution level, holdings, number of shares, overall balance, and more.
9. **Proof of Identity (PoID):** Each node in this approach proves its identity by sharing an encrypted part with its private key (user's secret) and attaching this part to every transaction to establish identity.
10. **Proof of Authority (PoAu):** An evolved version of PoS that requires real-world identity verification with official documents. Only verified administrators produce new blocks. This method is suitable for private networks.
11. **Proof of Stake Time (PoST):** Nodes with longer active network presence have a better chance of voting and block creation.
12. **Proof of Care (PoCe):** Activity in sharing information or network usage is taken into account. It's useful during network or application launches.

13. **Proof of Activity (PoA):** Combines PoW and PoS, where miners race to solve cryptographic puzzles in a short time. Only winners participate in block approval and reward sharing.
14. **Proof of Elapsed Time (PoET):** Participants mine at various intervals. The node with the shortest waiting time between consecutive participations in mining has the highest chance. The node then enters a quiescent state for a specified or random duration, allowing another node to participate in subsequent mining operations.
15. **Proof of Burn (PoB):** This algorithm is used to reduce the costs of PoW and PoS in terms of energy consumption. Miners are allowed to burn and destroy encrypted blocks to shrink the network's size. Burning is done by sending the block to designated addresses. Once burned, the block cannot be used. This process is effective in limiting network expansion, but its widespread adoption is limited. The higher a node's contribution to the burning process, the greater its chance of creating a new block.
16. **Proof of Capacity or Space (PoC):** Puzzles solved by each node accumulate in their storage disks. Thus, nodes with larger disk space have a better chance of block creation based on their network-contributed storage space.
17. **Proof of Weight (PoWt):** Node weight is determined by the number of coins held and the duration of holding them.
18. **Proof of History (PoH):** This aims to incorporate a time element into networks. It ensures data validity through a specific chronological timestamp associated with the data. PoH creates a historical record of transactions, proving that a specific event occurred at a specific time. A timestamp is added to each part of the transaction, with a hash calculated for each part until the transaction is complete. This creates a transparent chronological sequence of parts for each transaction, making it easy for auditors to verify the elapsed time in each verification fragment for accuracy.
19. **Directed Acyclic Graph (DAG):** Here, verification occurs between the nearest two nodes to the sending node. This lightweight algorithm is used in applications like Wireless Sensor Networks (WSNs).

Disadvantages of previous consensus algorithms and Proposed Algorithm "PoPR"

It is known that everyone strives for the success of the blockchain by involving a large number of participants. The more the number of Peers increases, the more significant the network becomes. Assigning equal voting power to all Peers, as in PoL or PoPA for instance, contradicts the required incentive condition on one hand and might contribute to increasing the impact of malicious nodes even in large networks. Relying on the computational activity and power, as in PoW or PoA, is also unjust and can lead to simi-centralization. Relying on stake, as in PoS and its enhanced versions, is considered good but is suitable only for specific applications like digital currencies.

Moreover, these methods affect the accessibility and participation criteria for everyone. Identity-based methods like PoI or PoID are not acceptable to many Peers as they expose the privacy of the contracts to potential threats and might not be suitable for applications involving sensitive data. Relying on time or weight factors like PoWt or PoET negatively affects the fairness among contracts on the one hand and impacts the network's performance on the other hand. The same applies when increasing the requirements for reliability, as in PoH. To enhance performance, some networks adopted the election of specific nodes or the selection of supervisors, as in algorithms based on delegation principles or relying on a specific number of most important supervisors, similar to certain versions of the PBFT algorithm.

To address the aforementioned challenges, the "Proof of Peer Reputation (PoPR)" algorithm is proposed, significantly boosting the functionality of public networks and thus enhancing key blockchain concepts. The significance of the proposed algorithm **PoPR** lies in its ability to integrate with any previous consensus algorithm to enhance its operational mechanism.

The idea of the algorithm is that all contracts have the right to vote initially. However, the voting weight of a Peer continuously increases and decreases after each voting operation based on the credibility of the participant. In other words, a participant whose voting aligns with the final result of the block gains an additional point, otherwise, they lose a point. Consequently, over time, participants accumulate points that reflect their credibility and their level of activity within the block.

The PoPR algorithm reflects the code specific to the proposed algorithm. This approach can also integrate with one of the previous methods to provide additional enhancements.

The PoPR algorithm achieves several advantages compared to other algorithms:

1. Energy efficiency, as it doesn't require solving complex puzzles that demand a time margin.
2. Speed in performance due to the absence of time delays.
3. Blocks are written under the name of the creator if their votes exceed a certain threshold.
4. Depending on the application's nature and sensitivity, an acceptable voting percentage can be adopted, providing error tolerance and resistance to attacks.
5. Any user can participate in the voting process without specific requirements, achieving inclusivity and fairness.
6. Users can use pseudonyms, enhancing user privacy.
7. The final Hash value is recalculated during the hashing process to solve the Fork problem, linking with the Previous Hash while remaining unread.
8. Applicability in various applications or integration with other algorithms, making it suitable for a wide range of applications.

```
//Alogrithm1 - Algorithm of PoPR
Double Reliability_Rate PoPR(New_Block, Owner_ID)
Start
        Broadcast (Chain.get_all_Active_Peers());
        Reliability_Rate = get_total_acceptance / Peers.Count ;
        If (Reliability_Rate > Threshold)
          Block = Broadcust (“Add”, Chain.get_all_Active_Peers(), New_Block, Owner_ID, Chain)
          Foreach Peer = Chain.get_all_Active_Peers() do
                  Decision = Peer.Get_decision(Block.ID)
                  If (Decision == True)
                          Peer.Reputation++;
                  Else
                          Peer.Reputation--;
          End For
          Broadcust(“Update Reputation”, Chain.get_all_Active.Peers(), Peers.Reputations);
        End If
End
```

Blockchain Challenges and Open Issues

Blockchain still suffers from open challenges today. Unfortunately, some of the features of consensus algorithms in particular, and the features of blockchain in general, such as immutability, stability, trust, transparency, audibility, and encryption, cause some challenges and weaknesses. These challenges can be summarized in the following points:

- The inability to delete data: Although it is an advantage, on the one hand, to ensure non-denial, on the other hand, it contributes to the inflation of the chain significantly, and this affects the performance of the system as a whole. The PoB algorithm provided a partial solution to the problem by enabling the burning of some blocks, but the deletion here of the entire block and not a transfer within it. Thus, there is no integrated method for deleting a block or part of a block and re-updating the chain in a way that does not affect the principles of the blockchain.

- Indexing and searching within the big data in the chain: Although some solutions are presented, such as the Merkel tree, it is only for searching for the block number and not the content of the block. Therefore, a method must be worked on to ensure a quick indexing and search process within the blockchain. One of the proposed solutions that we will work on in the upcoming works is to create a lightweight chain parallel to the main chain. The proposed chain in each corresponding block contains only keywords without coding instead of storing the entire block data.
- Privacy: The transparency feature in the blockchain contradicts the concept of user privacy and decentralized systems. Using encryption alone is not a solution to the privacy problem, and innovative ways must be worked on to achieve this, such as proposing a mechanism to manage pseudonyms within the chain without affecting the properties of the blockchain.
- Implementation cost: Blockchain applications are expensive, especially in the establishment and deployment phase in the case of public chains. Private chains can partially solve the problem, especially in government applications.
- Ownership of the block is not for the data owner: This problem needs to change some of the principles of creating the block. It can be easy in the case of private chains, but in public it requires many modifications, for example, a small block size, using cryptographic aliases, adding a statement in the block indicating the winner of the voting process instead of naming the block by his name as the owner.
- The problem of the fork in the chain when there are two blocks awaiting approval at the same time still needs a radical solution in the mechanism of blockchain work to prevent it.
- The security of the network and its immunity against attacks also requires the provision of smarter solutions that adapt to the nature of the network and the application used for it.

In short, as blockchain technology and its applications continue to evolve, we can work in the future on new consensus mechanisms that are more secure, applicable, and effective. The following is a comparison table of consensus algorithms in the blockchain based on their level of achievement for each criterion of consensus algorithms that must be met.

Table 1. Comparison among Blockchain Consensus Algorithms

Algorithm	**Decentralize**	**Preserving privacy**	**Equal voting**	**Providing award**	**Fault tolerance**	**Attacks resistance**	**performance**	**Accessiblity**	**Type of supported apps**
PoW	1	0.5	0.5	1	0.5	0.5	0	0	0
PoS	0.5	0.5	0	1	0	0.5	1	0	0.5
DPoS	0.5	0.5	0.5	1	0	0.5	1	0.5	0.5
LPoS	0.5	0.5	0.5	1	0	0.5	1	0.5	0.5
PBFT	0.5	0.5	0	1	1	0.5	0.5	1	0
PoL	1	0	1	0	1	0.5	0	1	0.5
PoPA	1	0	1	0	1	0.5	0	1	0.5
PoID	1	0	1	0	1	0.5	0	1	0.5

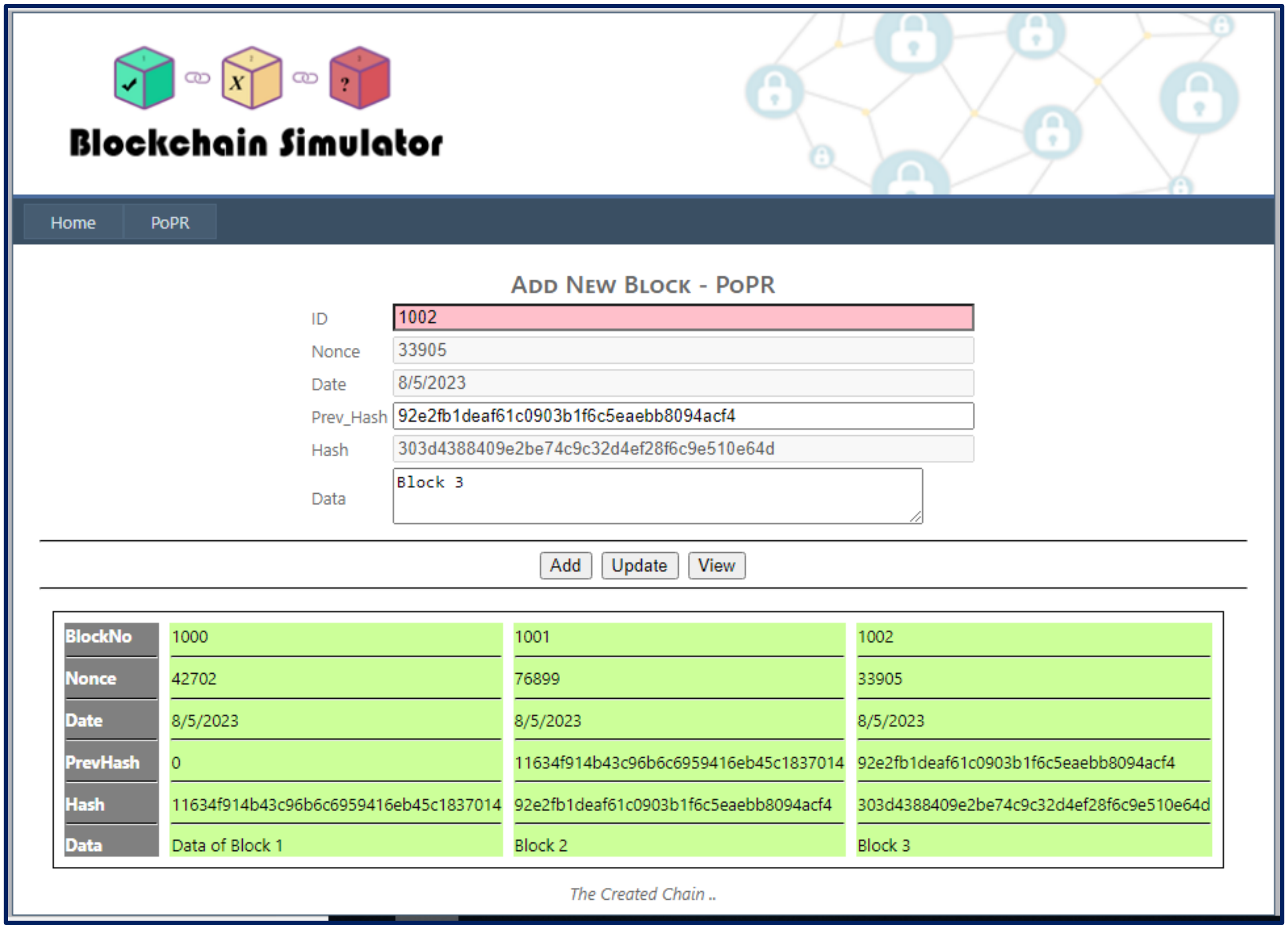
PoAU	1	0	1	0	1	0.5	0	1	0.5
PoST	1	0.5	0.5	1	0	0.5	0	0	0
PoCe	1	0.5	0.5	1	0	0.5	0	0	0
PoA	1	0.5	0.5	1	0	0.5	0.5	0	0
PoET	1	0.5	0.5	1	0	0.5	0	0	0
PoB	1	0.5	0.5	1	0	0.5	0.5	0	0
PoC	1	0.5	0.5	1	0	0.5	0	0	0
PoWt	1	0	1	0	1	0.5	0	1	0.5
PoH	1	0	0.5	1	0	0.5	0	1	0
DAG	0	0.5	1	0	0	0	1	0	0
PoPR	1	0.5	1	1	1	0.5	1	1	1

Discussion about PoPR Algorithm Usage and Implementations

Most consensus algorithms have been used in financial transactions (digital coins) or electronic contracts, or some tracking applications, such as supply chains, in addition to some government applications that have begun to rely on the concept of blockchain, but in private network applications. Private networks depend on a limited number of master nodes that make the decision rather than relying on a central authority. However, with the advent of new data collection models such as the Internet of Things and crowd-sourcing, the need for new uses of the blockchain has emerged to verify data validation and ensure its reliability, especially since many smart applications depend on the accuracy of the data itself. Also, in the event of pandemics and disasters, the importance and accuracy of the collected data increases, which must be verified in real-time. Blockchain can also play a very important role in these cases, especially since the accuracy of data in such applications is directly related to people's lives.

It is not useful in such applications to rely on algorithms that require a long time, such as PoW, and it is also not possible to guarantee the presence of master nodes in all places to be monitored, as in private networks or those that use PoS. In such cases and previous applications, it is possible to benefit from PoPR, where consensus and inclusiveness can express the degree of reliability of the data on the one hand, and the participation of all members means covering almost all regions on the other hand. Also, the degree of reliability of each node or person in transferring information previously will affect the credibility of the decision in emergencies, meaning that even if some malicious nodes try to influence the decision negatively, they will not be able to because their impact coefficient will be very low compared to nodes with high confidence during previous periods.

Finally, to prove the possibility of applying the proposed algorithm, we built a simulator using Asp.net C# language on the Visual Studio .NET platform. The simulation shows the chain formation mechanism. The process begins with the mechanism of creating a new block with the name of the generating node in case the vote is successful. The proposed platform also shows that any modification in the chain will be detected immediately and will extend its impact on the entire chain, in addition to verifying the synchronization between the chains in individuals. Figure 3 shows the state of the chain at one of the nodes without any modification to the data, while Figure 4 shows the state of the chain after one of the nodes attempts to modify one of the blocks within it.



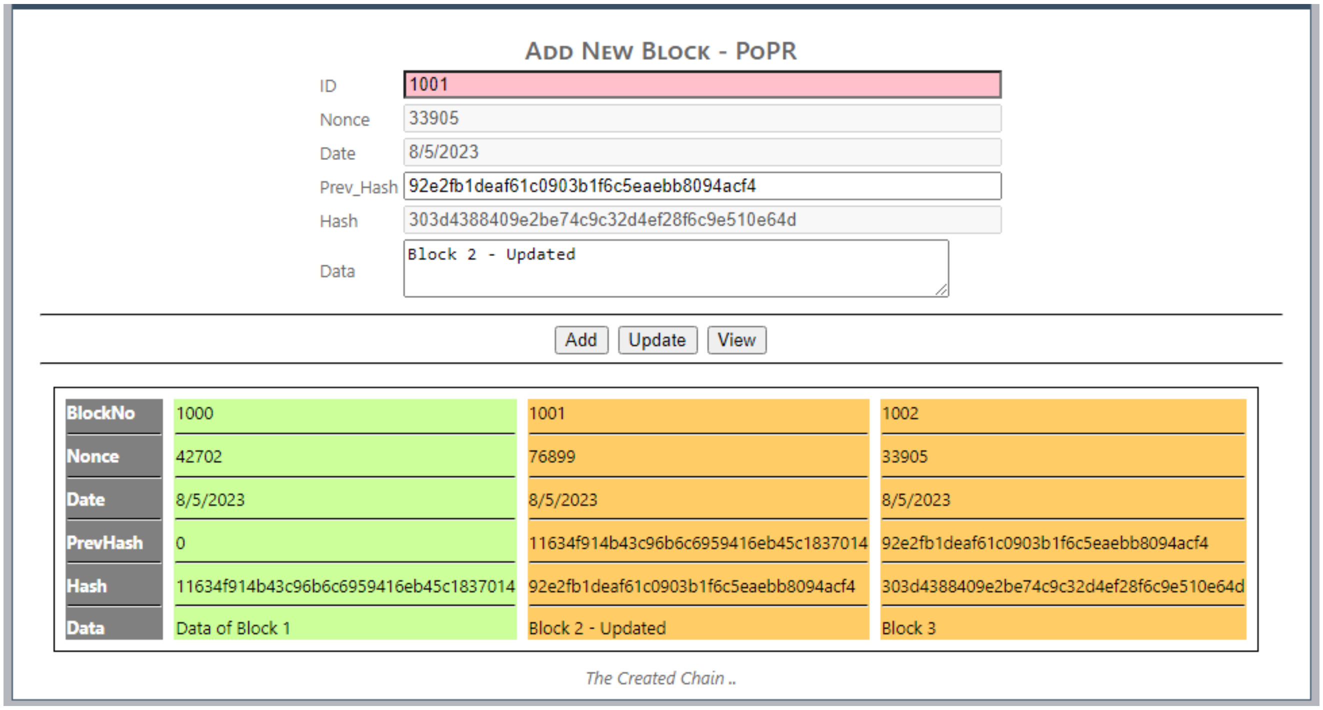
ADD NEW BLOCK - POPR

ID: 1002
Nonce: 33905
Date: 8/5/2023
Prev_Hash: 92e2fb1deaf61c0903b1f6c5eaebb8094acf4
Hash: 303d4388409e2be74c9c32d4ef28f6c9e510e64d
Data: Block 3

BlockNo	1000	1001	1002
Nonce	42702	76899	33905
Date	8/5/2023	8/5/2023	8/5/2023
PrevHash	0	11634f914b43c96b6c6959416eb45c1837014	92e2fb1deaf61c0903b1f6c5eaebb8094acf4
Hash	11634f914b43c96b6c6959416eb45c1837014	92e2fb1deaf61c0903b1f6c5eaebb8094acf4	303d4388409e2be74c9c32d4ef28f6c9e510e64d
Data	Data of Block 1	Block 2	Block 3

The Created Chain ..

Figure 3. The Chain with Normal and Valid Case



ADD NEW BLOCK - POPR

ID: 1001
Nonce: 33905
Date: 8/5/2023
Prev_Hash: 92e2fb1deaf61c0903b1f6c5eaebb8094acf4
Hash: 303d4388409e2be74c9c32d4ef28f6c9e510e64d
Data: Block 2 - Updated

BlockNo	1000	1001	1002
Nonce	42702	76899	33905
Date	8/5/2023	8/5/2023	8/5/2023
PrevHash	0	11634f914b43c96b6c6959416eb45c1837014	92e2fb1deaf61c0903b1f6c5eaebb8094acf4
Hash	11634f914b43c96b6c6959416eb45c1837014	92e2fb1deaf61c0903b1f6c5eaebb8094acf4	303d4388409e2be74c9c32d4ef28f6c9e510e64d
Data	Data of Block 1	Block 2 - Updated	Block 3

The Created Chain ..

Figure 4. The chain after update the block 2

Conclusion

This research provides an exhaustive exploration of blockchain technology, encompassing its defining features, characteristics, applications, and associated challenges. Nevertheless, its distinctiveness lies in its focus on a comparison of diverse consensus algorithms and the criteria employed for this purpose. Subsequently, the study furnishes a comparative analysis, tabulating prevailing algorithms alongside a novel consensus algorithm named PoPR. The underlying concept of the proposed algorithm is elucidated, highlighting its differentiating factors from established counterparts. Furthermore, the research underscores recent contexts where the proposed algorithm could wield a substantial influence. Towards its culmination, the research delves into the broader challenges confronted by blockchain applications, outlining avenues for prospective solutions. A pivotal component of this study involves the presentation of a simple simulator, employed to substantiate the viability of implementing the proposed algorithm.

References

[1] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.

[2] Balaji, S., Nathani, K., & Santhakumar, R. (2019). IoT technology, applications and challenges: a contemporary survey. *Wireless personal communications*, *108*, 363-388.

[3] Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. *Journal of Internet Services and Applications*, *6*(1), 1-15.

[4] Soomro, K., Bhutta, M. N. M., Khan, Z., & Tahir, M. A. (2019). Smart city big data analytics: An advanced review. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *9*(5), e1319.

[5] Allam, Z., & Dhunny, Z. A. (2019). On big data, artificial intelligence and smart cities. *Cities*, *89*, 80-91.

[6] Amodu, O. A., & Othman, M. (2018). Machine-to-machine communication: An overview of opportunities. *Computer Networks*, *145*, 255-2.

[7] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G. (2020). Applications of wireless sensor networks: an up-to-date survey. *Applied system innovation*, *3*(1), 14.

[8] Costa, F., Genovesi, S., Borgese, M., Michel, A., Dicandia, F. A., & Manara, G. (2021). A review of RFID sensors, the new frontier of internet of things. *Sensors*, *21*(9), 3138.

[9] Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A review of IoT sensing applications and challenges using RFID and wireless sensor networks. *Sensors*, *20*(9), 2495.

[10] Latif, M. Z., Hussain, I., Saeed, R., Qureshi, M. A., & Maqsood, U. (2019). Use of smart phones and social media in medical education: trends, advantages, challenges and barriers. *Acta informatica medica*, *27*(2), 133.

[11] Grossi, M. (2019). A sensor-centric survey on the development of smartphone measurement and sensing systems. *Measurement*, *135*, 572.

[12] Lohiya, R., & Thakkar, A. (2020). Application domains, evaluation data sets, and research challenges of IoT: A Systematic Review. *IEEE Internet of Things Journal*, *8*(11), 8774-8798.

[13] Niu, H., & Silva, E. A. (2020). Crowdsourced data mining for urban activity: Review of data sources, applications, and methods. *Journal of Urban Planning and Development*, *146*(2), 04020007.

[14] Lin, Y., & Li, R. (2020). Real-time traffic accidents post-impact prediction: Based on crowdsourcing data. *Accident Analysis & Prevention*, *145*, 105696.

[15] Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

[16] Daniel, W. K. (2014, April). Challenges on privacy and reliability in cloud computing security. In *2014 international conference on information science, electronics and electrical engineering* (Vol. 2, pp. 1181-1187). IEEE.

[17] Kamin, D. A. (2017). *Exploring security, privacy, and reliability strategies to enable the adoption of IoT* (Doctoral dissertation, Walden University).

[18] Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, *10*(3).

[19] Unigwe, M. (2022). *The Views of Information Security Professionals Toward Information Security Objectives: Confidentiality, Integrity, and Availability Triad* (Doctoral dissertation, Trident University International).

[20] De Capitani Di Vimercati, S., Foresti, S., Livraga, G., & Samarati, P. (2012). Data privacy: Definitions and techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *20*(06), 793-817.

[21] Rustad, M. L., & Koenig, T. H. (2019). Towards a global data privacy standard. *Fla. L. Rev.*, *71*, 365.

[22] [19] Abi Sen, A. A., & Basahel, A. M. (2019, March). A comparative study between security and privacy. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1282-1286). IEEE.

[23] Shihab, L. A. (2020). Technological tools for data security in the treatment of data reliability in big data environments. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, *11*(9), 1-13.

[24] Angelou, N., & Sjöholm, M. (2022). Data Reliability Enhancement for Wind-Turbine-Mounted Lidars. *Remote Sensing*, *14*(13), 3225.

[25] Albouq, S. S., Abi Sen, A. A., Almashf, N., Yamin, M., Alshanqiti, A., & Bahbouh, N. M. (2022). A survey of interoperability challenges and solutions for dealing with them in IoT environment. *IEEE Access*, *10*, 36416-36428.

[26] Rakovic, V., Karamachoski, J., Atanasovski, V., & Gavrilovska, L. (2019). Blockchain paradigm and internet of things. *Wireless Personal Communications*, *106*, 219-235.

[27] Vaassen, E. H. (2020). Blockchain and other distributed ledgers. In *The Routledge Companion to Managing Digital Outsourcing* (pp. 300-318). Routledge.

[28] Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary?. *Available at SSRN 2709713*.

[29] Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349-371). Academic Press.

[30] Faria, C., & Correia, M. (2019, July). BlockSim: blockchain simulator. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 439-446). IEEE.

[31] Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. *International Journal of Computer Network & Information Security*, *13*(2), 1-15.

[32] Wang, M., Duan, M., & Zhu, J. (2018, May). Research on the security criteria of hash functions in the blockchain. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts* (pp. 47-55).

[33] Semenzin, S. (2023). 'Blockchain for good': Exploring the notion of social good inside the blockchain scene. *Big Data & Society*, *10*(2), 20539517231205479.

[34] Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT express*, *6*(2), 93-97.

[35] Fu, X., Wang, H., & Shi, P. (2021). A survey of Blockchain consensus algorithms: mechanism, design and applications. *Science China Information Sciences*, *64*, 1-15.

[36] Stephen, R., & Alex, A. (2018, August). A review on blockchain security. In *IOP conference series: materials science and engineering* (Vol. 396, No. 1, p. 012030). IOP Publishing.

[37] Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134-117151.

[38] Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1972-1986.

[39] Rajasekaran, A. S., Azees, M., & Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, *52*, 102039.

[40] Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications–usage in different domains. *Ieee Access*, *7*, 45360-45381.

[41] Schedlbauer, M., & Wagner, K. (2018). Blockchain beyond digital currencies-a structured literature review on blockchain applications. *Available at SSRN 3298435*.

[42] Mohanta, B. K., Panda, S. S., & Jena, D. (2018, July). An overview of smart contract and use cases in blockchain technology. In *2018 9th international conference on computing, communication and networking technologies (ICCCNT)* (pp. 1-4). IEEE.

[43] Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, *1*, 1-13.

[44] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of network and computer applications*, *135*, 62-75.

[45] Blossey, G., Eisenhardt, J., & Hahn, G. (2019). Blockchain technology in supply chain management: An application perspective.

[46] Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR)*, *54*(3), 1-28.

[47] Grover, B. A., Chaudhary, B., Rajput, N. K., & Dukiya, O. (2021). Blockchain and governance: theory, applications and challenges. *Blockchain for Business: How It Works and Creates Value*, 113-139.

[48] Ma, Y., Sun, Y., Lei, Y., Qin, N., & Lu, J. (2020). A survey of blockchain technology on security, privacy, and trust in crowdsourcing services. *World Wide Web*, *23*, 393-419.

[49] Zheng, X., Zhu, Y., & Si, X. (2019). A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Applied Sciences*, *9*(22), 4731.

[50] Swarnkar, M., Bhadoria, R. S., & Sharma, N. (2021). Security, privacy, trust management and performance optimization of blockchain technology. *Applications of Blockchain in Healthcare*, 69-92.

[51] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C. A., Nyang, D., & Mohaisen, A. (2019). Overview of attack surfaces in blockchain. *Blockchain for distributed systems security*, 51-66.

[52] Ferdous, M. S., Chowdhury, M. J. M., Hoque, M. A., & Colman, A. (2020). Blockchain consensus algorithms: A survey. *arXiv preprint arXiv:2001.07091*.

[53] Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, *14*(1).

[54] Sharkey, S., & Tewari, H. (2019, April). Alt-PoW: an alternative proof-of-work mechanism. In *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)* (pp. 11-18). IEEE.

[55] Gaži, P., Kiayias, A., & Zindros, D. (2019, May). Proof-of-stake sidechains. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 139-156). IEEE.

[56] Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, *10*(2).

[57] Begicheva, A., & Kofman, A. (2018). Fair proof of stake. *Fair Block Delay Distribution, in Proof-of-Stake Project; Waves Platform: Moscow*.

[58] Chen, Y., Li, M., Zhu, X., Fang, K., Ren, Q., Guo, T., ... & Deng, Y. (2022). An improved algorithm for practical byzantine fault tolerance to large-scale consortium chain. *Information Processing & Management*, *59*(2), 102884.

[59] Wu, W., Liu, E., Gong, X., & Wang, R. (2020, June). Blockchain based zero-knowledge proof of location in iot. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

[60] Hasan, H. R., & Salah, K. (2018). Blockchain-based solution for proof of delivery of physical assets. In *Blockchain–ICBC 2018: First International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 1* (pp. 139-152). Springer International Publishing.

[61] Xiao, B., Jin, C., Li, Z., Zhu, B., Li, X., & Wang, D. (2021, December). Proof of Importance: A Consensus Algorithm for Importance Based on Dynamic Authorization. In *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*.

[62] Ebinazer, S. E., Savarimuthu, N., & Mary, S. B. S. (2021, September). PoI: Proof of Identity and PoDI: Proof of Data Integrity for Secure Data Deduplication in the Cloud. In *2021 2nd International Conference on Advances in Computing, Communication, Embedded and Secure Systems (ACCESS)* (pp. 319-323). IEEE.

[63] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In *CEUR workshop proceedings* (Vol. 2058). CEUR-WS.

[64] Hartl, A., Zseby, T., & Fabini, J. (2019, July). Beaconblocks: Augmenting proof-of-stake with on-chain time synchronization. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 353-360). IEEE.

[65] Howson, P., Oakes, S., Baynham-Herd, Z., & Swords, J. (2019). Cryptocarbon: The promises and pitfalls of forest protection on a blockchain. *Geoforum*, *100*, 1-9.

[66] Wang, D., Jin, C., Li, H., & Perkowski, M. (2020). Proof of activity consensus algorithm based on credit reward mechanism. In *Web Information Systems and Applications: 17th International Conference, WISA 2020, Guangzhou, China, September 23–25, 2020, Proceedings 17* (pp. 618-628). Springer International Publishing.

[67] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., & Shi, W. (2017). On security analysis of proof-of-elapsed-time (poet). In *Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19* (pp. 282-297). Springer International Publishing.

[68] Menon, A. A., Saranya, T., Sureshbabu, S., & Mahesh, A. S. (2022). A Comparatıve Analysis on Three Consensus Algorithms: Proof of Burn, Proof of Elapsed Time, Proof of Authority. In *Computer Networks and Inventive Communication Technologies: Proceedings of Fourth ICCNCT 2021* (pp. 369-383). Springer Singapore.

[69] Park, S., Kwon, A., Fuchsbauer, G., Gaži, P., Alwen, J., & Pietrzak, K. (2018). Spacemint: A cryptocurrency based on proofs of space. In *Financial Cryptography and Data Security: 22nd International Conference, FC 2018, Nieuwpoort, Curaçao, February 26–March 2, 2018, Revised Selected Papers 22* (pp. 480-499). Springer Berlin Heidelberg.

[70] Andrey, A., & Petr, C. (2019, September). Review of existing consensus algorithms blockchain. In *2019 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)* (pp. 124-127). IEEE.

[71] Abdo, A., Wu, G., & Abu-Ghazaleh, N. (2021, July). Secure ramp merging using blockchain. In *2021 IEEE Intelligent Vehicles Symposium (IV)* (pp. 401-408). IEEE.

[72] Cao, M., Zhang, L., & Cao, B. (2021). Toward on-device federated learning: A direct acyclic graph-based blockchain approach. *IEEE Transactions on Neural Networks and Learning Systems*.

[73] Wang, Q., Huang, J., Wang, S., Chen, Y., Zhang, P., & He, L. (2020). A comparative study of blockchain consensus algorithms. In *Journal of Physics: Conference Series* (Vol. 1437, No. 1, p. 012007). IOP Publishing.

[74] Sharma, K., & Jain, D. (2019, July). Consensus algorithms in blockchain technology: A survey. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

[75] Bamakan, S. M. H., Motavali, A., & Bondarti, A. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, *154*, 113385.

[76] Sharma, V., & Lal, N. (2020). A novel comparison of consensus algorithms in blockchain. *Advances and Applications in Mathematical Sciences*, *20*(1), 1-13.

[77] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *International Journal of Information Technology*, *10*, 189-200.

A Shuffling-Steganography Algorithm to Protect Data of IoT and Drone Applications

Alkodre, A. B., Bahbouh, N. M., Sendra, S., Abi Sen, A. A., Alsaawy, Y., Alqahtany, S. S., ... & Almoamari, H. (2024). A Shuffling-Steganography Algorithm to Protect Data of Drone Applications. Computers, Materials & Continua.

Abstract

The widespread utilization of drones has become a prevailing phenomenon across a multitude of smart and sensitive applications, encompassing domains such as security, military operations, traffic management, healthcare services, and other smart city applications. During disasters, drones can play a pivotal role in accessing hard-to-reach areas, collecting data, and expediting the delivery of crucial supplies. Regrettably, the data transmitted by drones can be vulnerable to hacking and espionage attempts, thereby yielding grave repercussions that might adversely impact the beneficiaries of such services. Steganography proffers an effective solution to this challenge, furnishing a robust data encryption mechanism alongside hiding data within inconspicuous information before transmission. Steganography serves to obliterate doubts surrounding transmitted data, thwarting a majority of potential attacks. This research introduces a novel approach to Steganography, termed the "Shuffling Steganography Approach (SSA)" predicated on five fundamental stages: encryption, division of encrypted data, hiding a small part within text utilizing a proposed method depends on commas, merging or blending parts, and ultimately, hiding within image based on simple proposed technique also. Through rigorous investigation and comparative analysis with existing methods, the proposed approach demonstrates superiority across various pertinent criteria encompassing levels of imperceptibility, robustness, capacity of secret message size, resistance to diverse attacks, and multilingual support.

Introduction

Many smart applications have come to rely extensively on drones to perform novel tasks across various domains. Notably, in smart transportation applications, drones are primarily utilized for data collection in hard-to-reach areas, particularly in cases of severe congestion. Similarly, in crowd management applications, drones are employed to read sensors distributed in remote locations or to rapidly disseminate alerts. In the security and military sectors, these drones have been adopted by numerous countries for monitoring checkpoints and border crossings, thereby reducing expenditures [1-2].

Moreover, the utilization of drones has proliferated widely in warfare and military sectors [3]. Within medical applications, drones have played a pivotal role in expediting the delivery of medical supplies to inaccessible regions, outpacing traditional emergency response teams. Additionally, they have facilitated the transportation of samples and minimized the need for direct contact during the spread of epidemics like COVID-19 [4]. In the realm of agriculture, drones are employed for pesticide spraying and crop monitoring [5]. In the business sphere, many companies now utilize drones for product delivery. Furthermore, drones have found application in the entertainment, advertising, and event management industries, creating illuminated displays and various others [6].

Collectively, these applications underscore the significant role that drones fulfill, providing a diverse array of services. Most of these services have emerged in recent years, coinciding with significant technological and communication advancements, particularly following the advent of the Internet of Things [7].

However, unfortunately, as the significance of drones' applications grow—especially considering critical applications or those linked to human lives, safety, and security—numerous challenges have arisen. Among these challenges, the most pressing is protecting the security and privacy of information transmitted through these drones to command centers or stations. In addition to these challenges, there is the necessity to establish suitable infrastructures for managing these drones and their applications [8-9].

Data security and privacy have become paramount requirements across all applications, but their importance escalates with drones due to the sensitive nature of the services they provide. It is expected that in any given application, many attackers and adversaries will attempt to steal data transmitted via drones and breach their security [10]. Indeed, relying on traditional encryption methods is no longer effective in ensuring provided services' security [11-12]. This is especially true given the evolution of attackers' skills and capabilities, as well as the availability of robust resources for executing penetration attacks or breaking the encryption used. Hence, there is a need to rely on more effective protection methods, such as Steganography [13].

Steganography primarily relies on hiding secret data within a carrier of seemingly unrelated information, known as the Cover. The cover can take the form of text, images, videos, or maps [14]. The carrier, loaded with the secret data, is sent to the target without arousing suspicions from potential attackers. Therefore, the strength of the steganography technique employed is measured by the level of doubt it avoids. Moreover, steganography methods integrate with encryption algorithms to hide secret data by encoding it within the cover. Consequently, even if an attacker is aware of the existence of confidential information within the transmitted data, they would face significant difficulty in accessing, detecting, or reconstructing this information [15]. There are numerous methods for employing steganography, varying in the level of protection they offer, the rate of secret data they can hide, their resistance to attacks or interference attempts, and their overall performance [16]. Figure 1. shows the main used steps in Steganography.

Steganography or Data hiding techniques are crucial for securing information in various communication channels, including text, video, and images. While text-based hiding offers superior performance but limited protection, video-based hiding is currently preferred but sacrifices performance. Image-based hiding is considered the safest and most efficient option. Additionally, the choice of hiding method is influenced by the data size to be hidden. Some hiding methods are resistant to changes in the cover, providing a limited impact on the encrypted message, while others can destroy it [17].

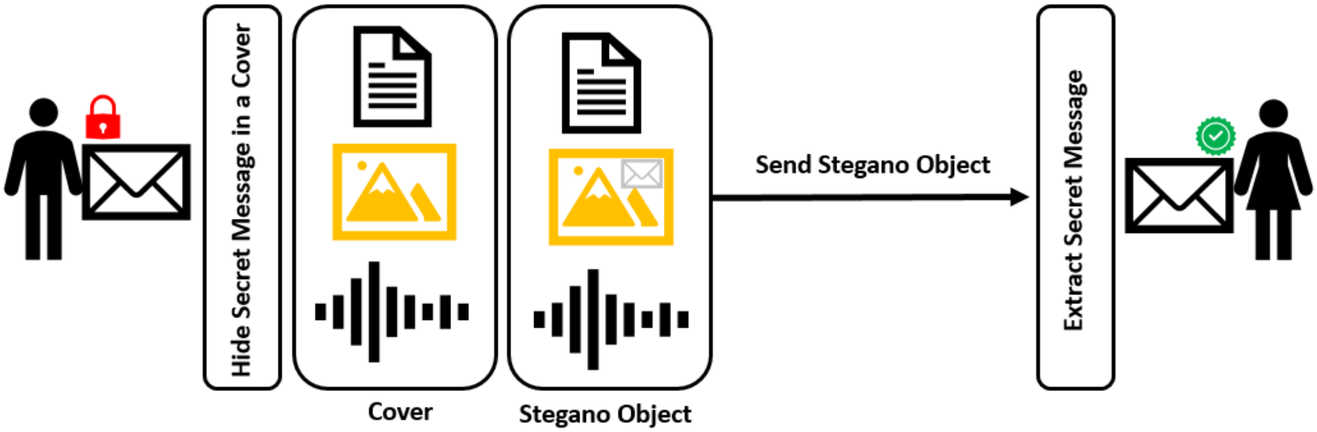


Figure 1. Main Steps of Steganography

Despite numerous existing techniques for steganography, the need for new methods persists, given the unique advantages and disadvantages of each approach [18]. This research introduces an innovative approach based on data dividing, mixing, and merging. In addition, the proposed approach uses the text hiding method for part of data, and the image hiding as another layer. So, the contributions of this research can be summarized as follows:

Proposing a new steganography approach included different protection techniques to protect data transmitted by drones.

Introducing a new method (text-hiding) for hiding portions of encrypted data within a textual cover.

Present a novel method (image-hiding) for hiding encrypted data within an image cover.

Demonstrating the effectiveness, security, and robustness of the proposed approach compared to other methods.

In the following section, we will review prominent Steganography techniques, both text-based and image-based, and provide a table summarizing the features and drawbacks of each method. Subsequently, we will detail the proposed approach and the associated algorithms. The results section will showcase the interfaces of the implemented application of the proposed approach and discuss its superiority over other methods. Finally, we will conclude with a summary of the research and future directions.

Previous works

This section provides an overview of the most significant methods employed in steganography within text and image mediums. We will categorize previous research into three main sections: text-based hiding techniques, image-based hiding techniques, and hybrid ones that involve treating text as an image (merging both).

Text-Based Steganography Techniques [19-20]:

We will focus on the Arabic language, which presents unique challenges due to characteristics such as script shaping, diacritics, and morphology, making it more suitable for hiding data.

- **KASHIDA [21]:** It is a technique where a character causes an extension in the width of the letter and can be connected to any letter in the Arabic language. It has been employed to conceal some data within the text. For example, the word "مدرسة" (school) would appear as "مـدرسـة," where two additional Kashida characters have been added, one after the letter "م" and the other after the letter "س." The proposed method involves selecting specific characters, and then a Kashida character is added after one of these selected characters if the value is "1," and it is not added after the character if the value is "0." It is known that the data being stored is converted into bits, meaning a sequence of zeros and ones. This method is characterized by being user-friendly but also susceptible to detection and intrusion.

- **Letter Encode [22]**: This method relies on the fact that some characters in certain languages, such as Arabic, have different forms, and each form is used in a specific position within a word (at the beginning, middle, or end of the word). For example, at the beginning of a word, it appears as "مـ," in the middle as "ـمـ," and at the end as "ـم" or "م." Consequently, this method involves altering the character code based on the data to be stored. During the decoding process, the character's position is matched with its corresponding code; if they match, it is considered as "1," and if they differ, it is considered as "0." Agreement on specific characters and their positions is necessary, but some text editors may display the character inappropriately, resulting in a noticeable discrepancy. In the English language, capitalization can be used similarly for the same character.

- **Spaces [23]**: A straightforward technique involving the duplication or manipulation of spaces within text based on the data to be hidden. However, it becomes noticeable in large datasets and can be easily detected.

- **ZWJ and ZWNJ [24]:** These are special characters added to text without any visible appearance. While difficult to detect visually, they increase text size and can be revealed by comparing the text's size before and after hiding.

- **Diacritics [25]**: Leveraging diacritics used in languages like Arabic, this method replaces certain diacritics with others based on the data to be hidden. However, it is susceptible to linguistic analysis and may reveal hidden data.

- **HAMZAT [26]**: This method focuses on keeping or hiding the Hamza on the Arabic letter "أ" or "إ" by replacing it with "ا." It requires an agreement on specific mappings between a sender and receiver and is suitable for hiding limited data.

Image-Based Steganography Techniques [27]:

There are two main types to hide data within images: the first type relies on the Spatial Domain, while the second type relies on the Frequency Domain [28]. The first type, Spatial Domain, involves modifying the least significant bits (LSB) of the image pixels. In other words, the pixel values, ranging from 0 to 255, are altered by one degree. This modification affects the pixel's color intensity by only one degree out of 256, making it virtually imperceptible to the human eye [29].

Figure 2 illustrates the fundamental concept of the LSB technique. This method is considered effective and easy to implement but is criticized for its susceptibility to changes that may occur during image compression or other editing processes during transmission. In terms of security, several enhanced techniques have been proposed. In [30], the method relies on changing the embedding starting point rather than starting from the first pixel in the image. In [31], pixels sequence reordering is performed using Zig-Zag instead of the natural sequence to facilitate the embedding process. [32] utilizes embedding within a specific color channel rather than embedding in all matrices. Another method [33], focuses on identifying the most significant objects in the image and embedding data within their pixels, while [34] adopts a reverse approach by embedding within edges, which are high-frequency regions.

The other type, Frequency Domain, involves transforming the image into a frequency form using functions like Discrete Cosine Transform (DCT) or Wavelet Transform (WDT). After the transformation, specific low-frequency or high-frequency bits are chosen for embedding, depending on the method. The embedding occurs in the frequency domain, and then the image is reconstructed by reversing transformation. Frequency domain methods are considered more secure and resistant to changes but are more complex, requiring higher computational performance and longer execution times [35-36]. Figure 3 illustrates the basic concept of frequency domain-based techniques.

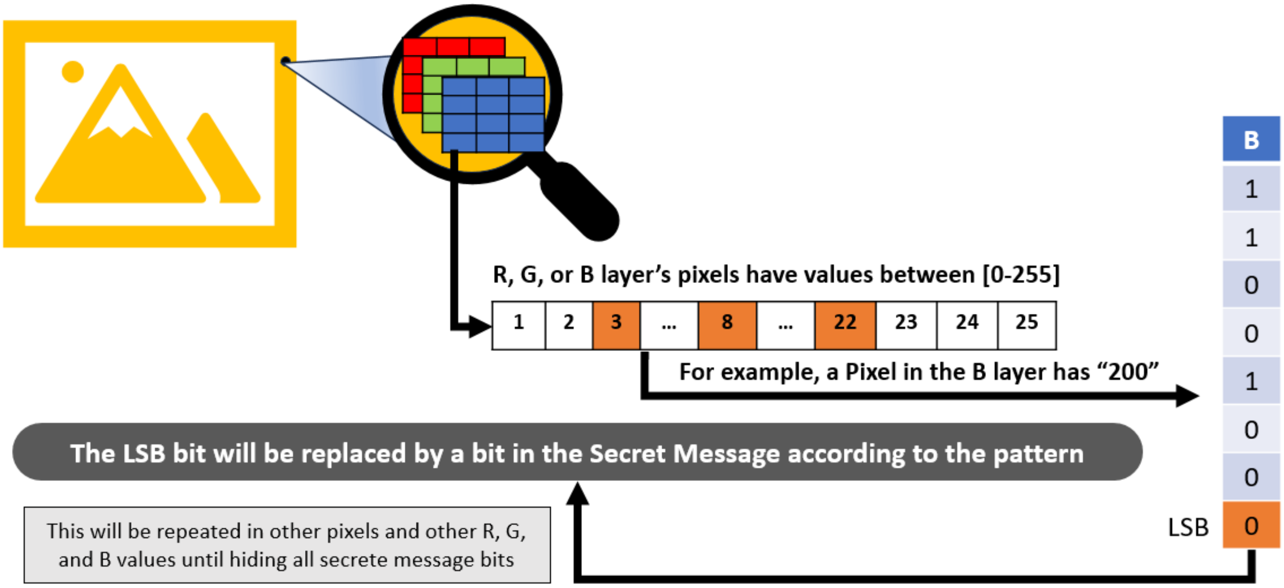

B
1
1
0
0
1
0
0
0
LSB
R, G, or B layer's pixels have values between [0-255]
1
2
3
...
8
...
22
23
24
25
For example, a Pixel in the B layer has “200”
The LSB bit will be replaced by a bit in the Secret Message according to the pattern
This will be repeated in other pixels and other R, G, and B values until hiding all secrete message bits

Figure 2. Steganography – Spatial Domain Technique (LSB Method)

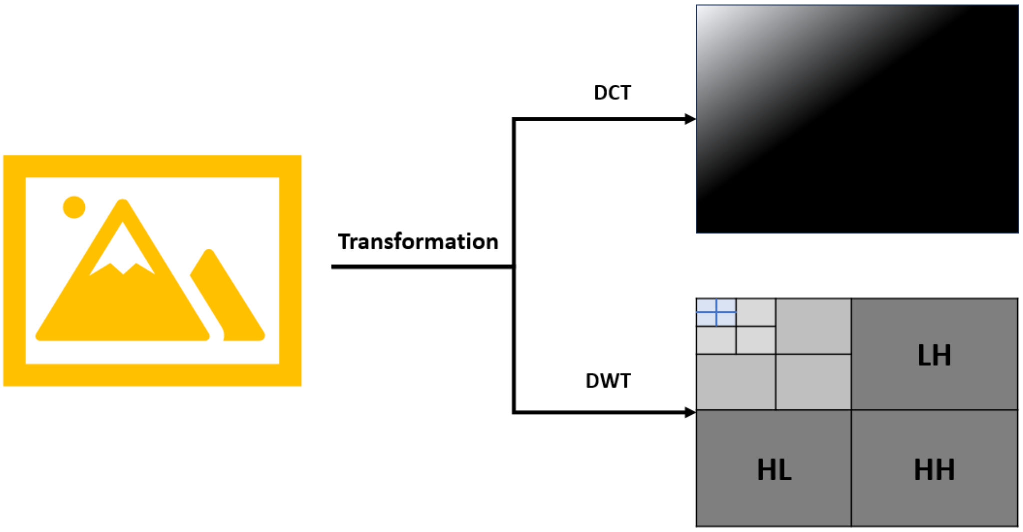


Figure 3. Steganography - Frequency Domain Technique (DCT and DWT)

Hybrid Techniques

These techniques rely on hiding data within an image which includes a text (Dealing with Text as the Image), or combining both image-based and text-based hiding methods. In [37], they modified the diacritics, as shown in Figure 4.A, which illustrates the Diacritics before and after modification. In [38], they focused on altering the shape of the character's endings in words, as depicted in Figure 4.B, illustrating the concept of this approach. However, it is worth noting that this method is time-consuming in the image creation and embedding processes, and it is also relatively easy to detect.

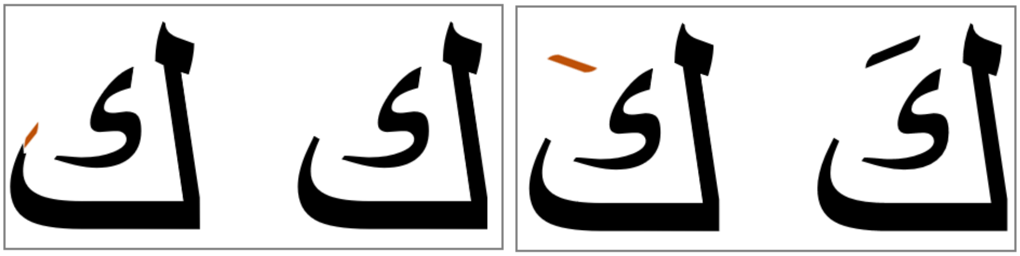


Figure 4. Change Text as an Image (A) (B)

Table 1. conclude the main method of steganography with Text-cover based on Imperceptibility, Capacity, Robustness, and Security metrics

Name	Main Idea	Advantages	Disadvantages
KASHIDA	Use "_" with Letters	Simple, Capacity	Easy to break and percept with large data
Letter Encode	Use on different codes for a letter	Simple, Capacity	Easy to break and suitable for private editor
Spaces	Use more than one space	Simple	Easy to break and percept
ZWJ	Use Hidden character "ZWJ"	Capacity, Imperceptibility	Easy to break, can be percept with large data
Diacritics	Change diacritic based on data	Simple, Capacity	Require a map
HAMZAT	Show or Hide Hamza	Simple	Easy to break, Capacity
Hybrid Diacritics	Change the direction of diacritic	Capacity	can be percept, Performance with large data
Hybrid Letter Edge	Change the edge of some letters	Capacity, good Security	Difficult Implementation, Performance with large data

The previous methods did not achieve the required level of security while maintaining flexibility and ease of implementation for both hiding and extraction. Even the hybrid methods have impacted performance and ease of verification, with some of them failing to provide the desired level of security. In this research, we introduce a hybrid approach as well, but in a completely different manner. The proposed method will address the drawbacks of previous techniques and achieve a high level of protection, and imperceptibility, while maintaining a high level of capacity and ease of verification. Furthermore, the proposed approach is suitable for applications in drone technology, as it does not require high computational resources for implementation.

The Proposed approach

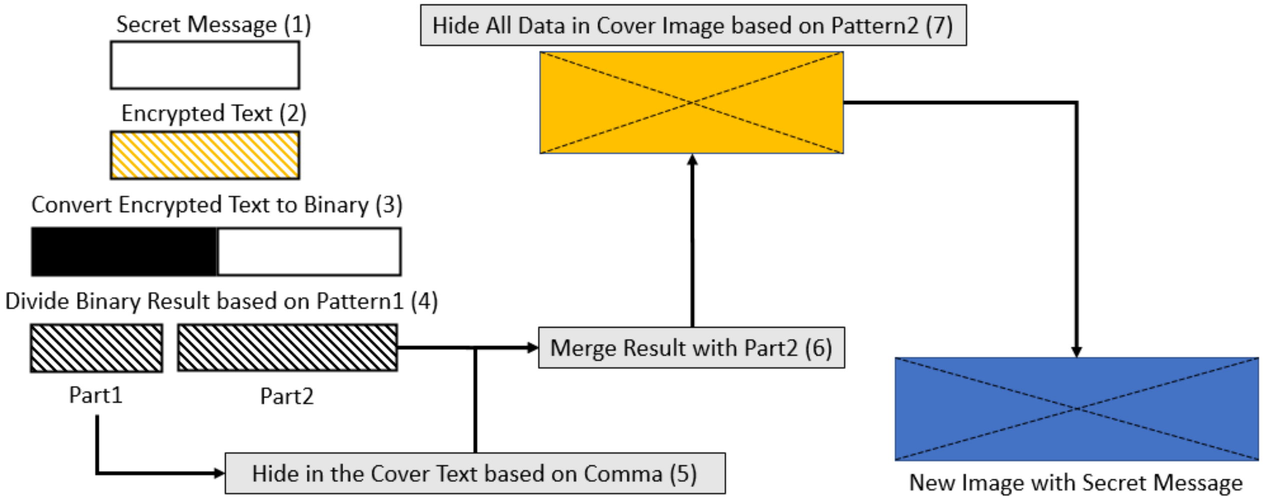
The proposed approach depends on the main ideas to create an effective steganography method with a high level of security. The main idea is splitting the encrypted message or data into two parts (one small and another large) based on agreed Pattern1 (e.g. 11101011) (Algorithm 3). The smaller part will be hidden in a text cover based on algorithm1 and creating new text has the secret information. The new text will be merged with the larger part and then hidden all inside an image cover based on Pattern2 and algorithm2 to determine the sequence of color layers (e.g. BBRGB). All the above will make the mission of any attacker impossible to detect, return, reorder, and decrypt data. In other meaning, the attacker needs to know:

- Pattern2 which is responsible for the method and sequence of hiding in the image's layers.
- Key2 of decryption data which is inserted inside the image
- Isolated the returned data to text and part2
- Break the method of hiding in the text and find the part
- Pattern1 to reorder the data of part1 and part2
- Key1 of decryption of the whole data (Part1+Part2)

For that, we said, it is very difficult to break the protection of the proposed approach. Moreover, users can use special cover-text which appears as a secret message by itself, so it simulates the honeypot method.

So, the proposed method provided a new method for employing steganography in text and steganography in images composed of multi-layers of protection. Where the proposed approach hides different parts of data in each layer. For that attackers can return the original data only if they return all encrypted bits from the image and text, and order all bits in the right way.

Note: Pattern1, Pattern2, Algorithm1, Algorithm2, and the proposed approach will be explained in detail in the next paragraphs:



Secret Message (1)
Encrypted Text (2)
Convert Encrypted Text to Binary (3)
Divide Binary Result based on Pattern1 (4)
Part1
Part2
Hide in the Cover Text based on Comma (5)
Merge Result with Part2 (6)
Hide All Data in Cover Image based on Pattern2 (7)
New Image with Secret Message

Figure 5. Main Step of the Proposed Method

Algorithm1- Steganography with Text

The proposed idea of Algorithm 1 depends on the punctuation marks especially the comma in Arabic and the comma in English. The algorithm replaces the "," with "," which is very similar. Any user will not note there is a difference in the text or size especially the natural of readers concerns on the main content more than other issue. So, even if the reader has good knowledge of syntax language will not detect or doubt.

Moreover, if the size of secret data is larger than the number of commas in the text, Algorithm1 will merge between the proposed method and KASHIDA one. This merging will enhance the capacity in addition it will mislead the attacker and make his task more difficult. The next paragraph (Algoirhtm1) shows the pseudocode of this algorithm.

```
//Proposed Algorithm1
String Encrypt1 (String message, String Key, String Pattern1, String CoverText)
Start
Int L1 = Length (Part1);
Int L2 = Find_Count( " , , ", CoverText ) ; // Number of all Ar or En Comma
Index = 0;
Int j =0;
If (L1 < L2)
        While (Index < L1)
                Bit b= msg[Index];
                j = find( ",", j)
                If (b)
                        CoverText [Index] = " , ";
                Else
                        CoverText [Index] = " , " ;
                End
                Index ++;
        End While
Else
        return "Error Length, Change Pattern or CoverText";
End IF
Return CoverText;
End Function
```

Algorithm2 – Steganography with Image

As the proposed method target is the drone applications, it is very important to use a simple algorithm that does not consume a lot of resources (memory, power, and CPU). For that, the Algorithm depended on a Special Domain, not a Frequency one. We enhanced the Low Significant Bit (LSB) method by agreeing on both sides (senders and receivers) on Pattern2. Pattern 2 presents the sequence of hiding in the color layers (R, G, and B) of the image cover. For example, if pattern2 equals "GBRR", then the first bit in the secret message will be hiding in the first pixel of layer "G", while the second bit in the layer B, and the third and fourth in layer "R". Then Algorithm2 repeats the process until hiding all bits of the secret data. The next paragraph (Algoirhtm2) shows the pseudocode of this algorithm.

```
//Proposed Algorithm2
Image NewImg Encrypt2 (String message, String Key, String Pattern2, String CoverText, Image img)
Start
String NewMsg = CoverText + Part2;
String Sec_msg2 = DES.Encrypt(NewMsg, Key);
Binary [] msg2 = Convert_To_Binary(Sec_Msg);
//Hiding in Image
Index = 0;
Int L = msg2.Length;
Int n =0;
For (int i=0; i<img.Length; i++) // Pattern2 like "RRGBB"
        If (Pattern2[index]=="R")
                Img[R][i].ConvertToBinary[0]=msg2[n];
```

```
    Else if (Pattern2[index]==”G”)
        Img[G][i].ConvertToBinary[0]=msg2[n];
    Else
        Img[B][i].ConvertToBinary[0]=msg2[n];
    If (n==L-1)
        Break;
    Index++;
    Index = index % index.Length;
End For
Return img;
End Function
```

Algoirthm3 - Split and Merge Algorithm

It is the most important phase in the proposed approach, In the first, the algorithm encrypts the data by using DES or AES algorithm (Symmetric Key). The results of encryption will be binary (bits). Then Algorithm 3 depends on an agreed Pattern (Pattern1 like “1110110”) between sender and receiver to split data. Where the bits that meet “0” will be in part1, and bits that meet “1” will be in part2. We will repeat the pattern on whole the secret message. In the end, we will have to series of bits (Part1, and Part2). The part1 will be inserted in Text-Cover based on Algorithm 1. The results of Algorithm1 will be merged with Part2 and encrypted again, then the whole encrypted data will be inserted in an Image-Cover based on Algorithm2. The next paragraph (Algoirhtm3) shows the pseudocode of this algorithm.

```
//Proposed Algorithm3
String Divide_Message (String message, String Key, String Pattern1, String CoverText, Image img)
Start
String Sec_msg = DES.Encrypt(message, Key);
Binary [] msg = Convert_To_Binary(Sec_Msg);
String Part1=””;
String Part2=””;
Int index=0;
For (int i=0; i<Pattern1.Length; i++)
    If (Patttern1[i]==”0”)
        Part1+=msg[index];
    Else
        Part2+=msg[index];
    If (Index<msg.Length-1)
        Index++;
    Else
        Break;
    If (i==Pattern1.Length)
        i=0;
End For
CoverText = Encrypt1 (string Part1, String Key, String Pattern1, String CoverText)
Image NewImg = Encrypt2 (string Part2, String Key, String Pattern2, String CoverText, Image img)
End Function
```

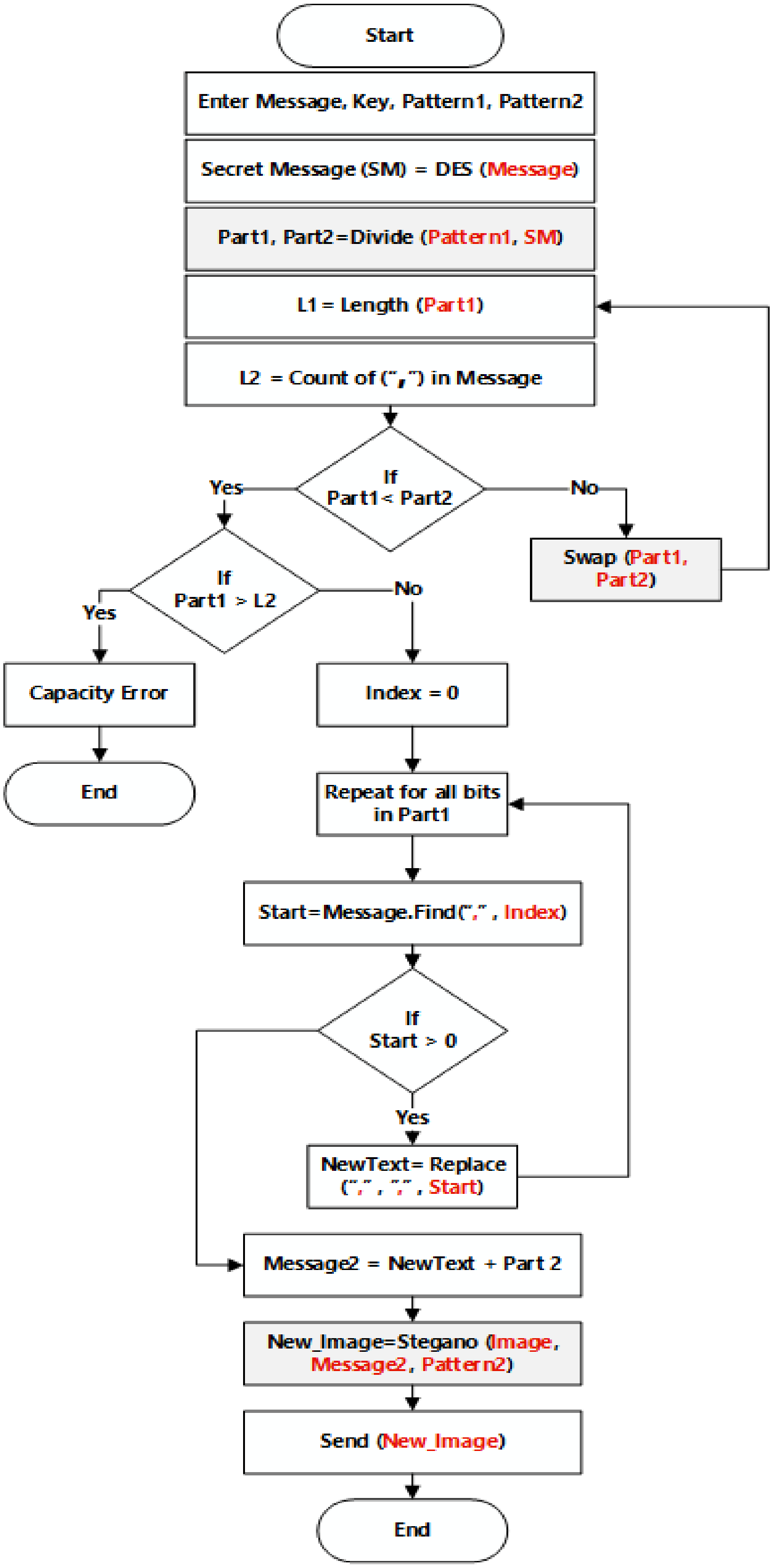

Start
Enter Message, Key, Pattern1, Pattern2
Secret Message (SM) = DES (Message)
Part1, Part2=Divide (Pattern1, SM)
L1 = Length (Part1)
L2 = Count of (“,”) in Message
If
Part1< Part2
Yes
No
Swap (Part1, Part2)
If
Part1 > L2
Yes
No
Capacity Error
End
Index = 0
Repeat for all bits in Part1
Start=Message.Find(“,” , Index)
If
Start > 0
Yes
NewText= Replace (“,” , “;” , Start)
Message2 = NewText + Part 2
New_Image=Stegano (Image, Message2, Pattern2)
Send (New_Image)
End

Figure 6. Steps of the Proposed Algorithm

Features of the Proposed Approach

The proposed approach encompasses several important features that can be summarized as follows:

1. **Dynamic and Mapping-Free:** The proposed approach is dynamic and does not require a predefined mapping between parties. It only necessitates an agreement on a shared encryption key along with two Patterns.
2. **High Imperceptibility:** It is extremely difficult to detect the proposed approach with the eye, whether in images or text.
3. **Language Agnostic:** The approach is not specific to any particular language, making it suitable for use with languages such as Arabic or English.
4. **Strong Security:** The approach offers robust security, as even if the encryption key is discovered, it remains highly challenging for an attacker to properly rearrange the encrypted data for decryption.
5. **Implicit Honeypot Concept:** The approach incorporates the honeypot concept implicitly, enhancing security levels.
6. **Minimal Impact on Performance:** The proposed approach has minimal impact on performance, ensuring efficient use in various applications.

Drawbacks of the Proposed Approach

The proposed approach has some limitations or constraints that can be summarized as follows:

1. **Limited Textual Data Capacity:** The amount of data that can be concealed within text is limited. Therefore, it is essential to consider this limitation when selecting the fragmentation Pattern or when choosing very long texts containing many punctuation marks. It's worth noting that the goal of using text is primarily to hide a portion of the encrypted data, making it difficult for attackers to reconstruct the encrypted string. Thus, they won't be able to decrypt it correctly, even if they uncover the encryption key. Moreover, increasing the hidden data within the text can easily be achieved by combining the proposed method with the KASHIDA method without significantly affecting the level of security.
2. **Robustness to Modifications or Compression Attacks:** The robustness of the hidden data to modifications or compression attacks, for example, can be compromised. The primary focus of the proposed approach is security and performance, and these aspects have been prioritized. However, if greater robustness is desired, the LSB technique can be replaced with one of the techniques based on Frequency Domain, albeit at the cost of some performance.
3. **Three Key Agreement:** The proposed approach requires an agreement on three keys: the encryption key and two Patterns, one for fragmentation and the other for the embedding algorithm within the images.

The previous requirement can be bypassed by agreeing on a specific algorithm for selecting the encryption key itself. This algorithm would include a part that represents the fragmentation Pattern and another part responsible for the embedding Pattern within the image layers. We will work on this point in the next work.

Implementation, Results, and Comparison

In this section, we will discuss the mechanism of implementing and testing the proposed approach, followed by a comparison of the proposed approach with other modern methods [25] [39] based on steganography fundamental evaluation criteria.

A. Investigation and Testing

The proposed algorithm was implemented using Visual Studio.Net 2019 with the C# programming language. This implementation aimed to verify the algorithm's effectiveness in both hiding and retrieving information. Figure 7. illustrates the application of the proposed algorithm for text hiding (Arabic Text) and Figure 8. with English text. While Figure 9 demonstrates the application of the algorithm for image hiding, and it displays the final results. Notably, there is no significant visual difference in the image before and after hiding.

To prove the effectiveness of the proposed approach according to the evaluation criteria for steganography methods, the following aspects were considered [40-42]:

Imperceptibility: From the previous two images, it is difficult for an ordinary person or even a suspicious individual to perceive the presence of hidden data within the image or text, even if the image encryption is broken. Therefore, the proposed approach is superior to other methods that rely on formatting or changes to diacritics, which can be noticed by anyone familiar with the language upon reading the text [40-41].

Security: The proposed approach achieves a very high level of security due to its multi-stage hiding using two hiding algorithms, in addition to the use of data partitioning and the concept of honeypots when selecting misleading information within the text.

Flexibility: The proposed approach offers a high level of flexibility in three key areas:

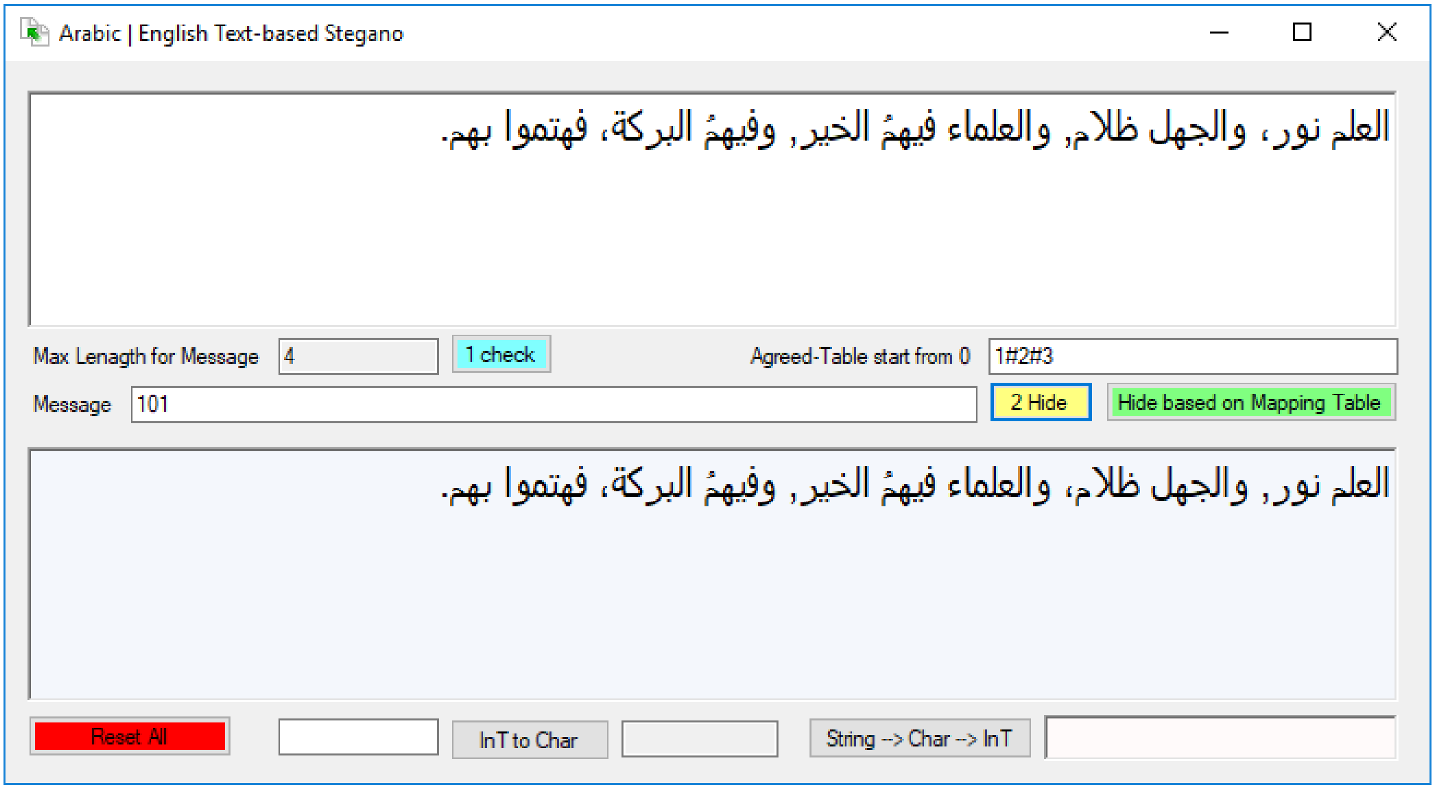
- It can be used with multiple languages, not limited to a specific language like Arabic in methods involving motion or diacritics.
- Users do not need to agree on a specific mapping or table for change locations before each encryption operation, as required by methods involving motion and diacritics.
- The proposed approach can be integrated with other hiding methods, such as KASHIDA, or using the Frequency domain instead of the Spatial Domain for image hiding.

Capacity: The proposed approach addresses the issue found in Multi-Layers or Double Steganography methods by using data partitioning with Pattern1, hiding a small portion within the text and a larger portion within the image. This achieves a higher level of security while maintaining a higher capacity [40-41].

Robustness: In the text-hiding process, immunity is maximized to the extent that compression algorithms do not affect the textual data. However, in the case of image hiding, hidden data may be affected during retrieval when applying compression or modifying the cover image. This is particularly true when using the LSB approach. Nevertheless, when utilizing the Frequency Domain approach, robustness is increased at the expense of performance.

Usability: The proposed approach offers ease of use, as users only need to agree on an encryption key with two Patterns. It does not impose strict requirements on the choice of text or cover image.

Performance: The proposed algorithm does not require high computational resources, as it employs a straightforward method for text hiding and image hiding. Through testing, the concealment time did not exceed [insert time]. However, it should be noted that, when working with the Frequency Domain approach, performance may be negatively affected compared to the LSB approach. Still, this trade-off can be managed based on available resources [42].


Arabic | English Text-based Stegano
1 check
2 Hide
Hide based on Mapping Table
Reset All
InT to Char
String --> Char --> InT

العلم نور، والجهل ظلام, والعلماء فيهمُ الخير, وفيهمُ البركة، فهتموا بهم.

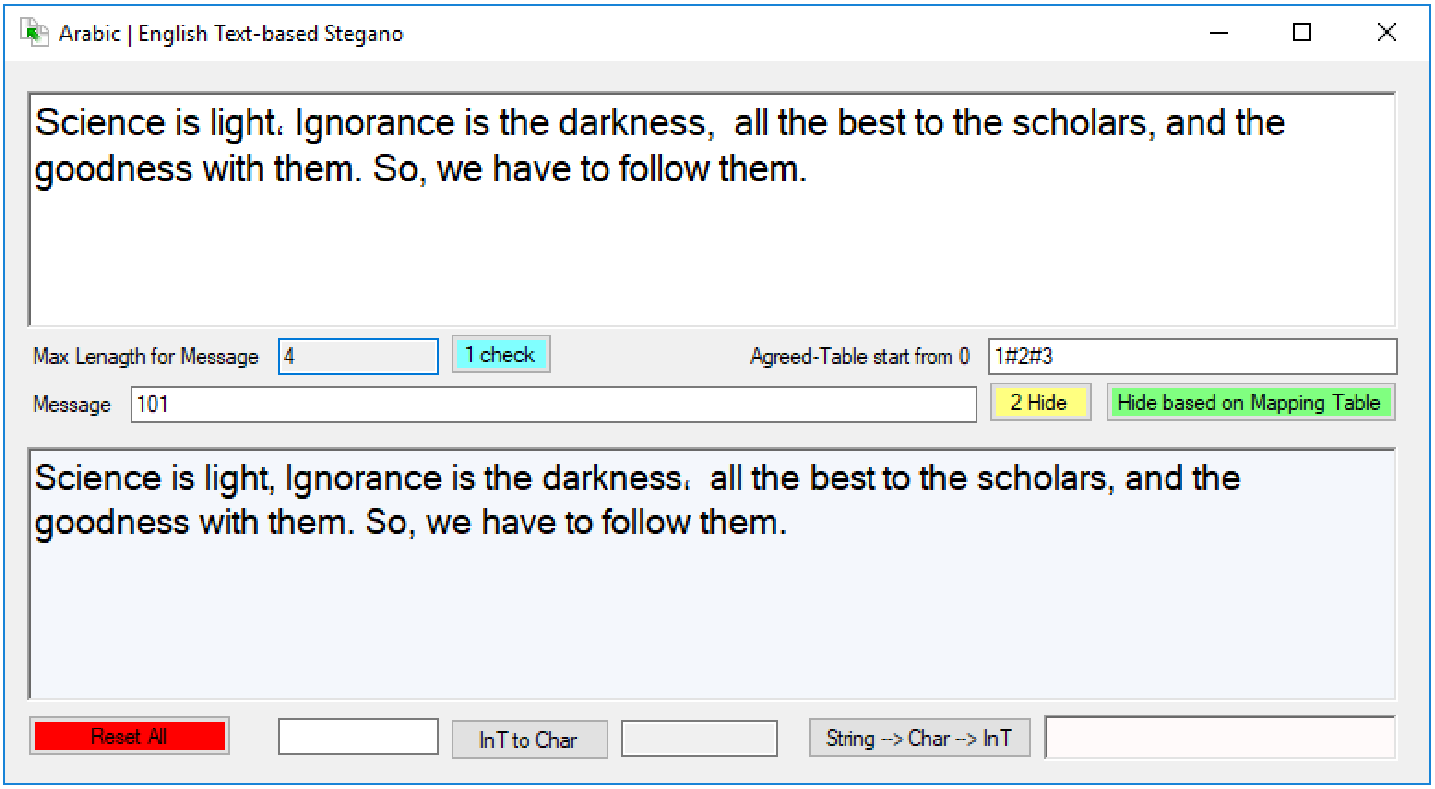
Max Lenagth for Message: 4

Agreed-Table start from 0: 1#2#3

Message: 101

العلم نور, والجهل ظلام، والعلماء فيهمُ الخير, وفيهمُ البركة، فهتموا بهم.

Figure 7. The implemented application for Text-based Steganography (Arabic Example)


Arabic | English Text-based Stegano
1 check
2 Hide
Hide based on Mapping Table
Reset All
InT to Char
String --> Char --> InT

Science is light، Ignorance is the darkness, all the best to the scholars, and the goodness with them. So, we have to follow them.

Max Lenagth for Message: 4

Agreed-Table start from 0: 1#2#3

Message: 101

Science is light, Ignorance is the darkness، all the best to the scholars, and the goodness with them. So, we have to follow them.

Figure 8. The implemented application for Text-based Steganography (English Example)

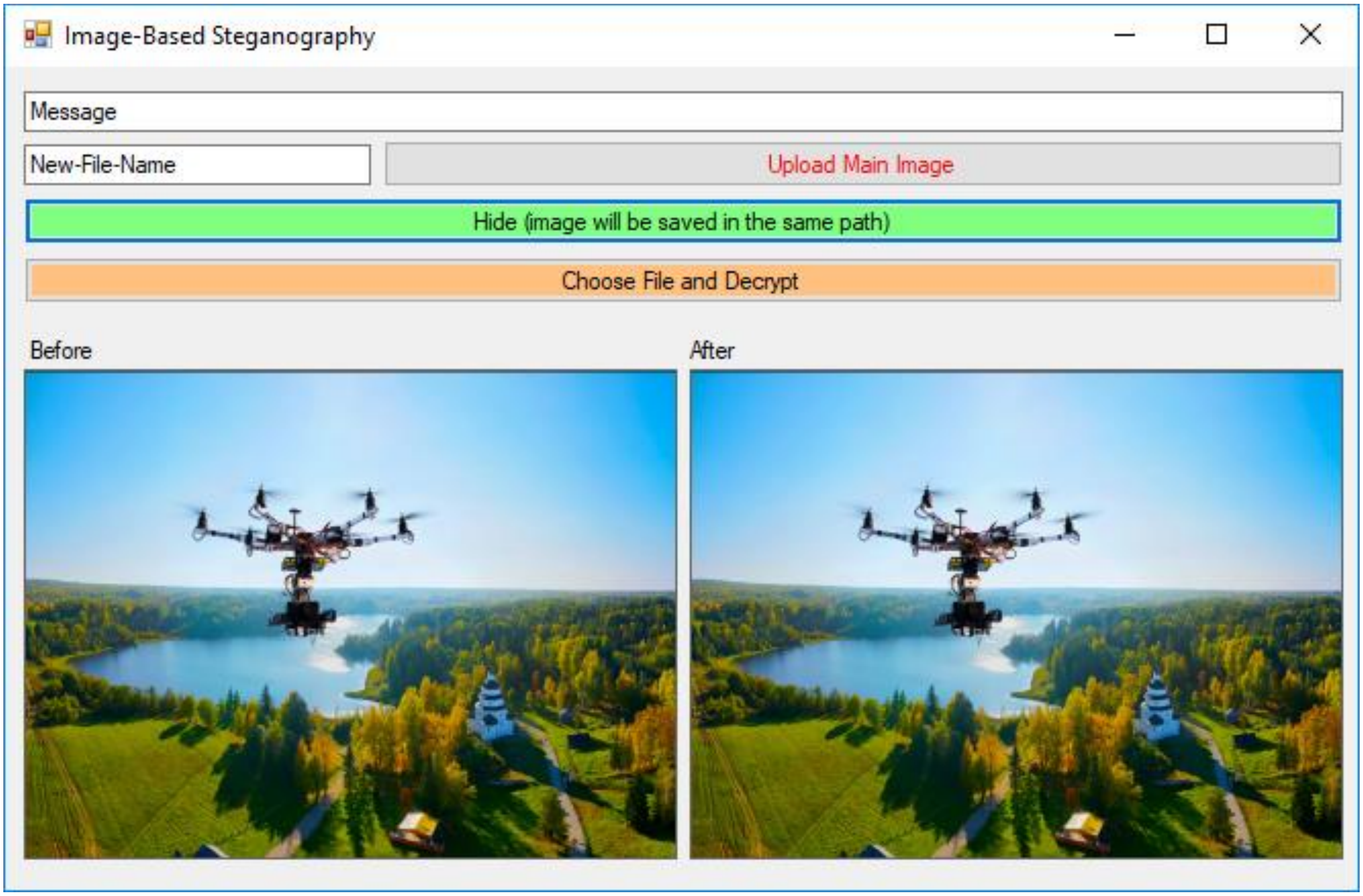


Figure 9. The implemented application of Image-based Steganography

Conclusion

This research presented a novel approach in steganography that integrates text and image hiding to enhance security in Internet of Things (IoT) applications in general, and drone applications in particular. This was achieved through a partitioning algorithm based on Patterns between the parties. The research also introduced a new method for text-based steganography using punctuation marks. Additionally, a simple method for image-based steganography depending on different layers sequencing using agreed Pattern. The proposed approach achieved excellent results in terms of steganography evaluation criteria and is adaptable to integration with other methods. In the next phase, we will work on proposing an automated algorithm for generating the patterns from the agreed encryption key itself. We will also explore other methods for text hiding or misleading attackers through dummy embedding or rearranging encrypted secret data.

References

[1] Daud, S. M. S. M., Yusof, M. Y. P. M., Heo, C. C., Khoo, L. S., Singh, M. K. C., Mahmood, M. S., & Nawawi, H. (2022). Applications of drone in disaster management: A scoping review. *Science & Justice*, *62*(1), 30-42.

[2] Gallacher, D. (2016). Drone applications for environmental management in urban spaces: A review. *International Journal of Sustainable Land Use and Urban Planning*, *3*(4).

[3] Sehrawat, A., Choudhury, T. A., & Raj, G. (2017, May). Surveillance drone for disaster management and military security. In *2017 international conference on computing, communication and automation (ICCCA)* (pp. 470-475). IEEE.

[4] Restás, Á. (2022). Drone applications fighting COVID-19 pandemic—Towards good practices. *Drones*, *6*(1), 15.

[5] Ahirwar, S., Swarnkar, R., Bhukya, S., & Namwade, G. (2019). Application of drone in agriculture. *International Journal of Current Microbiology and Applied Sciences*, *8*(01), 2500-2505.

[6] Shahmoradi, J., Talebi, E., Roghanchi, P., & Hassanalian, M. (2020). A comprehensive review of applications of drone technology in the mining industry. *Drones*, *4*(3), 34.

[7] Hoque, M. A., Hossain, M., Noor, S., Islam, S. R., & Hasan, R. (2021). IoTaaS: Drone-based Internet of Things as a service framework for smart cities. *IEEE Internet of Things Journal*, *9*(14), 12425-12439.

[8] Hassanalian, M., & Abdelkefi, A. (2017). Classifications, applications, and design challenges of drones: A review. *Progress in Aerospace Sciences*, *91*, 99-131.

[9] Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., Wahab, A. W. A., Nandy, T., Noor, N. M., & Bala, A. (2021). Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access*, *9*, 57243-57270.

[10] Yaacoub, J. P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, 100218.

[11] Abi Sen, A. A., Eassa, F. A., Jambi, K., & Yamin, M. (2018). Preserving privacy in internet of things: a survey. *International Journal of Information Technology*, *10*, 189-200.

[12] Abi Sen, A. A., & Basahel, A. M. (2019, March). A comparative study between security and privacy. In *2019 6th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 1282-1286). IEEE.

[13] Mishra, R., & Bhanodiya, P. (2015, March). A review on steganography and cryptography. In *2015 International Conference on Advances in Computer Engineering and Applications* (pp. 119-122). IEEE.

[14] Arora, N. (2022). Types and tools of steganography. *International Journal for Research in Applied Science and Engineering Technology*, *10*(6), 2049-2053.

[15] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.

[16] Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.

[17] Sharma, B. (2019). A Comparative Overview & Analysis Of Text And Image Steganography. *Think India Journal*, *22*(12), 297-305.

[18] Kumar, M., Kumar, S., & Nagar, H. (2020). Comparative Analysis of Different Steganography Technique for image or Data Security. *International Journal of Advanced Science & Technology (IJAST)*, *29*(4).

[19] Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. *Mathematics*, *9*(21), 2829.

[20] Kumar, R., & Singh, H. (2020). Recent trends in text steganography with experimental study. *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, 849-872.

[21] Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., Roslan, N. A., & Din, R. (2021). A comparative analysis of Arabic text steganography. *Applied Sciences*, *11*(15), 6851.

[22] Ali, R. H., & Kadhim, J. M. (2021). Text-based steganography using Huffman compression and AES encryption algorithm. *Iraqi Journal of Science*, 4110-4120.

[23] Zhang, S., Yang, Z., Yang, J., & Huang, Y. (2020). Linguistic steganography: From symbolic space to semantic space. *IEEE Signal Processing Letters*, *28*, 11-15.

[24] Alanazi, N., Khan, E., & Gutub, A. (2020). Functionality-improved Arabic text steganography based on unicode features. *Arabian Journal for Science and Engineering*, *45*, 11037-11050.

[25] Alqahtany, S. S., Alkhodre, A. B., Al Abdulwahid, A., & Alohaly, M. (2023). A Dynamic Multi-Layer Steganography Approach Based on Arabic Letters' Diacritics and Image Layers. *Applied Sciences*, *13*(12), 7294.

[26] Ali, R. H., Dhannoon, B. N., & Hamel, M. I. (2023). Arabic text steganography using lunar and solar diacritics. *Indonesian Journal of Electrical Engineering and Computer Science*, *31*(3), 1559-1567.

[27] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. *IEEE access*, *9*, 23409-23423.

[28] Din, R. (2023). Comparison Of Steganographic Techniques of Spatial Domain and Frequency Domain in Digital Images. *Borneo International Journal eISSN 2636-9826*, *6*(3), 109-118.

[29] Alhomoud, A. M. (2021). Image Steganography in Spatial Domain: Current Status, Techniques, and Trends. *Intelligent Automation & Soft Computing*, *27*(1).

[30] Maji, G., Mandal, S., & Sen, S. (2021). Cover independent image steganography in spatial domain using higher order pixel bits. *Multimedia Tools and Applications*, *80*(10), 15977-16006.

[31] Alam, S. T., Jahan, N., & Hassan, M. M. (2020). A New 8-Directional Pixel Selection Technique of LSB Based Image Steganography. In *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2* (pp. 101-115). Springer International Publishing.

[32] Ahmed, S. S., & Mehdi, S. A. (2022, November). Multi-layer Security for Color Image Based on Five-dimension Chaotic System and Image Steganography Algorithm. In *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)* (pp. 170-174). IEEE.

[33] Luo, Y., Qin, J., Xiang, X., & Tan, Y. (2020). Coverless image steganography based on multi-object recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *31*(7), 2779-2791.

[34] Mukherjee, S., & Sanyal, G. (2019). Edge based image steganography with variable threshold. *Multimedia Tools and Applications*, *78*, 16363-16388.

[35] Ahmed, S. N., Chandra, S., & Todwal, V. (2019). Image Steganography using Time and Frequency Domain. *International Journal of Research in Engineering, Science and Management*, *2*(8).

[36] Yadav, S. K., & Bhogal, R. K. (2018, April). A video steganography in spatial, discrete wavelet transform and integer wavelet domain. In *2018 International Conference on Intelligent Circuits and Systems (ICICS)* (pp. 258-264). IEEE.

[37] Memon, M. S., & Shah, A. (2015). A novel text steganography technique to Arabic language using reverse Fat5Th5Ta. *Pakistan Journal of Engineering, Technology & Science*, *1*(2).

[38] Roslan, N. A., Mahmod, R., & Udzir, N. I. (2011). Sharp-edges method in Arabic text steganography. *Journal of Theoretical and Applied Information Technology*, *33*(1), 32-141.

[39] Alsaawy, Y., Abi Sen, A. A., Alkhodre, A., Bahbouh, N. M., Baghanim, N. A., & Alharbi, H. B. (2021, March). Double Steganography-New Algorithm for More Security. In *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 370-374). IEEE.

[40] Al-Mohammad, A. (2010). *Steganography-based secret and reliable communications: Improving steganographic capacity and imperceptibility* (Doctoral dissertation, Brunel University, School of Information Systems, Computing and Mathematics Theses).

[41] Rabie, T., Baziyad, M., Bonny, T., & Fareh, R. (2020). Toward a unified performance metric for benchmarking steganography systems. *Journal of Circuits, Systems and Computers*, *29*(03), 2050042.

[42] Sharma, R., Ganotra, R., Dhall, S., & Gupta, S. (2018). Performance comparison of steganography techniques. *International Journal of Computer Network and Information Security*, *10*(9), 37-46.

Double-SP Method to Enhance Privacy and Security of Smart City Applications

Bahbouh, N. M., Hakami, A. A. H., Aljohani, Y. M., Abi Sen, A. A., Alkhodre, A., & Alsughayyir, A. (2023, March). Double-SP Method to Enhance Privacy and Security of Smart City Applications. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 557-561). IEEE.

Abstract

Smart cities promise a lot of well-being to their users in all areas of life through millions of applications and services. Smart services rely heavily on collecting data and the preferences of users. But on the dark side, the users' information is posed to threat and penetration during transmission or stored far in the clouds. Depending on encryption only is not sufficient if the attacker has strong resources or if the attacker is the service provider (SP) itself. In addition, changing data before sending is not a practical solution in many systems because of the adverse impact on the quality of a main service. This research presented a new idea to address the issue of protection. The proposed method enhanced the privacy and security of users' data without affecting the accuracy of service. The core of the suggested solution relies on a knowledge base of services that are managed by experts. Also, the solution depends on fog nodes to measure the level of security and privacy of users' queries without delay. Moreover, the fog nodes manage contact with SPs. Finally, the proposed method divided the SP into two, one for user queries and the other for user data. The simulation and analytical discussion on a practical case in smart cities demonstrated the superiority of the proposed approach over previous methods in the level of protection by maintaining the quality of services, and the resistance to attacks.

Keywords—Privacy, Security, IoT, Smart city, Fog.

Introduction

One of the most important outcomes of development in the world of modern technology is smart cities. The smart city is an umbrella for many smart applications and services. It ensures a more comfortable and sophisticated life with all daily tasks [1]. To form a smart city, there are many aspects like kinds of communications, and types of smart elements, in addition to a large number of important applications in different majors. The smart city depends on analyzing the big data that are collected from users or the environment around them. Thus, the smart city can provide more adapted services to users[2].

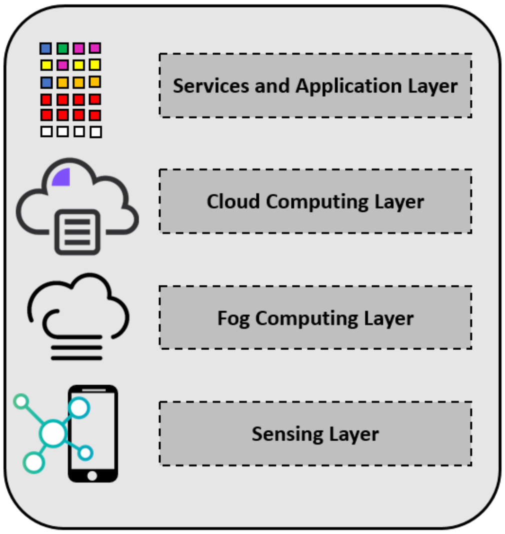


Fig. 1. Main Layers of Smart City

The smart city is the main application of the Internet of Things (IoT). The elements of IoT can be divided into three groups [3]:

- Radio Frequency identifiers (RFID), which give things their unique identifiers, so these things can cooperate through the unique ID. Moreover, users can interact with and track smart objects by their identifiers.
- Wireless network sensors (WSNs), which can be deployed everywhere within the city to continuously collect various kinds of data such as temperature, humidity, noise, pollution, pressure, etc. in addition to pictures of cameras and sounds of mics.
- Smart devices are used within smart cities, such as phones, tablets, vehicles, screens, and others.

These elements form the infrastructure of the smart city or what is known as the sensing layer (First Layer of Figure 1). Smart applications and services constitute the fourth layer within the smart city framework [4]. Many important applications should be available within smart cities, to mention but not limited to:

- Smart Traffic: It contains many smart services such as: managing traffic congestion through smart traffic signals, alerting drivers to places of congestion to stay away, providing electronic reservation for parking, mapping and navigating services, smart lighting, monitoring, and fast alerting to accidents to ensure the safety of streets [5].
- Smart Health: It requires providing smart hospitals, mobile hospitals, continuous monitoring of the vital measurements of individuals, and alerting to any emergency problem, in addition to providing electronic consultations and reservations [6].
- Smart Energy: Smart cities must rely heavily on alternative energy sources. Then it can contribute to saving energy consumption by automating switching on/off lighting, monitoring the consumption level of devices, and informing the user of periodic reports [7].
- Waste management: Smart cities must maintain their cleanliness and prevent any manifestation of distortion. So, the smart city can manage the containers with smart alerts in case of fulling. The sent alert will include the location of the nearest cleaning vehicles. The smart city supports the filtering and recycling of waste [8].
- Crowd management: Smart cities must maintain organized access to services. Also, the smart city has to prevent problems that accompany crowded places such as stadiums, theaters, races, and others. Many applications can help people in crowds to request help or volunteer, report an emergency event, and get important safety advice or news [9].

The second and third layers are computing layers for data processing. The fog layer, which is the second, provides rapid initial processing of data, as it is close to the data collection layer. So, the fog layer can provide an immediate response in emergencies, and it can reduce the load significantly for the cloud. The cloud is the large and permanent store of data of applications. It is the place that can process big data to extract the knowledge to support decisions and provide more adaptive and advanced services [10].

Since smart applications and services depend on user data and his/her identity so, there is a threat to the privacy and security of the collected data. Exposing such data to any party is considered a major breach of privacy and its results may pose a threat to the user's life, habits, and safety [11]. Therefore, protecting the privacy and security of users' data is one of the important challenges facing the future of smart cities.

The smart city must ensure the safety, security, and privacy of its users' data. Developed countries such as the United States of America and the European Union, in the past few years, have launched a special GDPR law to protect the privacy of users. This law, which came into effect in 2018, required adherence from all companies and SPs. Also, Saudi Arabia announced a similar privacy law in 2021 [12].

Although privacy differs from security in principle. Security is concerned with ensuring the confidentiality, integrity, and availability of data, while privacy is concerned with preventing the identification, tracking, and profiling of users. So, the SP should not obtain information about the user if this data is not related to the announced service. Within smart cities, the two concepts cannot be ignored, as they complement each other [13].

Unfortunately, with the increase in the number of services within smart cities, it is impossible for users to determine whether the required data from a SP is necessary to complete the service or not. This is an additional challenge to the protection methods that seek to solve the problem of privacy and security. Another protection challenge is related to the impact of the protection method on the quality of the main service, as some protection methods may modify data, add fake data, change the user's identity, or cause a large load and bad effect on the performance of the service [14].

This research presented a new approach to addressing previous issues and challenges with effective solutions. The new approach proposed forming a knowledge base for all services classifications by experts. This knowledge base determines the required data of any service in any classification. That will prevent SPs from exploiting users by requesting additional information. The proposed solution also discussed protecting the privacy of users in the case of penetrating SPs, as happened in the past years of global systems and companies in the world of technology like WhatsApp, Facebook, and Hotmail [15].

Therefore, our contributions to this research will be:

- Review the challenges of smart cities related to the privacy and security.
- Discuss current methods of protecting privacy and security with their weaknesses.
- Propose a new approach to protect the privacy and security of user data in smart cities and address the current challenges.
- Implement simulation to prove the superiority and efficiency of the proposed approach.

The following sections will be a literature review of common privacy protection methods, then a detailed review of the proposed approach, and finally few recommendations.

Literature Review

Due to the importance of data privacy and security, many studies have discussed this challenge within the various smart city applications. Many research have confirmed that data privacy and security are the biggest challenges for smart cities [16, 17]. Smart cities monitor the physical world in real-time. That increases security and privacy concerns because the collected and stored data can be stolen or spread illegally.

Research in [18] presented a method for giving its user the right to control his data and taking his acceptance to access his data. But this approach would not be useful if the attacker got the data or if the attacker was the SP itself.

Another research divided types of attacks on security and privacy into Passive or Active Attacks. In the passive attack, the attacker tries to steal data or penetrate its confidentiality without the user's realization, which is more dangerous. While, in the active attack, the attacker breaches availability, integrity, or authentication, which has a greater effect, but the user will realize it immediately [19].

In general, privacy concerns can be divided into five parts of protection: identity, query, location, time or footprint, and owner. Therefore, according to the application, one of these parts will be more important than the other, so attention must be increased to protect a particular part according to the application [20].

Common privacy protection techniques can be categorized based on the five parts that need protection accordingly:

The dummy approach sends additional incorrect data or queries to mislead the SP or any attacker trying to steal the data. Thus, most data collected about the user will be incorrect. This method is valid for the location or query protection. Unfortunately, this approach will affect the accuracy of the data and the quality of many services as traffic or health [21].

The obfuscation approach changes some data before it is sent by adding obfuscation or noise to it to prevent an attacker to obtain accurate data. This approach can be used to protect the location, query, or footprint. This approach has negatively affected the accuracy of data and the quality of services in smart cities [22].

The Mix-Zone approach is based on an alias instead of the real identity. It is switching the alias when a user moves to a new zone. It can be used to protect identity, but this approach is only valid in cases of static queries or that do not need to store data about the user [23].

Private Information Retrieval (PIR) uses encrypted queries and stores a huge amount of data internally to reduce the number of future contact with SPs. It is considered a good method for protecting queries, location, and footprint. But this approach significantly affects the performance of the core service [24].

The Peer Cooperation approach is used to anonymize a group of collaborators by using a unified nickname and location. It is good for static or dynamic queries which do not require permanent storing of the user’s data [25].

Data Mining or Statistics approach depends on collecting data locally, conducting some analysis or statistics on it, and then sending summarized data instead of sending the details of all collected values, and therefore it is good for Footprint protection, but it is not suitable if service sensitive for the delay [26].

There is no appropriate approach for all applications. At the same time, each approach has a set of drawbacks or weaknesses [27]. All previous methods did not address the SP penetration challenge in the case of services that require storing data of the user such as health systems. Also, the methods did not take into account if a malicious SP requests more data from the user. Moreover, some methods did not care about performance and time delay. In the next section, we will discuss in detail how the proposed approach provided effective solutions to these challenges based on the integration of all layers in the IoT environment (sensing, fog, cloud, and services).

Proposed Approach

We noticed in the previous sections that there are challenges so far in privacy and security. Where the user cannot determine whether the data requested from the SP is related to the service or not. Also, If the SP is hacked and users’ data is stolen. In addition to necessary to maintain the accuracy of the data after applying for protection. Finally, the protection method has not affected the performance of the service. As a solution to these challenges, we presented the proposed approach, which must consist of main elements, namely:

- Knowledge base: it is managed by experts in information technology and the main major of service. it contains the required data for each service according to its classification of it. This rule can be modified according to new types of services that can be launched within smart cities.
- Fog node: It is a small cloud that is densely distributed to cover all areas of smart cities. Each fog node manages a specific area, which users within that area connect to via wireless connection. The fog node acts as the first stage of data processing before it is sent to the cloud. The fog node determines the type of service and its classification, then it filters the user's data based on the roles in the base knowledge to protect the user. Further, the fog node may encrypt the sensitive data before sending it.

  In the case of highly sensitive services, the fog node receives the encrypted data from the user based on a public key of SP. So, even the malicious fog node cannot hack the data. Finally, in the case of static queries, the fog node replaces the user's ID with an alias and acts as an Anonymizer.

If there is a SP that requires saving the private data of the user such as health services, the fog node has to play an important role. The fog will divide the user data into two parts. The first part contains queries and required data related to the user. However, the fog will exchange the user ID with a unique number stored in the fog cache. The second part contains the user's identity, his Footprint, and the owner. each part will be sent to a different server in the smart city for permanent storage.

- SP which has to register its services to be indexed and classified within the knowledge base.
- User Identity Server (UIS) which manages the users' IDs without queries, the used unique IDs of the user, footprint, SPs name, and the code of requested service.
- Smart Servicer (SS) for enhancing the services based on the users' preferences, so this server has the right to access UIS.

Thus, when the SS or a particular SP needs to analyze user data to provide more adaptive services, firstly it must obtain the user's acceptance to access his data in UIS, then SS must have the right to access the queries of the user. After that, SS can analyze these queries to study user behavior and provide better services for him.

Figure 2 shows sequence of the main steps of the proposed approach and its structure, while Figure 3 depicts the algorithm of the fog node role.

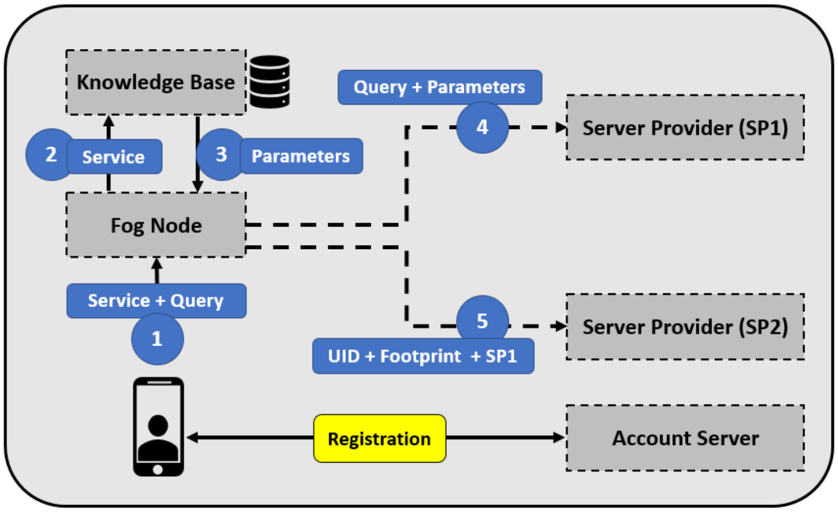
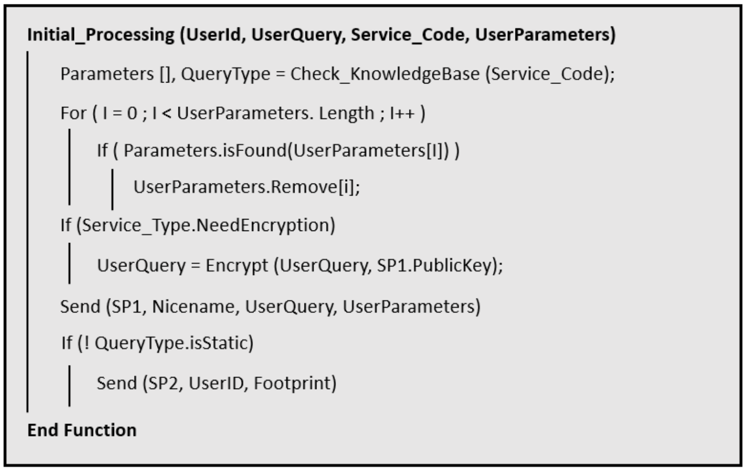


Fig. 2. Main Steps of the Proposed Approach



```
Initial_Processing (UserId, UserQuery, Service_Code, UserParameters)
    Parameters [], QueryType = Check_KnowledgeBase (Service_Code);
    For ( I = 0 ; I < UserParameters. Length ; I++ )
        If ( Parameters.isFound(UserParameters[I]) )
            UserParameters.Remove[i];
    If (Service_Type.NeedEncryption)
        UserQuery = Encrypt (UserQuery, SP1.PublicKey);
    Send (SP1, Nicename, UserQuery, UserParameters)
    If (! QueryType.isStatic)
        Send (SP2, UserID, Footprint)
End Function
```

Fig. 3. Algorithm of Fog Node's Functions

Results and Comparison

To prove the superiority and effectiveness of the proposed approach, we compared it to three common approaches in the field of privacy protection (the dummies approach, the obfuscation approach, and the peer-to-peer cooperation approach). We relied on two standard criteria which are Entropy (E) and Performance rate [27, 28]. E measures the amount of information that an attacker can detect and associate with a specific user. The second criterion is the performance rate, which is measured by the size of the data and the number of connections to the SP. Finally, we will compare the resistance of the protection methods against a malicious SP, in addition to the impact of protection steps on the quality of the main service.

The following hypotheses have been made

- Number of dummies is 3 so K= 3 with each query.
- The diameter of the obfuscation area is three times of original area of user R=3.
- Number of peers for cooperating in each area is 10 P=10.
- Number of queries ten N=10.
- Query time T=1 without any protection method.
- Communication time between the user and the fog node T1=0.1.
- Communication time between the user and another user T2 = 0.4.

Figure 4 presents the entropy value of the four methods, we note that the proposed approach achieves absolute protection E=1 (maximum) because the fog node hides the user's identity from the SP SP1.

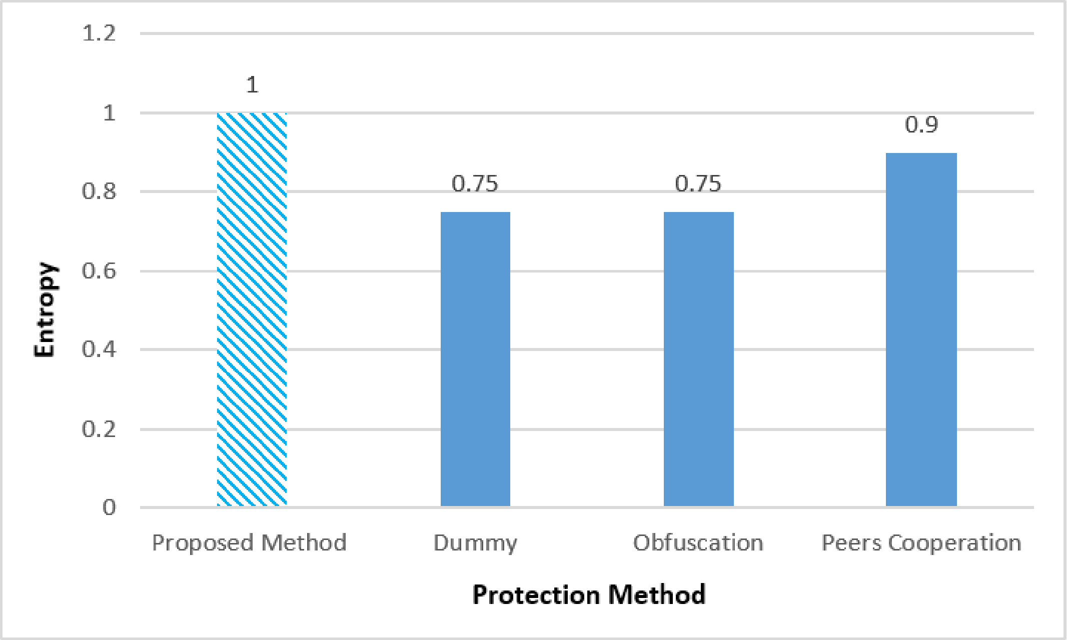


Fig. 4. Entropy Comparison

Figure 5 shows the superiority of the proposed approach in terms of performance. Because the proposed method only uses a specific fog node in the area, without the need to send four queries like the dummy approach, double the size of the query's area like the obfuscation, or cooperate with many peers like the peer-cooperation. Thus, the performance of the proposed approach was better than the other methods. Moreover, if the cache is employed within the fog nodes, it will improve the performance more and reduce the number of connections to the SP.

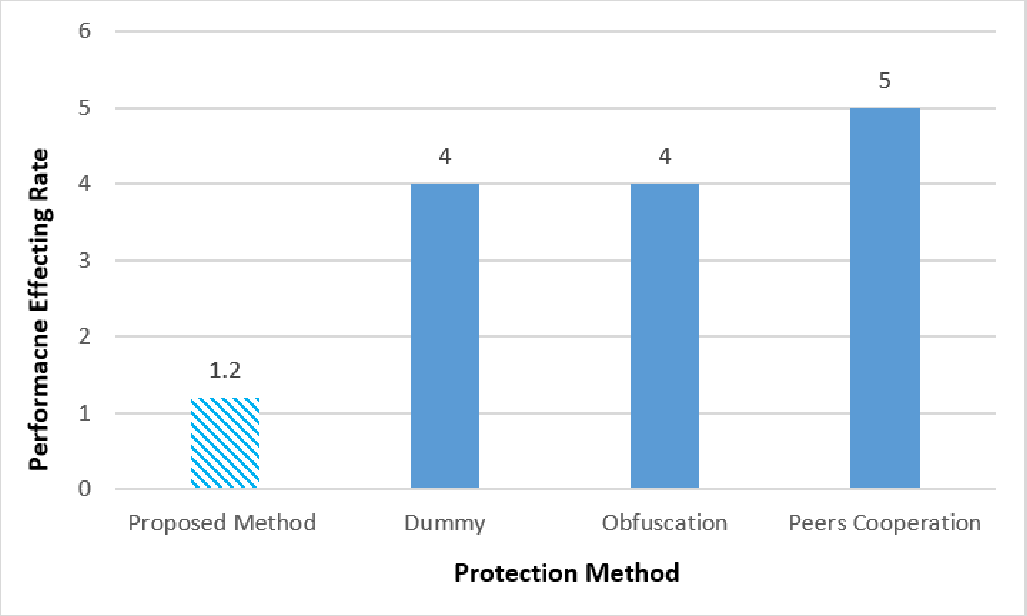


Fig. 5. Impact Applying Protection Methods on Performance

In the matter of data volume, the proposed approach will not affect the volume of data but may reduce the volume of data required from the SP in some cases. Moreover, if the SP is compromised, the proposed approach does not cause any theft of user data due to anonymity, while other methods contribute to the theft of some data with a percentage similar to the Entropy ratio.

Finally, for the impact factor on the accuracy of the service, the proposed approach does not cause any effect, it only saves the data that some services need for analysis in another server that needs the user's consent. While dummy, obfuscation, and cooperation affect the accuracy of the service due to noise, fake queries, or exchanging information between users, all of this is not acceptable in many services that require maintaining accuracy in user data, such as medical services.

Conclusion

This research proposed a new method to protect privacy within smart cities. The idea depended on creating a knowledge base for the available services within the city. The fog node filters the data according to the type of requested service by the user. The preprocessing will enhance the user's privacy and prevent SPs from collecting additional data about the user. The most important step was hiding the user's identity when sending the query to a SP. However, at the same time, the user ID is saved with his Footprint on another server. That enabled the smart city to access and analyze the data of the user and provide more adaptive services for him. Simulation and discussion proved the superiority of the proposed approach over the common methods in terms of privacy, especially since the proposed approach does not affect the performance of the main service. In the future, machine learning algorithms will be used to improve the knowledge base and manage it automatically without experts.

References

[1] C. S. Lai et al., “A Review of Technical Standards for Smart Cities,” Clean Technologies, vol. 2, no. 3, pp. 290–310, Aug. 2020, doi: 10.3390/cleantechnol2030019.

[2] M. Lytras, A. Visvizi, and A. Sarirete, “Clustering Smart City Services: Perceptions, Expectations, Responses,” Sustainability, vol. 11, no. 6, p. 1669, Mar. 2019, doi: 10.3390/su11061669.

[3] M. Yamin, A. M. Basahel, and A. A. Abi Sen, “Managing Crowds with Wireless and Mobile Technologies,” Wireless Communications and Mobile Computing, vol. 2018, pp. 1–15, Aug. 2018, doi: 10.1155/2018/7361597.

[4] A. A. Abi Sen, F. A. Eassa, and K. Jambi, “Preserving Privacy of Smart Cities Based on the Fog Computing,” Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 185–191, 2018, doi: 10.1007/978-3-319-94180-6_18.

[5] A. Alharbi, G. Halikias, A. A. A. Sen, and M. Yamin, “A framework for dynamic smart traffic light management system,” International Journal of Information Technology, vol. 13, no. 5, pp. 1769–1776, Jul. 2021, doi: 10.1007/s41870-021-00755-2.

[6] N. M. Bahbouh, S. S. Compte, J. V. Valdes, and A. A. A. Sen, “An empirical investigation into the altering health perspectives in the internet of health things,” International Journal of Information Technology, Jul. 2022, doi: 10.1007/s41870-022-01035-3.

[7] H. Kim, H. Choi, H. Kang, J. An, S. Yeom, and T. Hong, “A systematic review of the smart energy conservation system: From smart homes to sustainable smart cities,” Renewable and Sustainable Energy Reviews, vol. 140, p. 110755, Apr. 2021, doi: 10.1016/j.rser.2021.110755.

[8] M. Sharma, S. Joshi, D. Kannan, K. Govindan, R. Singh, and H. C. Purohit, “Internet of Things (IoT) Adoption Barriers of Smart Cities’ Waste management: an Indian Context,” Journal of Cleaner Production, vol. 270, p. 122047, May 2020, doi: 10.1016/j.jclepro.2020.122047

[9] M. M. Almutairi, D. Apostolopoulou, G. Halikias, A. A. Abi Sen and M. Yamin, "A Framework for Comprehensive Crowd and Hajj Management," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), 2022, pp. 63-68, doi: 10.23919/INDIACom54597.2022.9763174

[10] A. A. A. Sen and M. Yamin, “Advantages of using fog in IoT applications,” International Journal of Information Technology, Oct. 2020, doi: 10.1007/s41870-020-00514-9.

[11] T. Braun, B. C. M. Fung, F. Iqbal, and B. Shah, “Security and privacy challenges in smart cities,” Sustainable Cities and Society, vol. 39, pp. 499–507, May 2018, doi: 10.1016/j.scs.2018.02.039.

[12] A. Polat, “Effects of GDPR on the financial services sector in the Kingdom of Saudi Arabia”. Journal of Data Protection & Privacy, 4(3), 273-282, 2021

[13] A. A. A. Sen and A. M. Basahel, "A Comparative Study between Security and Privacy," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), 2019, pp. 1282-1286.

[14] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, “Security, Privacy and Risks Within Smart Cities: Literature Review and Development of a Smart City Interaction Framework,” Information Systems Frontiers, Jul. 2020, doi: 10.1007/s10796-020-10044-1.

[15] A. M. V. Venkata Sai and Y. Li, "A Survey on Privacy Issues in Mobile Social Networks," in IEEE Access, vol. 8, pp. 130906-130921, 2020, doi: 10.1109/ACCESS.2020.3009691.

[16] A. A. Abi Sen, “A comprehensive privacy and security framework for dynamic protection (CPSF),” International Journal of Information Technology, vol. 14, no. 5, pp. 2477–2485, May 2022, doi: 10.1007/s41870-022-00965-2.

[17] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, “Security and Privacy in Smart Cities: Challenges and Opportunities,” IEEE Access, vol. 6, pp. 46134–46145, 2018, doi: 10.1109/access.2018.2853985.

[18] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, “User Perceptions of Smart Home IoT Privacy,” Proceedings of the ACM on Human-Computer Interaction, vol. 2, no. CSCW, pp. 1–20, Nov. 2018, doi: 10.1145/3274469.

[19] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, “A classification of location privacy attacks and approaches,” Personal and Ubiquitous Computing, vol. 18, no. 1, pp. 163–175, Nov. 2012, doi: 10.1007/s00779-012-0633-z.

[20] A. Martinez-Balleste, P. A. Perez-martinez and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," in IEEE Communications Magazine, vol. 51, no. 6, pp. 136-141, June 2013, doi: 10.1109/MCOM.2013.6525606.

[21] M. Yamin and A. A. A. Sen, “Improving Privacy and Security of User Data in Location Based Services,” International Journal of Ambient Computing and Intelligence, vol. 9, no. 1, pp. 19–42, Jan. 2018, doi: 10.4018/ijaci.2018010102.

[22] S. S. Albouq, A. A. A. Sen, A. Namoun, N. M. Bahbouh, A. B. Alkhodre, and A. Alshanqiti, “A Double Obfuscation Approach for Protecting the Privacy of IoT Location Based Applications,” IEEE Access, vol. 8, pp. 129415–129431, 2020, doi: 10.1109/access.2020.3009200.

[23] A. A. Abi Sen, A. Alnsour, S. A. Aljwair, S. S. Aljwair, H. I. Alnafisah and B. A. Altamimi, "Fog Mix-Zone Approach for Preserving Privacy in IoT," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 405-408.

[24] M. M. Almutairi, A. A. Abi Sen and M. Yamin, "Survey of PIR Approach and its Techniques for Preserving Privacy in IoT," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), 2021, pp. 417-421.

[25] M. Yamin and A. A. Abi Sen, "A New Method With Swapping of Peers and Fogs to Protect User Privacy in IoT Applications," in IEEE Access, vol. 8, pp. 210206-210224, 2020, doi: 10.1109/ACCESS.2020.3038825.

[26] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, “Privacy Preservation in Big Data From the Communication Perspective—A Survey,” IEEE Communications Surveys Tutorials, vol. 21, no. 1, pp. 753–778, 2019, doi: 10.1109/COMST.2018.2865107.

[27] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” International Journal of Information Technology, vol. 10, no. 2, pp. 189–200, Feb. 2018, doi: 10.1007/s41870-018-0113-4.

[28] H. Xia, and W. Yang, “Information Entropy Models and Privacy Metrics Methods for Privacy Protection,” International Journal of Network Security, 24(1), 1-10, 2022.

****

Chapter 7 - Society and Environment and New Services

This chapter discusses the issue of community health and mechanisms to enhance and support it with innovative services and applications. It also explores ways to support and assist individuals with special needs. The chapter contains three research papers published in conferences.

The first paper proposed a method for quickly and effectively providing blood donors and quantities when needed. The second paper presented a framework specifically designed to support individuals with special needs. The third paper introduced a smart application for enhancing the awareness of the community.

Smart Application for Blood Donation Management in Health Domain

Basahel, A. M., Bahbouh, N. M., Abi Sen, A. A., & Yamin, M. (2023, March). Smart Application for Blood Donation Management in Health Domain. In *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 589-594). IEEE.

Abstract

The health sector is one of the most important sectors that needs permanent and continuous development because it is directly related to people's lives. One of the most important matters is to provide the required quantities of blood promptly as needed, as the delay in providing it by a few minutes may pose a threat to the patient's life. Unfortunately, the current blood donation campaigns are insufficient despite their importance. Smartphone applications are facilitating many tasks and improving their performance, so this research presents the idea of an electronic platform with a smart application that helps provide large quantities of blood required when needed by immediately notifying all volunteers. Moreover, the application will improve the health systems' management of the available quantities of blood in each center, creating an organized semi-automated distribution of these quantities to the centers according to the need, organizing the work of campaigns, and informing about them. A web application is built with a smartphone application and tested on a beta environment to ensure that the idea is easy to implement and effective. In the future, it will be presented to government agencies for approval within the Kingdom of Saudi Arabia, especially with the high rates of traffic accidents that require the availability of donors in many cases.

Keywords—Blood; Donation; Mobile App; Blood Bank; Health; IoHT.

Introduction

With the significant development in the world of technology and communications that has made the world a connected society, companies and research centers are competing to provide services in new ways that are faster, more convenient, and more efficient. To achieve this, it was necessary to remove the barrier of time and space and enable user access to services at any time and from anywhere [1].

The health sector received the most attention because of its humanitarian aspect, in addition to being a service and having a commercial aspect [2]. One of the main problems that countries suffer from in the health sector, especially developing countries, is the provision of the necessary quantities of blood in the necessary groups at the required time without delay [3]. Many lives could be at risk if the required blood is not quickly supplied. At the same time, the nature of storing and managing the collected amounts of blood adds another challenge, as it must be kept at a certain temperature and its validity monitored and tracked, as the blood's validity reaches a maximum of 45 days [4].

Blood is the fluid of life in the human body, where the human body contains from 4 to 6 liters of blood [5]. Each person has a specific blood group from one of four categories: A, B, AB, O, and each category is divided into positive and negative. A person cannot, for example, donate to a person of a different category or a person who has the same category but with a different polarity. The O- group is the rarest blood group in humans. Blood consists of three main components: platelets, blood cells, and plasma, and each has a certain validity period that a bank or blood center must pay attention to [6].

Unfortunately, the number of blood donors around the world, according to the statistics of the World Health Organization, is very small, not exceeding 1 percent, even though it is an important humanitarian process [7, 8]. The problem is magnified with the increasing number of people on Earth. More than that, the spread of diseases, wars, natural disasters, or traffic accidents generate an additional need to provide quantities of blood [4]. More than that, some diabetics or patients with leukemia or Thalassemia need to provide large amounts of blood periodically [9]. Relying on relatives and friends is insufficient and ineffective in critical or emergency circumstances, especially if the patient is from a minority group in the place where they live [10].

Therefore, it is very necessary to implement technology to improve management and organization of blood banks by helping to facilitate their collecting, preserving, storing, and distributing blood quantities, and thus obtaining higher quality, motivating donors to donate, and increasing the donors' numbers continuity, and loyalty. The Internet of Things [11] employs sensors within centers to monitor temperature and humidity, and radio identifiers contribute to tracking some patients or distribution operations. Also, web applications with clouds [12] can provide reliable and automated data management, and machine learning algorithms can analyze this data [13] to predict the requested quantities or the number of donors. Smartphone applications also facilitate accessing and communicating with users, especially location-based services.

Blockchain [14] can enhance data security, ensure reliability and transparency in supplying blood quantities, and manage distribution operations. Finally, social media can play an important media and awareness role to encourage people to donate.

Despite the advancement in technology, many countries like Saudi Arabia are still using a manual system [15]. The following the main steps take a lot of time and effort:

- Register: fill form for donation in certain times which advertises about them previously in health centers.
- Answering some questions.
- Medical check for donor status and their ability to donate in addition to the anatomy of blood group.
- Doing some medical checks to ensure that the blood is capable and there are no diseases.
- When the sample of blood arrives, it is to be put in tubing.
- Putting blood in the freezer at a suitable temperature.
- Storing the current amounts in the paper records.
- Saving donor data in the paper records.
- The demander for donation should do the previous process.
- Testing the availability of the requested amount for the patient in need.
- In case of unavailability of the requested amount, it will be advertised at the transmission or connecting with nearby centers or taking advantage from the sites that provide phone numbers for donors or relatives of patients.

Therefore, the focus of this research was also on a simple problem, which is providing quantities of blood in health centers when needed quickly and effectively to contribute to preserving the lives of those in need. In addition to motivating donors and communicating with them on a semi-permanent, effective, and easy-to-use basis to ensure that the necessary quantities are provided continuously. This research presents the idea of a web application to manage quantities, centers, awareness operations, and campaigns, with the idea of having a main center, a blood bank, with small centers within each health center. The system provides a live map showing the status of each center and the available quantities of each blood group in real-time so that the blood center can provide early supplies to these centers before blood shortage becomes a real problem.

The research also presents a new idea for a web application that motivates donors to donate by displaying information about the benefits and importance of donation, whether health, religious, humanitarian, or even societal. The application also sends alerts about campaigns and their locations, and most importantly, it allows the registration of accounts for donors, with the need to examine them at the nearest health center to verify their blood type and that they are free from chronic diseases. Finally, the application presents an idea for emergency management through its reliance on crowdsourcing.

The proposed applications were built taking into account the quality and the stakeholders' requirements, which were collected and classified within several previous types of research. We will detail these requirements in the next section. The rest of the sections will be a discussion of previous studies and solutions in the field of blood donation and related issues, and then we will discuss the proposed solution in detail, and finally, we will discuss some challenges and development prospects before the conclusion section.

Related Works

As it is known, health systems, in all countries of the world, even developed ones, still need further development and integration with modern technology to reach optimal solutions to current problems. In the management of blood donation operations, for example, there is a lot of wasted effort and cost and time which is suboptimal for centers and donors. There is also a large margin of risk for patients due to the delay in providing the required amounts of blood sometimes promptly or immediately. Therefore, the research focused extensively on presenting solutions to this problem, knowing that the donation process is still a voluntary matter. The following is a collection of research that provided different solutions to the research problem, and they were classified according to the proposed approach:

Questionnaires and statistical studies

This research [7] was a study of the preferences of users of smart applications in the field of blood donation with employees of donation centers. 418 people participated in the study, and the most important influencing features were: the ability to request a donor quickly when needed, the appearance of the nearest follow-up center and the locations of the centers on the map, protecting the privacy of donors' data, the need to provide educational materials to encourage donation, and the need to use reminder notifications. The researchers in [16] focused in their study on the factors that guarantee the loyalty and sincerity of donors, the most important of which was protecting the privacy and facilitating the donation process. In [17], the researchers found through a survey that the most important incentives for donation are that the patient is known to the donor and also the behavior of the staff working in the donation centers in addition to the level of privacy and safety provided in the center.

Employment of blockchain technology

This research [18] presented the idea of employing blockchain technology to solve the problems of great waste and lack of oversight in managing blood donations, transfusions, and examinations to verify its safety from viruses or infectious diseases. The network will link the donor, the medical center, and examination and verification centers to follow up on the quantities accurately and raise the level of transparency and reliability.

Promote blood donation

The research [19] presented the idea of an application that communicates permanently with the target audience, as the application displays a schedule for the available donation days, and information about the centers and their locations, in addition to reliable information about the benefits of donation. The research also referred to the role of medical institutes in drawing attention and conducting awareness campaigns and periodic donation campaigns. Some suggested the idea of scoring points for donors to further motivate them to donate [9]. Others in [20, 21] discussed the use of social media to provide information that facilitates donor communication with centers and provides them with the necessary information about campaigns, donation centers, and their benefits.

Management systems for blood banks

The research [8, 22] proposes the use of Internet of Things techniques to monitor blood quantities, and the conditions necessary to maintain the safety of samples and stored quantities. In [23] it was proposed to distribute RFID Tags to donors to facilitate tracking of their location with pseudonyms to protect privacy. The use of weight and temperature sensors would be used within the centers to regulate the available blood quantities. On the other hand, the researchers in [6] proposed building a smart system to monitor and organize the operations of the centers by linking and integrating them through a cloud. The researchers also proposed in [24] the idea of a central blood bank that manages the other centers and the quantities available in each of them to prevent waste and ensure optimal use of the available quantities.

Data analysis and smart algorithms

The research [9] suggested using data mining to analyze the donations' history and support the health administration's decision on the places and times of making available donations. In [4] the researchers employed neural networks to predict the amounts of blood required at a future date, which will contribute significantly to reducing the percentage of emergency cases turning into dangerous ones. In [25, 26] they used data mining and machine learning algorithms to match between donors and those in need of blood to send to the right person. The research in [27] improved the process of finding the closest donor by Dijkstra's algorithm.

Employment of smart applications

The researchers in [28, 29] discussed the quality standards that must be available in smart blood donation applications, and their importance to donor satisfaction, and the most important requirements are the protection of personal information, accessibility, ease of use, and the services and features provided by each application. The researchers in [30] presented the idea of an application to communicate with nearby donors easily to solve the problem of requesting from distant places. In [31], an application was proposed to schedule appointments and donation campaigns and facilitate access to them for donors. In [32], they proposed an application to record donor data and communicate with them when needed.

However, despite the previous suggestions, there are still challenges facing these solutions and systems [33]. The biggest of these challenges is the issue of privacy for donor data [34], the difficulty of use due to the spread of many applications with single solutions, and finally the ineffectiveness of the previous systems and solutions in emergencies. Therefore, this research provides an integrated solution to the problems and challenges of blood donation through a web system, central cloud management, and a mobile application that facilitates the process of managing information, campaigns, appointments, and donor data, with a quick and effective alert mechanism to solve the problem of emergency cases.

Proposed Solution

This research presents an integrated electronic system for managing medical centers, linking the centers with a central blood bank, and building an application that works on smartphones for donors so that it is easier to register and follow up on important information and alerts. The application takes into account the nature of the Saudi society; a statistical study showed that there is a weak level of knowledge about the importance of donation and campaign, and fear among females that donation may cause anemia, while for males the problem of time is the main obstacle. Respondents also emphasized the fear for the privacy of their data when they subscribed to some public web applications that let patients communicate directly with the donor [35].

The proposed electronic system provides a solution to all previous problems, as it provides a central mechanism for controlling and tracking blood quantities in each health center, in addition to controlling health information and preventing false information. The system supports the process of requests between the same centers when the quantity of a certain group decreases in one of the centers, thus achieving an optimal distribution and exploitation of the available quantities and reducing waste. The proposed system also provides a service for the center for urgent requests in emergency cases, where an alert is sent to all registrants close to the center who have the same required group. The application allows for managing donation campaigns and dates, managing medical centers and their location on a map that displays an updated real-time status of medical centers and the quantities available in each center of each blood group. The following are the functional requirements for the proposed system:

The user

- The user can create an account within the system, noting that the account becomes documented when the user visits the center and performs the necessary tests.
- System login.
- View the locations of health centers on the map, in addition to the status of each center, according to the quantities of blood available to it in each group.
- Receiving alerts about campaign dates or a center's need for blood (if the required blood group matches the user's group).
- Search for a specific health center.
- Enabling the user to take pictures during the donation and share them on social networking sites.
- View available donation schedules at each center.
- Read useful medical information about the importance and benefits of donating blood.

System Administrator

- Manage health centers and their condition.
- Manage user accounts.
- Send alerts.
- Manage donation dates and campaigns.
- Manage Medical news and articles.

Medical Center

- Manage the quantities of blood available in each group and synchronize them with the main center.
- Modify the status of the account to active after performing the necessary checks.
- Manage requests for nearby branches.
- Manage adjustments in blood quantities available after donation campaigns or dates.
- Send an emergency request for a blood group.

The non-functional requirements related to quality standards are:

- Usability: any user can use the app without needing training or previous information.
- Availability: the app will be operational 24/7 from anywhere at any time.
- Security and Privacy: the system provides privacy and security by following specific steps in the programming such as using encryption for users' accounts and data and using nicknames for donors.

Suggested interfaces

Figure 1 shows the visualization of the databases used for the proposed system. While Figure 2 shows the visualization of the user interfaces for creating an account and viewing the status of the centers, as each center appears on the map in a specific color that expresses the state of need, and when clicking on the marker for the center, the type of need appears.

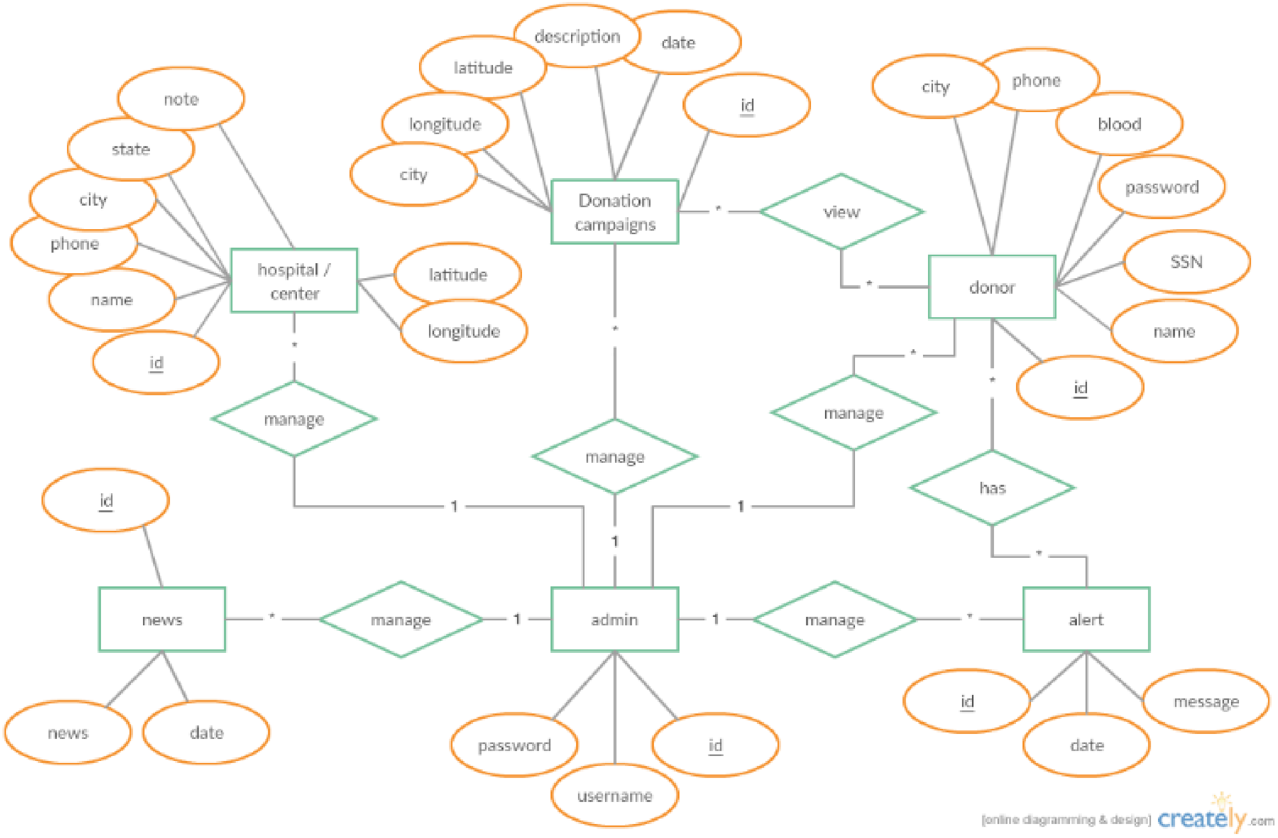


Figure 1 -ER Diagram for Proposed System

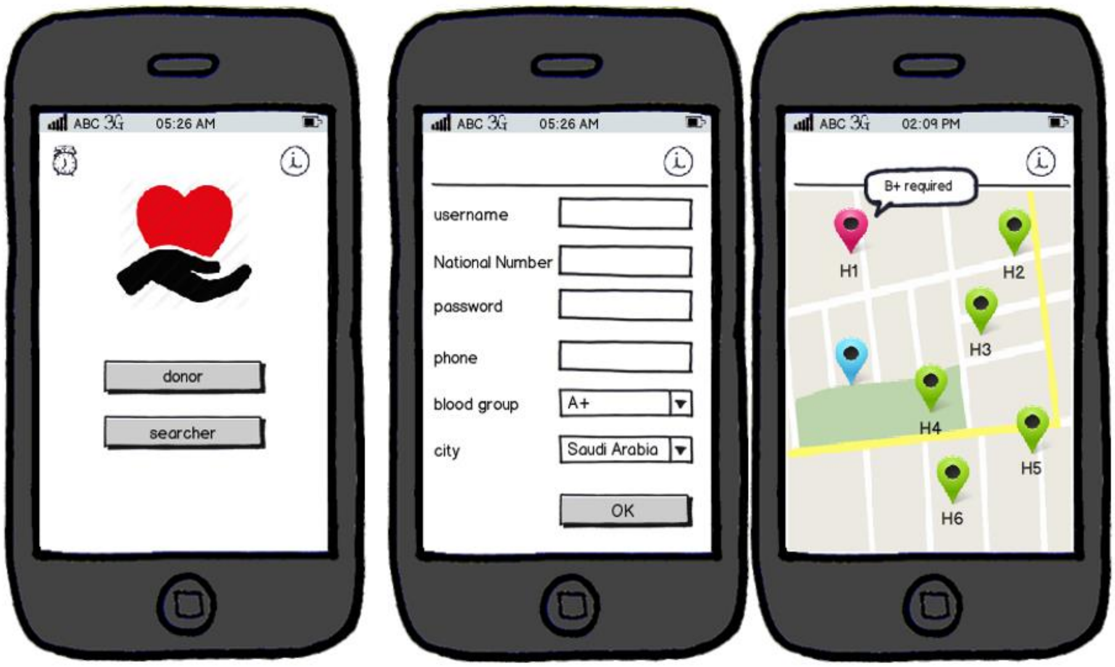
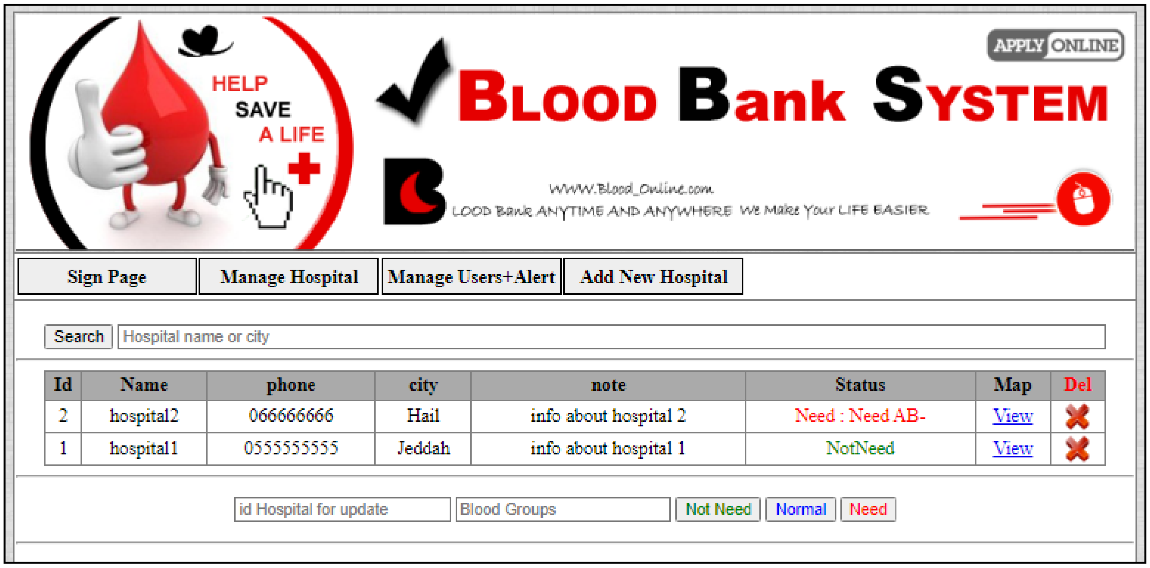


Figure 2 - Virtual visualization of user interfaces

Figure 3 displays the health centers management web page and the status of each center, contact number, and location of each on the map as shown in Figure 4. Note that the color of the Marker changes according to the condition of the hospital and the rate of need. Figure 5 shows the emergency alerts management page, where an alert can be sent to all donors in a specific city with a specific blood group. Finally, Figure 6 shows the simple interface of the user's services on the smartphone, where they can view the health centers' status, locations, and information, in addition to receiving alerts in case of an emergency or campaign dates.



Hospital name or city

Id	Name	phone	city	note	Status	Map	Del
2	hospital2	066666666	Hail	info about hospital 2	Need : Need AB-	View	✖
1	hospital1	0555555555	Jeddah	info about hospital 1	NotNeed	View	✖

id Hospital for update

Blood Groups

Figure 3 - Management of health centers and their case of need

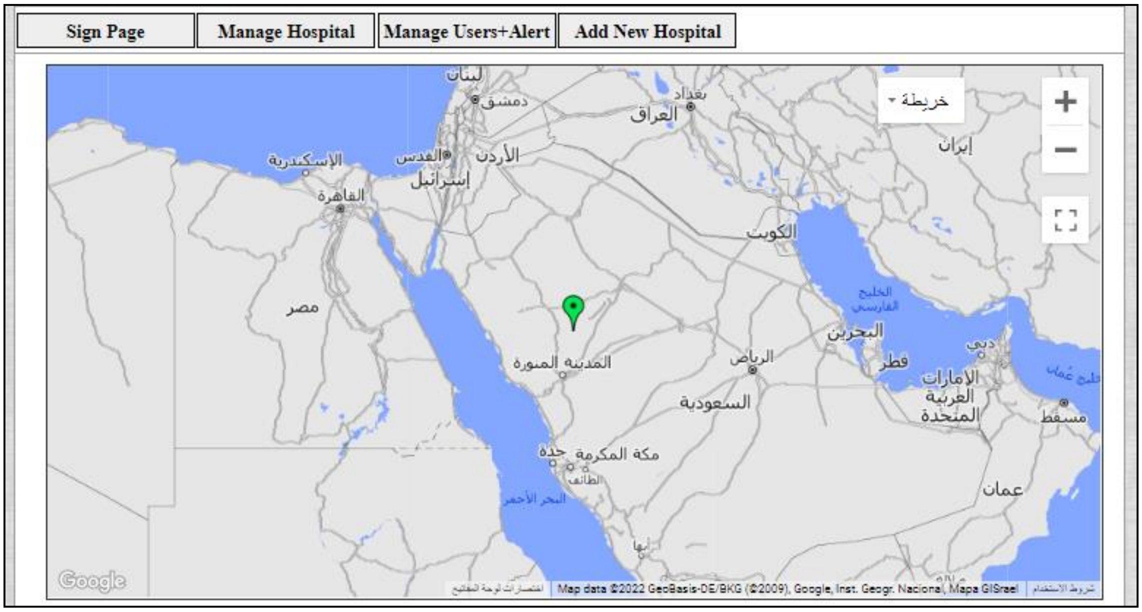
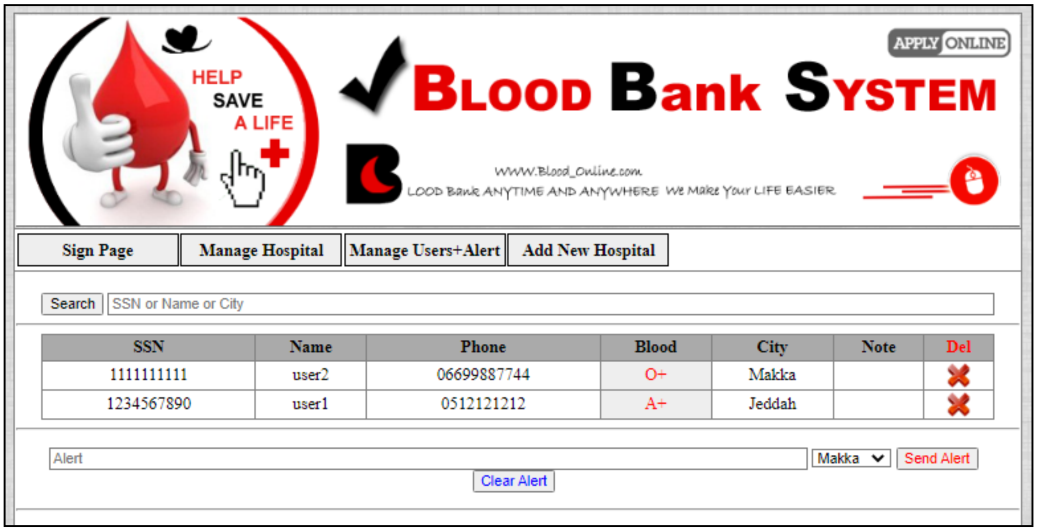


Figure 4 - Showing the location of centers on the map, with a distinctive color for the need case



SSN	Name	Phone	Blood	City	Note	Del
1111111111	user2	06699887744	O+	Makka		✖
1234567890	user1	0512121212	A+	Jeddah		✖

Figure 5 - Managing alerts according to donor data and locations

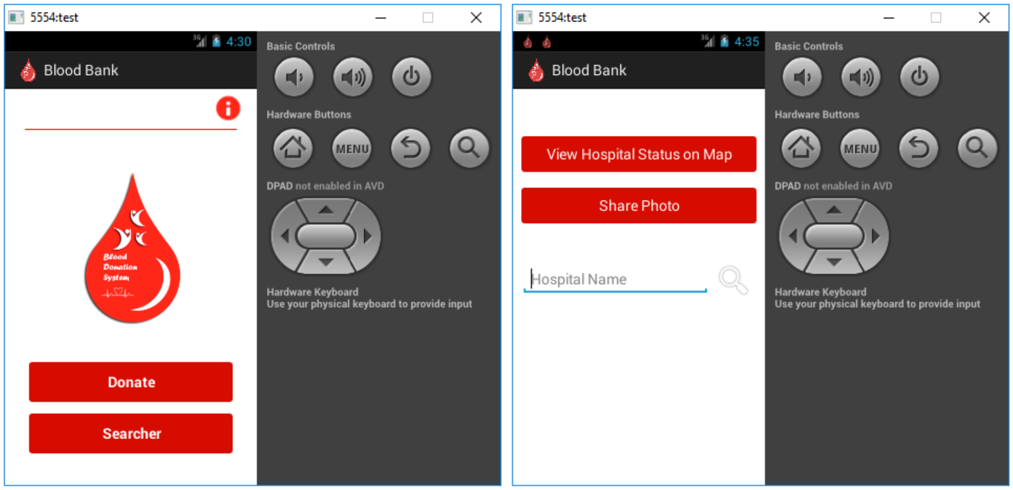


Figure 6 - Image of the main interface of the smartphone application on the emulator

Conclusion

The research discussed the problem of providing blood quantities in health centers, managing them in a way that prevents waste and reduces the risk of emergency cases, and providing a quick and effective alert mechanism for donors. It also discussed creating a support and motivation mechanism by notifying about donation campaigns and their dates, in addition to providing medical information about the benefits of donation, and allowing users to share their photos during donation on social media sites to motivate friends and family, and remove barriers of fear of donating. The research presented the idea of an integrated application, to manage the donation process, and presented an innovative idea to track the status of the centers on the map in an interactive manner with different colors in the degree of need, to help decision-makers determine more effective dates, times and places for donation campaigns. Pseudonym encryption is mainly used to protect the privacy and security of users' data. However, in the future, detailed work will be done to provide a more effective solution to the problem of privacy and the protection of donor sites, in addition to employing Internet of Things technologies in a way that makes the proposed solutions more intelligent and effective.

References

[29] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, "Preserving privacy in internet of things: a survey," *International Journal of Information Technology*, vol. 10, no. 2, pp. 189–200, Feb. 2018, doi: 10.1007/s41870-018-0113-4.

[30] N. M. Bahbouh, S. S. Compte, J. V. Valdes, and A. A. A. Sen, "An empirical investigation into the altering health perspectives in the internet of health things," *International Journal of Information Technology*, Jul. 2022, doi: 10.1007/s41870-022-01035-3.

[31] V. Siruvoru, N. V. Kumar, and Y. B. Santhosh Kumar, "Smart Blood Bank System Using IOT," *International Conference on Computer Networks and Communication Technologies*, pp. 755–765, Sep. 2018, doi: 10.1007/978-981-10-8681-6_69.

[32] A. M. Barhoom, "Blood donation prediction using artificial neural network," *International Journal of Academic Engineering Research (IJAER),*Vol. 3 Issue 10, Pages: 1-7, October – 2019.

[33] S. N. Diba, "Blood donation application with implementation of machine learning," *Doctoral dissertation, BRAC University*, 2018.

[34] R. R. Mahalle, and S. S. Thorat, "Smart Blood Bank Based On IoT: A Review," *International Research Journal of Engineering and Technology (IRJET),* Vol. 05 Issue: 01, 2018.

[35] A. A. Batis and A. Albarrak, "Preferences and features of a blood donation smartphone app: A multicenter mixed-methods study in Riyadh, Saudi Arabia," *Computer Methods and Programs in Biomedicine Update*, vol. 1, p. 100005, 2021, doi: 10.1016/j.cmpbup.2021.100005.

[36] R. D. Ismail, H. A. Hussein, M. M. Salih, M. A. Ahmed, Q. A. Hameed, and M. B. Omar, "The Use of Web Technology and IoT to Contribute to the Management of Blood Banks in Developing Countries," *Applied System Innovation*, vol. 5, no. 5, p. 90, Sep. 2022, doi: 10.3390/asi5050090.

[37] G. Maji, N. C. Debnath, and S. Sen, "Data Warehouse Based Analysis with Integrated Blood Donation Management System," *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, Jul. 2018, doi: 10.1109/indin.2018.8471988.

[38] J. K. Makin, K. L. Francis, M. J. Polonsky, and A. M. N. Renzaho, "Interventions to Increase Blood Donation among Ethnic/Racial Minorities: A Systematic Review," *Journal of Environmental and Public Health*, vol. 2019, pp. 1–14, Apr. 2019, doi: 10.1155/2019/6810959.

[39] M. Yamin, A. M. Basahel, and A. A. Abi Sen, "Managing Crowds with Wireless and Mobile Technologies," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–15, Aug. 2018, doi: 10.1155/2018/7361597.

[40] A. A. A. Sen and M. Yamin, "Advantages of using fog in IoT applications," *International Journal of Information Technology*, Oct. 2020, doi: 10.1007/s41870-020-00514-9.

[41] A. Namoun, A. A. Abi Sen, A. Tufail, A. Alshanqiti, W. Nawaz, and O. BenRhouma, "A Two-Phase Machine Learning Framework for Context-Aware Service Selection to Empower People with Disabilities," *Sensors*, vol. 22, no. 14, p. 5142, Jul. 2022, doi: 10.3390/s22145142.

[42] Y. Alsaawy, A. Alkhodre, N. M. Bahbouh, A. A. Sen, and A. Nadeem, "Lightweight Chain for Detection of Rumors and Fake News in Social Media," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 8, 2021, doi: 10.14569/ijacsa.2021.0120860.

[43] A. I. O. Yahia, "Management of blood supply and demand during the COVID-19 pandemic in King Abdullah Hospital, Bisha, Saudi Arabia," *Transfusion and Apheresis Science*, p. 102836, Jun. 2020, doi: 10.1016/j.transci.2020.102836.

[44] J. R. da Silva *et al.*, "MHealth Technology as a Tool to Promote Blood Donation," *Proceedings of the 11th International Joint Conference on Biomedical Engineering Systems and Technologies*, 2018, doi: 10.5220/0006597804710477.

[45] S. Mohammed and H. B. Essel, "Motivational factors for blood donation, potential barriers, and knowledge about blood donation in first-time and repeat blood donors," *BMC Hematology*, vol. 18, no. 1, Dec. 2018, doi: 10.1186/s12878-018-0130-3.

[46] B. Choudhury, N. Dewri, P. Das, and A. Nag, "Blockchain-IoT Based Blood Supply Chain Management System," *Proceedings of International Conference on Network Security and Blockchain Technology*, pp. 356–368, 2022, doi: 10.1007/978-981-19-3182-6_29.

[47] H. Hegedus, K. Szasz, K. Simon, T. Fazakas, A. Mihaly, and K. Nagy, "Blood Notes: Software System for Promoting and Facilitating Blood Donation," *2019 IEEE 17th International Symposium on Intelligent Systems and Informatics (SISY)*, Sep. 2019, doi: 10.1109/sisy47553.2019.9111536.

[48] Moh. Nabil, R. Ihab, H. El Masry, S. Said, and S. Youssef, "A Web-based blood donation and Medical Monitoring System Integrating Cloud services and Mobile Application," *Journal of Physics: Conference Series*, vol. 1447, p. 012001, Jan. 2020, doi: 10.1088/1742-6596/1447/1/012001.

[49] A. Sümnig, M. Feig, A. Greinacher, and T. Thiele, "The role of social media for blood donor motivation and recruitment," *Transfusion*, vol. 58, no. 10, pp. 2257–2259, Sep. 2018, doi: 10.1111/trf.14823.

[50] R. Akash, A. Singh, and S. Yadav, "Iot Based Blood Bank Management System," *easychair.org*, Jun. 2021, Accessed: Sep. 20, 2022. [Online]. Available: https://easychair.org/publications/preprint/hVhP.

[51] P. S. S. Kiruthika, "Blood Bank Monitoring and Blood Identification System Using Iot Device," *Annals of the Romanian Society for Cell Biology*, vol. 25, no. 6, pp. 182–192182–192, May 2021. [Online]. https://www.annalsofrscb.ro/index.php/journal/article/view/5270

[52] S. Pargaien, A. V. Pargaien, B. Chilwal, N. Tripathi, H. Joshi, and H. Negi, "Urge To Implement IOT For Monitoring and Preventing Blood Bank System Crisis," *2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT)*, Dec. 2021, doi: 10.1109/icacfct53978.2021.9837377.

[53] M. D. Kamalesh, A. M. J., Y. Felix, D. S., and M. Prasad, "Automation of Blood Donation by Data Integration Using Data Mining," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, Jun. 2020, doi: 10.1109/icoei48184.2020.9143010.

[54] S. N. Diba, "Blood donation application with implementation of machine learning," *dspace.bracu.ac.bd*, 2018. http://hdl.handle.net/10361/10130.

[55] S. Ahdan and S. Setiawansyah, "Android-Based Geolocation Technology on a Blood Donation System (BDS) Using the Dijkstra Algorithm," *IJAIT (International Journal of Applied Information Technology)*, vol. 5, no. 01, p. 1, Jul. 2021, doi: 10.25124/ijait.v5i01.3317.

[56] A. Idri, L. Sardi, and J. L. Fernández-Alemán, "Quality Evaluation of Gamified Blood Donation Apps using ISO/IEC 25010 Standard," *Proceedings of the 11th International Joint Conference on Biomedical Engineering Systems and Technologies*, 2018, doi: 10.5220/0006724806070614.

[57] L. Melián-Alzola and J. D. Martín-Santana, "Service quality in blood donation: satisfaction, trust and loyalty," *Service Business*, vol. 14, no. 1, pp. 101–129, Nov. 2019, doi: 10.1007/s11628-019-00411-7.

[58] H. D. Das, R. Ahmed, N. Smrity, and L. Islam, "BDonor: A Geo-localised Blood Donor Management System Using Mobile Crowdsourcing," *IEEE Xplore*, Apr. 01, 2020. https://ieeexplore.ieee.org/document/9115776/authors#authors (accessed Aug. 23, 2021).

[59] A. Casabuena *et al.*, “BloodBank PH: A Framework for an Android-based Application for the Facilitation of Blood Services in the Philippines,” *IEEE Xplore*, Oct. 01, 2018. https://ieeexplore.ieee.org/document/8650395 (accessed May 18, 2021).

[60] B. S. Shukur, M. M. Mijwil, and N. A. Al-Sammarraie, “Mobile-base Registration System for Blood Donation (MBRS-BD),” *Asian Journal of Research in Computer Science*, pp. 36–45, Oct. 2022, doi: 10.9734/ajrcos/2022/v14i4290

[61] S. AlZu’bi, D. Aqel, and A. Mughaid, “Recent intelligent Approaches for Managing and Optimizing smart Blood Donation process,” *2021 International Conference on Information Technology (ICIT)*, Jul. 2021, doi: 10.1109/icit52682.2021.9491125.

[62] S. Periyanayagi, A. Manikandan, M. Muthukrishnan, and M. Ramakrishnan, “BDoor App-Blood Donation Application using Android Studio,” *Journal of Physics: Conference Series*, vol. 1917, no. 1, p. 012018, Jun. 2021, doi: 10.1088/1742-6596/1917/1/012018.

[63] M. Abolfotouh, M. Al-Assiri, A. Al Askar, A. AL-Johar, M. AL-Omani, and A. AL-Hakbani, “Public awareness of blood donation in Central Saudi Arabia,” *International Journal of General Medicine*, p. 401, Aug. 2014, doi: 10.2147/ijgm.s67187

A Framework for Supporting Ambient Assisted Living for Users of Special Needs

Bahbouh, N. M., Abi Sen, A. A., Alsehaimi, A. A. A., & Alsuhaymi, E. A. (2022, March). A framework for supporting ambient assisted living for users of special needs. In *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 427-432). IEEE.

Abstract

Healthcare improvements cannot be ignored, especially in the face of advanced technology. Technology also plays a critical role in controlling the spread of viral diseases and providing assistance to physically challenged people. The organization of many health services is heterogeneous, and they often work in isolation from each other. This adversely affects the provision of a better quality of services, integration between them, and creates new issues. This paper has proposed a framework for supporting ambient assisted living. The framework integrates all services in one place and enables cooperation amongst them to make them smart services. In doing so, a review of the available services, used in the proposed framework, is also conducted. The proposed framework is designed to act as a broker between service providers and end-users, which would enhance the accessibility and usability of the services.

Keywords— Disabled Users, Special Needs, Interoperability, Integration, Internet of Health Things (IoHT), Smart Services.

Introduction

More than 15% of the world's population suffers from disability problems that limit their ability to live normally and participate in social and economic life [1]. Around 10% of the old age need exceptional care or require staying in health centers permanently. That means isolation from their social environment, their families hence increasing the expenses of treatment [2].

The Internet of things (IoT) and the great development in the speed and availability of communications (especially after the 5G and cloud services) have enabled the service providers to create millions of services and assist in solving the problems which we face in our daily life. People with special needs have the largest share of these new services [3]. Therefore, the IoT and modern technologies have brought hope for a better future and smarter life. Practically, IoT collects data of users and sends it to systems which analyze it to create more adaptive and advancing services [4].

For example, wearable sensors provide an effective and real-time monitoring mechanism between the patient and his family or his doctor. In this way, the patient does not need to stay in the hospitals and costs additional expenses. Sensors are accompanied by smart systems and applications that collect data coming from these sensors. The data includes vital signs and measurements about the patient (such as temperature, blood pressure, diabetes, heart rate, respiratory rate, oxygen percentage in the blood, muscle activity rate and person's activity rate and daily step count, etc.) [5].

Intelligent systems analyze the collected data quickly and automatically without human intervention. They predict any emergency event before it occurs, or they detect it early and send alerts to the health center or doctor to take the right action immediately and prevent the situation from deteriorating further. This action preserves the patient's life and reduces the risk significantly [6].

Often the objects of the IoT (Wireless Sensors Networks or Radio Frequency Identifiers) are limited in computing power, storage, and energy. So, we need cloud services to process data away from where is collected [7][8].

To address the problem of the time lag of cloud services and increase the level of availability and performance, fog computing is used also. Fog usually integrates with cloud computing, where fog nodes are deployed at the edge of the network near the end-user and its smart things. So, fog nodes process data immediately and respond to any emergency event in real time without delay [9]. Then, the data is transferred to the cloud to store it permanently and to perform more complex and intelligent analysis based on machine learning algorithms. This analysis will reveal a lot of information about the patient's behavior, health condition, and predict in advance the changes that may occur in his condition [10].

Figure 1 illustrates the common architecture of the Internet of Things and shows the four main layers. The layers are:

The first layer is the sensing layer that contains smart things and users. The second layer is the fog computing layer. The third layer is cloud computing. The last layer is the applications and services layer, which depends on the data and information reported from the previous layers to provide it to the end-user easily, anywhere, and anytime via different tools like computers, tablets, phones, and even smartwatches [11].

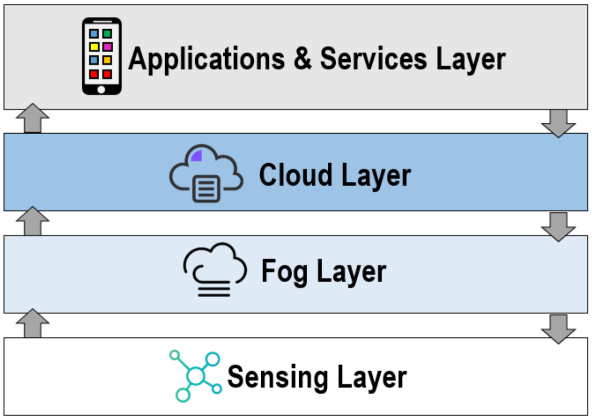


Fig. 2 Common Structure of IoT

Unfortunately, despite the progress and hope offered by the Internet of Things and the development of many sectors for people with special needs, the novel coronavirus (COVID-19) pandemic (that appeared in the last quarter of 2019) has created additional challenges for the health sector [12][13]. Most developed countries failed to effectively cope with this crisis in their initial years, which greatly affected their economies and the persistence of the pandemic. The health institutions in these nations have stated that they are unable to contain the high number of persons who have been infected with the virus. Fearing from infection, health clinics could not accept the elderly or those with chronic conditions [14].

All the above showed a flaw in the method of employing modern technologies. These technologies did not play their ideal role during crises and pandemics, despite the deployment of thousands of support services in the health sector. The main defect is the lack of integration of these services with each other. They are provided by different providers with different technologies, communication protocols, and devices. Also, the format of data, concepts, and standards are different. This means the difficulty of cooperation between these services on one hand and the difficulty of the end user's in dealing with all provided services [15]. There is a privacy challenge too, which requires the user to trust a large number of service providers [16]-[20].

Therefore, this research seeks to reduce the previous problem by designing a framework that contains different services in one place. In this case, the end-user could live with the help of the surrounding environment by facilitating access to all these services in one trusted place which is managed by a government agency. Moreover, all services must use standard way to present to end-user and that means more usability.

The services of the proposed framework are directed to people with special needs only like the elder, chronic diseases, or disabled users. Therefore, this framework can transform ordinary homes into smart mobile health centers. That is achieved by keeping the patient under constant observation, and by integrating many useful services provided at the user's home. So, the proposed framework maintains the user's safety and reduces his need for others.

In the next section, we reviewed some important services that were provided to help people with special needs. Then we presented the proposed framework with the services and main fields or majors of them. Finally, discussed prospects for developing and supporting the current work to implement it.

Literature Review

In this section, we discuss the different works that provided useful services to people with needs in different majors of the health domain. All the services seek to enable users to live normally and independently with most of their daily tasks.

Researchers in [21] presented the idea of an effective platform for communication between the people with needs and paramedics or medical staff who are notified in the event of any defect or problem.

Other researchers have worked on the issue of the alert patient, whether for medical appointments, medications, or other useful alerts for people with needs [23]. Others [23] went to a deeper issue, which is creating a special alert for users who have hearing problems (e.g., deaf users). They designed special wearable bracelets that generate a gentle vibration to alert the user, in addition to automatic calls to the doctor and ambulance according to the patient's current condition and degree of severity.

The researchers in [24] focused on people who suffer from other disabilities which as sight problems (e.g., blind users). The user can control the home's appliances through voice. This leads to facilitating the process of communication with family members, doctors, or even markets and drivers by voice commands and smartphones.

A large part of the researchers started working on data processing to provide special algorithms for proactively predicting events. For example, researchers in [27] provided a contextually adaptive environment for students with special needs based on machine learning algorithms.

Many researchers have presented different methods and tools of wearable sensors such as shoes, clothes, bracelets, necklaces, rings, glasses, hats, etc. where each of them can provide different types of information and measurements. All the collected data has an important role in understanding more about user needs and adapting services to the current context [28].

In other researches, such as [28][29], they reviewed and presented many different scenarios which need to employ technology to serve people with needs. Such as:

- A blind student needs to interact with his teacher in a distance learning session,
- A mentally disabled user needs to remind his medications and tasks,
- Elderly user needs mobile monitoring and mobility assistance,
- Users who have mobility problems need to control the house and appliances via voice in addition to control their wheelchairs,

- A wheelchair user needs to shop physically and browse the contents of the shelves without asking help,
- A young patient of obese must be kept under constant observation by a specialist to track his vital measurements and daily activity.
- A diabetic patient, that his case unstable needs continuous monitoring and rapid prediction of the possibility of any problem with reporting the cause of instability.

Thus, the most important question here is, how to enable the independence and improve the living conditions of people with special needs. And how we can employment the Internet of Things in the proposed solutions [30].

Actually, there are many studies which used the Internet of Things in different ways:

According to G. Delnevo, et al [25] presented the idea of a smart system based on the Internet of Things. This system helps disabled users who need to move without any assistance, whether inside or outside the house. Where it is possible to use a special stick for the blind user to notify them about barriers. Also, R. M. Fikri, and H. Mintae, provide research about communicating with volunteers remotely or by integrating with the parking systems of public transportation to facilitate the process of communication [26].

As for the researchers in [22], they have employed the Internet of Things and its various tools to create continuous monitoring of patients and their vital measurements according to their needs. Then medical staff is alerted of any abnormal condition or sudden change of patient data.

According to the above studies, all service providers seek to provide their services to address real problems. But unfortunately, these solutions are still like isolated islands. Therefore, the user is enforced to master working with all of them which is very difficult for him due to the lack of a standard method and three is no unified environment that contains all these services.

Imagine if there is a cooperation between the previous services, for example, continuous monitoring with effective communication methods and different alert methods according to the context of the user in addition to a few supporting services to perform daily tasks independently. This environment would be ideal and very useful for people with needs in creating real independence in their social, economic, and even healthy life. Finally, the interaction and integration among services (Interoperability) and the protection of their privacy are two challenges facing the future of smart services and greatly limitation for additional creative ideas and smarter services.

Proposed Framework

In this research, we propose an initial design for a comprehensive framework of services for people with special needs. The framework enables them to live independently by helping the surrounding environment. The framework is the place where service providers can provide their services.

However, all services must be restricted to specific conditions which are using standard format data, commonly available protocols for communication, and similar concepts in naming and describing the functions with their inputs and outputs. This facilitates the integration among services and paves the way for more quality of services with more intelligence and adaptability. Moreover, the framework enhances usability by accessing all services in a unified reliable method without the need for trust to hundreds of service providers and online services or mobile applications.

The following Figure 2 illustrates the proposed framework. It clarifies some of the main classifications and services which must be presented in the framework, for knowing that the framework will be dynamic, which means that it accepts more classifications or services in the future.

In the first layer, the framework collects information from the user or its surrounding environment, having many tools, such as uses wireless sensors network (WSNs), radiofrequency identifiers (RFID), smart devices (refrigerator, screen, watch, etc.), smartphones, periodic questioners, and generated data of social networks. All these data will be sent to the next layer (the nearest fog node).

The fog node will temporarily store and process the data, filter the abnormal or erroneous data, and summarize some redundant data to reduce the number of connections with the service provider. The fog node will reconfigure the data in a standard format to unify it before sending it to the cloud. Also, it analyzes the simple data collected in its cache to detect any abnormal movement or change in the data that could pose a danger to the user or could require intervention from the assistant or medical team. If any dangerous case is detected, alerts will be sent to the home, the patient, the companion, the family, or the medical team depending on the nature of the alert and the current situation.

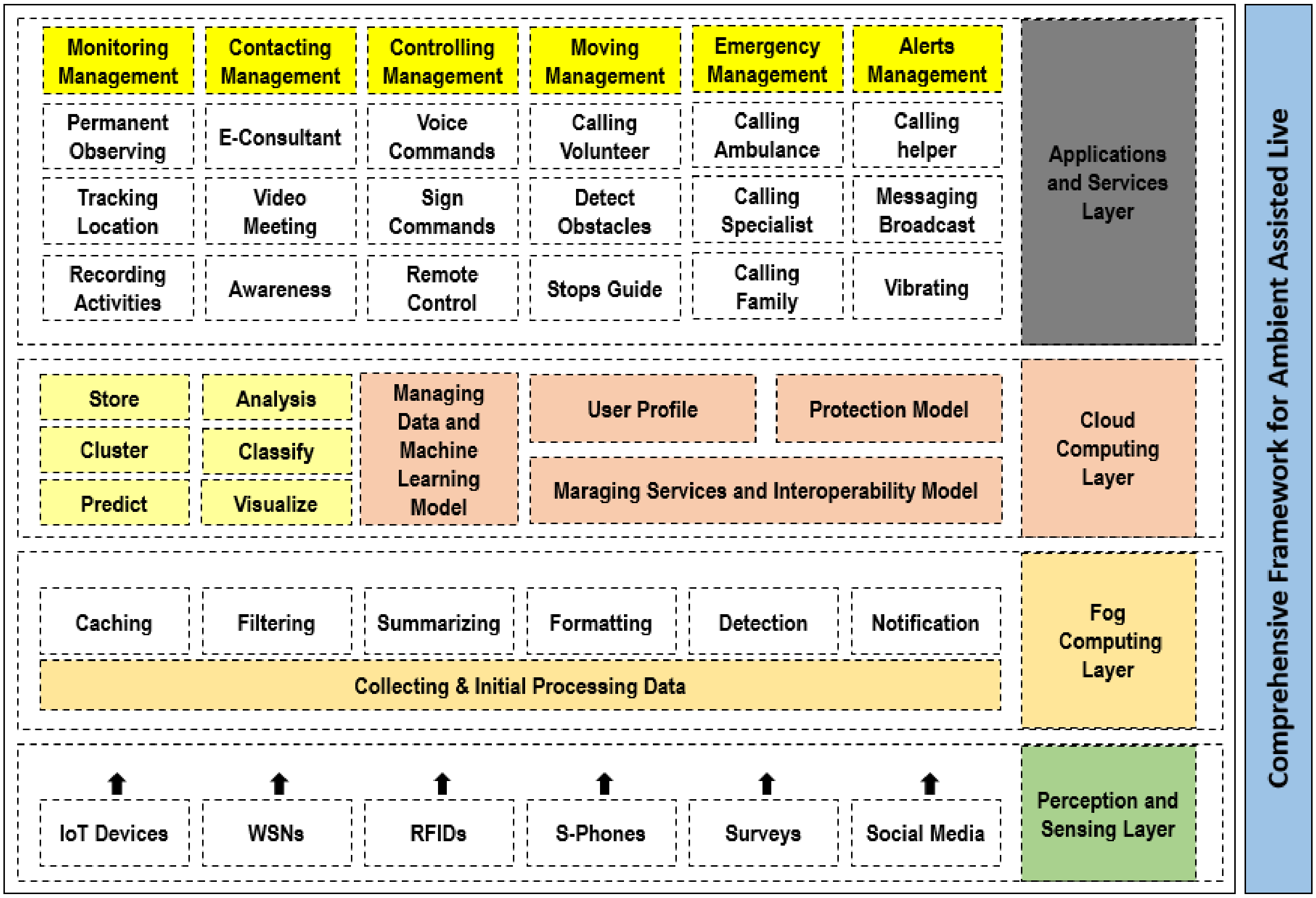


Fig. 2. Proposed Framework for Ambient Assisted Living

The cloud layer will store the summarized data permanently for future processing. All data will have a standard format and be represented by standard language (Extensible Markup Language (XML) or JavaScript Object Notation (JSON)). Cloud performs several important basic operations. The first is to protect data by encrypting it, the second is to support interoperability by providing a broker that can record the function data announced by service providers and verify that it is in the required format and verify its description. In addition, it manages the communication and cooperation between the different services. In this case, it can create more intelligent and adaptive composite services, which leads to speeding up the completion time of the composite services and not rebuilding them from scratch.

The third is related to manage data and applying machine learning algorithms. In this stage, it can be analyzed, categorized, and assembled to reveal a lot of useful information. For instance, about the health status or user behavior and needs, as well as predicting and responding to any emergency event before it becomes a major problem or danger to the user. Finally, the formation of a profile or a unified file for each user.

The last layer is the services layer, which is deployed after being registered in the cloud and ensuring that it meets the required standards. So, it enables collaboration between it and other services. The basic services are:

- Monitoring and tracking services: It may include permanent camera monitoring in some places and situations, permanent location tracking, continuous recording of user activities, etc.
- Communication services: It may be in the form of online consultations, a remote video interview, publishing a group message as awareness or alert, or even booking an appointment.
- Auxiliary services to control things: control may be via voice commands, signals, or remote control over the phone.
- Internal and external mobility assistance services: These include cooperating with a volunteer, discovering obstacles and alerting them automatically, or directing a special situation.
- Emergency response services by requesting the nearest ambulance, alerting the specialist doctor, or alerting the user's family.
- Alert services: There are several ways to alert the user such as calling an assistant, sending broadcast messages, or vibrating.

Note, there is an overlap among services and the need for cooperation among them to create a better level and more adaptive services. In addition, the various mentioned services in each section or major are to name a few. Also, the proposed framework is dynamic. So, it will be available for all service providers to provide more services and applications.

A. The features of suggested framework

There are several advantages of the proposed framework that will be achieved in the case of activation, namely:

- Usability and accessibility for all services in one place.
- Improving the level of trust where user deals with one party instead of dealing with hundreds of agencies and service providers.
- Forming a unified medical record/file for each patient to improve treatment methods and to understand the causes of diseases.
- Providing same service in different forms to improve the level of dynamism and adaptation with user’s context.
- Enabling the cooperation and integration between services to create a better level of sophisticated services.
- Improving the speed of response to emergencies without latency.
- Reducing pressure on the cloud by employing fog nodes.
- Providing health care everywhere, not only in the health centers.

B. The challenges of the proposed framework

There are some challenges which have to be addressed in the future to ensure that the proposed framework will achieve the required goals effectively. Which are:

- Privacy issue of users' data requires many solutions that are commensurate with the type of the services and data.
- Dealing with old services and systems to enable them in the proposed framework.
- Providing offers and features for service providers to motivate them to cooperate with the proposed framework.
- Creating an ontology of unified concepts for people with special needs to enable services to understand each other in the future.

Conclusion

With the increase in the number of people with special needs for care and with the new circumstances created by the Covid-19 pandemic; this research suggested a comprehensive framework for managing services and data for people with needs such as the elderly, the disabled, and those with chronic diseases. The proposed framework provides more effective and smarter services by enabling cooperation between providers to create new ones. The framework facilitates the user's accessibility to all services in one place and different ways, suitable to his situation and context. The framework enables building an accurate profile (for each user) which will play a significant role in adapting services and providing telehealth everywhere. This will improve treatment opportunities and save costs. At this stage, we just present the general design of the proposed framework structure. In the next work, we will describe all parts in detail, then we will work on applying and testing the framework within the Kingdom of Saudi Arabia. Finally, we will work hard to activate the role of the Internet of Health Things (IoHT) is an effective solution to face future pandemics.

References

[1] M. C. Domingo, “An overview of the Internet of Things for people with disabilities,” *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 584–596, Mar. 2012, doi: 10.1016/j.jnca.2011.10.015.

[2] M. Antonić, "IoT Technologies Offer New Potentials for People with Disabilities," *2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2021.

[3] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, “5G network-based Internet of Things for demand response in smart grid: A survey on application potential,” *Applied Energy*, vol. 257, p. 113972, Jan. 2020, doi: 10.1016/j.apenergy.2019.113972.

[4] Y. Perwej, K. Haq, F. Parwej, and M. M., “The Internet of Things (IoT) and its Application Domains,” *International Journal of Computer Applications*, vol. 182, no. 49, pp. 36–49, Apr. 2019, doi: 10.5120/ijca2019918763.

[5] G. Suseendran and D. Balaganesh, “Smart cattle health monitoring system using IoT sensors,” *Materials Today: Proceedings*, Mar. 2021, doi: 10.1016/j.matpr.2021.01.873.

[6] B. Muthu *et al.*, “IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector,” *Peer-to-Peer Networking and Applications*, Jan. 2020, doi: 10.1007/s12083-019-00823-2.

[7] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, “A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks,” *Sensors*, vol. 20, no. 9, p. 2495, Apr. 2020, doi: 10.3390/s20092495.

[8] B. B. Gupta and M. Quamara, “An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols,” *Concurrency and Computation: Practice and Experience*, p. e4946, Sep. 2018, doi: 10.1002/cpe.4946.

[9] A. A. A. Sen and M. Yamin, “Advantages of using fog in IoT applications,” *International Journal of Information Technology*, Oct. 2020, doi: 10.1007/s41870-020-00514-9.

[10] A. Baktyan and A. Zahary, “A Review on Cloud and Fog Computing Integration for IoT: Platforms Perspective,” *EAI Endorsed Transactions on Internet of Things*, vol. 4, no. 14, p. 156084, Dec. 2018, doi: 10.4108/eai.20-12-2018.156084.

[11] M. Tavana, V. Hajipour, and S. Oveisi, “IoT-based Enterprise Resource Planning: Challenges, Open Issues, Applications, Architecture, and Future Research Directions,” *Internet of Things*, vol. 11, p. 100262, Jul. 2020, doi: 10.1016/j.iot.2020.100262.

[12] M. Ciotti, M. Ciccozzi, A. Terrinoni, W.-C. Jiang, C.-B. Wang, and S. Bernardini, “The COVID-19 Pandemic,” *Critical Reviews in Clinical Laboratory Sciences*, vol. 57, no. 6, pp. 365–388, Jul. 2020, doi: 10.1080/10408363.2020.1783198.

[13] M. M. Almutairi, M. Yamin, G. Halikias, and A. A. Abi Sen, “A Framework for Crowd Management during COVID-19 with Artificial Intelligence,” *Sustainability*, vol. 14, no. 1, p. 303, Dec. 2021, doi: 10.3390/su14010303.

[14] M. Yamin, A. Ahmed Abi Sen, Z. Mahmoud AlKubaisy, and R. Almarzouki, “A Novel Technique for Early Detection of COVID-19,” *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2283–2298, 2021, doi: 10.32604/cmc.2021.017433.

[15] M. Noura, M. Atiquzzaman, and M. Gaedke, “Interoperability in Internet of Things: Taxonomies and Open Challenges,” *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, Jul. 2018, doi: 10.1007/s11036-018-1089-9.

[16] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” *International Journal of Information Technology*, vol. 10, no. 2, pp. 189–200, Feb. 2018, doi: 10.1007/s41870-018-0113-4.

[17] M. Yamin and A. A. Abi Sen, “A New Method with Swapping of Peers and Fogs to Protect User Privacy in IoT Applications,” *IEEE Access*, vol. 8, pp. 210206–210224, 2020, doi: 10.1109/access.2020.3038825.

[18] S. S. Albouq, A. A. A. Sen, A. Namoun, N. M. Bahbouh, A. B. Alkhodre, and A. Alshanqiti, “A Double Obfuscation Approach for Protecting the Privacy of IoT Location Based Applications,” *IEEE Access*, vol. 8, pp. 129415–129431, 2020, doi: 10.1109/access.2020.3009200.

[19] M. Yamin, Y. Alsaawy, A. B. Alkhodre, and A. A. Abi Sen, “An Innovative Method for Preserving Privacy in Internet of Things,” *Sensors*, vol. 19, no. 15, p. 3355, Jul. 2019, doi: 10.3390/s19153355.

[20] A. A. A. Sen, F. B. Eassa, M. Yamin, and K. Jambi, “Double Cache Approach with Wireless Technology for Preserving User Privacy,” *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–11, Aug. 2018, doi: 10.1155/2018/4607464.

[21] G. Kbar, and A. Shady, "SMART workplace for Persons with DISABiLitiEs (SMARTDISABLE)," *2014 International Conference on Multimedia Computing and Systems (ICMCS)*. IEEE, 2014.

[22] S. Meliá, S. Nasabeh, S. Luján-Mora, and C. Cachero, “MoSIoT: Modeling and Simulating IoT Healthcare-Monitoring Systems for People with Disabilities,” *International Journal of Environmental Research and Public Health*, vol. 18, no. 12, p. 6357, Jan. 2021, doi: 10.3390/ijerph18126357.

[23] K. Maczka and J. COWLEY, “Assessing Physically Disabled People at Home,” *International Journal of Rehabilitation Research*, vol. 14, no. 4, p. 364, Dec. 1991, doi: 10.1097/00004356-199112000-00016.

[24] R. SI, “A Framework on Health Smart Home Using IoT and Machine Learning for Disabled People,” *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 2, pp. 1–9, Feb. 2020, doi: 10.37200/ijpr/v24i2/pr200304.

[25] G. Delnevo, et al., "On enhancing accessible smart buildings using IoT," *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2018.

[26] R. M. Fikri, and H. Mintae, "Smart parking area management system for the disabled using IoT and mobile application," *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*. IEEE, 2019.

[27] M. H. Kabir, M. R. Hoque, H. Seo, and S.-H. Yang, “Machine Learning Based Adaptive Context-Aware System for Smart Home Environment,” *International Journal of Smart Home*, vol. 9, no. 11, pp. 55–62, Nov. 2015, doi: 10.14257/ijsh.2015.9.11.07.

[28] A. Koumpis and D. Tektonidis, “Accessible Internet-of-Things and Internet-of-Content Services for All in the Home or on the Move,” *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 6, no. 4, Oct. 2012, doi: 10.3991/ijim.v6i4.2190.

[29] A. Prakash, “Smart Mobility Solutions for a Smart City,” *IEEE Potentials*, vol. 40, no. 1, pp. 24–29, Jan. 2021, doi: 10.1109/mpot.2020.3023539.

[30] N. Vasco Lopes, “Internet of Things feasibility for disabled people,” *Transactions on Emerging Telecommunications Technologies*, p. e3906, 2020, doi: 10.1002/ett.3906.

A Smart Application to Enhance Health Society Awareness

Alanazi, K., Bahbouh, N. M., Abi Sen, A. A., & Yamin, M. (2024, February). A Smart Application to Enhance Health Society Awareness. In 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 93-99). IEEE

Abstract

Community health plays a pivotal role in establishing and sustaining a thriving society, serving as a vital indicator of a country's development, maturity, and progress. A key factor in advancing community health is fostering awareness among its members. Unfortunately, even in advanced countries, there is currently a lack of accredited, reliable, and comprehensive platforms for health awareness. This issue has become increasingly significant in the age of social media, where vast amounts of misinformation are easily disseminated. This research introduces the concept of a platform and a smart application designed to support and enhance health awareness within the community. The proposed application encompasses various essential health services, including a user-friendly search engine for medication queries, nutritional or exercise programs, and information about health centers. Furthermore, the application acts as a link between health management and community members, facilitating the dissemination of medical advice, news, campaign schedules, and workshop information. The application also provides an avenue for medical consultations and serves as a platform for recording and collecting individuals' daily health data for early warning purposes. The collected data not only presents an opportunity for research and testing but also supports medical decisions based on information and crowd-sourced data. In the current phase, we have developed a demo featuring proposed interfaces for the application in an Android environment, serving as a testing version.

Keywords — Health; Medical; Awareness; Search Engine; Advise, Pandemic, Diseases.

Introduction

The significant advancements in modern technology bring about numerous changes and a pressing need for the development of various aspects of life. Given the overall importance of the medical field, numerous research initiatives and projects have been dedicated to remarkably enhancing and providing medical services [1, 2].

Unfortunately, despite the revolution in health services, there is still a widespread prevalence of various diseases in our societies in recent years, along with the emergence of new types of viruses. This can be attributed to the limited health knowledge among ordinary users, coupled with the high costs associated with traditional health consultations at centers or hospitals. Furthermore, the fast-paced nature of the current era leaves many users with little time for frequent internet searches to obtain health and general information. There is a real need for tools that assist users in refreshing and enhancing their knowledge from anywhere, at any time, with ease and minimal effort. Additionally, these tools should provide frequent reminders about the latest health news and notifications [3-5].

The Health Annual Report of Saudi Arabia indicates a growing need for attention and further development to achieve health equity across all regions in the Kingdom. Figure 1 illustrates the structure of the health system in Saudi Arabia, emphasizing the significant proportion of health centers under the Ministry of Health. This underscores the importance of implementing a system, like the proposed one, to maximize the utilization of these centers and ensure equitable service deployment across all regions of the Kingdom. The table below presents statistics from the World Health Organization regarding the number of hospitals and centers in each region. It highlights the shortage of specialized hospitals in certain areas, emphasizing the necessity of addressing these gaps [6-7].

Medical awareness plays a crucial role in enhancing the efficiency of the healthcare sector, and smart devices can significantly contribute to the promotion of medical awareness. Consequently, there is potential for a decrease in the prevalence of diseases within society. The primary goal of this research is to impart health education to individuals, fostering a healthier society and, consequently, a more robust and resilient community [8-9].

Currently, the Kingdom of Saudi Arabia lacks a comprehensive medical awareness system. While there are occasional individual or governmental initiatives such as events in malls, television programs, advertisements on social networking sites, and general mobile messages, these methods prove to be ineffective due to users' limited time and availability. Additionally, many users tend to skip advertisements on social media, emphasizing the urgent need for a new, effective tool in this crucial area [10-11].

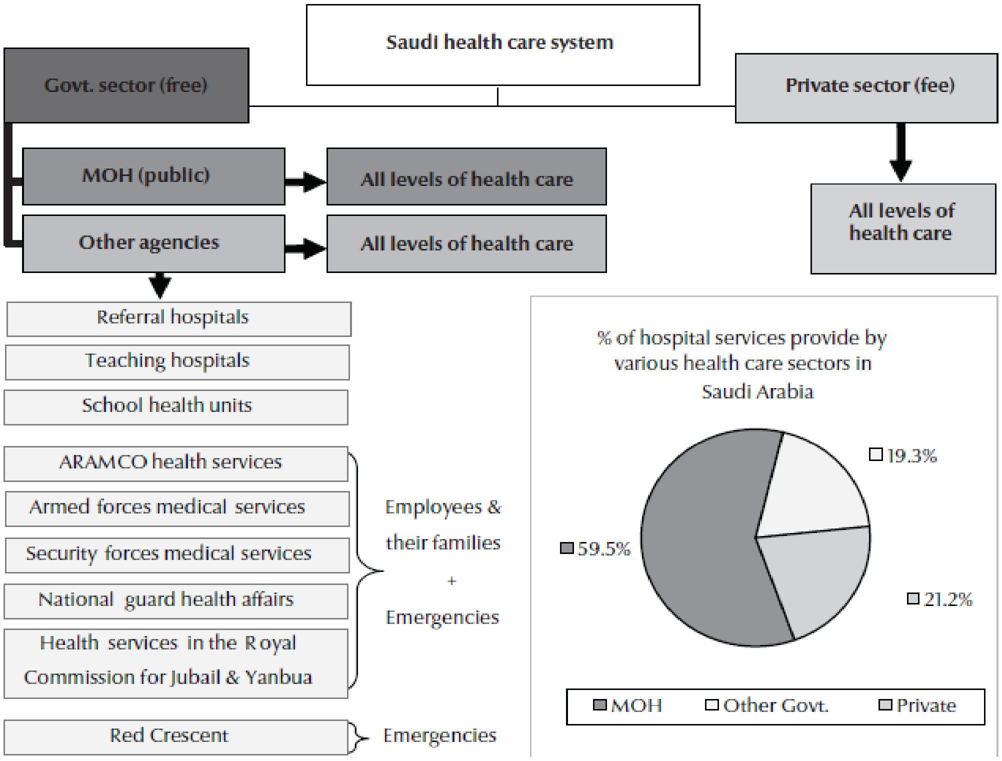

Saudi health care system
Govt. sector (free)
Private sector (fee)
MOH (public)
All levels of health care
Other agencies
All levels of health care
All levels of health care
Referral hospitals
Teaching hospitals
School health units
ARAMCO health services
Armed forces medical services
Security forces medical services
National guard health affairs
Health services in the Royal Commission for Jubail & Yanbua
Employees & their families + Emergencies
Red Crescent
Emergencies
% of hospital services provide by various health care sectors in Saudi Arabia
19.3%
59.5%
21.2%
MOH
Other Govt.
Private

Figure 1. Saudi Health-Care System

Smartphones have become ubiquitous over the last few years. We use these devices for multi-purpose tasks in our daily lives. It is very important to utilize this device to develop a system that can raise the health awareness of users, where the health sector is one of the most major in any society [12-14].

This research introduces a health platform with a smart application designed to enhance awareness in Saudi Arabia. The contributions of this research include:

1. Harnessing the smartphone revolution to disseminate knowledge to a wider audience.
2. Elevating the overall health and health awareness levels among the people in the kingdom.
3. Establishing an easy and effective communication channel between health experts and citizens.
4. Offering a rapid notification tool to alert citizens about any health issues in their area.
5. Providing a useful and user-friendly search tool for information on various diseases or medications.

The second section will present a variety of previous applications that offer services in this sector. Meanwhile, the third section will provide a comprehensive description of the proposed applications and services. The fourth section will detail the implementation process, followed by the conclusion and future trends.

Related Works

The health sector is considered one of the most important areas of life, and this is what most researchers have urged to work on developing, especially with the great development in the means of technology and communication such as smartphone applications and the Internet of Things IoT.

The research emphasizes the importance of health awareness through various awareness campaigns in improving the level and quality of healthcare services. It suggests choosing media that align with different age groups during awareness campaigns, in addition to focusing on initiatives and community participation. However, these methods face challenges in terms of evaluation [15].

During the COVID-19 pandemic, the international community received daily updates on new information related to the disease, especially given its novelty and rapid spread. People were highly receptive to this information and acted on the advice. The majority of individuals in the study area dealt with the COVID-19 pandemic similarly, regardless of age, education, or healthcare-related involvement. The community's perceptions were significantly influenced by the government's primary healthcare approach and behavioral changes through awareness [16].

The paper discusses technological changes, which can play a significant role in promoting health by raising health awareness. Health risks among teenagers, including smoking, alcohol consumption, obesity, lack of physical activity, and unhealthy diet, contribute to the increase in chronic diseases. Preventive measures against such diseases and unhealthy habits involve promoting health awareness through web and mobile applications that support self-monitoring and behavior change [17].

The study shows that individuals with higher education have better health compared to their less-educated peers, attributed to differences in health awareness. It also provides a comparison of health disparities between different countries, demonstrating the impact of education and awareness on health levels. Education creates self-awareness toward personal health, making healthcare more accessible [18].

The study highlighted the measures and precautions taken by the government of Saudi Arabia during the COVID-19 pandemic to mitigate its impact. The Ministry of Health relied on public awareness regarding virus transmission methods and the importance of quarantine. Despite strict measures such as curfews, people's awareness and practices remain the most critical factor in limiting virus spread [19].

The study presented survey results to assess the level of health awareness in a city in Saudi Arabia regarding viruses. The study showed an average level of awareness associated with education, occupation, and age group. People had general information from various sources, with the Ministry of Health being a prominent one. The research recommended continuous communication between healthcare providers, students, and individuals to help control and prevent the spread of viruses [20].

Here we present some applications that tried to increase the level of awareness of users through different ways and aspects.

- What’s up

An application that is used to treat user behavior, especially depression. Through the user's answer to more than 100 questions, the program can track the negatives and positives, and then encourage good habits, and send tips to stop negative habits.

- Mood Kit

This application is designed to address user behavior by offering over 200 diverse and beneficial activities to uplift mood. Developed by psychologists, the program aims to assist users in altering their moods and fostering health awareness during emergencies.

- Addiction App (Twenty-for-hours-a-day)

An important application to spread health awareness in the face of addiction, an electronic version of a famous book of the same name, especially helps to recover from addiction to stability and not return to addiction such as smoking and drinking alcohol.

- Talk space online therapy

The application facilitates communication between users and professionals, allowing users to express their feelings and struggles. Users can then receive advice and support from these professionals.

- Recovery Record

This application helps you to track your meals, feelings, behaviors, symptoms, and body condition according to your food to periodically report on what is best for you and your body to remain healthy as a form of health food education.

- LifeSum

This application allows you to identify and achieve your health goals such as the number of steps you need to make each day, healthy food or diet, exercise, and muscle building, as well as drinking water and eating throughout the day to build a better life.

- Health manager

A program to increase health awareness and organize the activities and habits of the user (such as eating, drinking, exercise) to achieve a healthy life better and helps the user to create a health file in which weight, height, age, and others to be consulted later and benefit from them and to monitor the level of progress of the user.

- Eye Exercises

An application to raise awareness about the health of the eye in humans, which provides exercises for the eye muscle in addition to relaxation exercises and useful tips, and provides tests to examine the problems of vision and alert the user faster.

- Stretch fitness

The application focuses on promoting health awareness through the organization of exercises, particularly stretching exercises for both women and men. It provides users with information on 17 different ways to achieve fitness while offering guidance to prevent muscle-related issues, aiming to contribute to the goal of "better health, longer life".

- Health Tab

A useful program for health awareness through the provision of expert medical consultations, but paid and the response to consultations through special video tutorials on primary care.

All studies have emphasized the importance of health awareness in assisting governments to provide better and more accessible healthcare, along with achieving greater control over the spread of infectious diseases, including new ones. However, there is a need for an effective and reliable communication tool between healthcare providers and all members of the community, regardless of their educational levels and age groups. This is what this research aims to provide through the proposed application. Unfortunately, even the smart applications that attempted to address the issue of health awareness focused on only one aspect of health and were not comprehensive. This makes it extremely difficult for users to benefit from these applications, as it is not logical to ask users to download dozens of different applications.

Proposed Framework and Application

To elevate health awareness and enhance the overall health level in society, we propose a comprehensive awareness platform. The platform consists of two main parts: a web-based application for the admin side (health experts) and a mobile application for users. On the admin side, health experts can manage various common diseases (e.g., heart disease, diabetes, hypertension, malaria, COVID-19, etc.). Each disease entry includes vital information such as description and definition, symptoms, causes, preventive measures, recommended actions, areas of prevalence, and available treatments, along with illustrative images and videos. Furthermore, the admin can send smart notifications to users in specific areas based on their location. These notifications can include reminders for vaccine schedules, general health advice, or alerts regarding the spread of infections or viruses.

On the user side, the second part of the platform is a mobile application that empowers users to search, receive, and access valuable information about various types of health data stored in the system (dates, texts, images, and videos). Additionally, users can search for information about a specific drug, receive notifications/alerts as needed, and submit questions or data to health experts for responses. Furthermore, users can explore and view the locations of health centers on the map.

The Health Expert is responsible for managing medical information across various fields such as Healthy Customs, drug search engines, Health Programs, Diets, Surveys, and electronic consultations. On the other hand, the regular user can search and view information, request consultations, receive notifications, and more. Additionally, there is an Admin user tasked with managing all user accounts, health centers, and general notifications.

There are many non-function requirements which this research ensures to be achieved

- Performance: It is characterized by the amount of useful work accomplished by a computer system or computer network compared to the time and resources used. When the number of users increases significantly, many applications experience a decrease in performance. However, in the case of web and mobile applications, the situation is different. The browser on the client's PC or mobile device absorbs some of the load, mitigating potential issues. This implies high response times and minimal utilization of server resources [21].

- Security and Privacy: Security and privacy are crucial issues, especially when dealing with important data or financial transactions. The application must prioritize these concerns and implement various measures, including encryption, strong password requirements, and limitations on login attempts, tracking the date of the last login, specifying parameters for processing, determining specific lengths for input data, and utilizing SSL (Secure Sockets Layer) for secure communication [22-31].

- Reliability: The application undergoes various types of testing before being released on the app store, ensuring that there are no issues affecting its reliability. Furthermore, any new problems that may arise can be easily addressed, and updated versions of the app can be released promptly. It's important to note that this type of application typically doesn't involve critical data, further mitigating potential risks [32].

- Availability: means that the application will stay working 24/7 and that is achieved in the web or mobile application.

- Usability: Usability refers to the simplicity of the application, making it easy for different users to learn and navigate. This research achieves this aspect by leveraging the widespread popularity of web applications, which most people are familiar with. Additionally, the application features straightforward interfaces to enhance usability [33].

- Adaptability: The application demonstrates adaptability to various environments and potential issues by ensuring flexibility in design, accommodating different screen sizes, resolutions, and memory capacities. Moreover, it is designed to cater to users with varying needs, including those who are visually impaired [34].

- Portability: Portability refers to the independence of the application from specific frameworks. In the server-side (web application), it is achieved as there are no specific operating system requirements. On the mobile application (client side), Android systems are required, but the concept of portability also extends to the application's ability to be mobile and easily moved [35].

- Interoperability: Interoperability involves facilitating cooperation between different services, providers, technologies, protocols, and devices. The application is designed to promote seamless interaction between various elements within the health awareness ecosystem [36].

Implementation and Results

To implement a prototype for the proposed application, we used open source platforms.

1. Eclipse with Java for Android to transform all of the diagrams to real functions and virtual interfaces to real mobile interfaces which interact with users.
2. Appserv App to convert our PCs to local server for using PHP and MySQL database

The following figures 2, 3, 4, 5, and 6 show the main interfaces in the proposed application.

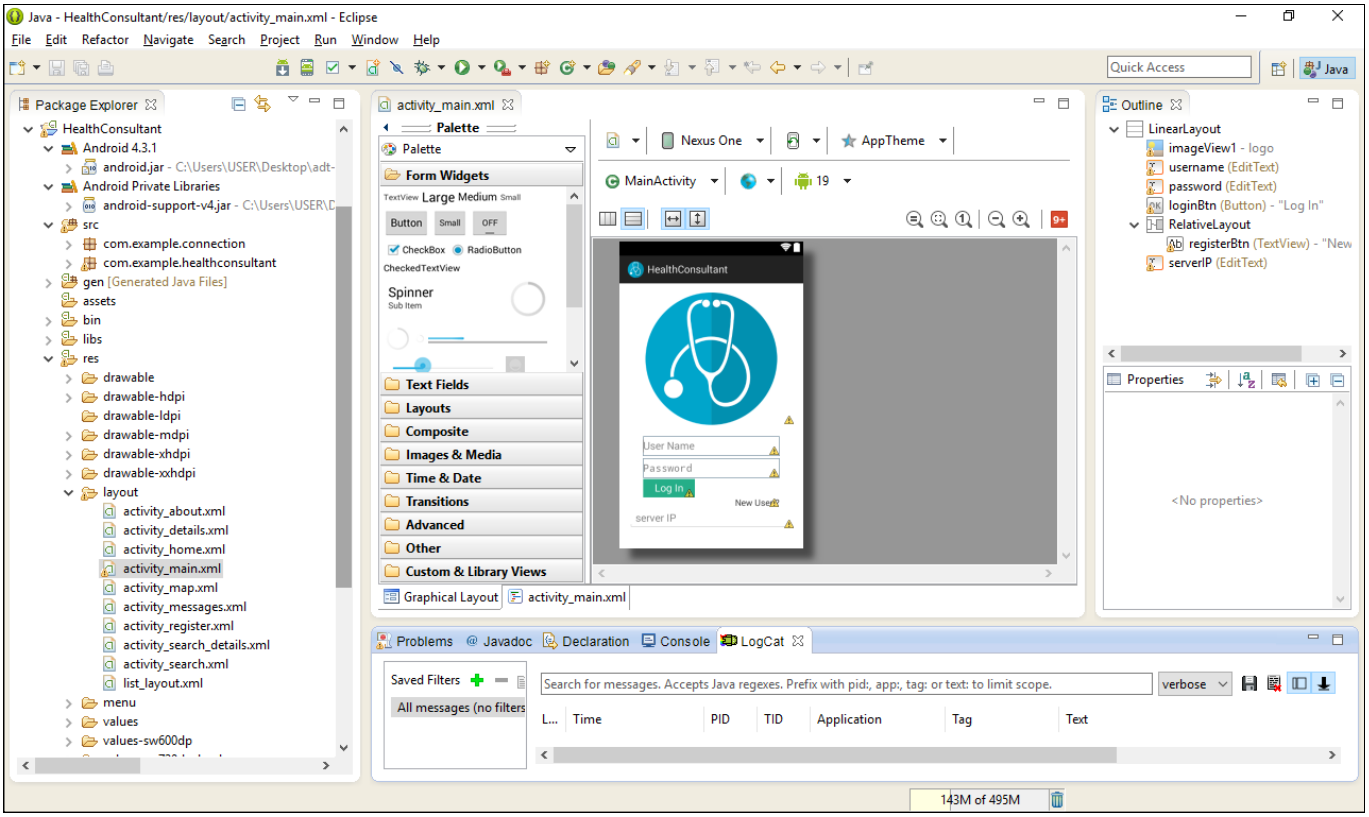


Figure 2. Login Interface in the Eclipse platform

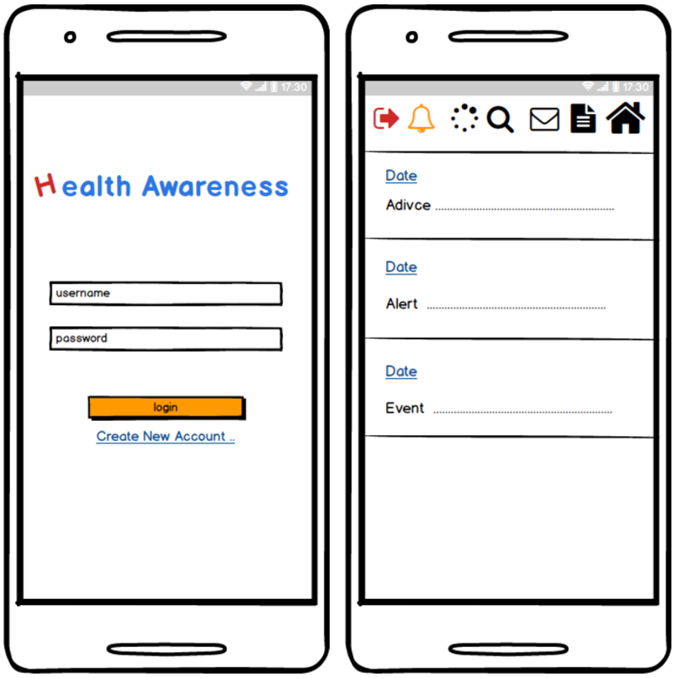


Figure 3. Consultation Interface

The actual environment of the Eclipse platform is depicted in Figure 2, showing the login screen executed on the simulator. Figure 3, on the other hand, illustrates the login screen and various notification types (medical tips, alerts and warnings, medical events such as donation campaigns, workshops, vaccination drives, etc.). The figure also displays the main services menu, including the search engine, medical consultations, notifications and news, medical programs, comprehensive medical files, and daily monitoring.

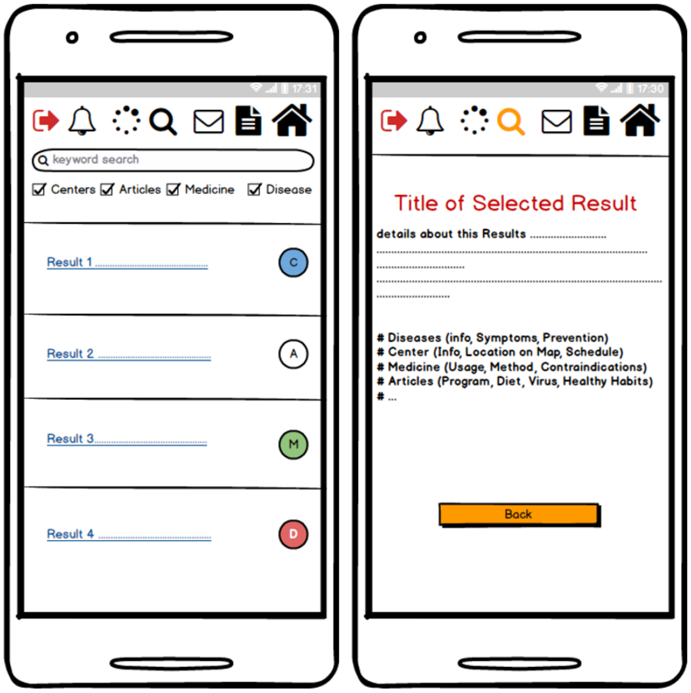

17:31
keyword search
☑ Centers ☑ Articles ☑ Medicine ☑ Disease
Result 1
C
Result 2
A
Result 3
M
Result 4
D
17:30
Title of Selected Result
details about this Results
# Diseases (info, Symptoms, Prevention)
# Center (Info, Location on Map, Schedule)
# Medicine (Usage, Method, Contraindications)
# Articles (Program, Diet, Virus, Healthy Habits)
# ...
Back

Figure 4. Details of consultation interface

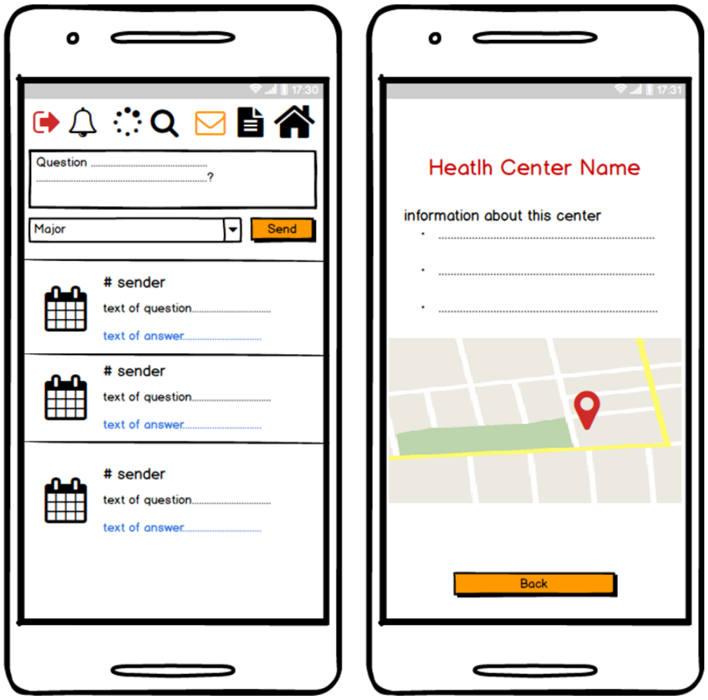


Figure 5. Search interface

Figure 4 illustrates the information search engine in the proposed application. Users can search for a health center (C) and view its location on the map or search for a specific medication (D) and review details such as uses, contraindications, and usage instructions. Users can also search for a medical article on a specific topic (A) or search for a particular disease, its symptoms, and prevention methods. Figure 5 shows a conceptual representation of the medical consultations interface and a virtual interface for the data of a medical center and its location on the map.

Finally, Figure 6 depicts the actual implementation on an emulator of the search engine interface after applying it on Eclipse as an Android application.

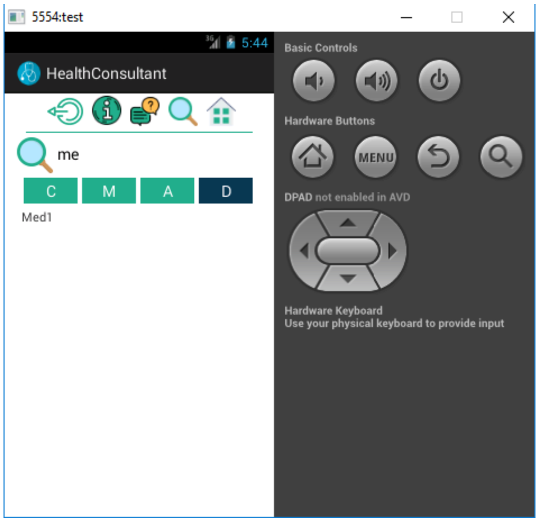


Figure 6. Search details interface

Conclusion

This research highlights the significance of health awareness and the necessity of supporting community health to create a better society. Health awareness aids in preventing numerous health issues. The research introduces the concept of a platform with a smart application used by the government to send notifications to users, such as schedules for blood donation campaigns, vaccinations, medical advice, or warnings for prevention in the case of a new virus outbreak.

The application includes an online consultation service when needed, along with a search engine for four important medical topics: information about diseases, their prevention, and symptoms; details about medications, their usage, and contraindications; medical articles and health programs; and finally, health centers and their locations on the map. A preliminary prototype of the application has been achieved in the Android environment.

Future work will focus on further developing the application to realize the central and comprehensive idea, creating a super health application that enables service providers to offer healthcare services through a single application for all users, aiming to facilitate usage and enhance the quality of healthcare services provided in the Kingdom of Saudi Arabia.

References

[1] N. M. Bahbouh, S. S. Compte, J. V. Valdes, and A. A. A. Sen, “An empirical investigation into the altering health perspectives in the internet of health things,” International Journal of Information Technology, Jul. 2022, doi: https://doi.org/10.1007/s41870-022-01035-3.

[2] S. Ketu and P. K. Mishra, “Internet of Healthcare Things: A contemporary survey,” Journal of Network and Computer Applications, vol. 192, p. 103179, Oct. 2021, doi: https://doi.org/10.1016/j.jnca.2021.103179.

[3] M. M. Almutairi, M. Yamin, G. Halikias, and A. A. Abi Sen, “A Framework for Crowd Management during COVID-19 with Artificial Intelligence,” Sustainability, vol. 14, no. 1, p. 303, Dec. 2021, doi: https://doi.org/10.3390/su14010303.

[4] B. khan et al., “Drawbacks of Artificial Intelligence and Their Potential Solutions in the Healthcare Sector,” Biomedical Materials & Devices, vol. 1, pp. 1–8, Feb. 2023, doi: https://doi.org/10.1007/s44174-023-00063-2.

[5] F. Nausheen and S. H. Begum, "Healthcare IoT: Benefits, vulnerabilities and solutions," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2018, pp. 517-522.

[6] S. R. Sharma, “Internet of Things IoT: IoT in Healthcare,” International Journal of Trend in Scientific Research and Development, vol. Volume-3, no. Issue-4, pp. 980–982, Jun. 2019, doi: https://doi.org/10.31142/ijtsrd23971.

[7] M. K. Al-Hanawi, S. A. Khan, and H. M. Al-Borie, “Healthcare human resource development in Saudi Arabia: emerging challenges and opportunities—a critical review,” Public Health Reviews, vol. 40, no. 1, Feb. 2019, doi: https://doi.org/10.1186/s40985-019-0112-4.

[8] D. E. Stubbe, “Practicing Cultural Competence and Cultural Humility in the Care of Diverse Patients,” Focus, vol. 18, no. 1, pp. 49–51, 2020, doi: https://doi.org/10.1176/appi.focus.20190041.

[9] L. Catarinucci et al., “An IoT-Aware Architecture for Smart Healthcare Systems,” IEEE Internet of Things Journal, vol. 2, no. 6, pp. 515–526, Dec. 2015, doi: https://doi.org/10.1109/jiot.2015.2417684.

[10] A. A. Alasiri and V. Mohammed, “Healthcare Transformation in Saudi Arabia: An Overview Since the Launch of Vision 2030,” Health Services Insights, vol. 15, no. 1, p. 117863292211212, Jan. 2022

[11] Patomporn Payoungkhamdee et al., “LimeSoda: Dataset for Fake News Detection in Healthcare Domain,” Dec. 2021.

[12] C. McCabe, M. McCann, and A. M. Brady, “Computer and mobile technology interventions for self-management in chronic obstructive pulmonary disease,” Cochrane Database of Systematic Reviews, May 2017, doi: https://doi.org/10.1002/14651858.cd011425.pub2.

[13] X. Zhao et al., “Smartphone application training program improves smartphone usage competency and quality of life among the elderly in an elder university in China: A randomized controlled trial,” International Journal of Medical Informatics, vol. 133, p. 104010, Jan. 2020, doi: https://doi.org/10.1016/j.ijmedinf.2019.104010.

[14] G. M. Harari, S. R. Müller, M. S. Aung, and P. J. Rentfrow, “Smartphone sensing methods for studying behavior in everyday life,” Current Opinion in Behavioral Sciences, vol. 18, pp. 83–90, Dec. 2017, doi: https://doi.org/10.1016/j.cobeha.2017.07.018.

[15] J. Seymour, “The Impact of Public Health Awareness Campaigns on the Awareness and Quality of Palliative Care,” Journal of Palliative Medicine, vol. 21, no. S1, p. S-30-S-36, Jan. 2018.

[16] R. Jose, M. Narendran, A. Bindu, N. Beevi, M. L, and P. V. Benny, “Public perception and preparedness for the pandemic COVID 19: A Health Belief Model approach,” Clinical Epidemiology and Global Health, vol. 9, Jun. 2020, doi: https://doi.org/10.1016/j.cegh.2020.06.009

[17] A. Holzinger, S. Dorner, M. Födinger, A. C. Valdez, and M. Ziefle, “Chances of Increasing Youth Health Awareness through Mobile Wellness Applications,” HCI in Work and Learning, Life and Leisure, pp. 71–81, 2010.

[18] V. Raghupathi and W. Raghupathi, “The influence of education on health: An empirical assessment of OECD countries for the period 1995–2015,” Archives of Public Health, vol. 78, no. 1, Apr. 2020.

[19] H. Alahdal, F. Basingab, and R. Alotaibi, “An analytical study on the awareness, attitude and practice during the COVID-19 pandemic in Riyadh, Saudi Arabia,” Journal of Infection and Public Health, vol. 13, no. 10, Jun. 2020, doi: https://doi.org/10.1016/j.jiph.2020.06.015.

[20] H. Z. Nooh et al., “Public awareness of coronavirus in Al-Jouf region, Saudi Arabia,” Journal of Public Health, Feb. 2020.

[21] A. A. A. Sen and M. Yamin, “Advantages of using fog in IoT applications,” International Journal of Information Technology, Oct. 2020, doi: https://doi.org/10.1007/s41870-020-00514-9.

[22] A. A. Abi Sen, F. A. Eassa, and K. Jambi, “Preserving Privacy of Smart Cities Based on the Fog Computing,” Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 185–191, 2018, doi: https://doi.org/10.1007/978-3-319-94180-6_18.

[23] A. A. Abi Sen, “A comprehensive privacy and security framework for dynamic protection (CPSF),” International Journal of Information Technology, vol. 14, no. 5, pp. 2477–2485, May 2022, doi: https://doi.org/10.1007/s41870-022-00965-2.

[24] M. Yamin, Y. Alsaawy, A. B. Alkhodre, and A. A. Abi Sen, “An Innovative Method for Preserving Privacy in Internet of Things,” Sensors, vol. 19, no. 15, p. 3355, Jul. 2019, doi: https://doi.org/10.3390/s19153355.

[25] Y. Alsaawy, A. A. Abi Sen, A. Alkhodre, N. M. Bahbouh, and H. B. Alharbi, "Double Steganography - New Algorithm for More Security," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. 370-374.

[26] S. S. Albouq, A. A. A. Sen, A. Namoun, N. M. Bahbouh, A. B. Alkhodre and A. Alshanqiti, "A Double Obfuscation Approach for Protecting the Privacy of IoT Location Based Applications," in IEEE Access, vol. 8, pp. 129415-129431, 2020, doi: 10.1109/ACCESS.2020.3009200.

[27] A. A. Abi Sen, F. A. Eassa, K. Jambi, and M. Yamin, “Preserving privacy in internet of things: a survey,” International Journal of Information Technology, vol. 10, no. 2, pp. 189–200, Feb. 2018, doi: https://doi.org/10.1007/s41870-018-0113-4.

[28] A. A. A. Sen, F. B. Eassa, M. Yamin, and K. Jambi, “Double Cache Approach with Wireless Technology for Preserving User Privacy,” Wireless Communications and Mobile Computing, vol. 2018, pp. 1–11, Aug. 2018, doi: https://doi.org/10.1155/2018/4607464.

[29] M. Yamin and A. A. Abi Sen, "A New Method With Swapping of Peers and Fogs to Protect User Privacy in IoT Applications," in IEEE Access, vol. 8, pp. 210206-210224, 2020, doi: 10.1109/ACCESS.2020.3038825.

[30] M. Yamin and A. A. A. Sen, “Improving Privacy and Security of User Data in Location Based Services,” International Journal of Ambient Computing and Intelligence, vol. 9, no. 1, pp. 19–42, Jan. 2018, doi: https://doi.org/10.4018/ijaci.2018010102.

[31] A. A. A. Sen and A. M. Basahel, "A Comparative Study between Security and Privacy," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 1282-1286.

[32] N. Bahbouh, A. Basahel, S. Sendra, and A. A. Abi Sen, “Tokens Shuffling Approach for Privacy, Security, and Reliability in IoHT under a Pandemic,” Applied Sciences, vol. 13, no. 1, p. 114, Dec. 2022, doi: https://doi.org/10.3390/app13010114.

[33] N. M. Bahbouh, A. A. Abi Sen, A. A. A. Alsehaimi and E. A. Alsuhaymi, "A Framework for Supporting Ambient Assisted Living for Users of Special Needs," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 427-432, doi: 10.23919/INDIACom54597.2022.9763212.

[34] A. A. Abi Sen, A. A. S Aljohani, and N. M. Bahbouh, "Designing a Smart Bracelet based on Arduino for Deaf Parents to Interact with their Children," 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2021, pp. 380-384.

[35] A. M. Basahel, N. M. Bahbouh, A. A. Abi Sen and M. Yamin, "Smart Application for Blood Donation Management in Health Domain," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 589-594.

[36] S. S. Albouq, A. A. A. Sen, N. Almashf, M. Yamin, A. Alshanqiti and N. M. Bahbouh, "A Survey of Interoperability Challenges and Solutions for Dealing With Them in IoT Environment," in IEEE Access, vol. 10, pp. 36416-36428, 2022, doi: 10.1109/ACCESS.2022.3162219

****

Chapter 8 – Conclusion and Future Trends

This is the final chapter of this thesis. It provides a summary of the thesis along with crucial research points that we will be working on in the upcoming period. Additionally, other researchers can work on these points to contribute further to the development of smart healthcare services that enhance the healthcare sector, community health, and the well-being of individuals.

Conclusion

In this thesis, the main objective was to address the challenges of the healthcare sector, given its significance as one of the most crucial sectors. This sector is intricately linked to individuals' lives, safety, and happiness, serving as an indicator of the progress and development of societies. The aim of this research was not to focus on a single research point but rather to work on providing solutions in all the details and aspects related to health relying on the Internet of Health Things (IoHT). In other words, our work on this thesis aimed to present useful and tangible contributions to our communities.

We reviewed hundreds of previous studies related to the healthcare sector, presenting an extensive reference study in which we classified numerous challenges associated with IoHT and the healthcare sector. We provide comprehensive solutions to cover all these challenges. We introduced a comprehensive framework that will play a significant role in effectively facing pandemics in the future. We offered compound and inclusive solutions for the challenge of binary operation, along with a health ontology. We also presented solutions for the performance challenge and handling big data by employing fog and cloud computing. We proposed an intermediary computational approach and demonstrated its importance in accelerating response in emergency situations.

Furthermore, we provided solutions to ensure the safety of crowds and enhance individual health. We offered multiple solutions to guarantee the security, privacy, and reliability of health data by utilizing blockchain, consensus, and various proposed privacy methods. We introduced numerous applications and ideas to support community health and assist individuals with special needs.

In reality, there is still much more to offer in the healthcare sector, as working in it is a humanitarian mission. We have classified numerous future points to work on, both for our future endeavors and to assist other researchers in identifying their specific research points. We have published numerous research papers in ISI journals, Scopus-indexed journals, and conferences. Additionally, we have prepared five draft papers for research that has been completed, and we are actively working on submitting them to ISI-indexed journals, with two of them currently under review.

The summarized outputs include:

- Two published papers in ISI journals.
- One published papers in Scopus-indexed journal.
- Four published papers in conferences.
- Five draft papers for completed research, two of which are currently under review.

We have also developed some applications for smartphones, a model of a bracelet and pendant to alert individuals with special needs, and designed a health framework and a specific protocol during pandemics. Furthermore, we introduced an algorithm for early disaster detection and threat level classification, along with an algorithm to process textual data coming from crowds. We have designed a health ontology and proposed a new consensus algorithm in blockchain, a robust consensus algorithm, and various methods to enhance privacy. We continue to work on presenting more ideas, approaches, and new healthcare services.

Future Trends and Our Next Works

- Provide Super Application for health
- Provide new smart services
- Auto-Select services and service providers based on the context and preference
- Provide public health services for different countries
- Support open data and a unified platform for developing health services
- Provide a platform for decision support in the health domain
- Deal with privacy and security in all phases of software development life cycle (SDLC)
- Provide a new protocol for protection
- Enhance the health of the crowd and provide auto-measure for adherence level of health roles
- Care about plant health
- Care about animal health
- Address environmental issues like waste management and saving energy
- Support the health of society and enhance awareness
- Provide early detectors for chronic diseases

THE END

****