future internet

MDPI

Article

Privacy Framework for the Development of IoT-Based Systems

Yaqin Y. Shaheen [1,2], Miguel J. Hornos [1,*] and Carlos Rodríguez-Domínguez [1]

[1] Software Engineering Department, Research Center for Information and Communication Technologies (CITIC-UGR), Aynadamar Campus, University of Granada, 18071 Granada, Spain; yshaheen@correo.ugr.es (Y.Y.S.); carlosrodriguez@ugr.es (C.R.-D.)
[2] Computer Engineering Department, Palestine Technical University-Kadoorie (PTUK), Hebron P7060796, Palestine
* Correspondence: mhornos@ugr.es

Abstract

Addressing privacy concerns is one of the key challenges facing the development of Internet of Things (IoT)-based systems (IoTSs). As IoT devices often collect and process personal and sensitive information, strict privacy policies must be defined and enforced to keep data secure and safe, ensuring security and regulatory compliance. Any data breach could compromise the security of the system, leading to various types of threats and attacks, some of which could even endanger human life. Therefore, it is crucial to design and build a comprehensive and general privacy framework for the development of IoTSs. This framework should not be limited to specific IoTS domains but should be general enough to support and cover most IoTS domains. In this paper, we present a framework that assists developers by (i) enabling them to build IoTSs that comply with privacy standards, such as the General Data Protection Regulation (GDPR), and (ii) providing a simplified and practical approach to identifying and addressing privacy concerns. In addition, the framework enables developers to implement effective countermeasures.

Keywords: Internet of Things (IoT); privacy; security; privacy policies; privacy guidelines

Academic Editors: Paolo Bellavista, Dinh-Thuan Do, Vitor Fialho, Luis Pires, Francisco Rego, Ricardo Santos and Vasco Velez

Received: 8 June 2025
Revised: 11 July 2025
Accepted: 16 July 2025
Published: 22 July 2025

Citation: Shaheen, Y.Y.; Hornos, M.J.; Rodríguez-Domínguez, C. Privacy Framework for the Development of IoT-Based Systems. *Future Internet* **2025**, *17*, 322. https://doi.org/10.3390/fi17080322

1. Introduction

The Internet of Things (IoT) is rapidly becoming one of the most transformative paradigms in the field of information and communication technology. It is increasingly influencing our daily lives in a wide range of areas, including healthcare, smart homes, transport systems, agriculture, industry, and tourism, to name but a few. At its core, the IoT is based on the integration of computing and communication capabilities into everyday objects [1,2]. These prominent IoT use cases have been made possible by recent technological advances, such as Radio Frequency Identification (RFID) technology and smart sensors, which continuously collect data and send it over the Internet to designated data centers for analysis [3,4]. By 2025, it is predicted that there will be 55.7 billion connected nodes worldwide, 75% of which will be connected to an IoT system (IoTS) [5].

IoTSs generate a huge amount of data related to many objects, such as plants, environmental elements (e.g., weather), machines, and people. According to the International Data Corporation (IDC), the amount of data generated by these IoT-connected devices will reach 73.1 zettabytes (ZB) by 2025, up from 18.3 ZB in 2019 [6]. This data should be handled carefully as it travels from source nodes and devices to the point where it becomes useful information for end users. A critical issue that needs to be addressed and resolved during this journey is ensuring security and privacy, as the data transmitted may contain sensitive

private information, such as health records, location history, banking information, and so on. The use of this vast amount of personal data should therefore be tightly controlled. As a result, legislative and regulatory initiatives, such as the General Data Protection Regulation (GDPR), have been introduced to address such concerns. GDPR establishes a set of rules that must be followed by all parties handling private and personal data of European Union (EU) citizens [7].

It is well known that IoTS development is difficult due to the heterogeneity of these systems, which include hardware devices, span multiple domains, and require multi-device programming [8]. Therefore, enhancing privacy in IoTSs is a complex and challenging task. In addition, creating IoTSs differs from creating conventional information systems (IS) in that the tools, models, and techniques used to build them are inadequate to handle their complexity [9,10]. For example, while different development methodologies, such as waterfall, spiral, or agile, are successfully used to develop conventional ISs, when applied to the development of IoTSs, some of the limitations arise when addressing the unique aspects of such systems, such as heterogeneity [8,11].

Several methodologies have been developed specifically for IoTSs, such as Ignite, which is an open-source methodology divided into two phases: (i) strategy execution and (ii) solution delivery. The strategy execution phase focuses on defining and deciding what to build by identifying opportunities, managing them, and initiating projects. The solution delivery phase focuses on delivering the solution to users through a lifecycle of planning, building, and running. Ignite aims to provide IoTSs with best practices in the form of a reusable and technology-agnostic methodology, providing project templates, checklists, and solution architecture schemes to support the design, configuration, and management of IoT projects. It is important to note that Ignite does not provide technical details on software development and testing [12]. Another notable methodology is High-Level Application Development for the IoT, introduced by Patel and Cassou [13]. Rooted in academia, the goal of this methodology is to facilitate the development of IoTSs by leveraging model-driven design methodology and sensor network macro programming. Recently, Guerrero-Ulloa et al. [14] proposed a Test-Driven Development Methodology for IoTSs (TDDM4IoTS), which focuses on such systems. This methodology consists of eleven stages, the sequence and implementation of which are left to the discretion of the project team.

Another important methodology specifically designed for IoTSs is the Three-Phase Methodology (TpM), which is a methodological approach designed for the teaching and development of IoTSs. TpM addresses each phase of the development of an IoTS solution in a vendor- and technology-agnostic manner [15]. It consists of three clearly identified phases: (i) business consideration, which focuses on establishing business goals for the IoTS; (ii) requirements gathering, which is dedicated to gathering operational and technical specifications; and (iii) implementation, which includes software configuration, testing, and the actual deployment of sensors and devices. Moreover, TpM has an extended version called TpM-Pro, which is based on the Situational Method Composition approach [16] and helps to select the artifact according to the characteristics of the project. The TpM-Pro approach outlines the most straightforward method for creating IoTSs and maintaining complete project documentation [17].

In software development, the Software Development Life Cycle (SDLC) is a structured process for building and maintaining software through five stages: planning, analysis, design, implementation, and maintenance [18]. Based on our own analysis, neither the SDLC nor the IoT-specific methodologies mentioned above, which often deviate from the traditional SDLC, have specific guidelines to help developers integrate privacy into the IoTS development process. In addition, they lack a clear methodological approach for identifying privacy requirements for specific IoTS projects or solutions.

In addition to the complexities mentioned above, building and developing IoTSs requires a group of software developers with a wealth of expertise. These developers must not only understand the needs of consumers, but also comply with regulatory requirements, such as GDPR. Unfortunately, many developers focus on meeting users' functional requirements without adhering to legal standards, as these regulations are often written from a legal perspective that is difficult for developers to interpret. This lack of understanding or focus contributes to IoTSs suffering from inadequate privacy protection, leaving them vulnerable to attacks that could compromise users' personal information and even endanger lives [19,20].

In this context, and based on the aforementioned issues for building IoTSs with enhanced privacy, this paper proposes a privacy framework as a systematic approach to help developers in their journey to develop more secure and privacy-compliant IoTSs. Our approach will help to integrate the required privacy policies into the IoTS development lifecycles and make it easier for developers to comply with them. Our study builds on the TpM-Pro approach proposed by Ferreira et al. [17], and extends it with systematic steps for extracting privacy requirements and with a set of updated and improved guidelines to obtain a more privacy-enhanced IoTS solution. The TpM-Pro approach was chosen because it starts with a strong focus on understanding the needs and business context of the project, which is usually critical for eliciting privacy requirements in IoTS projects. Furthermore, TpM-Pro includes a detailed phase to identify technical and operational requirements in an organized way, reducing hardware-software inconsistencies. Another advantage is its ability to help address various IoT-specific issues by facilitating incremental deployment with iterative validation, which can help verify the implementation of privacy concerns in an IoTS.

In summary, this study comprehensively explores IoTS privacy concerns and addresses issues highlighted in previous work by other authors. Our main contributions are as follows:

1. **Classification of existing research**: We categorized articles on IoTS privacy issues into different perspectives, simplifying the topic for readers and providing essential background on its challenges and opportunities.
2. **Proposal of a methodological approach:** A systematic approach is presented to help developers extract privacy requirements during the IoTS development process.
3. **Improvement of existing privacy guidelines**: We have critically reviewed and updated existing privacy guidelines.
4. **Evaluation of effectiveness**: The effectiveness of the newly created and improved privacy guidelines was measured using a questionnaire.

The combination of these contributions aims to provide developers with a privacy framework to help them develop privacy-enhanced IoTSs.

The rest of this paper is structured as follows: Section 2 outlines the motivation behind this study. Section 3 provides essential background information. Section 4 reviews related work in the field. Section 5 describes the proposed methodological approach, called Planning, Requirements, and Design (PRD), as it encompasses these three key stages of IoTS development. Section 6 presents the proposed privacy guidelines. Finally, Section 7 summarizes the conclusions and outlines potential directions for future research.

2. Motivation

Privacy is currently a critical concern in the development of IoTSs [21]. At the same time, there is a need for an approach that both streamlines such development processes and facilitates the creation of more privacy-enhanced IoTS solutions. Based on our analysis of the existing related research literature, already outlined in the introduction and further

detailed in the related work section, we propose a well-structured methodological approach to address such a challenge in a more effective way. Below, we clarify the specific challenges that we aim to address through this research:

1. **Guidelines should be better explained:** According to Perera et al. [22], who conducted several experiments based on existing guidelines, there is a need to simplify existing recommendations and present them in a clearer and more accessible way to developers.
2. **The design of IoTSs by software engineers is influenced by their own expertise:** Developers tend to rely on their own background and expertise when selecting and applying privacy policies, which can lead to incorrect design decisions during the development process. To address this issue, it is necessary to establish a comprehensive repository of detailed information on privacy guidelines, their implementation, and best practices. Such a resource could enable developers to search for guidance, ensuring consistency in their design approach and ultimately leading to more robust privacy-enhanced applications.
3. **Lack of a clear approach to implementing the guidelines:** After our analysis of the work presented by Perera et al. [22], it has become clear that developers need a structured roadmap that outlines the necessary steps to be followed to extract privacy concerns during the development phases of IoTS projects. Such a methodological approach should provide a well-defined framework, complete with tools and guidance, to facilitate the integration of privacy principles based on well-established guidelines.
4. **Minimize the number of privacy guidelines:** Reducing the number of privacy policies allows developers to focus on key objectives (i.e., the goals pursued by the respective policies), which should help them to identify and address critical privacy concerns more effectively. The process of policy minimization involves filtering, reviewing, and validating existing privacy policies. This effort should be undertaken by security and privacy experts in the IoTS field, both from academia and industry. Their feedback will be instrumental in refining the current privacy guidelines and presenting a final, curated set of them. In addition, a survey will be conducted to assess the complexity of the current guidelines. The results of this survey will be analyzed and integrated into our research to further refine the guidelines and ensure that they are both practical and understandable for developers.

In this context, we revisited Perera's guidelines and subjected them to expert evaluation, acknowledging their foundational value but also recognizing their limitations in addressing modern IoTS privacy challenges. To enhance relevance and applicability, we incorporated updated privacy recommendations reflecting recent advances in privacy engineering and IoT domains. These additions were empirically validated using a scientifically grounded research instrument (i.e., a structured questionnaire) that gathered expert feedback, assessed practical relevance, and guided the refinement of the proposed guidelines.

3. Background

This section provides a foundational understanding of key aspects of IoTSs, focusing on critical security and privacy considerations. These elements are essential for mitigating risks and fostering user trust in IoT environments.

3.1. IoTS Non-Functional Requirements

Non-functional requirements (NFRs) define the quality attributes of a system, such as security, privacy, reliability, and usability, to ensure its overall effectiveness and user confidence. Unlike functional requirements (FRs), which specify what a system should do, NFRs focus on how well the system performs under different conditions. In IoTSs, NFRs

play a critical role due to the complexity of interconnected devices, diverse technologies, and increased exposure to security threats. Despite their importance, NFRs—especially privacy and security—are often overlooked in IoTS development, as existing methodologies primarily emphasize functional aspects. This neglect can lead to vulnerabilities, performance inefficiencies, and privacy risks. Addressing NFRs from the early stages of IoTS design is essential to ensure secure and reliable applications [5,19].

3.2. Privacy by Design

Introduced by Ann Cavoukian in 1995, the term Privacy by Design (PbD) [23] advocates the proactive integration of privacy measures into system architectures and organizational practices from the very beginning. This approach emphasizes the importance of addressing privacy concerns early in the development process, rather than as an afterthought. PbD ensures that privacy considerations are inherent in the system design, making data protection a core component rather than a reactive adaptation. This philosophy is supported by the EU's GDPR, which mandates "data protection by design and by default," reinforcing the idea that privacy should be embedded throughout the development lifecycle. This is particularly important for modern digital systems, such as IoTSs, where privacy risks are amplified by the extensive collection and processing of personal data [24].

4. Related Work

After a thorough review of the literature, we classified the papers that covered our research interest into the perspectives discussed in the following subsections.

4.1. IoTS Security and Privacy Vulnerabilities and Attacks with Countermeasures

Attacks against IoTSs are aimed at compromising users' private information, which can lead to serious breaches. With this in mind, we reviewed a large number of studies addressing security threats in IoTSs. However, we found limited research that specifically focuses on the privacy aspect of IoTSs.

Adam et al. [25] discussed IoTSs and their three-layer architecture (i.e., physical, network, and application layers), and also provided an overview of cyberattacks targeting these layers. They identified heterogeneity as a major security and privacy concern within IoTSs.

Likewise, Pourrahmani et al. [26] presented a thorough review of current cybersecurity threats and vulnerabilities in IoTSs, as well as appropriate countermeasures. They addressed the vulnerabilities at different layers of the IoTS reference model. Furthermore, the authors proposed the use of blockchain technology for secure data transfer between IoT devices. Despite their detailed discussion of IoTS cybersecurity attacks, privacy-related issues were not specifically addressed. In a related effort, Mahmoud et al. [27] proposed a forensic investigation framework for IoT infrastructures to support incident analysis and enhance future security by capturing information on successful attacks.

A study by Swessi et al. [28] examined IoT security risks and the solutions that have been proposed so far. Their focus was placed on key security requirements, such as authorization and confidentiality. Their research highlighted the effectiveness of hybrid approaches, such as combining blockchain with artificial intelligence (AI), to enhance the security of IoTSs and defend against various threats. However, they also noted that, despite these advances, IoTS security remains an open challenge due to the constantly evolving nature of IoTSs.

Similarly, a study by Kaushal et al. [29] provided a basic understanding of IoTSs and the main privacy and security concerns raised by their rapid expansion. They also

presented security primitives and solutions to ensure secure communication and protect user data. The researchers highlighted that IoTSs cannot benefit from traditional security measures due to the large number and variety of sensors, limited resources, and unique system architectures used. Their study proposed a multi-layered security architecture that includes peer-to-peer data protection and robust encryption techniques tailored to resource-constrained sensors to prevent unauthorized access to user information.

4.2. AI-Based Approaches for IoTS Security and Privacy

Another aspect of our investigation into IoT security and privacy focuses on recent studies addressing the automatic detection through AI-based techniques of botnets and malware attacks—two of the most pervasive and disruptive threats in this domain. Effective detection of such threats is essential for safeguarding IoTS. The reviewed studies explore the application of machine learning (ML), deep learning (DL), and federated learning (FL) techniques for forensic analysis and malware detection, highlighting the growing role of these technologies as powerful tools for enhancing IoT security.

Nazir et al. [30] examined the application of ML and DL techniques for detecting IoT botnets, noting their high effectiveness—often surpassing traditional signature-based methods—and their significant potential to improve security. By analyzing several publicly available datasets, the study identifies key characteristics of botnet traffic and emphasizes critical challenges such as the lack of standardized benchmark datasets and the need for lightweight, real-time detection solutions suited to resource-constrained environments. The study also raises concerns about the ethical and privacy implications of the extensive data collection required by ML/DL models, which often rely on sensitive device and user information. To address these concerns, it highlights the need for privacy-preserving techniques such as FL, differential privacy, and encrypted model inference. Addressing vulnerabilities to adversarial attacks, enhancing model interpretability, and ensuring compliance with privacy regulations like GDPR are also essential for developing secure and privacy-aware ML/DL-based solutions.

A study by Qureshi et al. [31] delved into the use of DL techniques for detecting malware in IoT environments, with a particular focus on improving forensic analysis and real-time response. This research underlines the importance of extensive, IoT-specific datasets and interdisciplinary approaches. It also addresses the growing challenge of anti-forensic tactics that obscure malware behavior. Notably, the study emphasizes the integration of FL as a method to mitigate privacy risks by decentralizing the training process and ensuring data remains on local devices. FL is presented as an efficient approach for preserving device efficiency, reducing transmission overhead, and maintaining user confidentiality—all while supporting collaborative model training.

While both studies [31,32] emphasize the effectiveness of ML and DL in enhancing IoT security, they differ in focus and methodology. Nazir et al. [30] concentrate on privacy-preserving techniques to reduce the risks associated with centralized data collection. Moreover, these authors highlight the suitability of FL for privacy-sensitive and resource-constrained IoT environments. In contrast, Qureshi et al. [31] take a broader perspective, emphasizing scalable detection methods, the challenge of anti-forensic behaviors, and the potential of DL models to forecast malware events by analyzing evolving threat patterns. Both studies underscore the need for real-time, lightweight models and raise concerns about the lack of high-quality, standardized IoT-specific datasets—an obstacle to effective ML/DL deployment across diverse IoT scenarios.

Despite these shared themes, several critical gaps remain in the research. Both studies acknowledge the increasing complexity of IoT security and the privacy risks associated with IoTS, including challenges such as the scarcity of high-quality datasets, the difficulty

of achieving real-time threat detection under resource constraints, and the vulnerability of current models to adversarial attacks and anti-forensic techniques. Building upon these insights, our research addresses these persistent challenges by introducing a comprehensive privacy framework tailored for IoTS. Significant research efforts are still required to close these gaps. Therefore, our contribution focuses on embedding privacy at the stages of IoTS application development to enhance system-wide security and privacy outcomes.

As previously stated, given the growing concern over data privacy and security in IoTS environments, FL has emerged as a promising solution to address such challenges. However, FL must be designed in such a way that sensitive data is not shared across devices, thereby preserving privacy while maintaining high performance in IoTS.

The exposure of data in IoTS creates opportunities for several adversarial activities, such as malware exploits, Denial of Service (DoS) attacks, phishing schemes, and IoT botnet intrusions [32]. As a solution, FL enables collaborative model training by allowing users to share local parameters without exposing private data, which inherently provides higher security compared to centralized training. However, this decentralization also introduces new security challenges. Recent experiments reveal that distributed parameters in FL can be vulnerable to attacks where malicious actors could attempt to retrieve private data, such as images from face detection devices or medical data from wearable devices [33]. These security threats undermine the privacy benefits of FL and hinder its adoption for critical IoTS applications.

Despite these risks, FL continues to be seen as a promising method for improving privacy-preserving IoT security. For instance, Alahmari et al. developed a Privacy-Enhanced Federated Learning for Intrusion Detection using the Chameleon Swarm Algorithm and Artificial Intelligence (PEFLID-CSAAI) [33], which improved the intrusion detection capabilities in decentralized environments while ensuring data privacy. This innovative approach integrates FL to enable collaborative intrusion detection without compromising the confidentiality of sensitive data, ensuring compliance with privacy regulations, such as GDPR. Another proposal using FL to enhance privacy is presented by Zhao et al. [34], who propose an FL-based system that allows manufacturers to improve their products using user data while preserving user privacy.

Taking these contributions into account, FL could serve as a complementary future step that supports privacy and security in IoTS. This technique could be integrated in the future into the stages of IoTS development to provide greater protection of personal data, thereby enhancing the effectiveness of the application and ensuring the privacy of users.

4.3. Zero Trust Approaches for IoTS Security and Privacy

Zero Trust (ZT) approaches have emerged to address IoT security and privacy from an access control and trust management perspective. Traditionally, security measures focused on protecting the perimeter, assuming that everything inside the network could be trusted. However, ZT operates on the assumption that no entity, internal or external, should be trusted by default. Every access request must be authenticated, authorized, and continuously validated [35]. This is particularly critical in IoT environments where devices are often interconnected, and the risk of vulnerabilities from both inside and outside the network is high.

Liu et al. [36] conducted a comprehensive analysis to evaluate the current landscape of ZT research, with a particular focus on its practical applications within IoT environments. Their study further investigates existing IoT vulnerabilities and examines how ZT can effectively address these risks through a detailed assessment of contemporary security mechanisms. One key aspect highlighted by the authors is the critical issue of data security in IoT systems, where unauthorized access can lead to data theft, manipulation, or destruc-

tion. The ZT model effectively addresses this challenge by categorizing and monitoring sensitive data based on its importance and ensuring access is granted solely to authorized users and devices, thereby safeguarding IoT data. This approach helps protect sensitive data and ensures compliance with privacy regulations like GDPR.

While the research presented above highlights the critical role of ZT in enhancing security within IoT environments, it is also important to consider its future integration into privacy frameworks. Given its potential to safeguard sensitive data and its effectiveness in preventing unauthorized access, ZT should be further explored as an essential element of privacy strategies, future research, and recommendations for developers.

4.4. Frameworks and Guidelines for IoTS Security and Privacy

Paul et al. [37] developed a framework for managing privacy and data security risks in Wireless Body Area Networks (WBANs), taking into account both regulatory standards and legislative recommendations. In WBANs, sensor nodes collect, process, store, and send sensitive and private data to local servers or actuators. Therefore, requirements such as security and privacy are critical. Furthermore, WBAN programs run in an environment where most people have unrestricted access to the Internet, making them vulnerable to various risks and attacks. Such attacks can have a detrimental effect on the availability and performance of the service, sometimes posing life-threatening risks. The framework is specifically designed for healthcare and is limited by its reliance on domain-specific regulatory requirements, making it inappropriate for other types of IoTSs. Moreover, the framework lacks a systematic approach for developers to address security and privacy issues during IoTS development, making the framework difficult to implement.

On the other hand, a thorough set of IoT security and privacy rules for edge nodes and communication layers within the IoT reference architecture is proposed by Abdul-Ghani and Konstantas [38]. In addition, a number of implementation strategies have been developed to implement these policies and mitigate potential attacks. They also reviewed some of the privacy and security issues within IoTSs. Despite its highly valuable insights into IoTS threats and countermeasures, the study does not focus on the development of IoTSs. It also lacks a structured methodology that developers can follow to seamlessly integrate privacy considerations into the IoTS development lifecycle.

4.5. IoTS Privacy

There is a noticeable gap in research addressing IoTS privacy from a development perspective. In particular, there is a lack of studies that focus on integrating privacy considerations throughout the IoTS development lifecycle and providing developers with systematic methods for incorporating privacy principles into their designs. Following an extensive literature review, we identified a limited number of studies related to this issue, which were selected for in-depth analysis.

Perera et al. [22] proposed a PbD framework, which consists of a collection of 30 guidelines (briefly presented in Table 1) to assist software developers in incorporating privacy concerns into the design of IoTSs. The foundation of these guidelines is Hoepman's privacy strategies [39], which Perera et al. [40] considered as a starting point for creating a more comprehensive set of PbD guidelines for IoTSs. These authors examined the key challenges affecting the design process of IoTSs and found that their proposed framework significantly enhances the ability of software engineers to effectively incorporate privacy protection.

Table 1. PbD guidelines (adapted from Perera et al. [22]).

Guideline Name	
1-Minimize data acquisition	16-Distributed data storage
2-Minimize the number of data sources	17-Knowledge discovery-based aggregation
3-Minimize raw data intake	18-Geography-based aggregation
4-Minimize knowledge discovery	19-Chain aggregation
5-Minimize data storage	20-Time period-based aggregation
6-Minimize data retention period	21-Category-based aggregation
7-Hidden data routing	22-Information disclosure
8-Data anonymization	23-Control
9-Encrypted data communication	24-Logging
10-Encrypted data processing	25-Auditing
11-Encrypted data storage	26-Open source
12-Data granularity reduction	27-Data flow diagrams
13-Query response	28-Certification
14-Repeated query blocking	29-Standardisation
15-Distributed data processing	30-Compliance

4.6. Comparative Analysis of Existing Approaches

Several approaches have been introduced to address security and privacy concerns in IoTSs. Traditional security mechanisms focus on mitigating vulnerabilities across system layers—such as using blockchain for secure communication—but often neglect the integration of privacy-by-design principles and offer limited guidance for developers during the system lifecycle [25,26].

AI-based techniques, including machine learning, deep learning, and federated learning, have shown promise in detecting threats like botnets and malware [31,32]. However, their direct applicability to the IoTS development process remains limited.

Zero Trust models represent a shift from implicit trust to continuous verification [35], yet their implementation in resource-constrained IoT environments presents significant challenges.

Existing frameworks and guidelines provide valuable insights and domain-specific recommendations [37], but often lack a systematic, developer-centric approach to embedding privacy across all stages of IoTS development.

Privacy-by-Design frameworks—such as those by Perera et al. [22]—offer structured guidance for incorporating privacy, yet typically fall short in terms of tooling support and full lifecycle integration.

Our proposed framework seeks to bridge these gaps by delivering a systematic, lightweight, and developer-oriented approach that incorporates Privacy by Design principles throughout the IoTS development lifecycle. It emphasizes practical privacy require-

ment extraction, workflow support, and adaptive privacy risk management, making it particularly suitable for resource-constrained IoTS environments.

Table 2 summarizes and compares key characteristics of these approaches, highlighting their main focus areas and limitations:

Table 2. Comparative Analysis of Security and Privacy Approaches in IoTS Development.

Aspect	Security-Focused Approaches	AI-Based Detection	Zero Trust Models	Frameworks and Guidelines	Privacy-by-Design Frameworks	Proposed Framework
Main Focus	Vulnerabilities and countermeasures	Threat detection via ML/DL/FL	Access control and continuous verification	Regulatory compliance and policies	Developer privacy guidelines	Systematic privacy integration
Privacy-by-Design Integration	Limited or absent	Partial, privacy-preserving techniques	Limited privacy focus	Limited developer-focused integration	Strong focus on PbD	Core element throughout development
Developer Support	Minimal procedural guidance	Focus on detection, not development	Complex implementation	Limited developer methodology	Guidelines but limited tooling	Stepwise, developer-friendly tools
Alignment with IoTS Development	Limited	Limited relevance	Operational focus	Limited lifecycle integration	Design-phase focused	Full lifecycle integration
Resource Suitability	Moderate to high resource demands	Computationally intensive	Challenging for constrained devices	Domain-specific, variable	Lightweight	Lightweight and scalable
Privacy Risk Handling	General or minimal	Privacy-preserving ML techniques	Mainly access control	Limited beyond compliance	Emphasis on privacy protection	Adaptive risk management and enforcement

4.7. Positioning Against Existing IoTS Development Methodologies

While the comparative analysis focused on privacy- and security-oriented approaches, it is also relevant to consider IoTS development methodologies that provide a more general project structure. One such example is the Three-Phase Methodology (TpM), which organizes the development process into three vendor-agnostic stages: business consideration, requirements gathering, and implementation. Its extended version, TpM-Pro, incorporates a situational method composition approach to enable the selection of development artifacts based on specific project needs.

However, despite their practical value in structuring IoTS development activities, neither TpM nor TpM-Pro provides direct integration of privacy-by-design principles or specific support for privacy requirements across the development lifecycle. Our proposed framework addresses this shortcoming by systematically embedding privacy mechanisms, thereby offering developers structured, privacy-aware guidance throughout all phases of IoTS system development. More precisely, our proposal introduces the following key advantages over existing approaches:

- Integration of privacy concerns throughout the entire IoTS development lifecycle, addressing gaps present in existing solutions.
- A developer-oriented workflow with clear and practical steps for embedding privacy.
- Support emerging technologies, such as federated learning and zero trust, to enhance adaptability.

- Real-world applicability through actionable guidelines tailored to diverse IoTS environments.

5. Proposed Methodological Approach: Planning, Requirements, and Design (PRD)

Our methodological approach consists of three phases: planning, requirements elicitation, and design, as shown in Figure 1. This systematic approach is designed to systematically identify and address privacy concerns in the development of IoTSs. It also provides the details that developers should follow in order to have privacy-enhanced IoTSs. Once key privacy concerns and requirements have been identified, the features that protect users' privacy should be implemented. PRD relies on a user-centric philosophy that places the end user at the center of the design and development process. It also uses some tools to achieve this, such as user stories, to ensure that the focus remains on understanding and effectively integrating users' privacy needs. Figure 1 illustrates the general outline of our proposed approach.

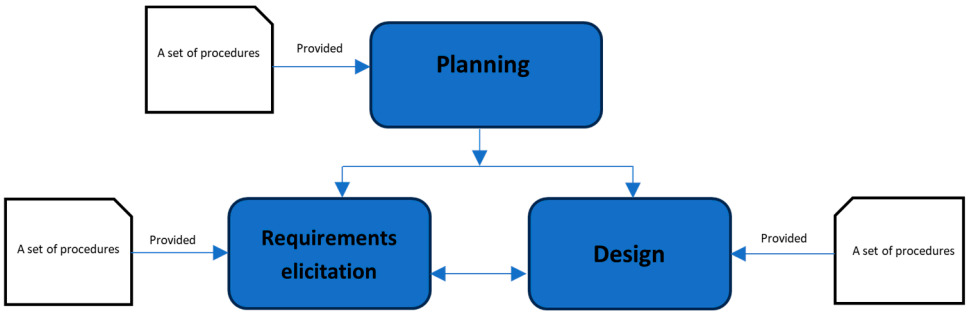

Figure 1. Phases of the proposed PRD approach. The process begins with Planning, followed by Requirements Elicitation, and then Design. Arrows indicate the logical flow between phases and the procedural feedback loops.

5.1. Foundations of PRD

The PRD approach is founded on a combination of best practices that ensure privacy is prioritized throughout the IoTS development lifecycle. It integrates privacy guidelines, a concise set of principles that are continuously reviewed and validated by developers to ensure data protection. The approach also leverages agile methodologies, emphasizing iterative development with user stories to capture evolving requirements and feedback, and promoting flexibility and responsiveness. At its core, our approach aligns with TpM-Pro, which structures the process into clear phases—*business understanding*, *requirements gathering*, and *detailed design*—creating a cohesive framework that balances privacy, user needs, and technical implementation. This integration ensures a privacy-preserving system design while maintaining adaptability and scalability throughout the project.

The TpM-Pro approach, proposed and validated by Ferreira et al. [17], is a methodical and structured framework that effectively addresses each phase of the development of an IoTS solution. Our main contribution lies in extending the systematic stages of this approach to more effectively extract IoTS privacy concerns, supported by a set of updated guidelines aimed at achieving privacy-enhanced IoTS solutions.

To fully understand our approach and its contribution, it is essential to first explain the TpM-Pro approach in detail. TpM-Pro consists of three core steps:

1. **Considering the Business:** In this initial phase, the business context is thoroughly analyzed to identify the key issues the IoT solution aims to address. The TpM-Pro methodology prioritizes a deep understanding of the solution's business value, ensuring alignment with customer needs. Key considerations during this phase include

business requirements, the entities to be measured or controlled, the involvement of specialized expertise, and applicable business rules. To support this process, the TpM-IoT-Canvas tool is used to systematically extract essential requirements and facilitate collaborative planning. This is achieved through a visual model with eight sections: business, justification, benefits, product, things, solution requirements, client, and team. This comprehensive approach ensures that all critical aspects of the business environment are addressed, establishing a strong foundation for the subsequent development phases.

2. **Gathering the Requirements:** In this phase, the process of gathering requirements focuses on breaking down the system into smaller, manageable components to ensure that both business objectives and technical needs are effectively addressed. The business context and the IoT Open-Source Reference Model (IoT-OSRM) serve as foundational frameworks that guide the identification and organization of system elements. The interrelationships among these components are carefully analyzed to ensure coherence and alignment throughout the system architecture. Functional and non-functional requirements are defined using a top-down approach, systematically categorizing them across six levels, beginning with sensor nodes and extending to data presentation. At each level, particular attention is dedicated to addressing security and privacy concerns, ultimately resulting in the creation of a Requirements Report, which consolidates all collected information and provides a solid foundation for stakeholder review and approval before the project progresses to the implementation phase.
3. **Implementation:** In this final phase, developers evaluate and select the most appropriate technologies to fulfill the previously defined requirements, following a bottom-up approach that aligns with the IoT-OSRM reference model. The implementation process is structured in six distinct levels: Level 1 focuses on the selection of components for sensors and actuators, forming the foundation for data collection and interaction with the physical environment. Level 2 involves determining the necessary network infrastructure to ensure reliable and secure communication between devices. Level 3 addresses the selection of the edge element, responsible for local data processing and initial filtering. Level 4 pertains to choosing the most suitable data storage solution, emphasizing scalability, security, and accessibility. Level 5 involves applying appropriate data-handling techniques for processing, analysis, and transformation of raw data into meaningful insights. Finally, Level 6 involves the deployment of user interface tools designed to present processed data to the end user in an intuitive and accessible manner. This structured approach ensures a cohesive and efficient implementation, maintaining consistency with the system's overall design while addressing critical aspects such as security, privacy, and user experience.

Figure 2 illustrates the agents and functions outlined in TpM-Pro, along with a depiction of its phases. It is important to emphasize that TpM-Pro employs an incremental and iterative process, allowing the cycle to continue until an appropriate and workable solution is achieved. This approach enhances the flexibility of TpM-Pro, enabling its application throughout the entire software lifecycle, including the maintenance stages. A detailed explanation of the key aspects of TpM-Pro relevant to our proposal is provided in the subsections below.

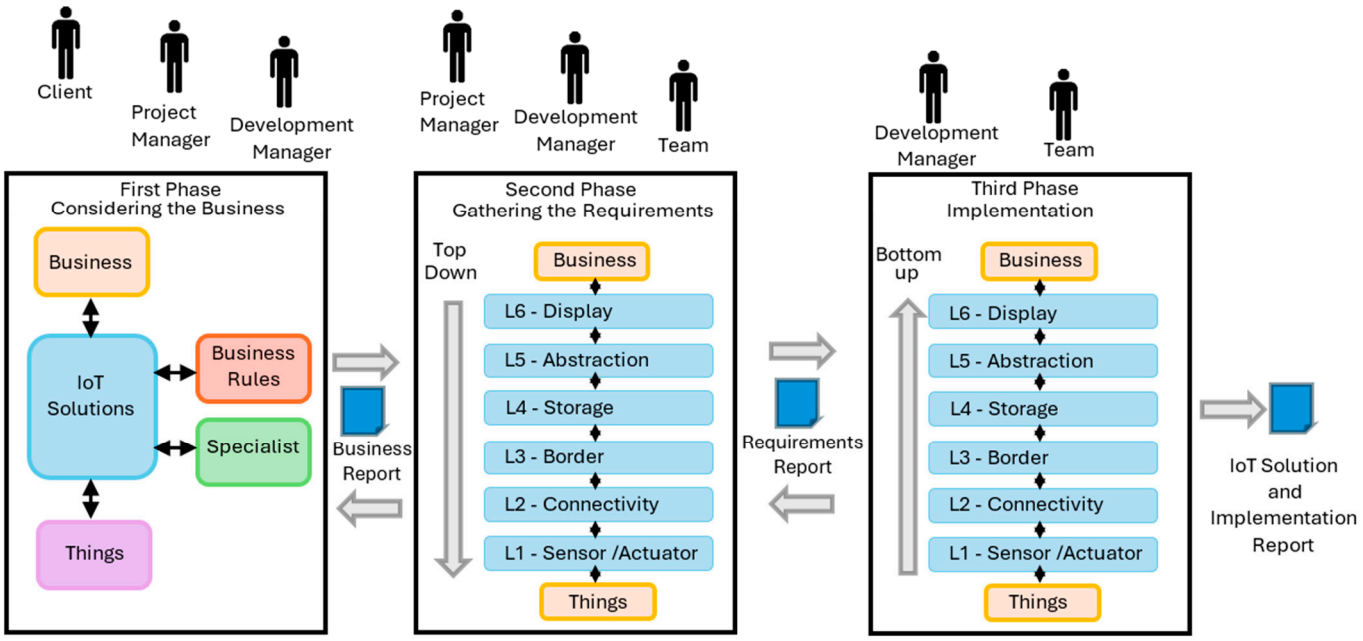

Figure 2. Graphical representation of the TpM-Pro methodology (adapted from Ferreira et al. [17]), highlighting the roles, iterative phases, and deliverables that serve as the basis for this study.

5.1.1. TpM-Pro Agents and Roles

TpM-Pro defines the following agents and roles, as illustrated in Figure 2:

- **Clients:** Includes all the stakeholders involved in the project.
- **Project Manager:** Acts as a liaison between the clients and the development manager. This person is responsible for gathering business data and, in collaboration with other participants, confirming the feasibility of the proposed solution.
- **Development Manager:** Oversees the interdisciplinary team and establishes key considerations for the solution's development. This role also involves monitoring the project's progress, assigning tasks across the different IoT-OSRM levels, and ensuring alignment with the overall project goals. Additionally, the development manager is responsible for gathering requirements and acts as a bridge between the project manager and the interdisciplinary team.
- **Multidisciplinary Development Team:** Consisting of experts with varying levels of IoT-OSRM expertise, this team contributes specialized knowledge throughout the different stages of the development process, ensuring that technical, security, and privacy requirements are effectively addressed.

5.1.2. TpM-Pro Phases

Phase 1: Considering the Business

In this phase, the business context is thoroughly analyzed to identify the key issues that the proposed solution aims to address. The TpM-Pro methodology places a strong emphasis on understanding the business value that an IoT solution provides, setting it apart from previous IoT approaches. The guiding principle here is that an ill-defined business context will inevitably result in a solution that fails to meet client needs. Therefore, the primary objective of this phase is to comprehensively capture customer requirements, expectations, and concerns, ensuring the development of a successful and effective solution.

Several critical factors must be considered when defining the problem to be solved:

- First, the ***business*** itself must be evaluated, recognizing that even projects within the same industry can have unique requirements. Overlooking these nuances could lead to solutions misaligned with end-user expectations.
- Second, it is essential to identify the ***things*** (whether physical or virtual) that the business seeks to quantify, measure, or control. The project manager plays a key role in clearly defining what these "things" are.
- Third, the involvement of ***specialists*** or domain experts, whether internal or external, is crucial as they provide valuable insights that guide informed decision-making.
- Finally, ***business rules***, including any assumptions, constraints, or operational guidelines, must be clearly understood and integrated into the development process to ensure that the solution remains aligned with client needs and complies with regulatory and organizational standards.

To streamline this phase, the TpM-IoT-Canvas tool is used. This tool facilitates the extraction of essential business and solution requirements while promoting collaborative project planning through a structured visual model. The TpM-IoT-Canvas is organized into eight core blocks: business, justification, benefits, product, things, solution requirements, client, and team. By providing a clear framework for organizing key information, this tool ensures that all stakeholders maintain a shared understanding of project goals and constraints, fostering a more cohesive development process.

Phase 2: Gathering of Requirements

Once the Business Report is approved, Phase 2 begins. With a comprehensive understanding of the business context, both functional and non-functional requirements are defined. FRs specify the core tasks and services that the system must perform, detailing the essential operations and features needed to meet user needs. In contrast, NFRs outline the system's quality attributes, technical standards, and design constraints that do not directly relate to functionality but are crucial for overall system performance. These include factors such as security protocols, scalability, system update methods, and regulatory compliance.

This phase follows a top-down approach, structured according to the IoT-OSRM reference model, beginning at the business level and systematically moving downward toward the "things" layer. To collect and document critical information, developers utilize various techniques, such as interviews, case studies, and stakeholder consultations. The gathered requirements are then categorized into the six levels outlined in Figure 2, ensuring a structured approach to system design and implementation:

- **Level 1—Sensor/Actuator Node:** Focuses on the selection of hardware components, including sensors, actuators, microcontrollers, memory, and processing units. Additional key considerations include the integration of edge/fog computing and local data processing to enhance system responsiveness and reduce network load.
- **Level 2—Connectivity:** Specifies the type of connection between the "things" and the border element, whether wired, wireless, or hybrid. Developers evaluate variables such as cost, scalability, environmental conditions, bandwidth, and reliability to determine the most effective communication method.
- **Level 3—Border:** Defines the "border element" that connects the system to the Internet and facilitates communication between IoT devices. This level may incorporate technologies such as network virtualization, middleware, and software-defined networks to optimize data flow and improve network efficiency.
- **Level 4—Storage:** Determines the most appropriate data storage method, considering options such as cloud-based, on-premises, or hybrid solutions. Key factors include data security, redundancy, scalability, and accessibility to ensure efficient data management and compliance with privacy regulations.

- **Level 5—Abstraction:** Identifies the processes through which raw data is transformed into meaningful information. This level leverages expert knowledge and advanced AI analytical techniques, such as ML and data mining, to interpret and contextualize complex data streams.
- **Level 6—Display:** Defines how information is presented to end users, focusing on intuitive and accessible formats, such as tables, graphs, and notifications. Effective data visualization at this level enhances user engagement and decision-making.

Given the complexity of IoT ecosystems, no single tool can fully ensure security and privacy. Therefore, a comprehensive, multi-layered approach is required, integrating diverse techniques and defining privacy guidelines at each level to address specific security challenges and compliance requirements.

At the conclusion of this phase, a detailed Requirements Report is compiled, documenting all functional and non-functional requirements. This report undergoes thorough review and validation by project stakeholders, including managers and developers. If approved, the project proceeds to Phase 3. If not, a revision cycle is initiated to address any outstanding issues or gaps before moving forward.

Phase 3: Implementation

Once the Requirements Report is approved, the implementation phase begins. In this phase, developers evaluate a range of technologies and select the most suitable ones to meet the previously defined requirements. Following a bottom-up approach, this phase aligns with the IoT-OSRM reference model and focuses on how devices are monitored, managed, and presented to the end user. The implementation process adheres to the six levels established during the requirements gathering phase, ensuring consistency and coherence throughout the system architecture:

- **Level 1—Sensor/Actuator Node:** Involves the selection of sensors, actuators, microcontrollers, transducers, and memory components. These hardware elements form the foundational layer of the IoT system, enabling data collection and interaction with the physical environment.
- **Level 2—Connectivity:** Establishes the networking infrastructure required to connect "things" to the edge components. The choice between wired, wireless, or hybrid connections is based on considerations such as bandwidth, latency, environmental factors, and scalability.
- **Level 3—Border:** Focuses on selecting the appropriate edge element, which may include a single-board computer, an inter-cloud computing system, or a dedicated cloud server. The chosen technology must comply with the requirements outlined in Phase 2, ensuring efficient data routing, pre-processing, and enhanced security.
- **Level 4—Storage:** Involves choosing the data storage solution that best meets the system's operational needs, whether through local databases, cloud storage, or a hybrid approach. This selection considers factors such as data security, redundancy, latency, and accessibility, ensuring that stored data remains both reliable and readily available.
- **Level 5—Abstraction:** Focuses on implementing data-handling techniques to process and transform raw data into actionable insights. This includes employing advanced methods such as big data analytics, ML, and DL to extract meaningful information and support informed decision-making for the end user.
- **Level 6—Display:** Involves deploying the user interface tools through which end users will interact with the system. This includes developing mobile applications, dashboards, alerts, graphs, and other forms of visual reporting to present data in an intuitive and accessible manner.

Throughout the implementation phase, maintaining alignment with the predefined requirements is essential to ensure the system's scalability, security, and usability. The bottom-up approach facilitates iterative development, allowing for adjustments at each level to optimize overall system performance and user experience.

5.2. PRD Phases

The proposed methodological approach follows a set of phases that are deeply integrated with TpM-Pro, as illustrated in Figure 3, where the dark blue rounded squares with dashed borders represent our proposed additions, denoted as PRD. The following subsections will detail each PRD phase and explain how this integration is achieved. A summary of the proposed phases, along with their expected objectives, key activities, and outputs, is presented in Table 3.

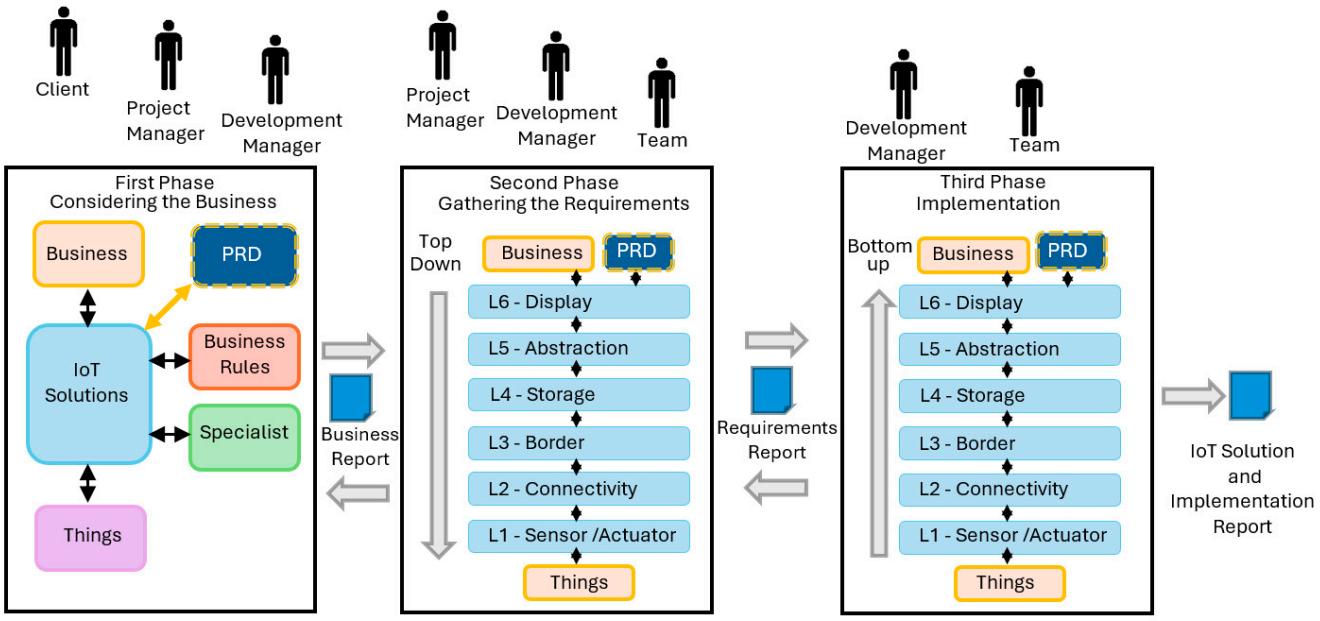

Figure 3. Integration of our proposed PRD approach into TpM-Pro.

Table 3. Overview of the proposed phases, highlighting their objectives, main activities, and resulting outputs.

Phase	Objective	Key Activities	Output
Planning	Define strategic privacy goals	Stakeholder analysis, Privacy Impact Assessment (PIA)	Strategic privacy framework, Aligned goals
Requirements elicitation	Translate goals into actionable requirements	Data flow mapping, Technical/operational requirement definition	Comprehensive requirements report
Design	Build and validate privacy mechanisms	Privacy by Design (PbD), Testing privacy features	Validated system design with embedded privacy tools

5.2.1. Phase 1—Planning

The planning phase serves as the foundational step in our approach and is seamlessly integrated at each stage of TpM-Pro, with distinct focuses and objectives tailored to each

phase. During the "Considering the Business" phase of TpM-Pro, our planning phase ensures that privacy considerations are embedded within the project's strategic alignment. This involves identifying stakeholders and understanding their privacy needs, defining measurable privacy objectives that align with both business priorities and regulatory requirements, and conducting a high-level Privacy Impact Assessment (PIA) to identify potential risks and opportunities early in the project lifecycle, as summarized in Table 3.

The key outputs of this phase include a strategic privacy framework that guides all subsequent phases, along with comprehensive documentation that embeds privacy goals within the broader business objectives. This ensures a privacy-first approach from the outset, fostering both regulatory compliance and stakeholder trust throughout the development process.

This phase also considers the specific domain of the project, such as healthcare, smart cities, or other IoT domains, each of which presents unique privacy considerations. For example, in healthcare, the privacy framework may prioritize patient data protection, compliance with the Health Insurance Portability and Accountability Act (HIPAA) (or equivalent regulations), and the use of robust anonymization techniques. Conversely, in smart cities, the focus might shift toward safeguarding residents' location data, ensuring secure communication between devices, and maintaining transparency in data usage policies. These domain-specific approaches ensure that the planning phase remains adaptable to the unique privacy and operational challenges inherent in each field.

As the methodology advances through the "Gathering the Requirements" and "Implementation" phases of TpM-Pro, the focus of our planning phase evolves to support the project's progression. During the "Gathering the Requirements" phase, the strategic privacy goals identified earlier are translated into specific technical and operational requirements tailored to the project's domain, such as specialized sensors for healthcare or distributed data systems for smart cities. In the implementation phase, the privacy framework developed during our planning phase is realized through tangible actions, including the deployment of privacy-enhancing technologies and the configuration of systems to comply with domain-specific privacy standards.

This iterative refinement ensures that privacy remains central throughout the entire IoT project lifecycle while effectively addressing domain-specific challenges and maintaining regulatory compliance.

5.2.2. Phase 2—Requirements Elicitation

The requirements elicitation phase in the PRD approach, integrated within TpM-Pro, highlights the essential role of accurately defining actionable technical and operational privacy guidelines. As a cornerstone of software development, requirement elicitation enables engineers to capture user needs and translate them into the system's foundational design. However, this process is often complex and iterative, as not all requirements can be fully identified during the initial stages of development. To effectively address this challenge, the approach leverages Agile methodologies, which promote iterative adjustments, accommodate continuous client feedback, and refine requirements throughout the development cycle. This adaptability ensures that evolving user needs, privacy concerns, and technical constraints are continuously addressed, resulting in a more robust and user-centered system design.

In this phase, tools such as user stories, scenarios, and use cases are utilized to gather and analyze both functional and non-functional requirements, with a particular focus on privacy considerations. To enhance the effectiveness of this process, the approach integrates extracted privacy guidelines and domain-specific methods, providing developers with structured guidance to address privacy needs throughout the requirements elicitation

process, as outlined in Table 3. These tools facilitate a comprehensive understanding of user stories, enabling a clear and precise articulation of both system and software requirements, while ensuring alignment with user needs and project objectives.

Aligned with TpM-Pro, the requirements elicitation phase translates strategic privacy goals into detailed technical specifications that guide subsequent design and implementation stages. During the "Considering the Business" phase of TpM-Pro, broad privacy objectives are transformed into initial requirements, ensuring their alignment with the overall project goals. In the "Gathering the Requirements" phase of TpM-Pro, these initial objectives are further refined into detailed user stories, enriched with privacy considerations to capture both technical and operational needs, while maintaining adaptability to evolving challenges.

By the time the project reaches the implementation phase, these refined requirements serve as the blueprint for system configuration, privacy feature deployment, and iterative validation. This integrated and domain-specific approach ensures that privacy is systematically embedded into the IoT project lifecycle, effectively addressing dynamic user needs while simultaneously mitigating potential risks and strengthening regulatory compliance.

5.2.3. Phase 3—Design

The design phase is a crucial stage of the PRD approach, ensuring that privacy-preserving mechanisms are seamlessly incorporated throughout the entire IoT project lifecycle. Within the framework of the TpM-Pro methodology, this phase plays a pivotal role across its various stages:

- **Considering the Business**: Aligns privacy goals with business objectives, ensuring that privacy considerations are integrated from the outset and remain consistent and aligned with the overall strategic vision.
- **Gathering the Requirements**: Defines privacy-specific requirements, such as data anonymization, encryption, and access control, and ensures their seamless integration into the system specifications, laying a solid foundation for a secure and compliant system architecture.
- **Implementation**: Provides a detailed system blueprint that guides developers in the effective implementation of privacy mechanisms. This includes outlining security best practices, testing procedures, and regulatory compliance checks to ensure the system meets all necessary privacy standards.

By embedding privacy considerations at these early stages, the design phase ensures that the entire system architecture is developed with privacy and security at its core. This proactive approach not only reduces potential risks but also ensures regulatory compliance and safeguards user data throughout the project lifecycle, an emphasis that is reflected in Table 3.

Privacy guidelines serve as the backbone of this phase, ensuring that the design remains consistently aligned with privacy objectives while fostering a system architecture that upholds data protection and strengthens user trust.

5.3. Brief Application Steps of the PRD Framework Integrated with TpM-Pro

1. **Planning**
   - Identify stakeholders and core privacy requirements.
   - Set clear privacy objectives aligned with business and regulatory needs.
   - Conduct an initial Privacy Impact Assessment (PIA).
   - Select and tailor relevant privacy guidelines to the project domain
2. **Requirements Gathering**

- Translate privacy objectives into specific technical and operational requirements.
- Use tools such as user stories and use cases to clarify requirements.
- Integrate the selected privacy guidelines into the requirement specifications.
- Continuously refine requirements based on feedback during development.

3. **Design**
   - Integrate privacy-preserving mechanisms (encryption, access control, anonymization) based on the privacy guidelines.
   - Develop a detailed blueprint guiding implementation while ensuring regulatory compliance.
   - Perform privacy testing and validation before final deployment.

6. Proposal of Privacy Guidelines

This section evaluates existing privacy guidelines and proposes enhancements to improve their clarity, implementation, and efficiency for IoTS developers. As previously stated, privacy guidelines should be simplified and clearly explained to ensure better accessibility and usability. Leveraging AI tools can further enhance guideline clarity, making them more actionable and easier for developers to implement in real-world scenarios.

Furthermore, there is a need for a structured roadmap that provides step-by-step instructions, tools, and methodologies to help developers integrate privacy considerations throughout the entire IoTS development process. Without a clear framework, the application of privacy guidelines can become challenging and inconsistent. Reducing the number of guidelines can also help developers focus on core privacy objectives, enabling them to identify key considerations and implement necessary actions more effectively.

By refining these aspects, privacy guidelines can become more practical and efficient, ultimately strengthening privacy protection in IoTSs. To support this goal, we have developed a comprehensive survey designed to assess existing privacy guidelines and gather feedback for further improvement. The details of this survey are presented in the following subsection.

6.1. Survey Design and Implementation

The primary objective of our survey is to evaluate 30 privacy-oriented guidelines, originally proposed by Perera et al. [22], which are designed to guide the development of secure and privacy-conscious IoTS solutions. The survey focuses on gathering participants' insights regarding the following aspects of each guideline:

- Clarity: The ease of understanding the guideline.
- Practicality: The feasibility of implementing the guideline.
- Relevance: The significance of the guideline in ensuring privacy in IoTSs.

Participants were also encouraged to offer suggestions for improvement to enhance the utility of these guidelines for developers working in the IoT field. Each of the above criteria was rated on a 5-point Likert scale, ranging from 1 (Low) to 5 (High). By collecting this feedback, the study aims to refine the guidelines, making them both actionable and aligned with the practical needs of IoTS solution development.

To ensure a diverse range of perspectives, the survey was distributed to a varied group of 75 participants, including developers, industry experts, academics, and students. The survey was conducted using SurveyMonkey, a widely recognized online data collection tool, which ensured ease of access for all participants. The selection of participants was intentional, aimed at capturing a wide range of experiences and expertise directly relevant to IoTS privacy.

The survey was structured into three sections:

1. **Demographic Information:** Collected data on participants' backgrounds and assessed their general understanding of IoTS privacy.
2. **Guideline Evaluation:** Asked participants to evaluate the 30 privacy guidelines based on their clarity, practicality, and relevance.
3. **Feedback and Suggestions:** Provided space for participants to offer additional comments, suggestions, and potential improvements to further refine the guidelines.

Figure 4 presents a segment of the demographic information of the participants, focusing specifically on their professional roles. The figure categorizes participants based on their roles, including software developers, IoT engineers, data scientists, and security specialists, as well as other specialized positions specified by the respondents themselves, such as cybersecurity researchers, Quality Assurance (QA) professionals, systems engineers, PhD students specializing in privacy or cybersecurity research, and professors working in areas like software engineering and software development. Although Figure 4 shows 0% for security specialists, this is because some relevant roles have been categorized under "Other" due to mismatches in exact job titles.

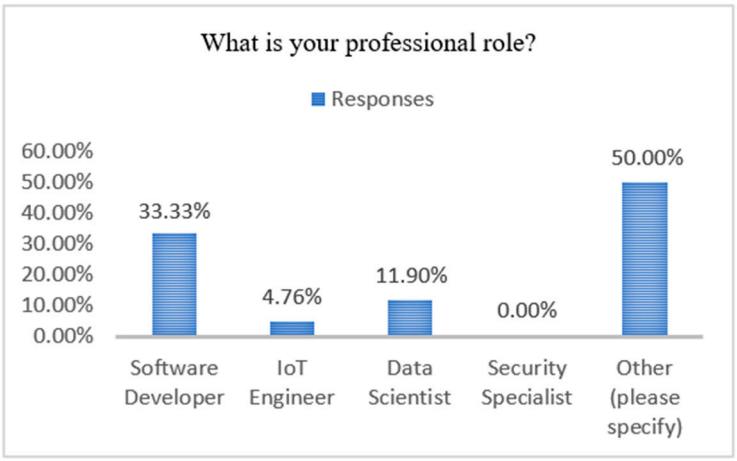

Figure 4. Demographic information of the participants, highlighting their professional roles.

This demographic breakdown highlights the diversity of the participant sample and emphasizes the relevance of their insights to the study, ensuring that the findings are informed by a wide range of perspectives from both academic and industry professionals.

Figure 5 illustrates the years of experience of the participants, providing valuable insight into their level of expertise and supporting the overall reliability of their responses. The data reveals that a significant portion of participants possesses extensive experience in their respective fields, which enhances the credibility of their feedback. The distribution of experience is categorized into four groups: 0–2 years, 3–5 years, 6–10 years, and over 10 years. The chart shows that a considerable proportion of participants have more than 10 years of experience, indicating that the sample includes a substantial number of seasoned experts. Additionally, a notable percentage of participants fall within the 6–10 years range, further reinforcing the depth of professional experience within the group. In contrast, the percentage of participants with 0–2 years or 3–5 years of experience is comparatively lower, suggesting that the number of less-experienced participants is minimal. Overall, this distribution supports the conclusion that the majority of participants have significant experience in the field, which contributes to the dependability and accuracy of their responses in the study.

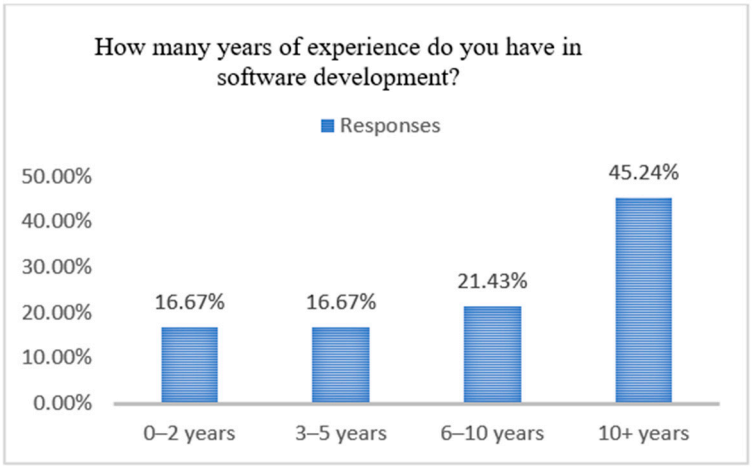

Figure 5. Distribution of participants by years of professional experience.

Figure 6 highlights participants' prior experience with IoT applications, providing further validation of the reliability of their responses. The figure indicates that a significant majority of respondents report having direct experience working on IoT projects, indicating that most participants possess practical expertise in the field. This hands-on experience is particularly valuable to the study, as it ensures that the feedback on IoT privacy guidelines is grounded in a real-world application. Conversely, the presence of participants with no prior experience in IoT development suggests that the sample also includes individuals who may offer theoretical knowledge of IoT, despite lacking direct industry exposure. This diversity in experience levels enriches the study by incorporating perspectives that balance both the practical challenges encountered in the field and the academic viewpoints that may highlight potential gaps or emerging trends. This combination of practical and theoretical insights ensures a more comprehensive evaluation of privacy guidelines, reflecting a broad spectrum of experiences and expertise within the IoT ecosystem.

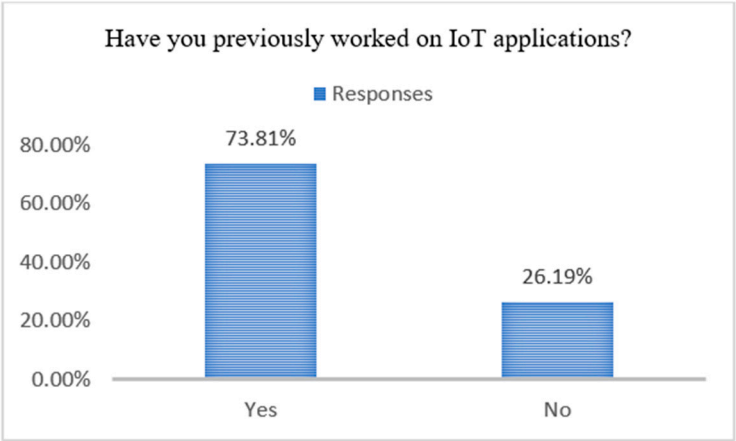

Figure 6. Participants' experience in developing IoT applications.

6.2. Survey Results

Building on the analysis of participant responses, this study identifies key trends in IoT privacy practices, highlights priority areas requiring attention, and critically examines the limitations of the collected data. By evaluating the *clarity*, *practicality*, and *relevance* of 30 IoT privacy guidelines, the findings provide a nuanced understanding of the challenges and considerations in implementing effective privacy measures. This analysis not only reflects prevailing industry perspectives but also contributes to the ongoing discourse on enhancing privacy frameworks in IoT applications.

However, it is essential to consider the scope of the dataset when interpreting these findings. Out of the 75 surveyed professionals, only 43 participants provided responses for this section, meaning that the reported averages reflect the views of this subset rather than the entire respondent group. Despite this limitation, the collected data offers valuable insights into how different stakeholders perceive and prioritize privacy guidelines in IoT, shaping a clearer understanding of practical implementation challenges and industry needs.

Before delving into the analysis of the guidelines, it is important to present additional contextual information about the participants. Figure 7 illustrates the participants' familiarity with privacy-focused design in IoT. The survey results reveal varying levels of familiarity, reflecting a broad spectrum of expertise within the participant pool. Most respondents reported being "Somewhat familiar" with privacy-focused design, indicating a moderate understanding of privacy considerations in IoTS development. A smaller subset of participants identified as "Very familiar", representing individuals with advanced expertise and strong engagement in privacy-centric practices. Conversely, a notable percentage of participants reported being "Not familiar", highlighting a potential gap in knowledge or awareness regarding privacy-centric design principles. These findings suggest that while privacy is recognized as an important aspect of IoTS development, it is not yet a primary focus for all professionals in the field. This underscores the need for greater emphasis on privacy education and specialized training within the IoT development community to promote broader adoption of privacy-centric approaches.

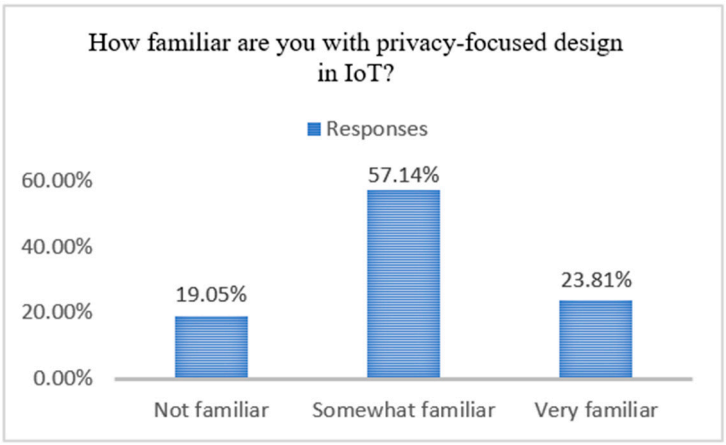

Figure 7. Participants' familiarity with privacy-focused design in IoT.

6.2.1. Analysis Part 1: Categorization of Guidelines Based on Importance and User Feedback

To conduct this analysis, each guideline was evaluated based on its *relevance*, *practicality*, and *clarity*, using a five-point Likert scale. This structured evaluation enabled a comprehensive assessment of the guidelines, grounded in participant feedback. Based on the analysis, the guidelines were categorized into three distinct groups:

(a) High-Importance Guidelines

These guidelines consistently received high ratings across all three dimensions, with a mean score of 4.0 and above, signifying their critical role in safeguarding IoTS privacy.

- Encrypted Data Communication (4.51)
- Encrypted Data Storage (4.44)
- Data Anonymization (4.42)
- Minimize Data Storage (4.23)
- Information Disclosure (4.40)
- Compliance with Regulations (4.35)

- Logging (4.30)
- Auditing (4.30)
- Minimize Raw Data Intake (4.0)

These guidelines focus on fundamental privacy practices, including data encryption, user awareness, and regulatory compliance, which are essential for ensuring robust security in IoTSs.

(b) Medium-Importance Guidelines

These guidelines, with scores between 3.7 and 3.99, were considered valuable but may require refinement or be context-dependent, affecting their applicability across different IoT scenarios.

- Minimize Data Acquisition (3.86)
- Minimize Number of Data Sources (3.79)
- Reduce Data Granularity (3.88)
- Knowledge Discovery-Based Aggregation (3.91)
- Distributed Data Storage (3.88)
- Category-Based Aggregation (3.79)
- Query Answering Without Raw Data (3.95)

These guidelines focus on data efficiency and control mechanisms; however, their feasibility often depends on the specific nature of IoTSs, as some systems require extensive data collection to operate effectively.

(c) Low-Importance Guidelines

These guidelines received scores below 3.7, indicating limited practical implementation or a lack of clarity.

- Minimize Knowledge Discovery (3.16)
- Open-Source Policy for Transparency (3.37)
- Hidden Data Routing (3.49)
- Chain Aggregation (3.21)
- Minimize Data Retention Period (3.5)
- Repeated Query Blocking (3.0)
- Distributed Data Processing (3.0)
- Geography-Based Aggregation (3.5)
- Time-Period Based Aggregation (3.0)
- Control (3.5)
- Data Flow Diagrams (3.5)
- Certification (3.0)
- Standardization (3.0)
- Encrypted Data Processing (3.5)

These guidelines may be perceived as too restrictive, too complex to implement, or insufficiently defined. The lower ratings suggest the need for revisions to improve their clarity and practical utility, with potential adjustments to make them more actionable.

Key Findings and Reflections

The study highlights that guidelines such as "Encrypted Data Communication" (4.51) and "Encrypted Data Storage" (4.44) are considered highly important, reflecting participants' emphasis on data security and regulatory compliance. These high scores suggest a shared understanding among participants of encryption as a fundamental privacy measure in IoTSs.

In contrast, medium-priority guidelines, such as "Minimize Data Acquisition" (3.86) and "Query Answering Without Raw Data" (3.95), were recognized for their privacy

benefits but viewed as context-dependent. Their practical feasibility is often limited by specific IoTSs that require large-scale data collection for core functionalities.

Lower-rated guidelines, like "Minimize Knowledge Discovery" (3.16) and "Chain Aggregation" (3.21), may have been perceived as too specialized or unclear in their implementation strategies. These lower ratings point to the need for clearer definitions or more adaptable versions of these guidelines to suit various IoT environments.

In summary, this data-driven categorization provides a balanced and objective evaluation of the guidelines, emphasizing their real-world applicability and reflecting the collective insights of the participants. However, while this analysis provides valuable insights, it remains unclear why participants rated certain guidelines higher or lower. To gain a deeper understanding, future studies could incorporate qualitative methods, such as in-depth interviews or focus groups, to explore the motivations behind participants' choices. This qualitative data could reveal additional factors influencing guideline adoption, offering a more comprehensive view of the challenges and preferences in IoT privacy practices.

6.2.2. Analysis Part 2: Detailed Analysis of Participant Recommendations

This section presents a detailed analysis of the recommendations provided by participants during the survey. Their feedback offers valuable insights into practical concerns, implementation challenges, and potential improvements for IoT privacy guidelines. These recommendations have been carefully examined to understand their implications and their impact on the overall context of the study. The objective is to provide in-depth insights that can contribute to enhancing future practices based on the participants' opinions and expertise.

The participants' feedback can be categorized into five major themes:

1. ***Need for More Precise Definitions and Examples***
   A recurring concern among respondents was the ambiguity in certain guideline definitions. Participants pointed out that terms such as "minimizing data acquisition" and "minimizing knowledge discovery" are vague and context-dependent. To address this, they suggested the following:
   (a) Incorporating specific use-case examples for each guideline to illustrate its practical applications more clearly.
   (b) Aligning definitions with established privacy frameworks, such as GDPR and the National Institute of Standards and Technology (NIST), to ensure consistency with regulatory standards.
   (c) Providing clear thresholds for implementation, such as specifying what constitutes "excessive data retention".
2. ***Balancing Privacy and Performance in Encrypted Data Processing***
   Although encryption was among the highest-rated guidelines, several respondents raised concerns about its computational cost. Advanced encryption methods, such as homomorphic encryption and multi-party computation, can introduce latency and processing overhead, making them impractical for resource-constrained IoT devices. Participants recommended the following:
   (a) Adopting hybrid encryption models that combine end-to-end encryption with selective decryption to enhance efficiency.
   (b) Utilizing lightweight cryptographic approaches, such as differential privacy and zero-knowledge proofs, to reduce processing demands.
   (c) Implementing adaptive encryption policies that dynamically adjust encryption levels based on data sensitivity and device capabilities.

3. ***Importance of Automated Privacy Enforcement***
   Several participants emphasized the need for automated privacy mechanisms, arguing that privacy policies should not depend solely on manual configurations. Key recommendations included:
   (a) Developing real-time privacy risk assessment tools to proactively identify potential violations before they occur.
   (b) Establishing automated data expiration policies to ensure compliance with minimal human intervention.
   (c) Leveraging ML-based anomaly detection to dynamically monitor and address privacy threats.
4. ***Improving Data Aggregation and Query Answering***
   Aggregation-based guidelines, such as Geography-Based Aggregation and Time-Based Aggregation, received moderate ratings, suggesting that their effectiveness is highly dependent on the specific use case. Respondents suggested the following:
   (a) Designing context-sensitive aggregation strategies that balance data usability with privacy protection.
   (b) Refining query-answering models to ensure differential privacy, preventing the exposure of individual data points.
   (c) Introducing threshold-based aggregation policies to limit the risk of sensitive data overexposure.
5. ***Expanding Privacy Guidelines to Cover Emerging Challenges***
   Several participants identified gaps in the current privacy guidelines, particularly in relation to emerging technologies and evolving privacy challenges. They proposed expanding the guidelines to address:
   (a) AI and Privacy: Strategies to ensure that AI-driven analytics handle IoTS data responsibly while preserving user privacy.
   (b) Edge Computing Privacy: Approaches for securing decentralized data processing at the network edge.
   (c) User-Controlled Privacy Mechanisms: The need for greater transparency and user-accessible privacy settings in IoTSs to empower end users.

6.2.3. Analysis Part 3: Exploring the Influence of Developers' Backgrounds on Their Interpretation of Privacy Guidelines

This section shows a detailed analysis of how developers' professional roles influenced their responses to the different aspects of privacy guidelines, particularly in terms of relevance, clarity, and practicality. The participants' job titles provide insights into their interpretation of guideline relevance. For instance, roles such as Data Scientist, Cybersecurity Specialist, and Privacy Engineer tended to assign higher relevance scores across most guidelines, likely due to their direct engagement with privacy-preserving systems and regulatory compliance. In contrast, participants with titles like Software Developer or Embedded Systems Engineer exhibited more variation in relevance ratings, possibly reflecting competing priorities such as functionality and performance in their development workflows.

Academic roles (e.g., Assistant Professor, Researcher) also demonstrated consistently high relevance scores, which may stem from a stronger theoretical understanding of privacy principles and ethical considerations. These differences highlight that the interpretation of guideline relevance is not uniform and can be shaped by practical responsibilities, regulatory exposure, and organizational focus. Thus, accounting for job roles provides valuable context for understanding how privacy guidelines are perceived and prioritized in real-world settings.

The observed variation in relevance ratings among software developers suggests a potential gap in understanding the practical significance of certain privacy guidelines. Unlike roles in academia or data security, developers may not always be directly exposed to privacy risks or regulations, which underscores the need for more targeted education and contextual examples when introducing privacy principles within development environments.

The evaluation results also revealed noticeable variations in how different professional roles perceive the clarity and practicality of the privacy guidelines. Academic participants, such as assistant professors and PhD students in cybersecurity, consistently rated the guidelines as clearer and more practical. This may be attributed to their familiarity with theoretical constructs and structured approaches to privacy, which align well with the guideline content. In contrast, roles with a more technical and implementation-focused background, such as software developers and quality assurance engineers, tended to provide lower ratings, especially regarding practicality. This suggests that while the guidelines may be conceptually sound, they may require additional contextualization or technical examples to enhance their applicability and clarity for practitioners in hands-on development environments.

Figure 8 highlights what was previously discussed regarding the variation in guideline evaluation based on professional roles. Academic and data-focused roles tend to assign higher scores in terms of clarity, practicality, and relevance, while technical roles such as software developers and QA engineers show more variability. This reflects a potential need for further clarification and practical adaptation of the guidelines to fit real-world development environments.

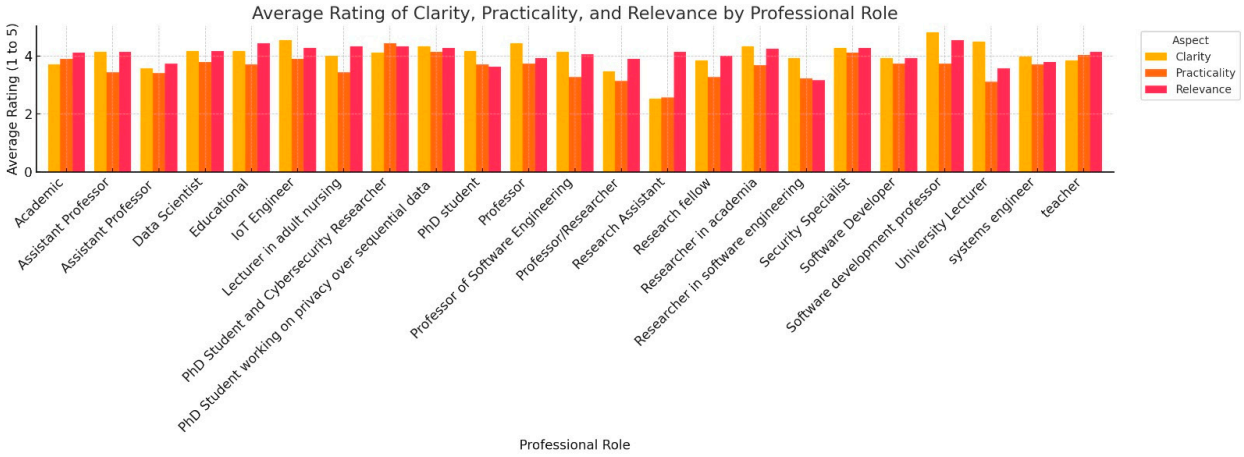

Figure 8. Average rating of clarity, practicality, and relevance scores by participants' professional role.

6.2.4. Summary

The participant recommendations highlight a fundamental trade-off in IoT privacy guidelines: the balance between strict privacy controls and practical feasibility. While more stringent guidelines offer stronger privacy protections, they often introduce computational, usability, and regulatory challenges. The *key takeaways* from the analysis are as follows:

1. **Clarity and precision are crucial**: Ambiguous guidelines hinder adoption. Definitions should be clear and grounded in real-world scenarios to ensure practical applicability.
2. **Performance constraints must be addressed**: Encryption and data processing techniques should be designed using lightweight and adaptive solutions to accommodate the resource limitations typical of IoT environments.
3. **Automation is the future of IoT privacy**: Privacy protection should move beyond manual enforcement, relying instead on intelligent, automated systems for greater efficiency and reliability.

4. **Aggregation strategies need flexibility**: Rather than rigid aggregation policies, a context-driven approach should be adopted to balance data usability and privacy protection.
5. **Emerging threats require new guidelines**: Future privacy frameworks must evolve to address challenges posed by AI, edge computing, and the increasing demand for user autonomy in IoTSs.

6.3. Proposal

Our proposal is divided into three parts, each of which is detailed in the following subsections.

6.3.1. Proposal Part 1: Proposed Privacy Guidelines for IoTS

Based on the recommendations and suggestions received, along with our subsequent analysis, we propose the following refined list of prioritized guidelines aimed at enhancing IoTS privacy. These guidelines address critical aspects of data collection, storage, and processing, as well as security, user control, and regulatory compliance, providing a comprehensive framework for safeguarding privacy in IoTSs.

1. ***Data Collection and Processing***
   - **Minimize Data Acquisition**: Collect only the data that is essential for the intended purpose, reducing unnecessary data collection.
   - **Reduce Data Granularity**: Limit the level of detail in collected data to the minimum required, avoiding excessive precision where it is not needed.
   - **Query Answering Without Raw Data**: Provide analytical insights without exposing complete raw datasets, ensuring sensitive data remains protected.
2. ***Data Security and Protection***
   - **Encrypted Data Communication**: Apply strong encryption protocols to secure all data transmissions and prevent unauthorized access.
   - **Encrypted Data Storage**: Store data using strong encryption methods to safeguard it against breaches and unauthorized retrieval.
   - **Data Anonymization**: Implement techniques such as pseudonymization and k-anonymity to protect user identities and reduce re-identification risks.
3. ***Data Storage and Retention***
   - **Minimize Data Storage**: Retain only data that is necessary for operational or legal purposes, reducing the risk of data exposure.
   - **Automated Data Deletion**: Establish automated processes to delete data once it is no longer required, ensuring compliance with data retention policies.
4. ***Aggregation and Decentralization***
   - **Knowledge Discovery-Based Aggregation**: Aggregate data to extract meaningful insights while ensuring privacy is maintained.
   - **Distributed Data Storage**: Implement decentralized storage solutions to avoid single points of failure and enhance data resilience.
5. ***User Control and Transparency***
   - **Information Disclosure**: Clearly inform users when their data is collected, ensuring transparency in data-handling practices.
   - **User Privacy Controls**: Provide users with flexible, dynamic privacy settings, empowering them to control how their data is used.
   - **Logging and Auditing**: Maintain comprehensive records of data activities to facilitate regular security audits and ensure accountability.

6. *Regulatory Compliance and Best Practices*
    - **Compliance with Privacy Regulations**: Ensure alignment with established privacy laws and standards, including GDPR, the California Consumer Data Privacy Act (CCPA), and International Organization for Standardization (ISO) frameworks.
    - **Privacy by Design and Default**: Integrate privacy considerations from the initial design phase and enforce them as the default operating standard.

Comparison of the Proposed Privacy guidelines with LINDDUN Privacy Threats

Table 4 provides a detailed comparison between the 15 proposed privacy guidelines and the 14 privacy threats from the LINDDUN framework [41], corresponding to the purple, orange, and red categories, which were identified as most relevant and aligned with the focus of our study. This mapping reveals varying degrees of overlap: several guidelines directly address known threats, either by reframing them as proactive design recommendations or by enhancing or extending them through more actionable, developer-focused implementation strategies. Notably, four of the proposed guidelines represent novel contributions that are not explicitly covered by the LINDDUN threat model. Specifically, these guidelines are as follows:

- **Guideline 3: Query Answering Without Raw Data**. This guideline supports privacy-preserving data querying by enabling analytical responses without exposing raw data. While LINDDUN highlights risks associated with personal data overexposure, it does not address mechanisms such as federated queries or privacy-preserving statistical summaries. Our approach empowers developers to provide meaningful insights while minimizing privacy risks.
- **Guideline 9: Knowledge Discovery-Based Aggregation.** This guideline promotes aggregation techniques aligned with privacy-preserving data mining principles. While LINDDUN warns against unnecessary data analysis, it does not propose practical methods for safely extracting knowledge from aggregated data. Our approach bridges this gap by offering developer-oriented strategies that enable useful analytics without compromising individual privacy.
- **Guideline 10: Distributed Data Storage.** This guideline encourages distributed data storage architectures to minimize single points of failure and increase resilience, thereby enhancing privacy protection. While LINDDUN addresses insufficient processing security, it lacks specific guidance on decentralization as a privacy-preserving architectural strategy. Our proposal introduces this concept as a concrete privacy-preserving design pattern tailored to IoT environments, helping developers adopt modern, resilient system architectures that support privacy goals.
- **Guideline 15: Privacy by Design and Default.** This guideline advocates for the proactive integration of privacy principles from the earliest stages of system design, ensuring that privacy protections are embedded by default. Unlike LINDDUN, which refers to general compliance with privacy standards, our approach provides explicit guidance for developers to integrate privacy throughout the entire system development lifecycle, enabling comprehensive and effective enforcement of privacy requirements.

Table 4. Mapping of proposed privacy guidelines to selected LINDDUN threats, highlighting novelty and contribution.

	Proposed Guideline	Mapped LINDDUN Threat(s)	Novelty/Comment	Contribution
1	Minimize Data Acquisition	Excessive Amount of Data Collected	Same objective, rephrased as a positive design principle	Direct Mapping
2	Reduce Data Granularity	Excessively Sensitive Data Collected	Emphasizes data precision control, not explicitly covered in LINDDUN	Enhanced
3	Query Answering Without Raw Data	Overexposure of Personal Data	Proposes concrete privacy-preserving querying mechanisms absent in LINDDUN	New
4	Encrypted Data Communication	Insufficient Security of Processing	Standard mitigation directly aligned with LINDDUN	Direct Mapping
5	Encrypted Data Storage	Insufficient Security of Processing	Standard mitigation directly aligned with LINDDUN	Direct Mapping
6	Data Anonymization	Excessively Sensitive Data Collected	Adds specific anonymization strategies	Enhanced
7	Minimize Data Storage	Unnecessary Data Retention	Same goal expressed as a design principle	Direct Mapping
8	Automated Data Deletion	Insufficient Rectification or Erasure	Adds automation aspects not explicitly covered by LINDDUN	Enhanced
9	Knowledge Discovery-Based Aggregation	Unnecessary Data Analysis	Suggests novel aggregation for privacy-preserving analytics absent in LINDDUN	New
10	Distributed Data Storage	Insufficient Security of Processing (Resilience Dimension)	Introduces architectural decentralization absent in LINDDUN	New
11	Information Disclosure	Insufficient Transparency	Same goal rephrased positively	Direct Mapping
12	User Privacy Controls	Insufficient Privacy Controls, Insufficient Access	Emphasizes user-centric, dynamic control mechanisms	Enhanced
13	Logging and Auditing	Improper Data Lifecycle Management	Adds concrete mechanisms for traceability and accountability	Enhanced
14	Compliance with Privacy Regulations	Non-Compliance of Processing with Applicable Regulations, Non-Adherence to Privacy Standards	Provides explicit reference to current regulations (e.g., GDPR), extending LINDDUN's approach	Enhanced
15	Privacy by Design and Default	Non-Adherence to Privacy Standards	Introduces proactive privacy integration across the lifecycle	New

These additions reflect original contributions specifically tailored to the constraints and development workflows of IoT systems. Overall, the comparison highlights both the alignment with and the added value of our guidelines relative to LINDDUN, reinforcing their relevance to practical and forward-looking privacy engineering in real-world IoT environments.

As illustrated in Table 4, the proposed guidelines demonstrate both alignment with and meaningful extension beyond the existing LINDDUN threat model. To further contextualize this comparison, we highlight four key aspects that distinguish our contributions from those of the LINDDUN framework:

1. **Transformation into developer-oriented recommendations:** While LINDDUN offers valuable theoretical descriptions of privacy threats, our guidelines build upon these concepts and introduce additional, original elements to deliver concrete, actionable practices for developers. For example, whereas LINDDUN identifies *Insufficient*

Security of Processing, our guideline goes further by recommending *Encrypted Data Communication* as a practical and developer-friendly mitigation strategy.

2. **Added technical and architectural contributions:** Several guidelines extend beyond LINDDUN's scope by introducing technical implementation patterns and architectural solutions specifically tailored to IoT environments and their constraints. For instance, *Distributed Data Storage* and *Knowledge Discovery-Based Aggregation* explicitly address resilience and privacy-preserving analytics in distributed IoT architectures, areas not explicitly covered in LINDDUN's original formulation.
3. **Objective prioritization:** The scoring-based approach guarantees that the guidelines align with stakeholder priorities in terms of clarity, practicality, and relevance, thereby reinforcing their applicability to real-world IoT systems.
4. **Avoiding developer overload:** We have considered the cognitive burden placed on developers, recognizing that an excessive number of guidelines can lead to developer fatigue, reducing their ability to effectively implement privacy protections.

6.3.2. Proposal Part 2: Balancing Security and Performance in IoTS

Designing privacy-aware IoTS often involves a delicate trade-off between ensuring strong security and maintaining acceptable performance. Many IoT devices operate with limited computational resources, making it important to choose encryption methods that provide adequate protection without overloading the system [29]. In this section, we explore how lightweight and more robust encryption techniques can be applied in practice, based on insights from recent studies. These considerations are incorporated into our framework to ensure it remains both secure and practically efficient in real-world IoT environments.

Traditional Internet communication typically relies on faster, more secure wired or wireless methods, whereas IoT nodes face significant challenges due to their limited resources and the complexity of wireless protocols. These nodes often lack an operating system, and their data formats vary depending on the specific application. Many IoT systems also collect large amounts of personal data, often controlling physical environments. Unlike traditional devices, which benefit from robust security measures, the decentralized nature of IoT networks makes them inherently more vulnerable to security threats. To mitigate these challenges, IoT systems must implement lightweight and scalable security protocols that can operate effectively within the constraints of these resource-limited devices [42].

As part of our investigation into selecting appropriate lightweight cryptographic algorithms for IoT applications, a comprehensive review of recent studies was conducted. These studies classified and compared cryptographic algorithms from various perspectives, reflecting the multifaceted nature of IoT environments and their diverse security requirements. For instance, Abosata et al. [43] adopted a classification based on the communication layer perspective, such as the transport and network layers. Their study highlighted critical issues, such as the high energy consumption required by the ECC algorithm, which poses challenges for energy-constrained IoT devices.

Thabit et al. [44] presented a detailed great classification and comparison of lightweight block ciphers based on performance and resource-efficiency parameters. Building on their work, Table 5 offers a summary of the most relevant lightweight block ciphers currently in use. The study assessed these algorithms using well-established evaluation criteria, including structure, block size, key size, key space, time complexity, CPU clock cycles (cycles per block), code size, RAM usage, cipher type, and overall security strength.

Table 5. Recommended lightweight cryptographic algorithms for different IoT application domains.

IoT Domain	Recommended Algorithm	Performance/Rational
Smart Home	PICCOLO, SIMON, SPECK, TWINE	Low memory and processing requirements
RFID/Logistics	SPECK, PICCOLO, SIMON	Limited space, no power backup
Smart Agriculture	TWINE, SIMON, SPECK, PRESENT	Energy efficiency, minimal processing, remote deployment
Healthcare	SIMON, SPECK, PICCOLO, PRESENT, MIDORI	Privacy, real-time response, low resources
Industrial Systems	MIDORI, PRINCE	Wireless communication, hard-to-access sensors
5G World	PRINCE, PRESENT, SIMON, MIDORI	Secure real-time communication
Remote Keyless Entry	KEELOQ	Secure lightweight cipher for cars and buildings

This domain-specific classification provides a strong foundation for identifying candidate cryptographic algorithms appropriate for different IoT domains based on structural and theoretical criteria. However, practical evaluation is crucial to confirm real-world performance. A recent benchmarking study [45] evaluated 122 lightweight cryptographic algorithms on metrics like code size, memory use, speed, and energy consumption. Results showed similar code size and ROM usage across platforms, but Raspberry Pi outperformed others significantly in RAM usage, processing speed, and energy efficiency. These benchmarking results complement the theoretical classification by offering practical insights into how lightweight ciphers perform on real IoT platforms. Such empirical evaluation is crucial for making informed decisions about cryptographic algorithm selection, ensuring both security and efficiency in resource-constrained IoT environments.

6.3.3. Proposal Part 3: Automated Privacy Enforcement in IoTS

In dynamic and resource-constrained IoT situations, automatic privacy enforcement is a viable approach to privacy management. Without requiring human interaction, it helps guarantee data protection by modifying privacy settings in real-time circumstances, such as user behavior or network conditions. This method improves system privacy overall and lessens user strain. Given the wide range of IoT application domains, from smart homes to healthcare and industrial systems, the conventional manual configuration of privacy settings becomes inadequate and prone to errors. Automated privacy, frequently powered by AI, ML, or context-aware rule-based systems, allows privacy protections to be adjusted in real time according to contextual variables including network status, device behavior, and user presence [46]. In this section, we explore the automated privacy enforcement and highlight key approaches and technologies that enable its implementation.

AI-Based Privacy Preservation

The growing emphasis on privacy in IoT systems has led to the increased use of ML techniques to support privacy-preserving solutions. ML can detect usage patterns, identify anomalies, and recommend privacy settings based on past user behavior. Moreover, it enables adaptive responses to frequent contextual changes by aligning them with user privacy preferences [47].

Building on this, Nazir et al. [30] emphasized the importance of ML and DL in detecting IoT botnets, which represent a critical threat to both privacy and security. ML

algorithms can be trained to recognize patterns in network traffic or device behavior that may indicate a botnet attack, and they can automatically respond to such threats and protect users' privacy. However, while these techniques are powerful, they also raise privacy concerns, particularly when large volumes of sensitive data are involved. Therefore, there is a need for privacy-preserving ML and DL models that can operate on encrypted or decentralized data, thereby avoiding the direct exposure of personal information.

FL has been highlighted by Qureshi et al. [31] as a promising solution for privacy preservation. FL decentralizes data processing, allowing IoT devices to collaboratively train models while keeping all training data local. This mitigates privacy risks and reduces transmission overheads, aligning well with privacy-by-design principles.

Furthermore, advancements in communication technologies—such as 5G and emerging 6G networks—offer high bandwidth, ultra-low latency, and edge computing capabilities. These developments enable IoT devices to utilize local edge resources to train and execute ML models more efficiently and privately. As highlighted by Sun et al. [48], both FL and edge learning paradigms show strong potential in addressing both scalability and privacy limitations inherent in centralized approaches.

Thus, adopting adaptive AI methods is recommended to enhance privacy in IoT environments. However, further research is needed to ensure their efficiency and accuracy under real-world constraints.

Context-Awareness and Privacy

The concept of context awareness, first introduced in 1994 [49], has evolved significantly, with several researchers providing domain-specific definitions. In the realm of IoT security, context awareness is described as the ability of a system to detect, sense, interpret, and respond to aspects of a user's environment and computing devices. This is especially important in IoTS, where the security and privacy requirements of users must adapt to varying contexts such as location (e.g., home, office, workplace) [50].

In this sense, context-based security involves explicitly considering context in the specification of security solutions such as access control models and cryptographic protocols. These solutions must incorporate mechanisms that dynamically adjust to the user's environment, ensuring that the IoT system continuously protects the user's privacy and security. Thus, enhancing the overall effectiveness and appropriateness of security measures based on the user's current situation. For example, rule-based strategies are employed in context-aware privacy enforcement to make automatic decisions based on predefined rules that govern system behavior across different contexts. These systems can enforce privacy policies without manual intervention, making them efficient and responsive. Additionally, they can be integrated with other technologies, such as ML, to adapt to changing user behaviors and dynamic environments over time.

An illustrative example is the Privacy Oracle, introduced by Chaaya et al. [51]. This context-aware approach helps users safeguard their privacy by identifying risks in real time. It utilizes semantic user environment modeling (SUEM) ontologies to represent and update user information and environmental data. Privacy risks are dynamically inferred through a reasoning process based on a set of privacy rules.

Blockchain for Privacy Management

In the realm of IoT, secure data storage is often achieved through cloud-based solutions, where differential privacy mechanisms are employed to ensure confidentiality and protect user data against unauthorized access [52].

To strengthen access control in such distributed environments, Wang et al. [52] proposed a dynamic and lightweight attribute-based access control framework specifically designed for blockchain-enabled IoT systems. This framework leverages decentralized

applications to maintain tamper resistance and accommodate delay-sensitive applications, offering fine-grained authorization while reducing central dependencies. Complementing this, Saha et al. [53] emphasized the importance of decentralization in enhancing privacy and transparency through blockchain technologies. Blockchain has been increasingly integrated across various IoT applications—ranging from sensor networks and data storage to identity management, timestamp services, and supply chain monitoring—bringing forth enhanced transparency, security, credibility, and operational efficiency. These contributions collectively demonstrate the growing reliance on blockchain-based solutions to address the privacy and security challenges in IoT ecosystems [48].

This highlights the importance of implementing blockchain-based solutions in a well-considered and monitored manner to prevent potential performance issues in resource-constrained IoT environments, while ensuring adherence to established security and privacy standards.

7. Conclusions and Future Work

This study highlights the critical importance of privacy in IoTSs, given the vast amount of sensitive data they collect and process. Robust privacy protections are essential to safeguard this data and mitigate risks associated with data breaches and unauthorized access. As IoTSs expand across diverse sectors, such as healthcare, smart cities, and industrial systems, the need for comprehensive privacy frameworks becomes increasingly urgent.

To address these challenges, we have proposed the PRD methodological approach, a structured framework designed to help developers integrate privacy considerations throughout the IoTS development lifecycle. Integrated within the broader TpM-Pro methodology, PRD supports privacy-aware design from the initial planning stages through to final implementation. It emphasizes data minimization, secure data handling, and regulatory compliance, ensuring that privacy is treated as a foundational element rather than an afterthought. The PRD framework advances privacy integration by providing updated privacy guidelines tailored to the unique challenges of IoTS environments. It offers developers a novel, structured, and practical step-by-step approach that not only incorporates continuous privacy risk assessment and adaptive management but also ensures the systematic integration of privacy from the early planning stages to deployment, which is a level of operationalization not explicitly addressed in prior works, such as TpM-Pro or Perera's framework. Additionally, PRD embraces emerging technologies such as federated learning and zero-trust security models, thereby enhancing its suitability for modern, resource-constrained IoTS systems. In contrast, the original TpM-Pro approach does not explicitly support or operationalize these advanced privacy mechanisms, which limits its effectiveness in addressing the evolving privacy requirements of contemporary IoTS deployments.

A key contribution of this study is the refinement of existing IoT privacy guidelines. Based on insights from a survey conducted among IoT professionals, researchers, and developers, the guidelines were simplified and clarified to enhance their practical applicability. The survey revealed areas for improvement, such as the need for precise definitions, actionable examples, and a stronger focus on balancing privacy and system performance. In response, we proposed a curated set of guidelines addressing data collection, security, user control, and regulatory compliance, while incorporating feedback from both academics and industry stakeholders.

In conclusion, this study lays a solid foundation for privacy-centric IoTS development, offering practical solutions that bridge the gap between academic research and industry needs. However, continued work in this area will be vital to ensuring that privacy remains a core principle as IoT ecosystems evolve. While the proposed framework offers a struc-

tured approach to integrating privacy into IoTS development, comprehensive practical verification through real-world implementation and testing remains a crucial direction for future research.

Consequently, future research should focus on validating the PRD methodology in real-world IoTS projects to evaluate its effectiveness and applicability across diverse domains. This includes experimental validation involving prototype implementation and real-world case studies. This will provide practical insights into the framework's applicability and effectiveness in diverse IoTS environments. Moreover, further investigation into automated privacy enforcement tools, adaptive data aggregation strategies, and the integration of privacy safeguards in emerging technologies like AI and Edge Computing is also essential. Emerging technologies such as AI-driven privacy enforcement and blockchain-based security models offer promising directions for enhancing privacy in IoT systems. Enhancing user control and transparency, through the development of user-friendly privacy dashboards, could strengthen trust and user engagement. Collectively, these initiatives will contribute to building more resilient, secure, and privacy-conscious IoT ecosystems.

Author Contributions: The authors confirm their contribution to the paper as follows: Conceptualization and methodology: Y.Y.S., M.J.H. and C.R.-D.; investigation, data curation, formal analysis, visualization, and writing—original draft preparation: Y.Y.S.; writing—review, and editing, supervision, project administration, and funding acquisition: M.J.H. and C.R.-D. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by grants PID2023-149185OB-I00, PID2022-139297OB-I00, and TED2021-132262A-I00, all funded by MICIU/AEI/10.13039/501100011033, i.e., the Spanish Ministry of Science, Innovation and Universities (State Research Agency), and co-financed by ERDF/EU (for the first two grants) and by NextGenerationEU (for the latter).

Data Availability Statement: Dataset available on request from the authors.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Samizadeh Nikoui, T.; Rahmani, A.M.; Balador, A.; Haj Seyyed Javadi, H. Internet of Things architecture challenges: A systematic review. *Int. J. Commun. Syst.* **2021**, *34*, 1–42. [CrossRef]
2. Lin, H.; Bergmann, N.W. IoT Privacy and Security Challenges for Smart Home Environments. *Information* **2016**, *7*, 44. [CrossRef]
3. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
4. Himeur, Y.; Sohail, S.S.; Bensaali, F.; Amira, A.; Alazab, M. Latest trends of security and privacy in recommender systems: A comprehensive review and future perspectives. *Comput. Secur.* **2022**, *118*, 102746. [CrossRef]
5. Ismail, S.; Dawoud, D.W. Software Development Models for IoT. In Proceedings of the 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 26–29 January 2022; IEEE: New York, NY, USA, 2022; pp. 0524–0530. [CrossRef]
6. Reinsel, D. IDC Blog. 2019 [cited 2023 Mar 4]. How You Contribute to Today's Growing DataSphere and Its Enterprise Impact. Available online: https://blogs.idc.com/2019/11/04/how-you-contribute-to-todays-growing-datasphere-and-its-enterprise-impact/ (accessed on 4 March 2023).
7. Greenberg, P. 2021 Consumer Data Privacy Legislation. National Conference of State Legislatures [Internet]. Available online: https://www.ncsl.org/technology-and-communication/2021-consumer-data-privacy-legislation (accessed on 10 November 2024).
8. Hornos, M.J.; Quinde, M. Development methodologies for IoT-based systems: Challenges and research directions. *J. Reliab. Intell. Environ.* **2024**, *10*, 215–244. [CrossRef]
9. Guerrero-Ulloa, G.; Rodríguez-Domínguez, C.; Hornos, M.J. Agile Methodologies Applied to the Development of Internet of Things (IoT)-Based Systems: A Review. *Sensors* **2023**, *23*, 790. [CrossRef] [PubMed]
10. Nakagawa, H.; Ogata, S.; Aoki, Y.; Kobayashi, K. A model transformation approach to constructing agent-oriented design models for CPS/IoT systems. In Proceedings of the 35th Annual ACM Symposium on Applied Computing, Brno, Czech Republic, 30 March–3 April 2020; Association for Computing Machinery: New York, NY, USA, 2020; pp. 815–822. [CrossRef]

11. Shaheen, Y.; Hornos, M.J.; Rodríguez-Domínguez, C. IoT Security and Privacy Challenges from the Developer Perspective. In *Ambient Intelligence—Software and Applications—14th International Symposium on Ambient Intelligence*; Springer Nature: Cham, Switzerland, 2023; pp. 13–21. [CrossRef]
12. Jacobson, I.; Spence, I.A.N.; Ng, P.-W. Is There a Single Method for the Internet of Things? *Commun. ACM* **2017**, *60*, 46–53. [CrossRef]
13. Patel, P.; Cassou, D. Enabling high-level application development for the Internet of Things. *J. Syst. Softw.* **2015**, *103*, 62–84. [CrossRef]
14. Guerrero-Ulloa, G.; Hornos, M.J.; Rodríguez-Domínguez, C. TDDM4IoTS: A Test-Driven Development Methodology for Internet of Things (IoT)-Based Systems. In *Applied Technologies*; Springer International Publishing: Cham, Switzerland, 2020; pp. 41–55. [CrossRef]
15. Ferreira, L.C.B.C.; Yamaguti, R.; Branquinho, O.C.; Cardieri, P. A TpM-based collaborative system to teach IoT. *Comput. Appl. Eng. Educ.* **2022**, *30*, 292–303. [CrossRef]
16. Bucher, T.; Klesse, M.; Kurpjuweit, S.; Winter, R. *Situational Method Engineering BT—Situational Method Engineering: Fundamentals and Experiences*; Ralyté, J., Brinkkemper, S., Henderson-Sellers, B., Eds.; Springer: Boston, MA, USA, 2007; pp. 33–48. [CrossRef]
17. Ferreira, L.C.B.C.; Chaves, P.R.; Assumpção, R.M.; Branquinho, O.C.; Fruett, F.; Cardieri, P. The Three-Phase Methodology for IoT Project Development. *Internet Things* **2022**, *20*, 100624. [CrossRef]
18. Valacich, J.S.; George, J.F.; Hoffer, J.A. *Modern Systems Analysis and Design*; Pearson Eudcation: London, UK, 2017.
19. Alhirabi, N.; Rana, O.; Perera, C. Security and Privacy Requirements for the Internet of Things: A Survey. *ACM Trans. Internet Things* **2021**, *2*, 1–37. [CrossRef]
20. Shaheen, Y.Y.; Hornos, M.J.; Rodríguez-Domínguez, C. Addressing Privacy Challenges in Internet of Things (IoT) Applications. In *Ambient Intelligence—Software and Applications—15th International Symposium on Ambient Intelligence*; Novais, P., Parameshachari, B.D., Satoh, I., Inglada, V.J., González, S.R., Jove Pérez, E., Domínguez, J.P., Chamoso, P., Alonso, R.S., Eds.; Springer Nature: Cham, Switzerland, 2025; pp. 45–54. [CrossRef]
21. Dias, J.P.; Ferreira, H.S. State of the Software Development Life-Cycle for the Internet-of-Things. *arXiv* **2018**, arXiv:1811.04159.
22. Perera, C.; Barhamgi, M.; Bandara, A.K.; Ajmal, M.; Price, B.; Nuseibeh, B. Designing privacy-aware internet of things applications. *Inf. Sci.* **2020**, *512*, 238–257. [CrossRef]
23. Cavoukian, A. Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity Inf. Soc.* **2010**, *3*, 247–251. [CrossRef]
24. European Parliament and of the Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, *OJ L 119/1*, 1–88. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (accessed on 10 July 2025).
25. Adam, M.; Hammoudeh, M.; Alrawashdeh, R.; Alsulaimy, B. A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems. *IEEE Access* **2024**, *12*, 57128–57149. [CrossRef]
26. Pourrahmani, H.; Yavarinasab, A.; Monazzah, A.M.H.; van Herle, J. A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. *Internet Things* **2023**, *23*, 100888. [CrossRef]
27. Hossain, M.; Kayas, G.; Hasan, R.; Skjellum, A.; Noor, S.; Islam, S.M.R. A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives. *Future Internet* **2024**, *16*, 40. [CrossRef]
28. Swessi, D.; Idoudi, H. A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures. *Wirel. Pers. Commun.* **2022**, *124*, 1557–1592. [CrossRef]
29. Kaushal, N.; Singh, G.; Singh, J. An Addressing Techniques for Maintaining Security and Privacy Framework for Internet of Things. In Proceedings of the 2023 3rd International Conference on Intelligent Technologies (CONIT), Hubli, India, 23–25 June 2023; pp. 1–7. [CrossRef]
30. Nazir, A.; He, J.; Zhu, N.; Wajahat, A.; Ma, X.; Ullah, F.; Qureshi, S.; Pathan, M.S. Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101820. [CrossRef]
31. Qureshi, S.U.; He, J.; Tunio, S.; Zhu, N.; Nazir, A.; Wajahat, A.; Ullah, F.; Wadud, A. Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. *J. King Saud Univ.-Comput. Inf. Sci.* **2024**, *36*, 102164. [CrossRef]
32. Li, J.; Lyu, L.; Liu, X.; Zhang, X.; Lyu, X. FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4059–4068. [CrossRef]
33. Alahmari, S.; Alkharashi, A. Privacy-Aware Federated Learning Framework for IoT Security Using Chameleon Swarm Optimization and Self-Attentive Variational Autoencoder. *Comput. Model. Eng. Sci.* **2025**, *143*, 849–873. [CrossRef]
34. Zhao, B.; Ji, Y.; Shi, Y.; Jiang, X. Design and implementation of privacy-preserving federated learning algorithm for consumer IoT. *Alex. Eng. J.* **2024**, *106*, 206–216. [CrossRef]
35. Dhar, S.; Bose, I. Securing IoT Devices Using Zero Trust and Blockchain. *J. Organ. Comput. Electron. Commer.* **2021**, *31*, 18–34. [CrossRef]

36. Liu, C.; Tan, R.; Wu, Y.; Feng, Y.; Jin, Z.; Zhang, F.; Liu, Y.; Liu, Q.X. Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity* **2024**, *7*, 20. [CrossRef]
37. Paul, P.C.; Loane, J.; McCaffery, F.; Regan, G. Towards Design and Development of a Data Security and Privacy Risk Management Framework for WBAN Based Healthcare Applications. *Appl. Syst. Innov.* **2021**, *4*, 76. [CrossRef]
38. Abdul-Ghani, H.A.; Konstantas, D. A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *J. Sens. Actuator Netw.* **2019**, *8*, 22. [CrossRef]
39. Hoepman, J.H. Privacy design strategies. In *ICT Systems Security and Privacy Protection*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 446–459. [CrossRef]
40. Perera, C.; McCormick, C.; Bandara, A.K.; Price, B.A.; Nuseibeh, B. Privacy-by-design framework for assessing internet of things applications and platforms. In Proceedings of the 6th International Conference on the Internet of Things, Stuttgart, Germany, 7–9 November 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 83–92. [CrossRef]
41. Consortium, L. LINDDUN GO Threat Modeling Tool [Internet]. 2024. Available online: https://downloads.linddun.org/linddun-go/cardbrowser/v241203/index.html (accessed on 20 June 2025).
42. Deb, S.; Bhuyan, B. Performance analysis of current lightweight stream ciphers for constrained environments. *Sādhanā* **2020**, *45*, 256. [CrossRef]
43. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654. [CrossRef] [PubMed]
44. Thabit, F.; Can, O.; Aljahdali, A.O.; Al-Gaphari, G.H.; Alkhzaimi, H.A. Cryptography Algorithms for Enhancing IoT Security. *Internet Things* **2023**, *22*, 100759. [CrossRef]
45. El-hajj, M.; Mousawi, H.; Fadlallah, A. Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. *Future Internet* **2023**, *15*, 54. [CrossRef]
46. Halgamuge, M.N.; Niyato, D. Adaptive edge security framework for dynamic IoT security policies in diverse environments. *Comput. Secur.* **2025**, *148*, 104128. [CrossRef]
47. Kounoudes, A.D.; Kapitsaki, G.M. A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet Things* **2020**, *11*, 100179. [CrossRef]
48. Sun, P.; Wan, Y.; Wu, Z.; Fang, Z.; Li, Q. A survey on privacy and security issues in IoT-based environments: Technologies, protection measures and future directions. *Comput. Secur.* **2025**, *148*, 104097. [CrossRef]
49. Schilit, B.N.; Theimer, M.M. Disseminating active map information to mobile hosts. *IEEE Netw.* **1994**, *8*, 22–32. [CrossRef]
50. Alotaibi, A.I.; Oracevic, A. Context-Aware Security in the Internet of Things: What We Know and Where We are Going. In Proceedings of the 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 23–26 October 2023; pp. 1–8. [CrossRef]
51. Bou Chaaya, K.; Barhamgi, M.; Chbeir, R.; Arnould, P.; Benslimane, D. Context-aware System for Dynamic Privacy Risk Inference: Application to smart IoT environments. *Future Gener. Comput. Syst.* **2019**, *101*, 1096–1111. [CrossRef]
52. Wang, T.; Yang, Q.; Shen, X.; Gadekallu, T.R.; Wang, W.; Dev, K. A Privacy-Enhanced Retrieval Technology for the Cloud-Assisted Internet of Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4981–4989. [CrossRef]
53. Saha, R.; Kumar, G.; Conti, M.; Devgun, T.; Kim, T.H.; Alazab, M. DHACS: Smart Contract-Based Decentralized Hybrid Access Control for Industrial Internet-of-Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 3452–3461. [CrossRef]