Journal for Educators, Teachers and Trainers
The PROFESIOLab electronic, peer-reviewed, open-access Magazine

ISSN 1989-9572

DOI:10.47750/jett.2024.15.05.25

Blockchain System with Credit-Based Consensus Mechanism for Industrial Internet of Things: An Application of Industry 4.0

B. Vasantha, K. Bhavana, K. Kavya, M. Varshini

Journal for Educators, Teachers and Trainers, Vol.15(5)

https://jett.labosfor.com/

Date of Reception: 24 Oct 2024

Date of Revision: 20 Nov 2024

Date of Publication : 31 Dec 2024

B. Vasantha, K. Bhavana, K. Kavya, M. Varshini(2024). Blockchain System with Credit-Based Consensus Mechanism for Industrial Internet of Things: An Application of Industry 4.0,Vol.15(5).250-264.

Journal for Educators, Teachers and Trainers
The LabOSfor electronic, peer-reviewed, open-access Magazine

Journal for Educators, Teachers and Trainers, Vol. 15(5)

ISSN1989 –9572

https://jett.labosfor.com/

Blockchain System with Credit-Based Consensus Mechanism for Industrial Internet of Things: An Application of Industry 4.0

B. Vasantha[1], K. Bhavana[2], K. Kavya[2], M. Varshini[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Information Technology

[1,2]Malla Reddy Engineering College for Women (UGC-Autonomous), Maisammaguda, Hyderabad, 500100, Telangana.

ABSTRACT

The convergence of Blockchain technology with the Industrial Internet of Things (IIoT) has emerged as a strategic response to the challenges inherent in traditional industrial systems. In the backdrop of Industry 4.0, where the optimization of industrial processes relies heavily on data-driven decision-making, there is a pressing need for a robust and secure infrastructure. The primary issues stem from the vulnerabilities of centralized systems, including data security risks, lack of transparency, and susceptibility to unauthorized access. To address these challenges, a proposed solution involves the implementation of a Blockchain system tailored specifically for industrial applications. By leveraging the decentralized and tamper-resistant nature of Blockchain, this system ensures the security and immutability of data within the IIoT ecosystem. Furthermore, the introduction of a Credit-Based Consensus Mechanism adds an innovative layer to the solution, where participants gain influence or voting power based on their reputation or "credit" within the network. The significance of this approach lies in its capacity to enhance security, reliability, and trust in IIoT operations. The decentralized architecture mitigates the risks associated with single points of failure, fostering a more reliable IIoT system. Moreover, the credit-based consensus mechanism promotes trust among participants, facilitating collaboration and information sharing in the dynamic landscape of Industry 4.0. In essence, the integration of Blockchain and the credit-based consensus mechanism presents a comprehensive solution to fortify the Industrial Internet of Things, addressing the shortcomings of traditional centralized systems and ensuring a secure and transparent foundation for Industry 4.0 advancements.

Keywords: Industrial Internet of Things, Blockchain, Decentralized System, Consensus Mechanism

1. INTRODUCTION

The convergence of Blockchain technology with the Industrial Internet of Things (IIoT) represents a pivotal moment in the evolution of industrial systems. [1] The concept of Industry 4.0, characterized by the integration of digital technologies into manufacturing and production processes, has been gaining momentum since its inception. Traditional industrial systems, marked by centralized control and legacy infrastructure, have faced numerous challenges, including data security vulnerabilities, lack of transparency, and inefficiencies in decision-making. As industries increasingly rely on data-driven insights to optimize operations, the need for a robust and secure infrastructure has become paramount.

[2] The emergence of Blockchain technology, initially popularized by cryptocurrencies, has sparked interest across various sectors due to its decentralized and tamper-resistant nature. The inherent features of Blockchain, such as immutability, transparency, and cryptographic security, make it an ideal candidate for addressing the shortcomings of traditional industrial systems. [3] The genesis of applying Blockchain to the IIoT context can be traced back to the recognition of these potential benefits and the desire to create a more secure and efficient industrial ecosystem.

Over time, as the concept of Industry 4.0 gained traction, researchers and practitioners began exploring the integration of Blockchain technology into industrial applications. [4] This led to a deeper understanding of the unique challenges and opportunities within the IIoT landscape and laid the groundwork for innovative solutions that combine Blockchain with other emerging technologies, such as the Credit-Based Consensus Mechanism.

2. LITERATURE SURVEY

Wen et al. [6] present an information distributing system that uses blockchain within Supply Chain networks using IIoT. The system combines IIoT nodes to the blockchain, and the system monitors IIoT nodes and stores concurrent information inside the network using smart contracts. Additionally, a supply chain design based on blockchain is proposed. The proposed design suggests cooperation resolutions connecting several items inside the supply chain. Within this design for the supply chain, a well-grained distributing information system is proposed. Li and Kang [7] have exploited the consortium blockchain technique to suggest an energy blockchain safe power business scheme. This type of blockchain is widely used in universal P2P power buy and sell businesses, removing a mediator. Moreover, to reduce the contract restriction effects from contract verification slowdowns on the energy blockchain, the researchers have proposed a credit-based fee scheme to encourage short and recurrent power buy and sell by businesses. Teslya et al. [8] have given a summary of blockchain platforms being used in Industrial IoT. The researchers provide an analysis of the most widely used consensus mechanisms and specific features of the public (permissionless) and private (permissioned) blockchains. Furthermore, an outline of blockchain platforms that satisfy the necessities for the IIoT platform development is provided. The authors [9] have proposed a storage space arrangement, namely ChainSplitter, based on a hierarchical blockchain where the bulk of the blockchain is warehoused inside the clouds. The foremost new blocks are stored inside the overlying network, the separate IIoT networks. The ChainSplitter flawlessly attaches native IIoT networks, the overlay network of blockchain, and therefore the cloud communications are enabled using two connectors, the blockchain and the cloud connector. Liu et al. [10] have proposed a blockchain-enabled IIoT based deep reinforcement learning (DRL) framework. The objectives of the proposal are three-fold: 1) presenting a policy for assessing the scheme using the features of decentralization, scalability, security and latency; 2) enhancing the measurability of the fundamental blockchain without disturbing the scheme's latency, decentralization, and safety; 3) outlining a blockchain which is modulable, where the producers, size and interval of the block, consensus algorithm, are chosen by the technique of Deep Reinforcement Learning (DRL). Currently, there are surveys available on the integration of IIoT with blockchain. Explicitly, Alladi et al. [11] have given a scientific literature review on Blockchain Applications Industrial IoT and Industry 4.0. The work of [12] has reviewed blockchain technology alongside its usage in industrial IoT. Furthermore, Silva et al. [13] have surveyed the convergence of Blockchain and Industry 4.0. Fraga-Lamas et al. [14] have reviewed the use of blockchain technologies with IoT for a complicated and cyber-resilient automotive industry. Lu et al. [15] have proposed a review of applications, changes, challenges, and dangers for Blockchain technique within the gas and oil industry. Xie et al. [16] have proposed a blockchain technique survey that applies to smart cities. Juma et al. [17] have proposed the survey of trade supply chain resolutions. Furthermore, Soni [18] have planned a review on Blockchain Urgency within the IoT in the Healthcare environment.

3. PROPOSED SYSTEM

Now-a-days all industries like banking (ATM's, sensor-based transaction devices), hospitals (transaction Machines) are using IIOT (Industrial Internet of Things which means small devices communicate with centralized servers to exchange data) devices to communicate with their servers. These devices will have internet connection to communicate with industries servers and these devices will have limited battery power so heavy cryptographic algorithms cannot be implemented to provide/improve security. To overcome from this issue author, us using Blockchain based algorithms such as POW (proof of work) and credit consensus. Entire Blockchain technique cannot be implement as these devices are small and run on battery so author is using POW and Credit Consensus concept from Blockchain technique.

Below 3 problems make author to utilize only POW and Credit Consensus concept from entire Blockchain technique.

- Efficiency and Security: All transactions are safe under block chain Credit Consensus and if we use entire Blockchain then efficiency problem will raise in devices (sensors) to run entire Blockchain technique. This makes author to use only Credit Consensus.
- Transparency and Privacy: All transaction done in Credit Consensus are available publicly and there is no privacy for data. So, to provide security to data author is using symmetric encryption technique to hide data from public and can only be decrypted by industrial manager. When sensors or devices setup then industrial manager share public keys with sensors via GATEWAYS. All sensors encrypt data using public key and send to GATEWAY and GATEWAY will store at industrial server where manager can decrypt all data using keys.
- High concurrency and low throughput: As sensors report huge data to servers so concurrent requests will arrive from all sensors and then server can produce low throughput or output. To increase throughput, we are using DAG (directed acyclic graph architecture) concept. In DAG each transaction referred as node instead of maintaining multiple blocks. Running transaction as nodes take less time compare to blocks generation.

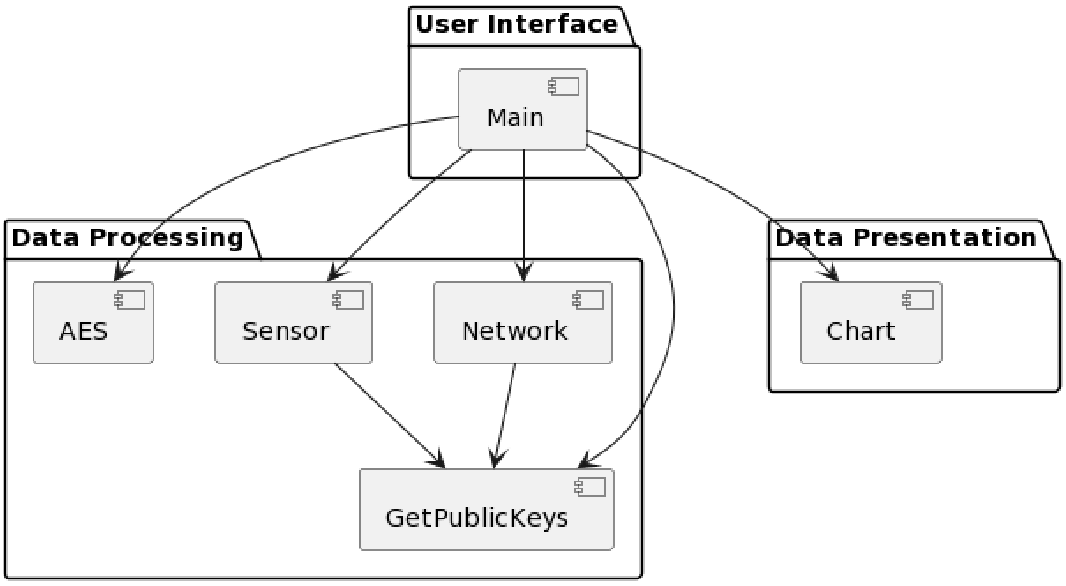


Figure 1: Block Diagram of Proposed System

Blockchain

Blockchain technology serves as the foundational framework for ensuring the security, integrity, and transparency of data transactions within the Secure Industrial IIOT research.

Here's a detailed exploration of the purpose of Blockchain in the context of this research:

- **Decentralization**: The primary purpose of Blockchain in the Secure Industrial IIOT research is to establish a decentralized network architecture. Traditional centralized systems are vulnerable to single points of failure and susceptible to cyber attacks. By distributing the ledger across multiple nodes in the network, Blockchain mitigates the risk of data manipulation and unauthorized access.

- **Immutable Ledger**: Blockchain maintains an immutable ledger of transactions, meaning that once data is recorded on the Blockchain, it cannot be altered or deleted retroactively. This feature ensures data integrity and transparency, critical requirements in industrial IoT applications where accurate and tamper-proof records are essential for compliance and audit purposes.

- **Data Security**: Blockchain employs cryptographic techniques to secure data transactions within the IIOT network. Each transaction is cryptographically linked to the previous one, forming a chain of blocks. This ensures that data transmitted between IoT devices remains confidential and tamper-resistant, safeguarding sensitive information from unauthorized access or tampering.

- **Smart Contracts**: Smart contracts are self-executing contracts with predefined rules and conditions encoded on the Blockchain. In the context of the Secure Industrial IIOT research, smart contracts automate and enforce agreements between network participants, streamlining processes such as data validation, access control, and revenue sharing. Smart contracts enhance efficiency, reduce transaction costs, and minimize the need for intermediaries.

- **Enhanced Transparency**: Blockchain technology provides enhanced transparency by enabling all network participants to view and verify transactions in real-time. This transparency fosters trust among stakeholders, as they can independently verify the accuracy and authenticity of data transactions without relying on centralized authorities. In industrial IoT applications, transparency is crucial for ensuring compliance with regulatory standards and industry best practices.

- **Auditability and Traceability**: The immutable nature of Blockchain facilitates auditability and traceability of data transactions within the IIOT network. Each transaction is time-stamped and linked to the previous one, creating an audit trail that can be traced back to its origin. This audit trail enables efficient root cause analysis, forensic investigations, and compliance audits, enhancing accountability and regulatory compliance.

- **Resilience to Attacks**: Blockchain's decentralized and distributed nature makes it inherently resilient to cyber attacks and data breaches. Unlike centralized databases, which present lucrative targets for hackers, Blockchain networks distribute data across multiple nodes, making it extremely challenging for malicious actors to compromise the entire network. This resilience enhances the overall security posture of the Secure Industrial IIOT research, reducing the likelihood of data breaches and system downtime.

- **Scalability and Interoperability**: Blockchain technology offers scalability and interoperability, enabling the Secure Industrial IIOT research to accommodate a growing number of IoT devices and diverse data formats. Through techniques such as sharding, sidechains, and off-chain protocols, Blockchain networks can handle increased transaction volumes without sacrificing performance or compromising security. Interoperability standards allow different IIOT platforms and protocols to seamlessly communicate and exchange data, fostering collaboration and innovation across the industrial IoT ecosystem.

Advantages

The proposed model for Secure Industrial IIOT, leveraging Blockchain technology with Credit-Based Consensus Mechanism, offers several advantages over traditional approaches. Here are the key advantages of the proposed model:

— **Enhanced Security**: By utilizing Blockchain technology, the proposed model ensures data security through cryptographic techniques and the immutability of transaction records. This enhances the protection of sensitive industrial data from unauthorized access, tampering, or cyber-attacks.

— **Decentralization**: The decentralized nature of Blockchain eliminates single points of failure, making the IIOT network more resilient to disruptions and attacks. It also enhances network scalability and reduces dependence on centralized intermediaries, leading to greater reliability and efficiency.

— **Data Integrity and Transparency**: Blockchain's immutable ledger ensures the integrity and transparency of data transactions. This feature is particularly important in industrial settings, where accurate and tamper-proof records are critical for compliance, auditing, and regulatory purposes.

— **Smart Contracts Automation**: The integration of smart contracts automates and enforces agreements between network participants, streamlining processes such as data validation, access control, and revenue sharing. This automation enhances operational efficiency, reduces manual errors, and minimizes the need for intermediaries.

- **Improved Traceability and Auditability**: The Blockchain ledger provides an immutable and transparent record of all transactions, enabling efficient traceability and auditability. This facilitates root cause analysis, forensic investigations, and compliance audits, enhancing accountability and regulatory compliance.
- **Resilience to Cyber Attacks**: The decentralized and distributed nature of Blockchain makes the IIOT network more resilient to cyber attacks and data breaches. Even if individual nodes are compromised, the integrity of the overall network remains intact, reducing the risk of data loss or system downtime.
- **Scalability and Interoperability**: Blockchain technology offers scalability and interoperability, allowing the IIOT network to accommodate a growing number of devices and diverse data formats. This scalability ensures that the network can handle increased transaction volumes without sacrificing performance or security.
- **Cost Efficiency**: By eliminating the need for centralized intermediaries and automating manual processes through smart contracts, the proposed model reduces transaction costs, operational overheads, and the risk of human error. This leads to overall cost savings and improved return on investment (ROI) for industrial stakeholders.
- **Incentivized Consensus Mechanism**: The Credit-Based Consensus Mechanism incentivizes network participants to contribute computing resources and validate transactions by rewarding them with credits. This promotes network participation, enhances consensus efficiency, and ensures the integrity of the Blockchain network.
- **Future-Proofing**: The proposed model is designed to accommodate future advancements in IIOT technology and adapt to evolving industry requirements. Its modular architecture and flexible design enable seamless integration with emerging technologies, standards, and protocols, ensuring long-term viability and sustainability.

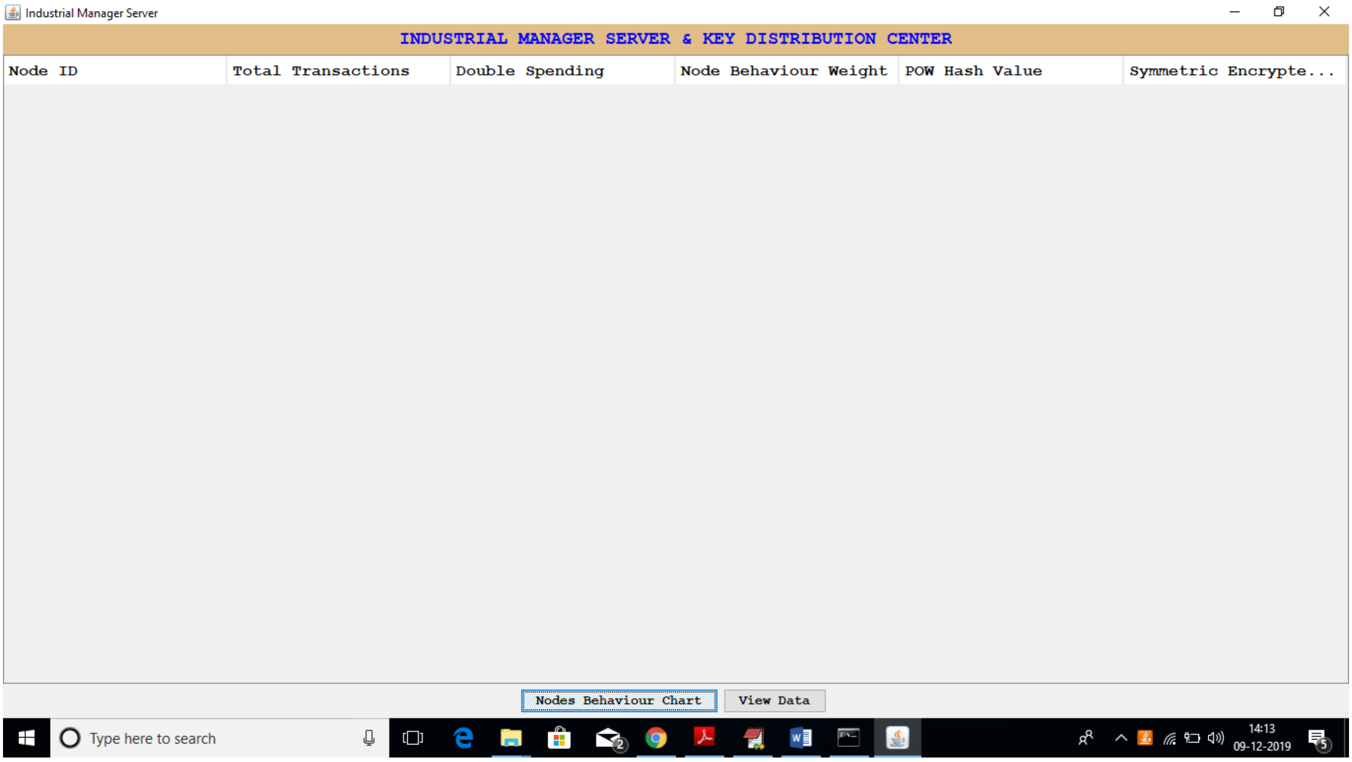
4. RESULTS AND DESCRIPTION

Implementation Description

To implement above concept, we are using SHA256 for hashing and AES for data encryption to provide privacy. Here, we have designed two applications called ‘IndustrialManager and Wireless_Sensors’.

- IndustrialManager: This application responsible to generate keys for sensors and then run Credit Consensus POW algorithm to process/check each transaction send by sensors.
- Wireless_Sensors: This is a simulation-based application which request gateways to receive keys and then send encrypted transaction to gateways for processing.

Results Description



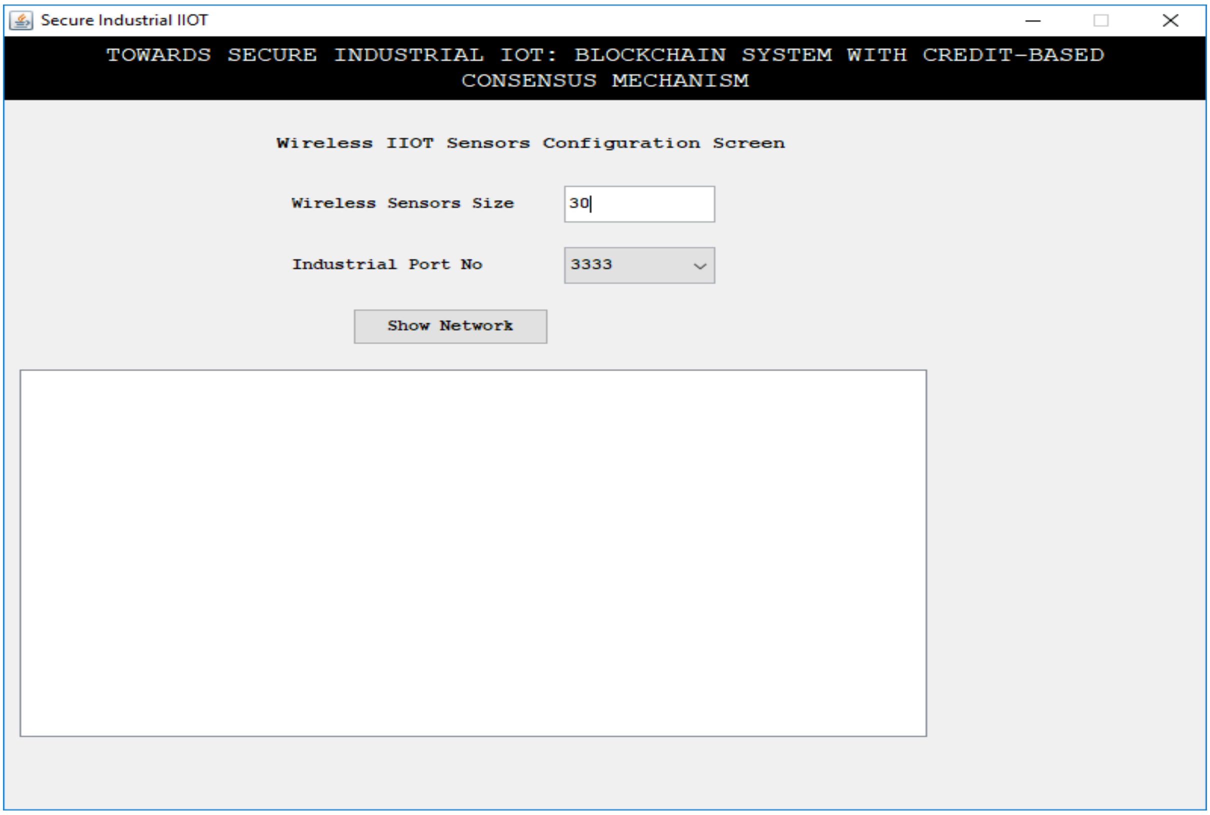
Industrial Manager Server

INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...

Figure 2: Presents the GUI of Industrial Manager server.

Figure 2 showcases the graphical user interface (GUI) of the Industrial Manager server, designed to facilitate interaction and management of industrial processes. It likely includes features and controls for monitoring, configuring, and managing industrial operations, providing a user-friendly platform for administrators or managers.



Secure Industrial IIOT

TOWARDS SECURE INDUSTRIAL IOT: BLOCKCHAIN SYSTEM WITH CREDIT-BASED CONSENSUS MECHANISM

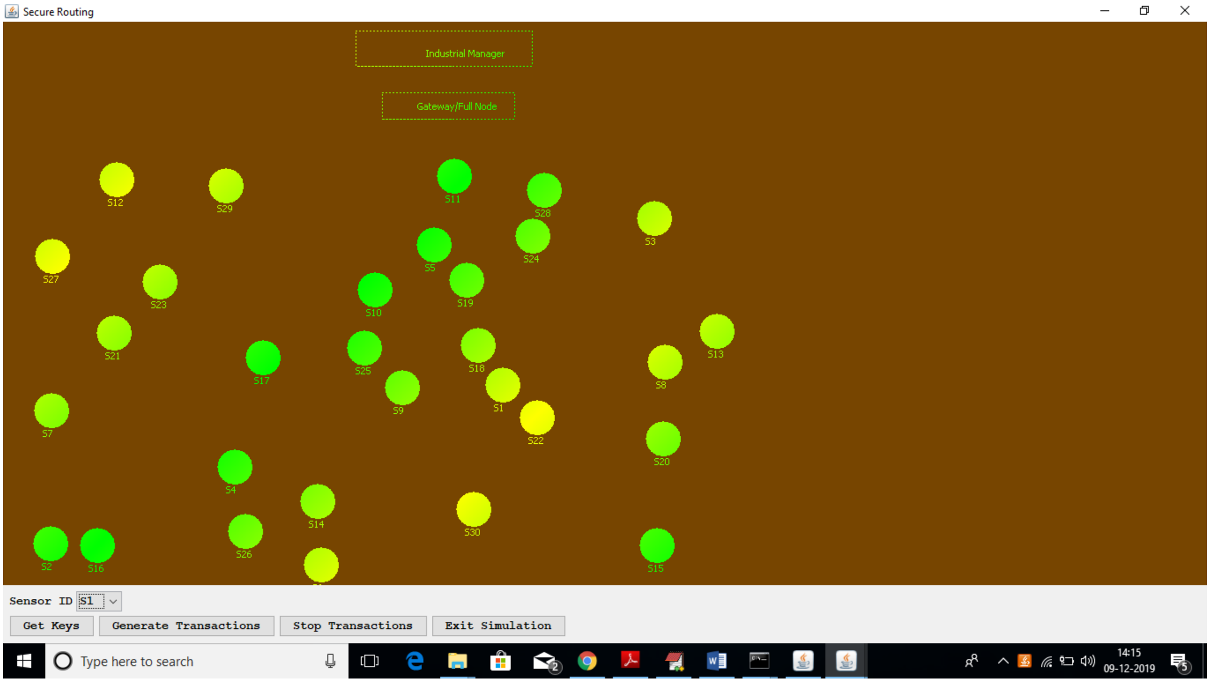
Wireless IIOT Sensors Configuration Screen

Wireless Sensors Size: 30

Industrial Port No: 3333

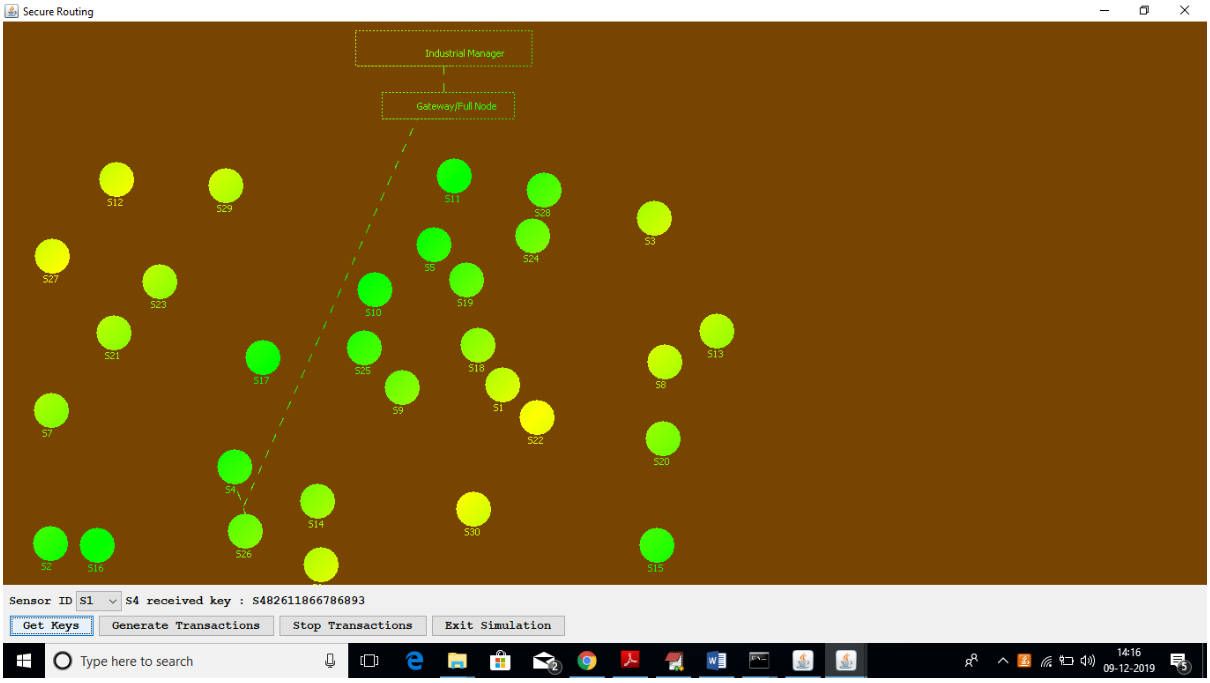
Figure 3: Displays the IOT sensor Configuration.

Figure 3 illustrates the configuration of IoT sensors, showcasing how the sensors are set up and interconnected within the system. It likely includes details about sensor types, communication protocols, data flow, and integration with other components to enable efficient data collection and processing in an IoT environment.



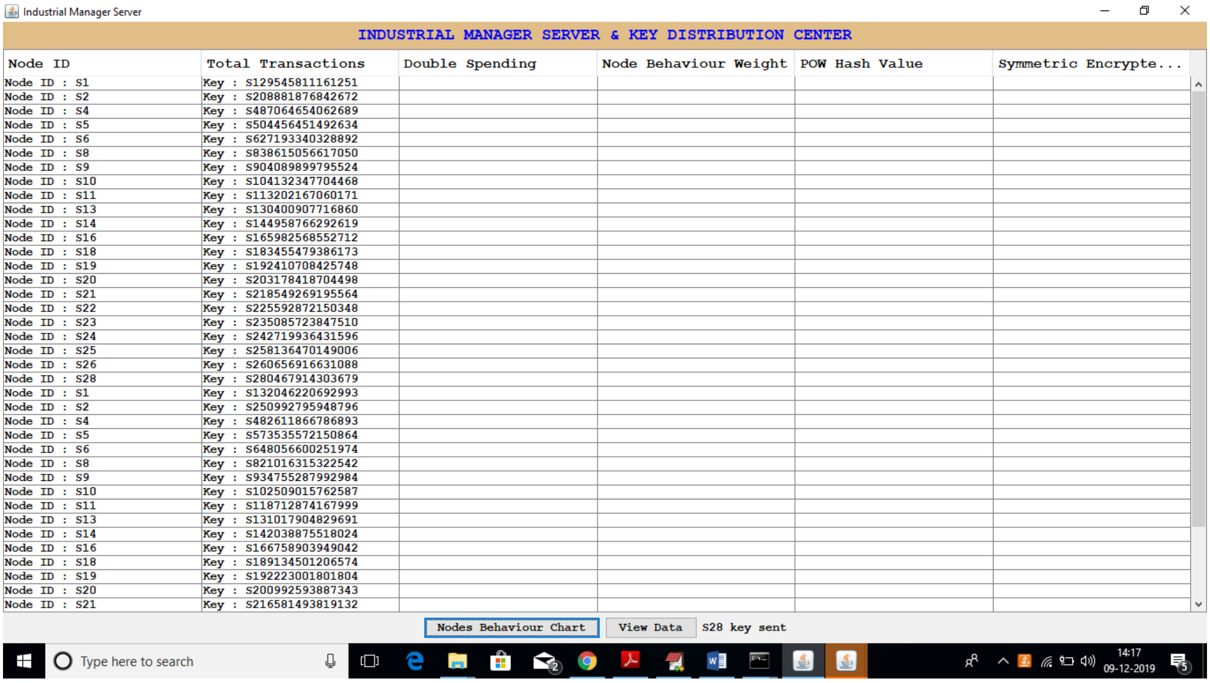
Sensor ID S1

Figure 4: Shows the IOT Devices in the GUI.



Sensor ID S1 S4 received key : S482611866786893

Figure 5: IOT devices network communication with industrial manager.



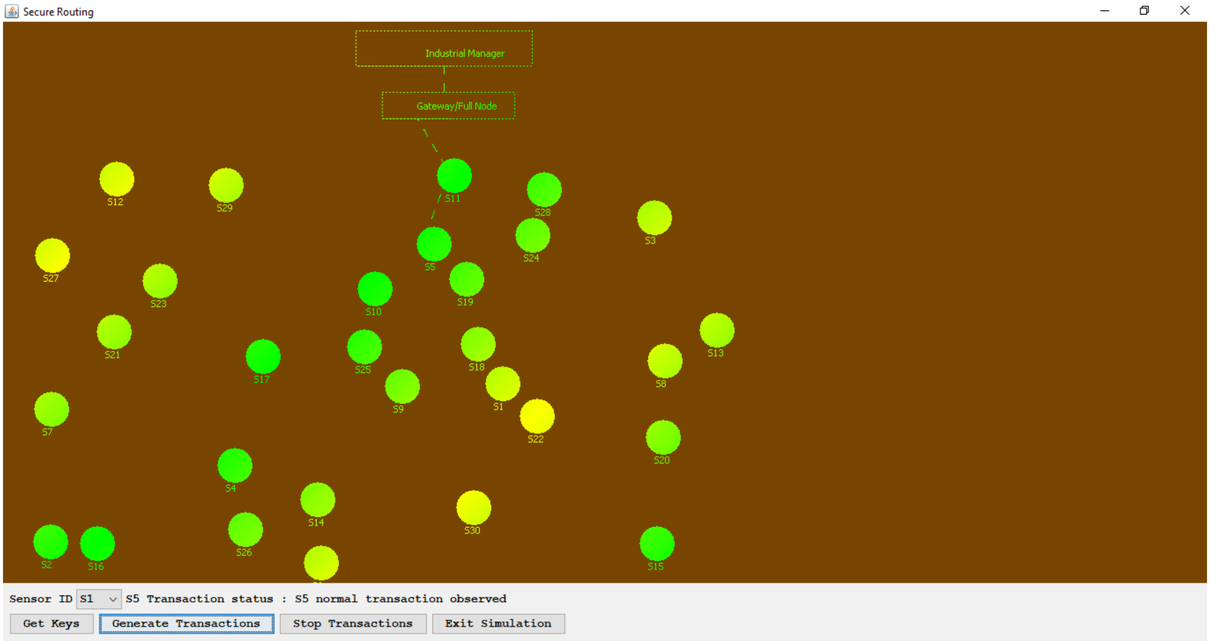
INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...
Node ID : S1	Key : S129545811161251				
Node ID : S2	Key : S208881876842672				
Node ID : S4	Key : S487064654062689				
Node ID : S5	Key : S504456451492634				
Node ID : S6	Key : S627193340328892				
Node ID : S8	Key : S838615056617050				
Node ID : S9	Key : S904089899795524				
Node ID : S10	Key : S104132347704468				
Node ID : S11	Key : S113202167060171				
Node ID : S13	Key : S130400907716860				
Node ID : S14	Key : S144958766292619				
Node ID : S16	Key : S165982568552712				
Node ID : S18	Key : S183455479386173				
Node ID : S19	Key : S192410708425748				
Node ID : S20	Key : S203178418704498				
Node ID : S21	Key : S218549269195564				
Node ID : S22	Key : S225592872150348				
Node ID : S23	Key : S235085723847510				
Node ID : S24	Key : S242719936431596				
Node ID : S25	Key : S258136470149006				
Node ID : S26	Key : S260656916631088				
Node ID : S28	Key : S280467914303679				
Node ID : S1	Key : S132046220692993				
Node ID : S2	Key : S250992795948796				
Node ID : S4	Key : S482611866786893				
Node ID : S5	Key : S573535572150864				
Node ID : S6	Key : S648056600251974				
Node ID : S8	Key : S821016315322542				
Node ID : S9	Key : S934755287992984				
Node ID : S10	Key : S102509015762587				
Node ID : S11	Key : S118712874167999				
Node ID : S13	Key : S131017904829691				
Node ID : S14	Key : S142038875518024				
Node ID : S16	Key : S166758903949042				
Node ID : S18	Key : S189134501206574				
Node ID : S19	Key : S192223001801804				
Node ID : S20	Key : S200992593887343				
Node ID : S21	Key : S216581493819132				

S28 key sent

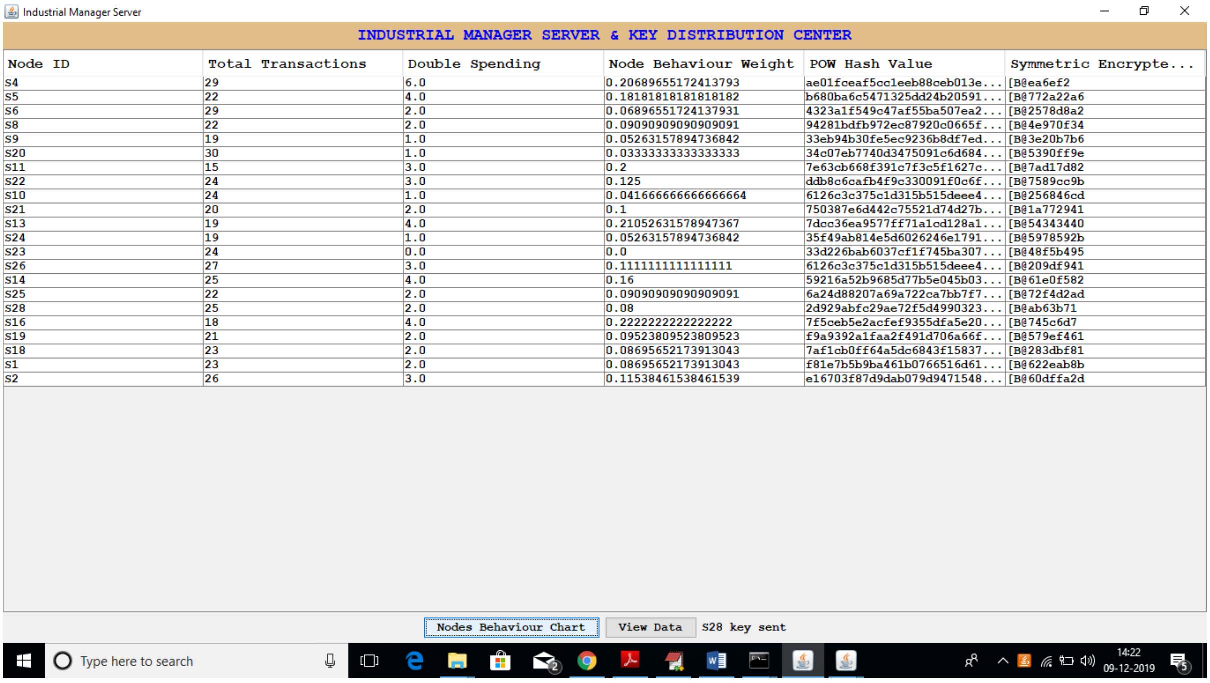
Figure 6: Presents the total node id’s and its transactions.

Now go to simulation screen and click on ‘Generate Transactions’ button to select random nodes and to send random transaction data to gateway. Due to random data sometime nodes will report same transaction then POW detect it as abnormal transaction. This random data and continuous data sending concept just I am using to make some node to report same data and POW can record it. After some time, you can click on ‘Stop Transaction’ to stop it.



Sensor ID S1 S5 Transaction status : S5 normal transaction observed

Figure 7: Transaction sending to gateway for processing.



INDUSTRIAL MANAGER SERVER & KEY DISTRIBUTION CENTER

Node ID	Total Transactions	Double Spending	Node Behaviour Weight	POW Hash Value	Symmetric Encrypte...
S4	29	6.0	0.20689655172413793	ae01fceaf5cc1eeb88ceb013e...	[B@ea6ef2
S5	22	4.0	0.18181818181818182	b680ba6c5471325dd24b20591...	[B@772a22a6
S6	29	2.0	0.06896551724137931	4323a1f549c47af55ba507ea2...	[B@2578d8a2
S8	22	2.0	0.09090909090909091	94281bdfb972ec87920c0665f...	[B@4e970f34
S9	19	1.0	0.05263157894736842	33eb94b30fe5ec9236b8df7ed...	[B@3e20b7b6
S20	30	1.0	0.03333333333333333	34c07eb7740d3475091c6d684...	[B@5390ff9e
S11	15	3.0	0.2	7e63cb668f391c7f3c5f1627c...	[B@7ad17d82
S22	24	3.0	0.125	ddb8c6cafb4f9c330091f0c6f...	[B@7589cc9b
S10	24	1.0	0.041666666666666664	6126c3c375c1d315b515deee4...	[B@256846cd
S21	20	2.0	0.1	750387e6d442c75521d74d27b...	[B@1a772941
S13	19	4.0	0.21052631578947367	7dcc36ea9577ff71a1cd128a1...	[B@54343440
S24	19	1.0	0.05263157894736842	35f49ab814e5d6026246e1791...	[B@5978592b
S23	24	0.0	0.0	33d226bab6037cf1f745ba307...	[B@48f5b495
S26	27	3.0	0.1111111111111111	6126c3c375c1d315b515deee4...	[B@209df941
S14	25	4.0	0.16	59216a52b9685d77b5e045b03...	[B@61e0f582
S25	22	2.0	0.09090909090909091	6a24d88207a69a722ca7bb7f7...	[B@72f4d2ad
S28	25	2.0	0.08	2d929abfc29ae72f5d4990323...	[B@ab63b71
S16	18	4.0	0.2222222222222222	7f5ceb5e2acfef9355dfa5e20...	[B@745c6d7
S19	21	2.0	0.09523809523809523	f9a9392a1faa2f491d706a66f...	[B@579ef461
S18	23	2.0	0.08695652173913043	7af1cb0ff64a5dc6843f15837...	[B@283dbf81
S1	23	2.0	0.08695652173913043	f81e7b5b9ba461b0766516d61...	[B@622eab8b
S2	26	3.0	0.11538461538461539	e16703f87d9dab079d9471548...	[B@60dffa2d

Nodes Behaviour Chart | View Data | S28 key sent

Figure 8: Displays the Nodes Behavioural Chart.

In above screen each node data report is recording and their hash values checking to collect their behaviour, if they send old transaction data hash value then it will be considering as 'abnormal behaviour'. In above screen I am showing all nodes sending abnormal attack data and in real time this will not happen. Just to show the concept of old hash values I sent random continuous request and all nodes send repeated data and becomes in abnormal behaviour. From above screen we can see first nodes sent total 29 transaction and out of that 6-transaction report old hash values then it will detect as abnormal behaviour. If it reports 1 or 2 times then it can be managed and consider as normal behaviour. Now in above screen click on 'Node Behaviour Chart' button to see which nodes report same old hash value more no of times.

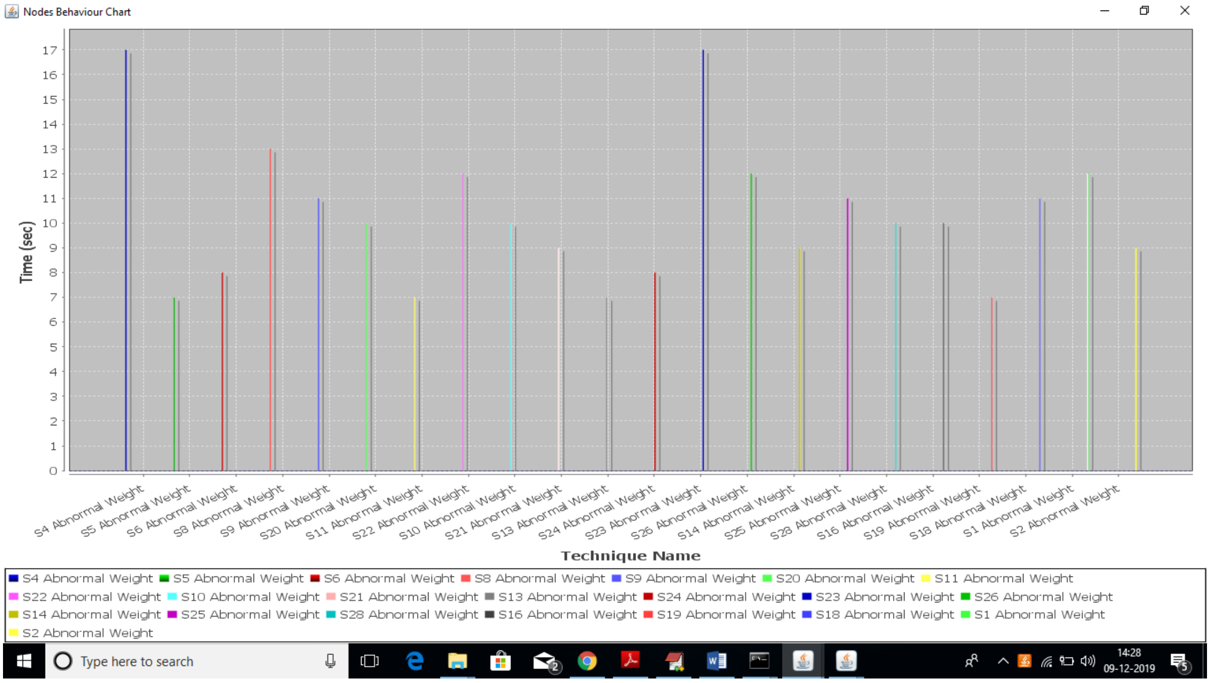
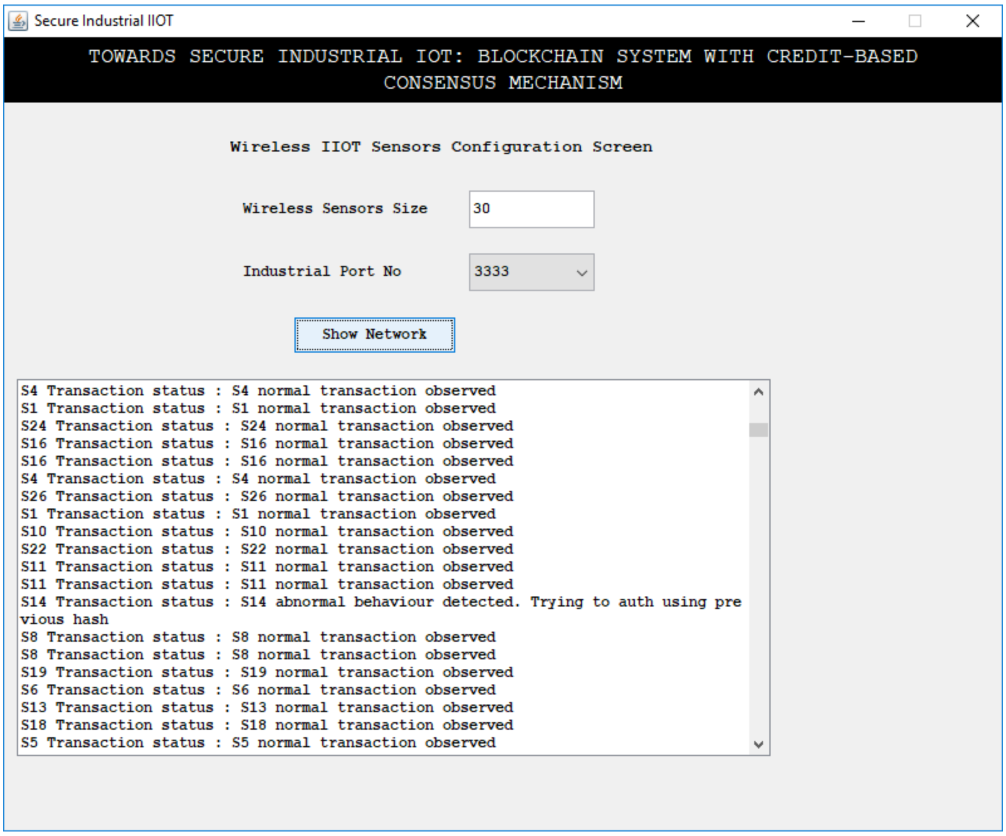


Figure 9: Represents the node id and its Spending Weight.

In above screen only 2 nodes report old hash values a greater number of time and he consider as abnormal nodes. S4 and S23 are the two nodes whose Double Spending Weight is 17 and other are not up to that. In above graph x-axis represents node id and y-axis represents Double Spending Weight.



TOWARDS SECURE INDUSTRIAL IOT: BLOCKCHAIN SYSTEM WITH CREDIT-BASED CONSENSUS MECHANISM

Wireless IIOT Sensors Configuration Screen

Wireless Sensors Size: 30

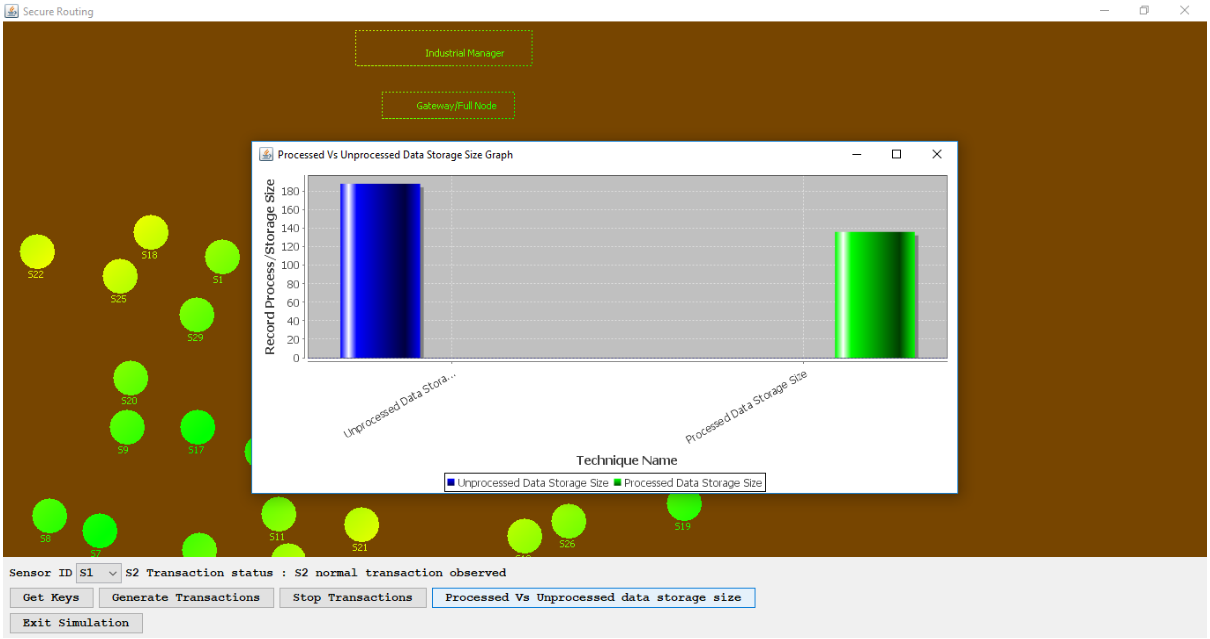
Industrial Port No: 3333

```
S4 Transaction status : S4 normal transaction observed
S1 Transaction status : S1 normal transaction observed
S24 Transaction status : S24 normal transaction observed
S16 Transaction status : S16 normal transaction observed
S16 Transaction status : S16 normal transaction observed
S4 Transaction status : S4 normal transaction observed
S26 Transaction status : S26 normal transaction observed
S1 Transaction status : S1 normal transaction observed
S10 Transaction status : S10 normal transaction observed
S22 Transaction status : S22 normal transaction observed
S11 Transaction status : S11 normal transaction observed
S11 Transaction status : S11 normal transaction observed
S14 Transaction status : S14 abnormal behaviour detected. Trying to auth using pre
vious hash
S8 Transaction status : S8 normal transaction observed
S8 Transaction status : S8 normal transaction observed
S19 Transaction status : S19 normal transaction observed
S6 Transaction status : S6 normal transaction observed
S13 Transaction status : S13 normal transaction observed
S18 Transaction status : S18 normal transaction observed
S5 Transaction status : S5 normal transaction observed
```

Figure 10: Displays the normal or abnormal behaviour.

As an addition to this research, we are adding techniques for processing and cleaning sensor data so that we don't have to pay extra for storage and processing when we get bad or corrupted data. Because of attacks or problems, sensors may sometimes produce corrupted data, and it can cost a lot to process and store this data. In almost every field, sensors are used to collect data. For example, in health care, sensors will be implanted in patients and send data collected to a hospital server to be processed. This processing includes running a complicated algorithm to encrypt the data and then storing it. The storage space and processing power will be wasted if we work with damaged data. So, before we process that kind of data, we will find it and get rid of it.

So, in health care, for example, the sensor has to be able to read body temperature between 10 and 105. If it reads something else, we will drop it. We can save money on storage and processing by using this method.


Secure Routing
Industrial Manager
Gateway/Full Node
S22
S18
S1
S25
S29
S20
S9
S17
S8
S7
S11
S21
S26
S19
Processed Vs Unprocessed Data Storage Size Graph
Record Process /Storage Size
180
160
140
120
100
80
60
40
20
0
Unprocessed Data Stora...
Processed Data Storage Size
Technique Name
■ Unprocessed Data Storage Size ■ Processed Data Storage Size
Get Keys
Generate Transactions
Stop Transactions
Processed Vs Unprocessed data storage size
Exit Simulation

```
Sensor ID S1 S2 Transaction status : S2 normal transaction observed
```

Figure 11: Shows the Processed vs Unprocessed Data.

In the Figure 11: I'm getting rid of data that isn't related while sensing it, which lowers the cost of storage. The x-axis in the above graph shows the cost of storing all data and process data that is not related, and the y-axis shows the size. Based on the graph above, we can say that process data can lower both costs.

5. CONCLUSION

In conclusion, the integration of Blockchain technology with a Credit-Based Consensus Mechanism presents a comprehensive solution to fortify the Industrial Internet of Things (IIoT) and address the shortcomings of traditional centralized systems in the era of Industry 4.0. By leveraging the decentralized and tamper-resistant nature of Blockchain, the proposed system ensures the security, transparency, and reliability of IIoT operations, thereby enabling industries to optimize processes and unlock new opportunities for innovation and growth.

Looking ahead, there are several avenues for future research and development in this field. Firstly, further refinement and optimization of the proposed Blockchain system and consensus mechanism are needed to ensure scalability, interoperability, and usability in real-world industrial applications. Additionally, exploring the potential integration of other emerging technologies, such as artificial intelligence and edge computing, could further enhance the capabilities and performance of IIoT systems. Moreover, continued collaboration between researchers, industry stakeholders, and policymakers is essential to address regulatory and governance challenges associated with the adoption of Blockchain technology in industrial settings. By fostering an ecosystem of innovation and collaboration, we can accelerate the adoption and deployment of Blockchain-enabled IIoT solutions and drive positive impact across various industrial sectors.

REFERENCES

[1] Y. Yang, L. Wu, G. Yin, L. Li, H. Zhao, "A survey on security and privacy issues in internet-of-things", IEEE Internet Things J., 4 (5) (2017), pp. 1250-1258.

[2] Guizi Chen, Wee Siong Ng, “An Efficient Authorization Framework for Securing Industrial Internet of Things”, Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017.

[3] M. Tiago Fernández-Caramés, Paula Fraga-Lamas, “A Review on the Use of Blockchain for the Internet of Things”, IEEE Access VOLUME X (2018), 10.1109/ACCESS.2018.2842685.

[4] Hoang Giang Do, Wee Keong Ng, “Blockchain-based System for Secure Data Storage with Private Keyword Search”, 2017 IEEE 13th World Congress on Services, DOI 10.1109/SERVICES.2017.23, 2017.

[5] J. Huang, L. Kong, G. Chen, M.Y. Wu, X. Liu, P. Zeng, "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism", IEEE Trans. Ind. Inf., 15 (6) (Jun. 2019), pp. 3680-3689.

[6] Q. Wen, Y. Gao, Z. Chen, D. Wu, "A Blockchain-based Data Sharing Scheme in The Supply Chain by IIoT", 2019 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS) (2019).

[7] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things", 2017 IEEE Transactions on Industrial Informatics (2017).

[8] N. Teslya, I. Ryabchikov, "Blockchain Platforms Overview for Industrial IoT Purposes", 2019 IEEE proceeding of the 22nd conference of fruct association (2019).

[9] G. Wang, Z. J. Shi, M. Nixon and S. Han, “ChainSplitter: Towards Blockchain-based Industrial IoT Architecture for Supporting Hierarchical Storage”, 2019 IEEE International Conference on Blockchain (Blockchain) DOI 10.1109/Blockchain.2019.00030.

[10] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, M. Song, “Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach”, 2018 IEEE Transactions on Industrial Informatics, DOI 10.1109/TII.2019.2897805.

[11] T. Alladi, V. Chamola, R.M. Parizi, K.K.R. Choo, "Blockchain Applications for Industry 4.0 and Industrial IoT: A Review", IEEE Distributed Computing Infrastructure for Cyber-Physical Systems (November 2019), 10.1109/ACCESS.2019.2956748.

[12] Rathee G., Gupta S.D., Jaglan N., "A Review on Blockchain and Its Necessitate in Industrial IoT", In: Saini H., Sayal R., Buyya R., Aliseri G. (eds) Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, vol 103 Springer, Singapore, 2020.

[13] Silva T.B, Morais E.S, Almeida L.F.F, Rosa Righi R, Alberti A.M., "Blockchain and Industry 4.0: Overview, Convergence, and Analysis", In: Rosa Righi R., Alberti A., Singh M. (eds) Blockchain Technology for Industry 4.0. Blockchain Technologies Springer, Singapore, 2020.

[14] P. Fraga-Lamas and T. M. Fernández-Caramés, “A review on blockchain technologies for an advanced and cyber-resilient automotive industry,” IEEE Access, vol. 7, pp. 17 578–17 598, 2019.

[15] H. Lu, K. Huang, M. Azimi, and L. Guo, “Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks,” IEEE Access, vol. 7, pp. 41 426–41 444, 2019.

[16] J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, "A survey of blockchain technology applied to smart cities: Research issues and challenges", IEEE Commun. Surv. Tutorials (2019).

[17] H. Juma, K. Shaalan, I. Kamel, "A Survey on Using Blockchain in Trade Supply Chain Solutions", IEEE Access, 7 (December 2019), 10.1109/ACCESS.2019.2960542.

[18] R. Soni, G. Kumar, "A Review on Blockchain Urgency in the Internet of Things in Healthcare", IEEE Int. Conf. Intell. Sustain. Syst. (ICISS) (November 2019), 10.1109/ISS1.2019.8908021.