International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

A Lightweight Decentralized Framework for Secure Data Integrity in Industrial IoT

E Pavithra [1], B G Selvam [2], K Keerthana[3]

[1] Assistant Professor, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: epavithra526@gmail.com, ORC-ID: https://orcid.org/0009-0006-8871-4551

[2] P.G Scholar, Department of MCA, Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: bgselvam7@gmail.com ORC-ID:https://orcid.org/0009-0000-9278-4268

[3]Assistant Professor, Department of CSE(AI & ML), Sri Venkatesa Perumal College of Engineering & Technology, Puttur, E-mail: keerthanakalasamudram17@gmail.com , ORC-ID: https://orcid.org/0009-0009-1485-1731

Abstract: Internet of Things (IoT) devices are commonly used in industrial settings to keep an eye on things like furnace temperature and the state of agricultural soil. The data they collect is usually sent to central computers to be stored and analyzed. Centralized storage, on the other hand, can be changed by people inside or outside the company. To check its accuracy, third-party tools are often needed, which raises both the cost and the security risk. To solve this problem, blockchain technology is used to create an autonomous end-to-end security system that stores data in a way that can't be changed or tampered with and doesn't depend on third-party verifiers. Each data exchange is saved as a block with a unique hashcode that checks the integrity of the entries that come after it. This makes it easy to spot changes that were not made by the intended person. Lightweight SPECK encryption and SHA-256 hashing are also used to protect data while it's being sent, which improves speed for IoT devices that don't have a lot of resources. To make things even safer and more efficient, CHACHA20 encryption is built in to speed up computations and lower the risk of attack, and compressed SHA hashcodes cut down on storage needs. By using smart contracts for automated control and consensus techniques to make sure transactions are true, this method supports scalability, privacy, and strong authentication. Overall, this method protects the privacy and integrity of data in Industrial IoT applications without slowing down devices or letting outside verification systems see sensitive data.

"Index Terms: *Internet of Things, blockchain, privacy, security, lightweight clients".*

1. INTRODUCTION

As a result of the Industrial Internet of Things (IIoT), smart, linked devices like sensors, actuators, controllers, and industrial machinery are being used in more areas to make them safer, more productive, and more efficient [1]. When operational technology (OT) and information technology (IT) come together, they make it possible to collect, send, and analyze huge amounts of data in real time. This is important for automating tasks, planning maintenance, making the best use of resources, and making strategic decisions [2]. IIoT devices, unlike traditional automation systems, can communicate and act intelligently on their own, which is what is making smart businesses possible [3].

IIoT can be used in many areas, such as healthcare, industry, agriculture, oil and gas, energy, transportation, and agriculture. IIoT makes predictive maintenance easier in manufacturing by looking at the state of equipment to avoid unplanned downtimes and increase the life of machinery [4]. IIoT-enabled systems are used in farmland to keep an eye on the weather, soil conditions, and moisture levels in order to get the most out of irrigation and increase crop yields [5]. IIoT is used in the oil and gas business to monitor and control drilling operations from afar, which reduces the need for human input and raises safety [6]. Wearable medical gadgets and biosensors are connected to IIoT networks in healthcare to track patients' vital signs in real time. This helps improve patient outcomes and biosafety management [7].

The rising use of IIoT brings about a lot of problems, especially when it comes to data security, privacy, and the ability of the system to grow. Every IIoT device could be a cyber threat entry point, and the fact that different industrial settings don't use the same security measures makes the risk of data breaches and operational interruptions even higher [1, 8]. Also, current IT systems might not be able to handle the huge amount of real-time data that IIoT systems

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

produce, which raises worries about the integrity and scalability of the network [3].

As more businesses use IIoT as part of their digital transformation, it's important to make sure that these networks are safe and reliable. To protect against vulnerabilities, keep people's trust in automated systems, and fully utilize the IIoT revolution [6, 8], it is necessary to create frameworks that are scalable, safe, and strong. Taking care of these problems is necessary for long-term economic growth in a world that is becoming more and more connected.

2. LITERATURE REVIEW

J. V. Arputharaj and S. K. Pal [9] looked at how IIoT is changing Industry 5.0, focusing on tracking and making decisions in real time. In their work, they stressed that IIoT is a key part of creating long-lasting industrial ecosystems where self-driving devices talk to each other to make processes run more smoothly and increase overall efficiency. The writers talked about how edge intelligence and integrated sensor systems are changing industrial settings by giving us predictive information and reducing the need for human action.

Because IIoT systems need to be smart and scalable, M. Kumar et al. [10] came up with an AI-based sustainable offloading scheme that works well with cloud-fog architectures that work together. This framework uses AI to handle the processing loads across the cloud and fog layers, making sure that performance is fast and uses little energy. Their model gets around the problems that come with centralized processing by allowing spread intelligence, which is necessary for dealing with the huge amounts of data that IIoT devices create.

A thorough look at the role of federated learning in IIoT settings was done by D. Kumar et al. [11]. Their research showed how important it is to use privacy-protecting methods so that corporate data stays in one place and models are trained together across many nodes. This decentralized method makes data safer while keeping prediction analytics working well across all fields.

K. S. Hawaou et al. [12] did a study on industrial workflow scheduling in Industry 4.0. They looked at scheduling and workflow management. They looked into algorithmic methods for making the best use of resources and tasks in smart factories, with a focus on how IIoT and edge computing can be combined to make decisions in real time. Their results showed how important flexible scheduling is for increasing the speed of production and making better use of resources.

In terms of security, H. Alshahrani et al. [13] created an intrusion monitoring system for IIoT environments that uses software-defined networking (SDN). The suggested system constantly checks traffic trends and finds strange behavior by using SDN's programable features, which let us respond quickly to possible threats. Network security is becoming more of a worry in interconnected industrial ecosystems, and this framework makes it better.

Using blockchain technology, A. Sasikumar et al. [14] looked at how to build trust in IIoT. They suggested using a blockchain-based trust system along with digital twin frameworks to make sure that data is real and can be tracked across all industry assets. Their research shows how digital twins, which are computerized copies of real systems, can work with blockchain in a safe and open way to keep things in sync and stop cheating.

A. Aljuhani et al. [15] took it a step further by combining deep learning with blockchain to make IIoT systems safer. To find and stop unauthorized access, their hybrid system uses both the immutability of blockchain and the predictive power of deep learning. The writers created a strong model that can keep security and system efficiency high across distributed industrial networks by combining these technologies.

In a similar paper, A. Sasikumar et al. [16] created a hierarchical attribute-based encryption (HABE) system that is backed by blockchain to make sharing information safely in the IIoT. Based on role-based permissions and cryptographic attributes, this model makes sure that only authorized entities can view certain types of data. They made decentralized access control that works well with growth and dependability by building this encryption model into a blockchain infrastructure.

Y. Guo et al. [17] suggested a safe and useful end-to-end authentication method that is especially made for tactile IIoT systems that need to respond quickly and have very little delay. Their authentication procedure uses simple cryptography and session key exchanges

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

to keep communication smooth while protecting data integrity and user identity. The plan takes into account the special issues that come up with tactile systems, which are common in industrial robotics and tasks that are done from afar.

L. Fu et al. [18] suggested a blockchain-based system for safe device order operations in the IIoT, which would make device security even better. Their method stores orders and interactions between devices in a blockchain ledger, which makes sure that everything can be tracked and can't be changed. This method lowers the risks of command injection attacks and unauthorized device changes, which are very important issues in automated factory settings.

A. Ali et al. [19] fixed the security problems in the Industrial Internet of Medical Things (IIoMT) by adding a group blockchain-based hybrid deep learning model and homomorphic encryption. This method lets calculations be done on protected data, so privacy is kept even when analytics are being done. Their research is mostly about how IIoT can be used in healthcare, where both protecting data and analyzing it in real time are important for keeping patients safe and making sure medical care is correct.

Finally, N. Mishra et al. [20] gave a broad look at IIoT security from the point of view of cryptography. They looked at different encryption standards, safe communication protocols, and cryptographic systems that can be used with IIoT. The study showed that even though the use of IIoT is growing, many applications still don't have full security plans. This makes the role of advanced cryptographic systems even more important.

3. MATERIALS AND METHODS

To get around the problems with centralized data storage, the suggested system uses blockchain to create a decentralized end-to-end security system for the Industrial Internet of Things (IIoT). Traditional centralized databases are replaced by an Ethereum-based blockchain, which makes sure that data keeping can't be changed or tampered with. The lightweight SPECK method, which works well on devices with limited resources, is used to encrypt data from IIoT sensors, like fake temperature readings. The SHA-256 hashing algorithm is used to securely sign each encrypted data packet before it is sent to the blockchain. Solidity-written smart contracts are used to handle tasks like storage, data validation, and authentication. Consensus methods check that transactions are real and valid across the blockchain network. The published contract address is used to make web3 calls from an easy-to-use Python-based interface to the blockchain. To make things even better, we're trying out the CHACHA20 method for better encryption and hashcode compression to lower the cost of storage. This system protects privacy, stability, and scalability in IIoT settings without using extra tools from outside the system.

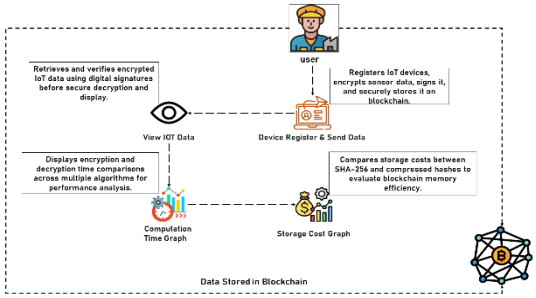


Fig.1 Proposed Architecture

a) Modules:

Industrial User Registration: This module lets new industry users sign up by giving basic information like the name of their company, an email address, and a password. Once a user has successfully registered, they are verified and added to the blockchain-based system. This makes sure that their actions and name are safely stored and can be tracked within the decentralized network.

Industrial User Login: This module lets registered industrial users use their passwords to safely log in. Blockchain verification methods handle authentication, making sure that only authorized users can use the system's features. After logging in, users can safely look at analytics, keep an eye on device data, and connect with other modules.

Device Register & Send Data: This module lets industrial users register IoT devices by giving them unique IDs and other information. Devices start sending real-time data to the system, like temperature, pressure, or humidity, as soon as they are entered. All gadget data is safely stored on the blockchain, which makes sure that data logs can't be changed and are clear and easy to check.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

View IoT Data: Users can get to IoT sensor data sent from registered devices in real time through this feature. The structured data format lets users keep an eye on industrial processes, find problems, and keep track of performance. Using blockchain makes sure that the information shown is correct and reliable.

Computation Time Graph: This module shows how long it takes for the blockchain to handle and record data transactions. It measures the times it takes to do calculations in different situations, which helps users understand how well the system is working and find ways to make it better. Graphs are made on the fly based on real-time device behavior and the times that smart contracts are executed.

Storage Cost Graph: This section shows a comparison of the storage costs that come up when you store data directly on the blockchain versus putting it on an open storage service like IPFS. The graph helps people think about ways to save money while keeping the data safe, which gives them ideas on how to handle data effectively.

Logout: This module safely ends the user session, making sure that no one else can do anything after the user leaves. The browser deletes all login information and session data. This keeps the system safe and stops people from abusing open or idle sessions.

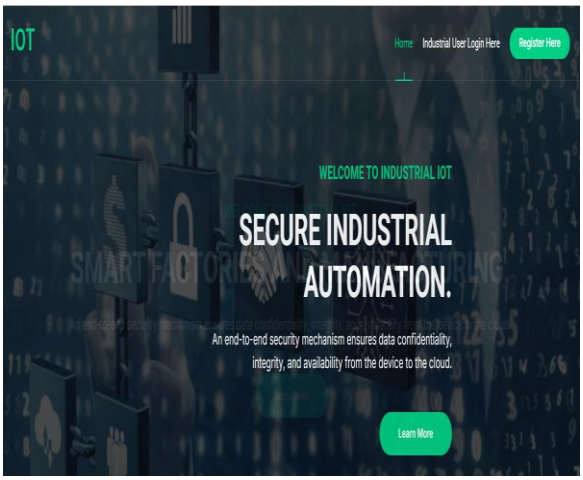
b) Methods/Technologies:

1. Ethereum: Ethereum is an open-source, decentralized blockchain platform that lets smart contracts and decentralized apps (DApps) be built. In this project, Ethereum is used to store and handle IIoT data safely without having to rely on servers in one place. Its tamper-proof and immutable ledger protects data integrity and makes it possible for industrial IoT processes to run without trust.

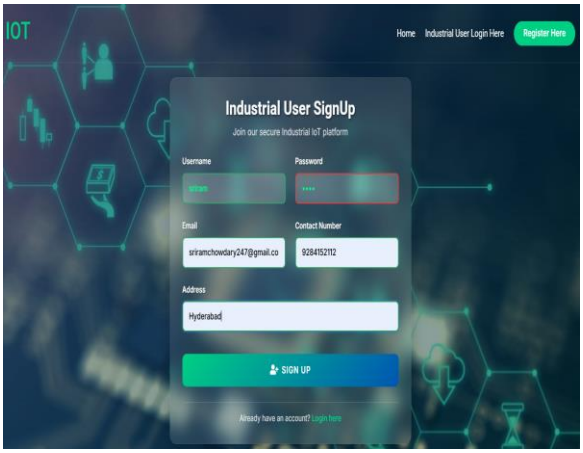
2. Solidity: Solidity is a high-level computer language for making smart contracts that run on the Ethereum blockchain. For the project, Solidity scripts describe how to store, retrieve, and verify IIoT data. These smart contracts make sure that exchanges between IIoT devices and the blockchain are safe and clear by automatically carrying out actions that have already been set up.

3. Ganache: Ganache is an individual Ethereum blockchain that is used for testing and building. Before putting them on the main network, it lets developers test transactions, deploy contracts, and see how the blockchain works in a safe setting. Ganache helps mimic the IIoT data storage and retrieval processes in this project, which makes sure that the smart contract runs smoothly and without any errors.

4. EXPERIMENTAL RESULTS

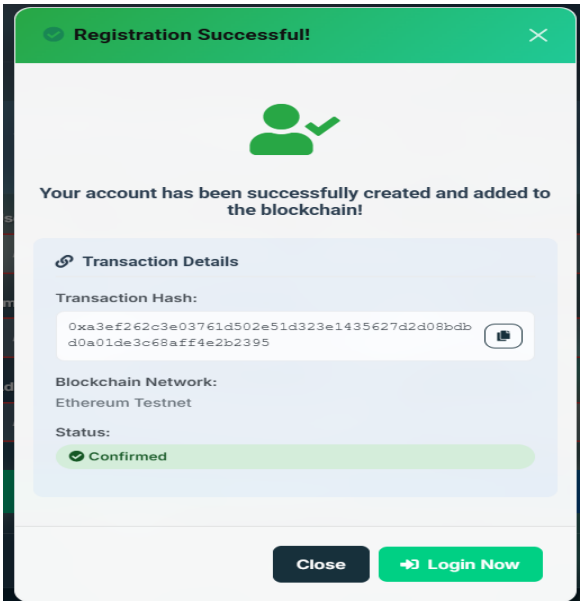


After that, the project window shows up like in the picture above.

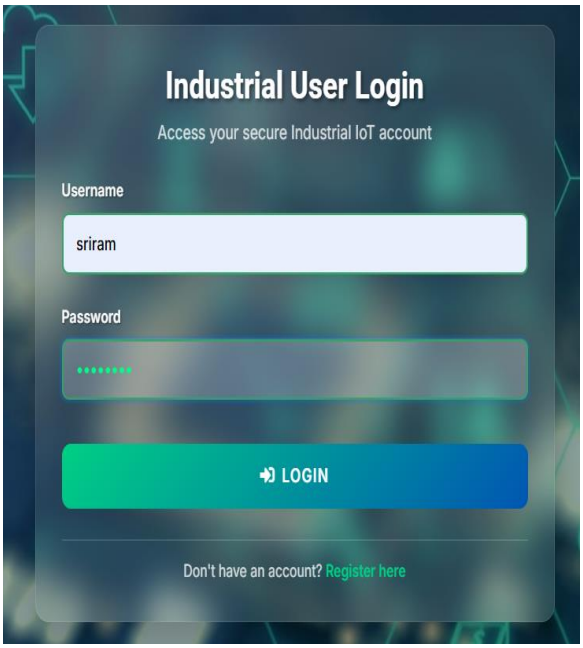


To keep your data safe, fill out the IoT platform application using the information below.

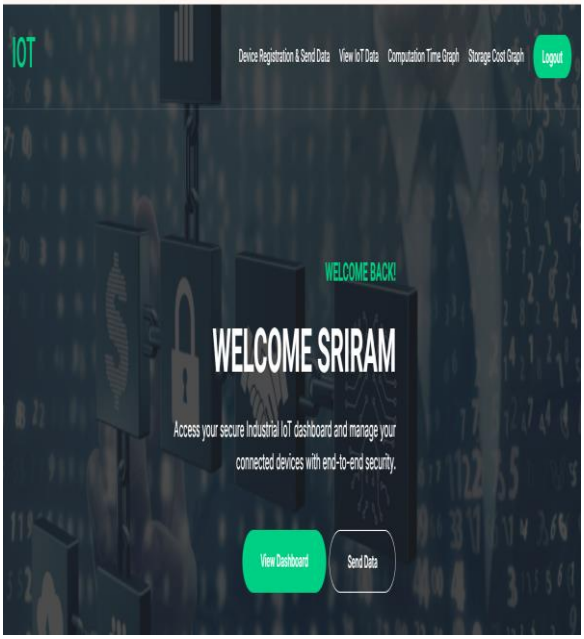
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



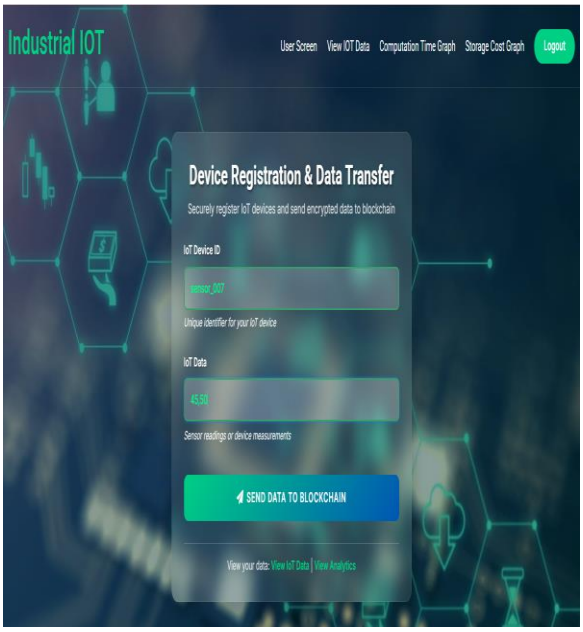
After signing up, the system encrypts user data safely and saves it on the blockchain along with transaction information.



To get into your user account, enter your username and password.

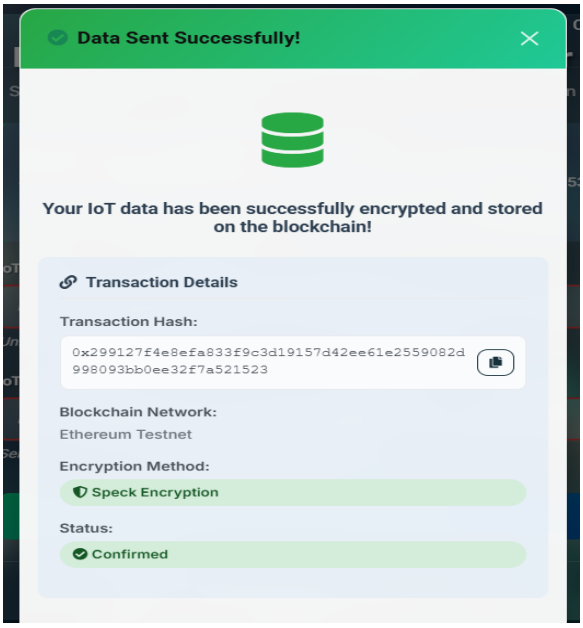


The home page is shown on the screen below after the person logs in to their account.

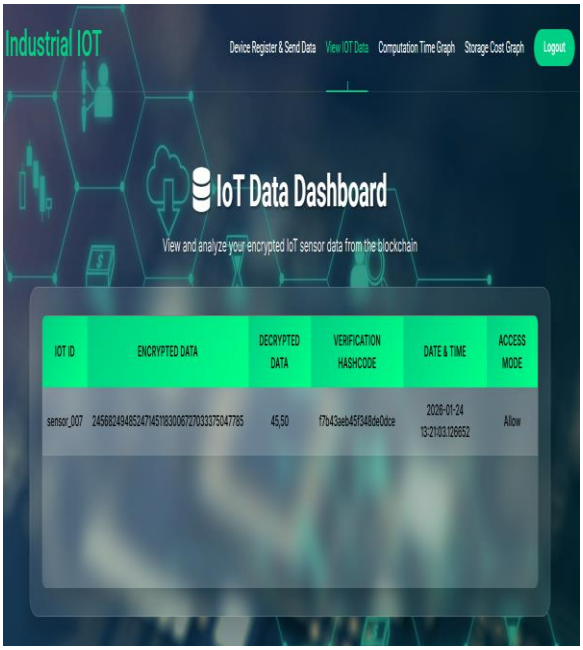


To allow encryption and protect data, register the IoT device ID along with its data.

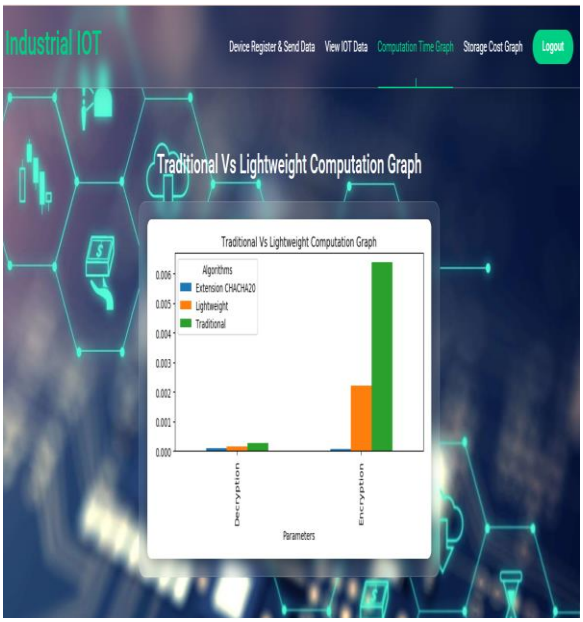
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper



After the device is registered, the system shows information about transactions that happened with the encrypted data that is saved on the Ethereum blockchain.



The hash, timestamp (date and time), and sensor name are all protected IoT data that is shown by the system.



A comparison of standard and lightweight methods for encrypting and decrypting data is shown in the computational graph.

The line shows how much it costs to store plain sensor data on the blockchain versus compressed sensor data.

5. CONCLUSION

End-to-end security for the Industrial Internet of Things (IIoT) is suggested. It uses a decentralized blockchain framework to protect sensitive industrial

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

data, so there is no need for third-party verification tools. The dataset is made up of fake IIoT sensor inputs like temperature records and text messages. The SPECK lightweight cryptographic algorithm is used to encrypt data. This method works well on IIoT devices that don't have a lot of power or resources. SHA-256 is used to make digital signatures that can be used to check the security of data. If there are any hash mismatches, it is possible to tell if someone has changed the data. The protected data and digital signatures are kept on the Ethereum blockchain by smart contracts written in Solidity. A Python-based web frontend lets users sign up, prove their identity, register devices, and send and receive private data. Performance tests show that SPECK encrypts data faster than standard AES algorithms, and CHACHA20, when added as an extension, does better in both encryption and decoding times. The storage cost graph also shows that using compression methods on SHA-256 hashcodes greatly lowers the cost of storing blockchains. This system protects the privacy, validity, and integrity of data while also being scalable and energy-efficient. This makes it a strong choice for managing IIoT data securely in real time in industrial settings.

The next step for this project is to add advanced consensus methods to the blockchain-based IIoT security framework so that it can be used for real-time, large-scale industrial deployments. This will make the system more scalable and efficient. Better methods for protecting privacy, like homomorphic encryption and zero-knowledge proofs, can be used to make secrecy stronger. Interoperability with multi-cloud and edge systems will also help more people use it. In the future, improvements could include AI-driven anomaly detection, predictive analytics, and automated reaction mechanisms to make industrial IoT ecosystems even safer and better at protecting themselves from new cyber threats.

REFERENCES

[1] G, Viswanath., N, Madhvik., K, Bhaskar., K, Supriya. (2024). Machine-Learning-Based Cloud Intrusion Detection. International Journal of Mechanical Engineering Research and Technology, 16(9), 38-52.

[2] Javed, I. T., & Qureshi, K. N. (2023). Role of blockchain for IoE infrastructures and applications. In Cybersecurity Vigilance and Security Engineering of Internet of Everything (pp. 127-139). Cham: Springer Nature Switzerland.

[3] Khan, A. A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. IEEE Access, 10, 122679-122695.

[4] Pal, K. (2022). Cryptography and blockchain solutions for security protection of internet of things applications. In Information security practices for the internet of things, 5G, and next-generation wireless networks (pp. 152-178). IGI Global.

[5] Wang, G. (2021). Sok: Applying blockchain technology in industrial internet of things. Cryptology ePrint Archive.

[6] B.Babayigit and M. Abubaker, ‘‘Industrial Internet of Things: A review of improvementsovertraditionalSCADAsystemsforindustrialautomation,’’ IEEE Syst. J., vol. 18, no. 1, pp. 120–133, Mar. 2024.

[7] Singh, M., Tiwari, S. K., Swapna, G., Verma, K., Prasad, V., Patidar, V., Sharma, D. & Mewada, H. (2023). A Drug-Target Interaction Prediction Based on Supervised Probabilistic Classification. Journal of Computer Science, 19(10), 1203-1211. https://doi.org/10.3844/jcssp.2023.1203.1211

[8] D. Berestov, O. Kurchenko, L. Zubyk, S. Kulibaba, and N. Mazur, ‘‘Assessment of weather risks for agriculture using big data and industrial Internet of Things technologies,’’ in Proc. Cybersecur. Providing Inf. Telecommun. Syst., 2023, pp. 1–13.

[9] J. V. Arputharaj and S. K. Pal, ‘‘Transforming industry 5.0: Real time monitoring and decision making with IIOT,’’ in Sustainability in Industry 5.0. Boca Raton, FL, USA: CRC Press, 2024, pp. 76–106. [Online]. Available: https://www.taylorfrancis.com/chapters/edit/10.1201/9781032686363-5/transforming-industry-5-0-vijay-arputharaj-sanjoy-ku mar-pal

[10] M. Kumar, G. K. Walia, H. Shingare, S. Singh, and S. S. Gill, ‘‘AI-based sustainable and intelligent offloading framework for IIoT in collaborative cloud-fog environments,’’ IEEE Trans. Consum. Electron., vol. 70, no. 1, pp. 1414–1422, Feb. 2024.

[11] D. Kumar, P. Pawar, H. Gonaygunta, and S. Singh, ‘‘Impact of federated learning on industrial

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

IoT—A review,'' Int. J. Adv. Res. Comput. Commun. Eng., vol. 13, no. 1, pp. 1–12, Dec. 2023.

[12] K. S. Hawaou, V. C. Kamla, S. Yassa, O. Romain, J. E. N. Mboula, and L. Bitjoka, ''Industry 4.0 and industrial workflow scheduling: A survey,'' J. Ind. Inf. Integr., vol. 38, Mar. 2024, Art. no. 100546.

[13] H. Alshahrani, A. Khan, M. Rizwan, M. S. A. Reshan, A. Sulaiman, and A.Shaikh,''Intrusion detection frameworkfor industrial Internet of Things using software defined network,'' Sustainability, vol. 15, no. 11, p. 9001, Jun. 2023.

[14] Dr, K, Pushpa Latha., Mr, M, N, Mallikarjuna Reddy., Dr, B, Rajalingam., Malleswari Akurati., Dr, G, Swapna., Bakkala Santha Kumar., (2026). Blockchain-Enabled Trade Finance Framework for Secure Drug Supply Chain Transactions., International Journal of Drug Delivery Technology, 16(3s), 884-889.

[15] A. Aljuhani, P. Kumar, R. Alanazi, T. Albalawi, O. Taouali, A. K. M. N. Islam, N. Kumar, and M. Alazab, ''A deep learning integrated blockchain framework for securing industrial IoT,'' IEEE Internet Things J., vol. 11, no. 5, pp. 7817–7827, Mar. 2024.

[16] Gudditti, V., & Krishna, P. V. (2021). Adaptive Light Weight Encryption Algorithm for Securing Multi-Cloud Storage. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(9), 545–554.

[17] Y. Guo, Y. Guo, P. Xiong, F. Yang, and C. Zhang, ''A provably secure and practical end-to-end authentication scheme for tactile industrial Internet of Things,'' Pervas. Mobile Comput., vol. 98, Feb. 2024, Art. no. 101877.

[18] L. Fu, Z. Zhang, L. Tan, Z. Yao, H. Tan, J. Xie, and K. She, ''Blockchain enabled device command operation security for industrial Internet of Things,'' Future Gener. Comput. Syst., vol. 148, pp. 280–297, Nov. 2023.

[19] A. Ali, M. F. Pasha, A. Guerrieri, A. Guzzo, X. Sun, A. Saeed, A. Hussain, and G. Fortino, ''A novel homomorphic encryption and consortium blockchain-based hybrid deep learning model for industrial Internet of Medical Things,'' IEEE Trans. Netw. Sci. Eng., vol. 10, no. 5, pp. 2402–2418, Sep. 2023.

[20] N. Mishra, S. H. Islam, and S. Zeadally, ''A survey on security and cryptographic perspective of Industrial-Internet-of-Things,'' Internet Things, vol. 25, Apr. 2024, Art. no. 101037