International Journal of Information Technology and Management
Vol. 20, Issue No. 1, February-2025, ISSN 2249-4510

DOI: https://doi.org/10.29070/4k7w8k35

Check for updates

Blockchain Integration with Edge Computing for Securing IoT Networks Through Distributed Ledger Technology

Shelke Bharat Abhimanyu [1] *

1. Associate Professor, Shri Chhatrapati Shivaji College, Omerga, Dist. Dharashiv, Maharashtra, India
bashelke@gmail.com

Abstract: Scalability and automation in "Industrial Internet of Things (IIoT)" aims to improve productivity in smart factory setting. For scalability, protection, collaboration, optimization, and automation in industry, smart systems, Internet of Things (IoT), and information and communication technologies (ICTs) are integrated as an individual organism. This study proposes a safe data-sharing system based on blockchain to provide security in industry with IoT. As per blockchain's reputation, end-to-end authentication is developed and smart contract can validate security measures of nodes. With categorization and integrity verification in industry and node terminals, the paradigm of blockchain manages dissemination and data collection. The "Proof of Authentication (PoAh)" is a consensus mechanism developed with blockchain network to develop a collaborative network for retaining verification and log data in IIoT. It achieves tracing of endpoint activity and trusted authentication. Blockchain nodes also uses edge computing to provide authentication of devices using PoAh and smart contracts. The proposed architecture achieves high response rate and cuts the time for authentication. The service time in the proposed system shows efficiency of blockchain system for IIoT in comparison to current works. Finally, several block sizes were evaluated for efficient transaction.

Keywords: Proof of Authentication, blockchain, Industrial Internet of Things, IoT, PoAh, automation, scalability

----------X----------

INTRODUCTION

"Industrial Internet of Things (IIoT)" has come a long way with adoption of industrial facilities with "Information and Communication Technologies (ICTs)" to enable reliable production. With smart computing and IoT, self-dependent processing, automation, and computing are adopted for smart factories (Maurya et al, 2024). The primary blockchain uses a layer to perform several roles supporting customer replies and production in traditional operations with a management layer (Sasikumar et al, 2022). These days, industries are equipped for meeting productivity needs and growing demands of users with IIoT. In autonomous machines and robotics, recent advancements have replaced human interventions. The machine-operated jobs can analyze, improve, and aggregate the practices of data management and customer replies.

Applications and infrastructure are available in cloud environment as amenities. Mathematical models, tools used for data visualization, applications, people, IoT, and smart computing work together in the cloud. With several communication and automated tools, customer services can be improved. "Internet of Things (IoT) has enough potential to improve the capabilities and features of any service it supports or provides, irrespective of use case. Another aspect of challenges will come up with near future and current use cases. Another major obstacle is centralized data storage. In IoT system, the existing storage system, number of IoT devices, and amount of data collected go hand in hand.

There are concerns related to administration and data ownership due to this consolidation of central data. Centralized aggregation of data may be appealing to attackers and they might manipulate the IoT solution for their advantage, resulting in devastating events (Ozay et al, 2013). It increases security issues and confidentiality issues in the IoT environment. A system is needed which can use the features of edge computing platform and addresses some of these challenges to promote the scaled future. IoT systems should integrate and interact with their environments effectively and safely (Tawalbeh et al, 2020). These IoT technologies provide enough data which can be analyzed and processed instantly to help in the process of decision-making.

Such processing should take place near the edge of the network to reduce bandwidth requirements and enhance timeliness. Data can be analyzed by edge computing to make decisions at the edge. Hence, it is vital to know the pros and cons of edge computing. Since the development of bitcoin, everyone has been discussing about blockchain, i.e., a "distributed ledger technology (DLT)", where financial transactions can be recorded (Hamilton, 2020). Most recent block in the blockchain is connected to the one came before the previous block by the hash label. A blockchain block contains the following data –

- Data about the activities like date, time, and amount;
- Facts related to transaction participants; and
- A unique hash code which differentiates blocks

A new block is added to the end of blockchain. As all the transactions are stored in a public ledger by the blockchain, a kind of blockchain open to all, it ensures complete transparency. Identity of the users and other sensitive data will be retained securely on the public blockchain for privacy protection (Sai et al, 2021). Along with the hash of data within, each block also covers the hash of the block on the blockchain. Hence, "distributed ledger technology (DLT)" is a decentralized technology used in blockchain. A hacker may alter the transaction in blockchain without changing the hash of every block. Blockchain is best suited in different industries due to its security, including finance, government agencies, healthcare, and managing supply chain (Sunny et al, 2022).

Blockchain transactions are verified and confirmed with "consensus protocol" unlike traditional systems depending on a core authority. Every node in the blockchain may agree on the existing state of blockchain with a consensus approach (Xiao et al, 2020). It is important to implement a consensus model to ensure that all the nodes agree on existing condition of chain every time for producing a new block through transactions. The consensus mechanism is conducted with each node added to the blockchain. Hence, consensus models play a vital role in setting the trustworthiness of every blockchain node to ensure security and reliability of blockchain.

Some of the most well-known consensus models are fault tolerance, Proof of Burn, Proof of Capacity, and Proof of Stake. Smart contracts are used on blockchain for guaranteeing that transaction sticks to the certain limitations and conditions. Adopted with a few lines of code, smart contracts ensure that each transaction fulfills specified conditions. This smooth automation reduces manual confirmation of transactions for more accurate and quick decisions. The transparency, decentralization, and immutability are some of the benefits of blockchain.

All the data was stored in a single location where everyone could access it before blockchain came into the mainstream. In case of failure, cyber risks, and other issues, centralized systems become vulnerable. As all the nodes have data in a decentralized system, it can evade these issues with centralized solutions. On the blockchain, data cannot be changed due to consensus models. Blockchain can be used in a lot of industries due to its quality, including SCM, regulation, and banking (Altaş et al, 2022). Each blockchain is open-source. Every transaction is observed on the blockchain. As changes in the network needs approval from a lot of nodes, transactions or technology stay safe irrespective of their transparency. Complex techniques can hide user data (Hellani et al, 2021)." In decentralized systems like IoT, blockchain technology has a lot of challenges irrespective of its several benefits. On the blockchain, consensus also causes significant energy consumption and network latency. IOT devices have lack of resources for dispersed networks, which can be a dealbreaker for applications. Another issue is low rate of data transfer in blockchain.

LITERATURE REVIEW

The IIoT has become the game changer over the past decade, drawing interest from academics seeking to enhance manufacturing (Qi et al, 2023). Various industries have observed the benefits of IIoT in areas like proactive upkeep, eco-friendly processes, and accurate data processing in real-time. Blockchain may respect human rights while offering openness and traceability in industrial settings. This chapter summarizes several recent studies which have addresses the potential uses of blockchain in industrial IoT.

Minoli and Occhiogrosso (2018) argued that blockchain may be ideal for IoT devices for untampered archives and genuine transactions in their studies with blockchain as IoT system. When it comes to implement blockchain in IoT, most challenging part is looking for ideal hosting infrastructure. Fog computing is found to be superior to cloud infrastructure as potential platform after testing. Feng et al (2020) have proposed a prototype in their works related to edge computing in endpoints for blockchain. Mobile devices may use edge network and access computing power to help blockchain in the apps. As more miners register for the network, service provides can be benefitted by the integration as per their experimental findings and testbed.

For using blockchain for transcoding in video streaming, Liu et al (2018) suggested an approach in edge computing for splitting resources. A system is devised to incentivize transcoding and found two ways for removing the workload from edge network. Findings of their simulation have confirmed the ability of model to improve average profits in dynamic allocation of schemes and offloading. Alzoubi et al (2022) conducted a literature survey know if it would be possible to use "peer-to-peer (P2P) communication" and blockchain for creating decentralized design for IoT.

Accountability and security of recorded data of resource administration are important aspects of efficient system for resource management. In such architecture, blockchain technology may be integrated to guarantee data security and offer reliable setting. To achieve decentralized building of environments during the DevOps process and systematically integrated resource management, Akbar et al (2022) proposed a blockchain-based management system. Blockchain and smart contracts are used in the structure to provide trusted services and separate from third party. Blockchain technology can be used for recording hash values of sensitive information and provide tracking to ensure accountability and accuracy (Ahmed et al, 2022).

Kumar et al (2020)proposed an application framework, BlockEdge, which is based on blockchain, to improve the dependence of "collaborative edge computing (CEC)". Edge computing can also use smart contracts from blockchain to improve its security. As per deposit balances and validation findings on the chain, BlockEdge develops a rating system for trust. For privacy in terms of data security and trust management and addressing trust assessment approach, TrustChain is a new blockchain system recommended by Otte et al (2020). Asaithambi et al (2022) offered a trust process based on blockchain to transfer the tasks to analyze "mobile edge computing (MEC)". This mechanism avoids self-centric edge servers and counterfeit records with the use of blockchain to manage and store trust data. In addition, consensus protocol is developed which combines PoS and PoW.

Zhang et al (2019) proposed the use of IIoT for efficient "certificate-less signing" in cloud platforms. Light certificate-less verification is good for third-party security and data reliability. Signature forgeries may be prevented with "Reliable Certificateless Signatures (RCLS)". Zheng and Cai (2020) proposed a secure sharing system to ensure IIoT data privacy, which is important with rising concerns about data security and privacy in IIoT solutions. Data sharing is the key feature of this system on request and differentiated privacy based on profits. From bandwidth usage and confidentiality of data, this framework is excellent in security of IT networks. A credit-based consensus approach is the foundation for secure industrial IoT. The PoW system based on IoT device was explored by Huang et al (2019). Blockchain ledger protects the sensitive data of IoT device.

Research Objectives

- To discuss the features IoT systems based on edge computing
- To propose the structure to handle operations safely in smart industrial environments

METHODOLOGY

Based on studies which have been integrated for applications, this knowledge is based on broad challenges of integration and complex world of controlling specific concerns of blockchain. This study is based on proposing a practical solution for adopting blockchain in IoT with distributed ledger technology, while meeting the need for flexibility and security needs for decentralized, safe storage.

This study adopts descriptive and qualitative research approach, which relies majorly on secondary data sources to provide valuable insights on the realism of combining edge computing and blockchain for IoT solutions. To gather insights to modern advancements, this study reviews peer-reviewed journal articles, authoritative reports, and conference papers. The approach synthesizes current knowledge to conceptualize a practical model.

First, literature review was conducted on IoT, blockchain, and edge computing to identify existing challenges like security, scalability, and latency issues in core architecture. Second, proposed models and case studies were analyzed to determine how consensus mechanisms, smart contracts, and immutability could improve data safety and trust in Industrial IoT. Third, this study proposes a conceptual model which integrates PoAh with the nodes of edge computing to reduce delays with verification and authentication.

Overall, this methodology enhances understanding of blockchain-based IoT and edge computing. The outcome provides decentralized, scalable, and secure framework for future industrial implementations.

DATA ANALYSIS

IoT Systems based on Edge Computing

The huge incursion of data from IoT is damaging cloud computing because of high latency and costly bandwidth. To meet the basic industry needs in areas like "artificial intelligence (AI), real-time enterprise, and privacy and security, edge computing provides a model for service computing which is near data sources or objects, enabling quick response to several services (Xiong et al, 2020). This section outlines the characteristics of edge computing. Processing power is conceptually and physically close to endpoints with edge computing. Hence, everything occurs near the data source from data production to processing to data usage to ensure quick response to terminal requests.

Edge servers can operate individually and self-recover in a network outage. The central cloud can execute flexible offloading and assigning roles to ideal edge servers. A lot of adaptable and diverse edge devices can meet the rising demands of IoT. Additionally, edge computing servers may improve potential for cloud computing by offering closest edge devices with improved processing, storage, and communication. These features cover increased capacity of data storage, improved bandwidth, and faster speeds in data processing, contributing to the performance and efficiency of edge computing. Security is improved as a lot of information doesn't need to pass over the network, especially private data.

IoT becomes an important topic for administration of trust for edge computing for finding dependable system to connect the nodes of IoT to the edge network. Figure 1 illustrates security challenges for IoT systems based on edge computing.

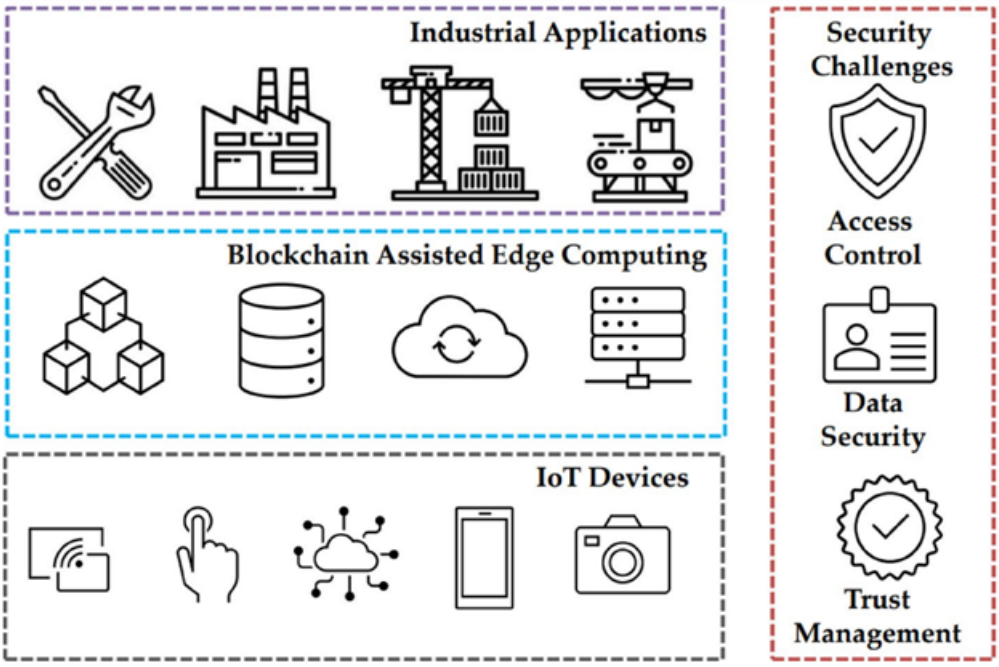

Figure 1: IoT systems based on edge computing along with challenges

Source – Asaithambi et al (2024)

Characteristics of IoT systems based on edge computing

- **Precision** – It suggests how closely a computed trust value is to the node to its trust or fundamental value when all information is known about its behavior. Accuracy is needed for the trust system (Sasikumar et al, 2023).
- **Accessibility** – It means guarantee of trust management system that all services will be available completely irrespective of attack on resources or non-availability for any reason. It is frequent in edge computing networks.
- **Security** – To ensure security of edge-based IoT system, trust should be built. In infrastructure layer of servers, it provides approaches for guaranteed security.
- **Dependability** – Trust management approaches act as important parameter and rely on it. With the lifespan of edge-based network, it is guaranteed that all functions act accurately.
- **Lightweight** – As part of IoT systems, restricted networks and devices operate at the edge. Edge-based trust management and IoT frameworks should be efficient and small enough to work well across different IoT networks nodes, and servers, even with limited resources (Wardana et al, 2024).
- **Diversity** – Diverse nodes, subnets, edge servers, and edge nodes are some of the typical aspects of edge-based IoT networks. To meet the criteria for diversity for trust management system, it could accommodate objects with different levels of computational potential, complexity, and use of energy.
- **Flexibility** – IoT systems are evolving rapidly, edge-based IoT should be highly flexible and peers engaged in trust-based transactions for rapid changes. For determining the credibility of nodes and edge servers, regulations may change with device changes and their resources may not be available all the time (Tyagi et al, 2023).

Proposed Blockchain Structure

Figure 2 illustrates the proposed blockchain-based computing architecture which provides a lot of benefits. IoT users can send tasks with a unified interface to the industry. The structures of blockchain specifies dependencies of data and streamlines industry task organization. The manager uses blockchain structure to devise a coordination plan with resource usage, operations, and network of edge servers. The manager uses blockchain for authenticity and security of user data. If actions of a user are unauthorized, the manager can halt the allocation of resources immediately. Ultimately, the edge servers perform the tasks, install and download the needed images, and report the outcomes. An authorized network is given to each user, which reports to calculated models. The results of job computation and user data are stored securely on the blockchain to ensure highest protection and security.

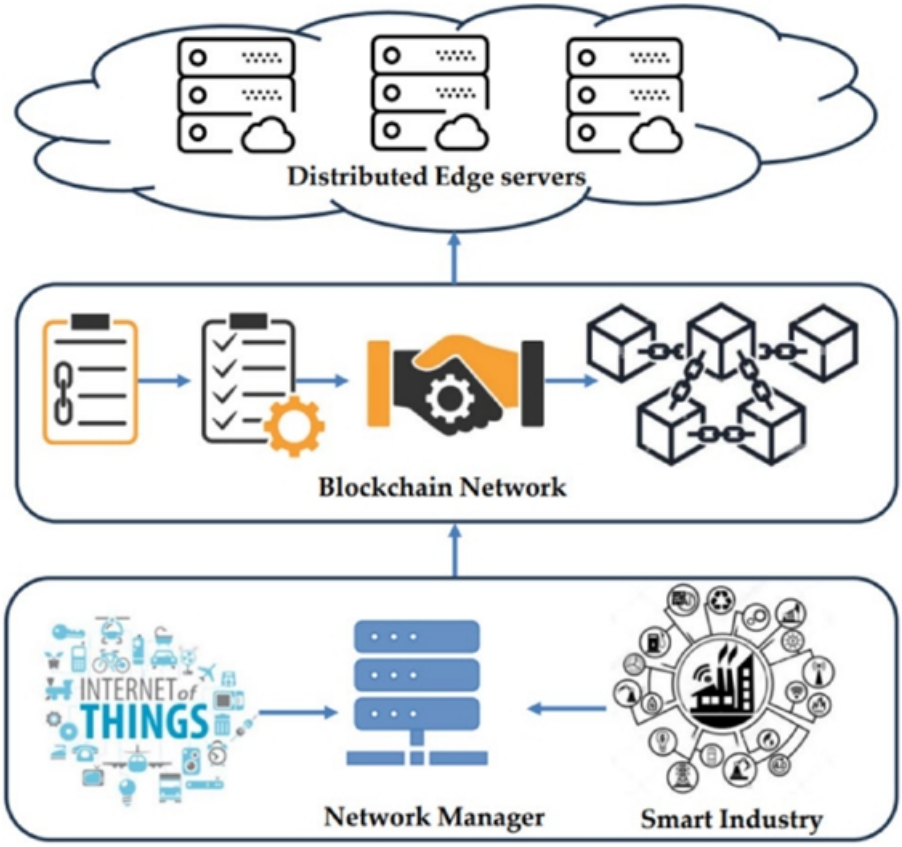

Figure 2: Proposed Edge Computing based Blockchain architecture for IoT systems

Source – Asaithambi et al (2024)

All the approved user data is handled by the gateway and uploaded to the constantly updated blockchain. The data of the blockchain is easy to access after getting query response from the management. Users can enjoy simple implementation, least latency, and control on the edge computing in this setup. With robust security and protection for reputation, blockchain ensures integrity of the service. IoT devices and clients smoothly register in the blockchain in the stage of setup. This process is needed for reauthentication of device and users.

Manager can collect data, coordinate subtasks, separate tasks, conserve interim outcome, handle resources, and perform user authentication. The proposed structure encrypts the system securely with blockchain and manages the whole system across the world. Processes are split across edge servers, which listen to work needs and provide resource data to the management." After receiving tasks, it launches the pictures of container needed and establishes interaction ports. The industry acts as per manager's directions to respond to relevant user. The calculations of the edge servers can determine instructions.

The blockchain ensures reliability and security of the program as a decentralized verifier. It validates and stores transactions with decentralized bodies. Information structure of the transaction is formed by the hash values of data submitted by the users and outcomes estimated by edge nodes. Each transaction consists of IDs and digital signatures of relevant servers with a timestamp. Data analysis process is validated by the smart contracts document to improve security of the system.

DISCUSSION AND CONCLUSION

Innovative sectors are modernized by industrial IoT with the integration of edge computing and blockchain, which has drawn a lot of interest in the fields of research and industry. A smart sector may benefit from modern benefits provided by blockchain, such as, protection, efficiency, trust, consistency, and decentralization. This study proposes a blockchain framework for smart edge computing. A lightweight, safe, and decentralized IIoT network based on private blockchain to perform various important tasks, such as, data storage, trusted management, device and user registration with PoAh-based blockchain infrastructure.

This study presents implementing authentication on edge-level which reduces burden of computation and improves security of industry platform. A lot of characteristics of performance are considered when it comes to determine the efficiency of architecture.

References

1. Maurya, M., Panigrahi, I., Dash, D., & Malla, C. (2024). Intelligent fault diagnostic system for rotating machinery based on IoT with cloud computing and artificial intelligence techniques: a review. Soft Computing, 28(1), 477-494.
2. Sasikumar, A., Ravi, L., Kotecha, K., Saini, J. R., Varadarajan, V., & Subramaniyaswamy, V. (2022). Sustainable smart industry: A secure and energy efficient consensus mechanism for artificial intelligence enabled industrial internet of things. Computational intelligence and neuroscience, 2022(1), 1419360.
3. Ozay, M., Esnaola, I., Vural, F. T. Y., Kulkarni, S. R., & Poor, H. V. (2013). Sparse attack construction and state estimation in the smart grid: Centralized and distributed models. IEEE Journal on Selected Areas in Communications, 31(7), 1306-1318.
4. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12), 4102.
5. Hamilton, M. (2020). Blockchain distributed ledger technology: An introduction and focus on smart contracts. Journal of Corporate Accounting & Finance, 31(2), 7-12.
6. Sai, A. R., Buckley, J., Fitzgerald, B., & Le Gear, A. (2021). Taxonomy of centralization in public blockchain systems: A systematic literature review. Information Processing & Management, 58(4), 102584.
7. Sunny, F. A., Hajek, P., Munk, M., Abedin, M. Z., Satu, M. S., Efat, M. I. A., & Islam, M. J. (2022). A systematic review of blockchain applications. IEEE Access, 10, 59155-59177.
8. Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. IEEE communications surveys & tutorials, 22(2), 1432-1465.
9. Altaş, H., Dalkiliç, G., & Cabuk, U. C. (2022). Data immutability and event management via blockchain in the Internet of things. Turkish Journal of Electrical Engineering and Computer Sciences, 30(2), 451-

468.

10. Hellani, H., Sliman, L., Samhat, A. E., & Exposito, E. (2021). On blockchain integration with supply chain: Overview on data transparency. Logistics, 5(3), 46.

11. Qi, Q., Xu, Z., & Rani, P. (2023). Big data analytics challenges to implementing the intelligent Industrial Internet of Things (IIoT) systems in sustainable manufacturing operations. Technological Forecasting and Social Change, 190, 122401.

12. Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. Internet of Things, 1, 1-13.

13. Feng, J., Yu, F. R., Pei, Q., Du, J., & Zhu, L. (2020). Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems. IEEE Transactions on Wireless Communications, 19(6), 4321-4334.

14. Liu, M., Yu, F. R., Teng, Y., Leung, V. C., & Song, M. (2018). Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing. IEEE Transactions on Wireless Communications, 18(1), 695-708.

15. Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: security, privacy, technical, and design challenges. Future Internet, 14(7), 216.

16. Akbar, M. A., Mahmood, S., & Siemon, D. (2022, June). Toward effective and efficient DevOps using blockchain. In Proceedings of the 26th international conference on evaluation and assessment in software engineering (pp. 421-427).

17. Ahmed, A., Abdullah, S., Bukhsh, M., Ahmad, I., & Mushtaq, Z. (2022). An energy-efficient data aggregation mechanism for IoT secured by blockchain. IEEE Access, 10, 11404-11419.

18. Kumar, T., Harjula, E., Ejaz, M., Manzoor, A., Porambage, P., Ahmad, I., ... & Ylianttila, M. (2020). BlockEdge: Blockchain-edge framework for industrial IoT networks. IEEE Access, 8, 154166-154185.

19. Otte, P., de Vos, M., & Pouwelse, J. (2020). TrustChain: A Sybil-resistant scalable blockchain. Future Generation Computer Systems, 107, 770-780.

20. Asaithambi, S., Ravi, L., Kotb, H., Milyani, A. H., Azhari, A. A., Nallusamy, S., ... & Vairavasundaram, S. (2022). An energy-efficient and blockchain-integrated software defined network for the industrial internet of things. Sensors, 22(20), 7917.

21. Zhang, Y., Deng, R. H., Zheng, D., Li, J., Wu, P., & Cao, J. (2019). Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT. IEEE Transactions on Industrial Informatics, 15(9), 5099-5108.

22. Zheng, X., & Cai, Z. (2020). Privacy-preserved data sharing towards multiple parties in industrial IoTs. IEEE journal on selected areas in communications, 38(5), 968-979.

23. Huang, J., Kong, L., Chen, G., Cheng, L., Wu, K., & Liu, X. (2019, July). B-IoT: Blockchain driven

Internet of Things with credit-based consensus mechanism. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS) (pp. 1348-1357). IEEE.

24. Xiong, X., Zheng, K., Lei, L., & Hou, L. (2020). Resource allocation based on deep reinforcement learning in IoT edge computing. IEEE Journal on Selected Areas in Communications, 38(6), 1133-1146.

25. Wardana, A. A., Kołaczek, G., & Sukarno, P. (2024). Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. Applied Sciences, 14(10), 4109.

26. Tyagi, H., Kumar, R., & Pandey, S. K. (2023). A detailed study on trust management techniques for security and privacy in IoT: Challenges, trends, and research directions. High-Confidence Computing, 3(2), 100127.

27. Asaithambi, S., Nallusamy, S., Yang, J., Prajapat, S., Kumar, G., & Rathore, P. S. (2024). A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things. Scientific Reports, 15(1), 15410.