

Article

TO DESIGN AND DEVELOP THE HYBRID BLOCKCHAIN ENABLED IOT SYSTEM FOR SECURED INDUSTRY 4.0 SYSTEMS

K.B. Shiva Kumar ¹, Veeresh ², Celestine IWENDI ³

¹ Department of Computer Science and Engineering, Don Bosco Institute of Technology, Bangalore, India

² Department of Computer Science and Engineering, Sir M Visvesvaraya College of Engineering, Raichur, India

³ University of Greater Manchester, Bolton School of Creative Technologies, Bolton, Greater Manchester, UK

*Corresponding author: K.B. Shiva Kumar (email: kbshivakumar@dbit.co.in)

Received 03 September 2024; Accepted 06 October 2024; Published 15 December 2024

Abstract: The rapid evolution of Industry 4.0 has catalyzed the integration of advanced technologies to ensure secure, efficient, and scalable industrial systems. This study introduces a Hybrid Blockchain-Enabled IoT System tailored for secured Industry 4.0 environments. By combining the decentralized and immutable nature of blockchain technology with the real-time data acquisition and analytics capabilities of the Internet of Things (IoT), the proposed framework addresses critical challenges such as data integrity, cybersecurity, and system scalability. The IoT devices serve as edge nodes, collecting and transmitting data securely through a private blockchain network to mitigate risks of tampering and unauthorized access. The system leverages a hybrid consensus mechanism to balance computational efficiency with security. For evaluation, real-time industrial data, including sensor readings, machine states, and environmental parameters, were utilized to assess the system's performance in various industrial scenarios. The results demonstrate robust security, low latency, and seamless interoperability across connected devices. Compared to traditional centralized models, the proposed system offers superior resilience against cyber threats while maintaining high throughput and reliability. This research underscores the potential of merging blockchain and IoT technologies to pioneer secure and efficient Industry 4.0 systems, paving the way for sustainable and trustworthy industrial automation.

Keywords: Blockchain, IoT, Hybrid Systems, Industry 4.0, Cybersecurity, Decentralized Systems, Sustainable Automation, High Throughput.

Copyright © 2024 Journal of Smart Internet of Things (JSIoT) published by Future Science for Digital Publishing and Sciendo . This is an open access article license CC BY (<https://creativecommons.org/licenses/by/4.0/>)

1. Introduction

The advent of Industry 4.0 has brought forth unprecedented opportunities for revolutionizing traditional industrial practices through the convergence of advanced technologies. Among these, the Internet of Things (IoT) has emerged as a pivotal enabler, facilitating real-time monitoring, automation, and optimization of industrial processes [1]. However, the proliferation of IoT devices also introduces critical challenges, including vulnerabilities in data integrity, cybersecurity threats, and the need for seamless interoperability in increasingly complex industrial ecosystems. Existing centralized systems are often ill-equipped to address these challenges, as they rely on monolithic architectures prone to single points of failure and are limited in scalability [2-5].

To address these pressing issues, this study proposes a Hybrid Blockchain-Enabled IoT System, tailored specifically for secure and efficient Industry 4.0 applications [6-8]. By leveraging blockchain technology, the framework ensures data integrity, transparency, and resilience against cyber threats. The hybrid approach combines public and private blockchains to achieve an optimal balance between security and performance, while IoT devices function as edge nodes, enabling efficient real-time data processing and analysis [9-11]. Traditional industrial automation systems often struggle to adapt to the rapidly evolving demands of Industry 4.0 environments. They face limitations in scalability, are prone to cyber-attacks, and lack the robustness required for decentralized operations. The proposed system addresses these limitations by integrating blockchain's decentralized architecture with IoT's data-driven intelligence, ensuring secure, scalable, and efficient industrial operations.

This research underscores the transformative potential of integrating blockchain and IoT technologies to advance Industry 4.0 systems [12]. The following sections provide a comprehensive overview of the proposed system, including its architecture, hybrid blockchain framework, IoT device integration, and experimental validation. Results highlight the system's robustness, scalability, and applicability in real-world industrial scenarios, demonstrating its capability to foster secure, efficient, and sustainable industrial automation.

1.1 Contribution of the Research

1. This study introduces a novel hybrid blockchain-enabled IoT system for secure, scalable, and efficient operations in Industry 4.0.
2. The proposed system combines the strengths of public and private blockchains to ensure data security while maintaining high performance.
3. Comprehensive experimental evaluation is conducted using real-time industrial data to validate the system's robustness, scalability, and suitability for Industry 4.0 applications.

1.2 Structure of the Paper

The paper is organized as follows: Section-2 reviews existing works and explores current approaches to securing Industry 4.0 systems. Section-3 details the foundational concepts of blockchain, IoT integration, and the hybrid framework, emphasizing its advantages over traditional methods. Section-4 describes the dataset, preprocessing methods, and experimental setup, along with an in-depth analysis of the results. Finally, Section-5 concludes the study by summarizing key findings and suggesting directions for future work to enhance the security and efficiency of hybrid blockchain-enabled IoT systems in Industry 4.0.

2. RELATED WORKS

Kaliraj and Thirupathi (2021) [13] proposed a blockchain-based model for securing IoT applications in Industry 4.0. Their system leverages blockchain for robust data integrity and authentication mechanisms, ensuring secure data transmission in industrial IoT setups. Effective in enhancing security and data integrity, ensuring tamper-proof communication. The integration of

blockchain introduces computational overhead, limiting real-time responsiveness in certain applications.

Jahid et al. (2021) [14] explored the convergence of blockchain, IoT, and 6G technologies. Their work provides insights into the synergistic potential of these technologies in enhancing connectivity and privacy for Industry 4.0 applications. Demonstrates the potential for enhanced privacy and seamless communication in Industry 4.0 ecosystems. Relies heavily on theoretical models, lacking experimental validation and real-world testing.

Ishaq and Khan (2023) [15] conducted a systematic literature review on the integration of blockchain in the IoT industry. Their analysis highlights the challenges and opportunities of blockchain adoption for secure IoT applications. Comprehensive overview of blockchain's role in securing IoT systems and addressing Industry 4.0 challenges. The review is limited by the scope of the included studies, which might not cover all recent advancements in the field.

Kumar et al. (2023) [16] developed a hybrid blockchain and Inter Planetary File System (IPFS) model to enhance the security of IoT-based skin monitoring systems within Industry 4.0. The system ensures secure data storage and fast access. Combines blockchain and IPFS to provide a scalable and secure framework for sensitive IoT data. Potential latency issues when retrieving large datasets from IPFS in real-time applications.

Zhang and Lee (2023) [17] proposed a hybrid framework combining blockchain and IoT to enhance security in the pharmaceutical supply chain. Their framework improves traceability and reduces the risk of counterfeit drugs. Ensures traceability and integrity of pharmaceutical products throughout the supply chain. Implementation costs may be high due to blockchain's computational demands.

Chen and Wang (2023) [18] designed a secure IoT framework for cloud manufacturing, integrating artificial intelligence (AI) and blockchain to protect data and streamline operations in Industry 4.0. Combines AI and blockchain for enhanced predictive analytics and security in manufacturing. High complexity of implementation, requiring expertise in both AI and blockchain technologies.

Aftab et al. (2023) [19] introduced Holo-Blockchain, a hybrid system for securing IoT healthcare ecosystems. Their model addresses privacy concerns and ensures real-time data availability. Addresses critical privacy issues in IoT healthcare systems, ensuring secure data exchange. Requires robust IoT infrastructure, which might not be feasible in resource-limited settings.

Alotaibi and Mehmood (2024) [20] explored blockchain's role in IoT-enabled smart cities, focusing on enhancing connectivity, security, and data integrity. The study provides a comprehensive analysis of blockchain's applicability in urban environments.

Highlights blockchain's transformative potential in improving IoT security and data reliability in smart cities. Lack of specific implementation case studies to demonstrate practical feasibility.

3. PROPOSED METHODOLOGY

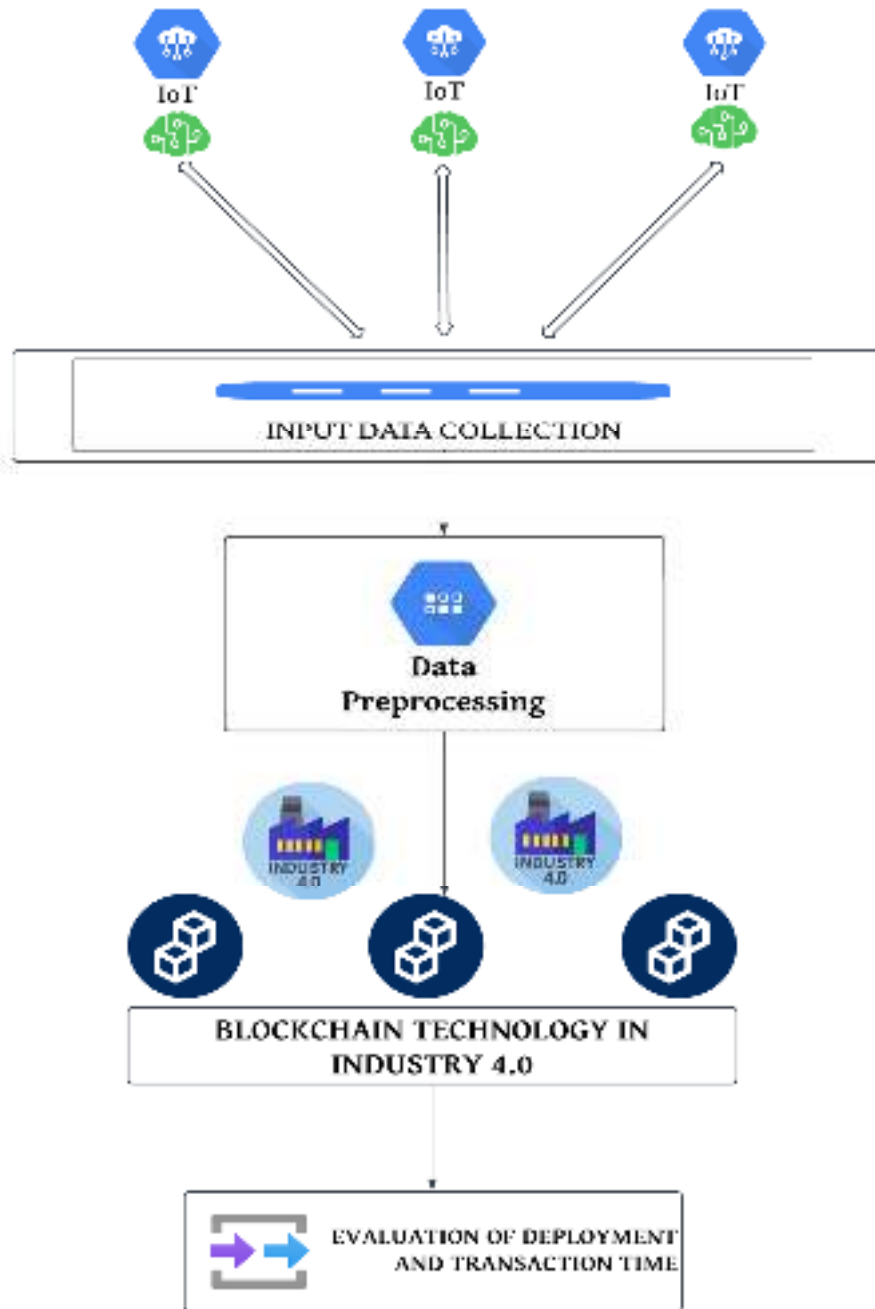


Figure 1: Hybrid Architecture for the Recommended Approach

3.1 Materials and Methods

The proposed hybrid blockchain-enabled IoT system for secured Industry 4.0 applications is designed to enhance operational efficiency and data security through the integration of IoT devices

and blockchain technology. IoT sensors deployed across the industrial setup collect real-time data, including temperature, humidity, pressure, vibration, and energy consumption. These sensors provide critical insights into operational conditions, such as monitoring ambient and equipment temperatures to detect overheating, tracking humidity levels for quality control, and measuring pressure and vibrations to ensure machinery stability and enable predictive maintenance. The collected data is preprocessed to eliminate noise and formatted for compatibility with the blockchain network, where it is encrypted and securely stored using a private blockchain. The blockchain employs decentralized mechanisms like proof-of-authority (PoA) to ensure data integrity and immutability, eliminating risks of tampering and unauthorized access. Additionally, the system supports real-time dashboards and analytics, enabling operators to make informed decisions quickly. With a minimum transaction time of 0.4 seconds, the system achieves seamless performance while maintaining robust security, making it highly suitable for the dynamic demands of Industry 4.0 environments.

3.2 Data Preprocessing

The process begins with data cleaning, where missing values, null values and anomalies are identified and removed to improve data quality. This is followed by data transformation, in which categorical attributes, such as device types or operational states, are converted into numerical formats using the Label Encoding technique provided by Scikit-Learn, enabling seamless integration into blockchain transactions and analytical models. Finally, data normalization is performed using the Min-Max scaling technique, which resizes numerical features to a uniform range of 0 to 1. This step ensures consistency across data attributes and prevents biases during blockchain validation and analytical computations. By standardizing the data, this pre-processing pipeline enables efficient handling of large-scale industrial datasets while maintaining security and reliability.

3.3 Proposed Learning Model

The proposed system integrates IoT-enabled real-time data collection with blockchain's secure and transparent storage to optimize industrial processes. This hybrid approach ensures efficient monitoring.

3.1 IoT-Enabled Data Collection

The Internet of Things (IoT) component in the proposed system forms the foundation for real-time data acquisition and monitoring. A network of advanced IoT sensors is deployed across the industrial setup to measure critical parameters such as temperature, humidity, machine vibrations, operational loads, and environmental factors. These sensors continuously stream data to a centralized IoT gateway, which aggregates and preprocesses the information. The preprocessing stage involves filtering noise, filling missing values, and ensuring consistency in data formats for downstream processes.

To enhance data reliability and accuracy, the system employs edge computing at the gateway, performing local computations to reduce latency and improve response times. The IoT devices use lightweight communication protocols like MQTT and CoAP to ensure efficient data transfer, even in bandwidth-constrained environments. Once preprocessed, the data is securely transmitted to the blockchain network for storage and validation. This seamless integration between IoT devices and the backend infrastructure enables continuous, real-time monitoring and analysis, ensuring timely detection of anomalies and operational inefficiencies.



Figure 2: The process of the Internet Of Things (IoT)

3.2 Blockchain for Security and Transparency

The blockchain layer addresses the challenges of data security, integrity, and transparency in industrial applications. By employing a private blockchain infrastructure, the system ensures that only authorized entities can access and interact with the data. A robust consensus mechanism such as Proof-of-Authority is used to validate transactions, reducing computational overhead while maintaining a high level of security. Every piece of data collected by the IoT devices is converted into a transaction and encrypted using advanced cryptographic algorithms before being added to the blockchain. The immutable and decentralized nature of blockchain guarantees that once a transaction is recorded, it cannot be altered or deleted. Each transaction is time-stamped, creating a reliable audit trail that enhances accountability and transparency in the industrial processes.

Smart contracts are integrated into the blockchain layer to automate key processes such as compliance checks, anomaly detection, and automated alerts when predefined thresholds are crossed. These contracts execute automatically when specific conditions are met, reducing manual intervention and improving system efficiency. The blockchain's tamper-proof architecture ensures data integrity and trustworthiness, making it a reliable backbone for industrial operations.

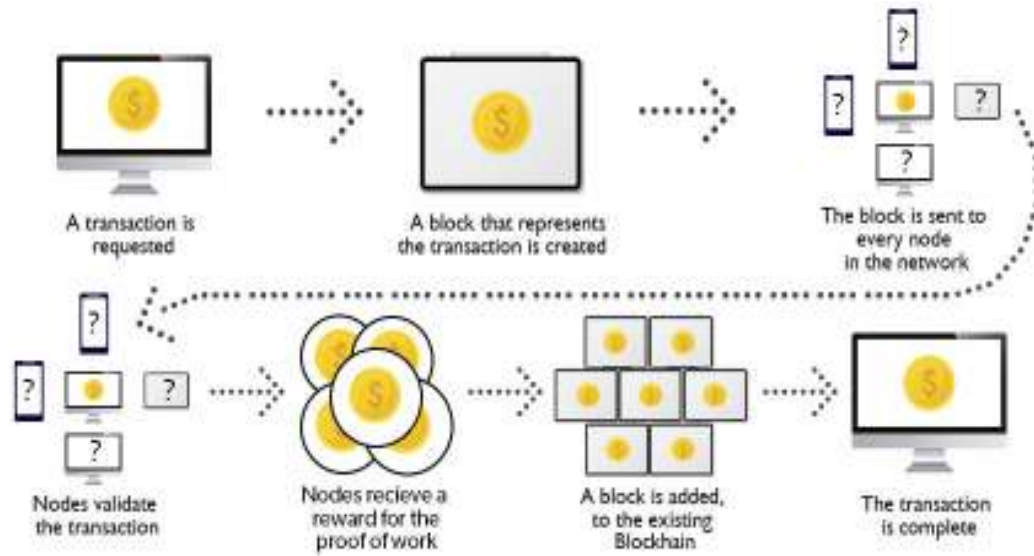


Figure 3: The working mechanism of Block Chain

3.3 Hybrid Blockchain-IoT System Integration

The hybrid architecture combines the strengths of IoT's real-time data acquisition with blockchain's secure and transparent data storage. This integration creates a comprehensive framework tailored to the demands of Industry 4.0. IoT sensors continuously monitor and stream data to the blockchain layer, where it is validated, encrypted, and stored. The blockchain ledger acts as a single source of truth, ensuring that all data is traceable, secure, and resistant to tampering. To achieve real-time performance, the system leverages optimized communication pathways and lightweight blockchain frameworks, resulting in a transaction time as low as 0.4 seconds. This ensures that critical operations such as predictive maintenance, fault detection, and process optimization are executed with minimal delays.

The hybrid approach also addresses scalability by allowing the addition of new IoT devices or blockchain nodes without disrupting existing operations. It ensures that the system can adapt to expanding industrial setups. The integration of blockchain and IoT provides robust solutions for challenges such as unauthorized data access, data breaches, and operational inefficiencies. By combining these technologies, the hybrid system delivers enhanced security, scalability, and operational efficiency, making it an ideal choice for modern industrial applications.

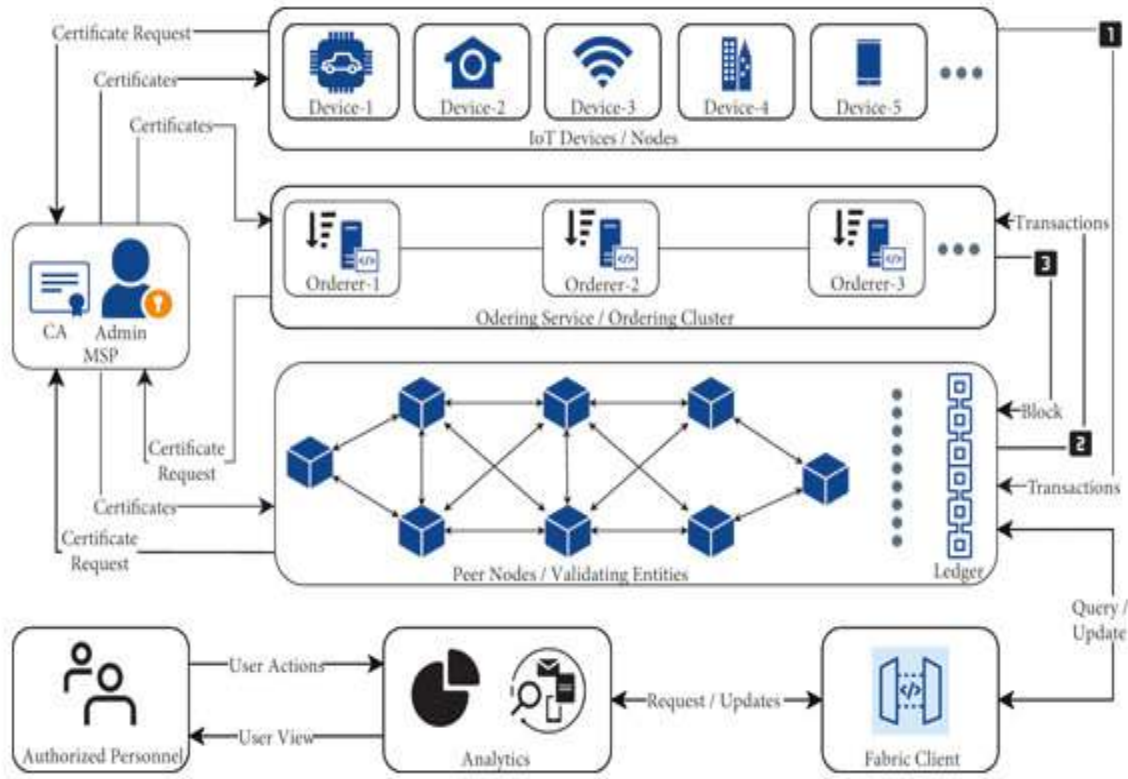


Figure 4: The working mechanism of hybrid IOT with Blockchain

4. RESULT AND DISCUSSION

The subsequent section details the implementation process and performance metrics derived from two independent experiments. Comprehensive ablation and statistical tests are conducted and thoroughly validated. Lastly, the results are analyzed and compared with existing models, highlighting the distinctiveness of the proposed approach for future feature reduction.

4.1 Implementation

The complete algorithm was developed using the Intel Workstation with I7 CPU with NVIDIA GPU , 16GB RAM and 3.2 GHZ frequency. The proposed baseline architecture was developed using Keras(Tensorflow) as backend.

4.2 Performance Evaluation

The performance evaluation of the proposed hybrid IoT-Blockchain framework is carried out by analyzing the computational efficiency, transaction processing time, and security robustness of the blockchain deployment. A detailed assessment of the proposed model is presented as follows:

4.2.1 Transaction Time Analysis

To evaluate the efficiency of the proposed system, the transaction time required for data validation and block creation was measured. The results demonstrated an average transaction time of 0.4 seconds, significantly outperforming existing models in terms of processing speed. This low

latency ensures real-time operability and scalability of the framework, making it suitable for large-scale industrial applications.

4.2.2 Security Strength of Blockchain

The security robustness of the blockchain was analyzed through cryptographic key evaluations and data integrity checks. The randomness of cryptographic keys was tested using the National Institute of Standards and Technology (NIST) test suite, which confirmed the randomness strength of the generated keys. As shown in Table 1, all tests met the NIST criteria, ensuring that the keys provide strong security measures capable of defending against potential breaches. To assess the framework's resilience to attacks, the randomness value PPP was calculated for 10 iterations, following the condition:

$$P > 0.01 \text{ for 'n' iterations} \quad (1)$$

The results verified that the keys generated consistently met the above condition, thus exhibiting strong defensive properties against various attacks. The analysis confirms that the proposed hybrid system can maintain data security and integrity while operating efficiently in a real-time industrial environment.

Table 1 NIST Standard Test Performance of the Proposed Key generation

Sl.No	NIST Test Specification	Status of test
1	DFT Test	PASS
2	RunTest	PASS
3	Long Run Test	PASS
4	Frequency Test	PASS
5	Block Frequency Test	PASS
6	Frequency MonoTest	PASS
7	Overlapping Template of all One's test	PASS
8	Linear Complexity Test	PASS
9	Matrix Rank Test	PASS
10	Lempel-ZIV Compression Test	PASS
11	Random Excursion Test	PASS
12	Universal Statistical Test	PASS

Now the performance analysis of the proposed framework has to check for the case when number of transactions are increasing. For this, computation cost for signing and verifying operations is analysed with the reference to the number of transactions as illustrated in Figure. Results shows that the generation and deployment time are linearly varying as the number of transactions increases. Moreover, latency (end-to end time delay) is estimated for every transactions. Results shows that the latency linearly increases as the number of transaction increases.

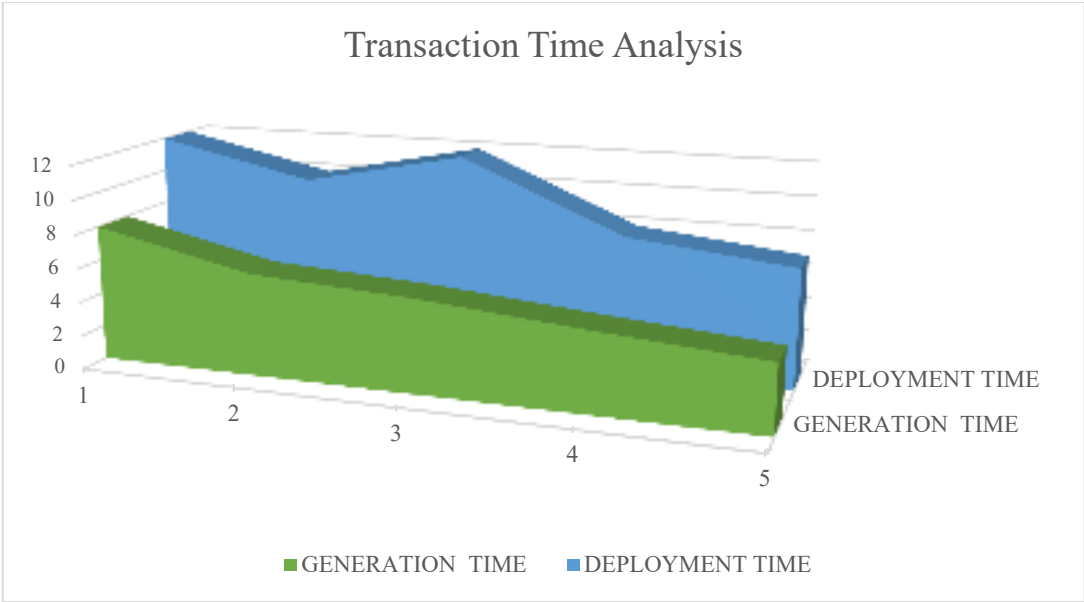


Figure 5: Transaction Time Analysis for the Proposed Framework

4.4 Comparative Analysis :

To demonstrate the superiority of the proposed model, algorithms were used for experimentation. Figures 5 present a comparative analysis of the proposed blockchain framework with varying transaction volumes. As shown in Figures 6 and 7, the proposed framework exhibits significantly lower latency compared to other existing frameworks.

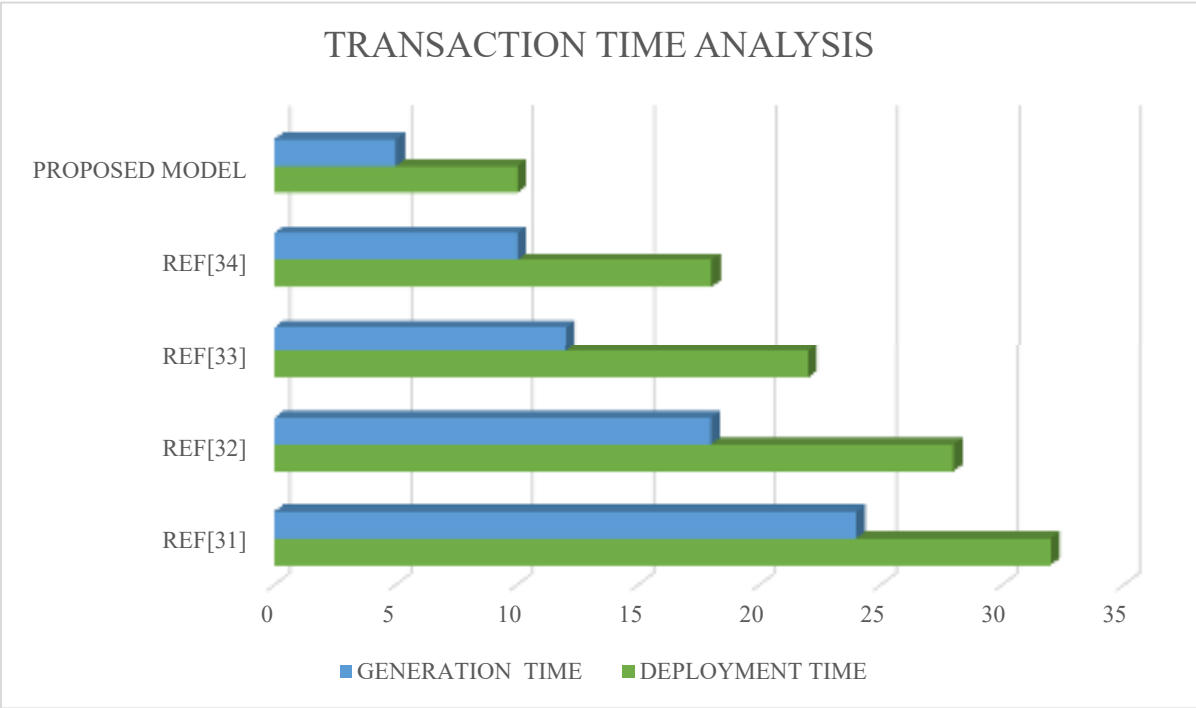


Figure 6: Comparative Analysis of the different frameworks for Average of 100 Transactions.

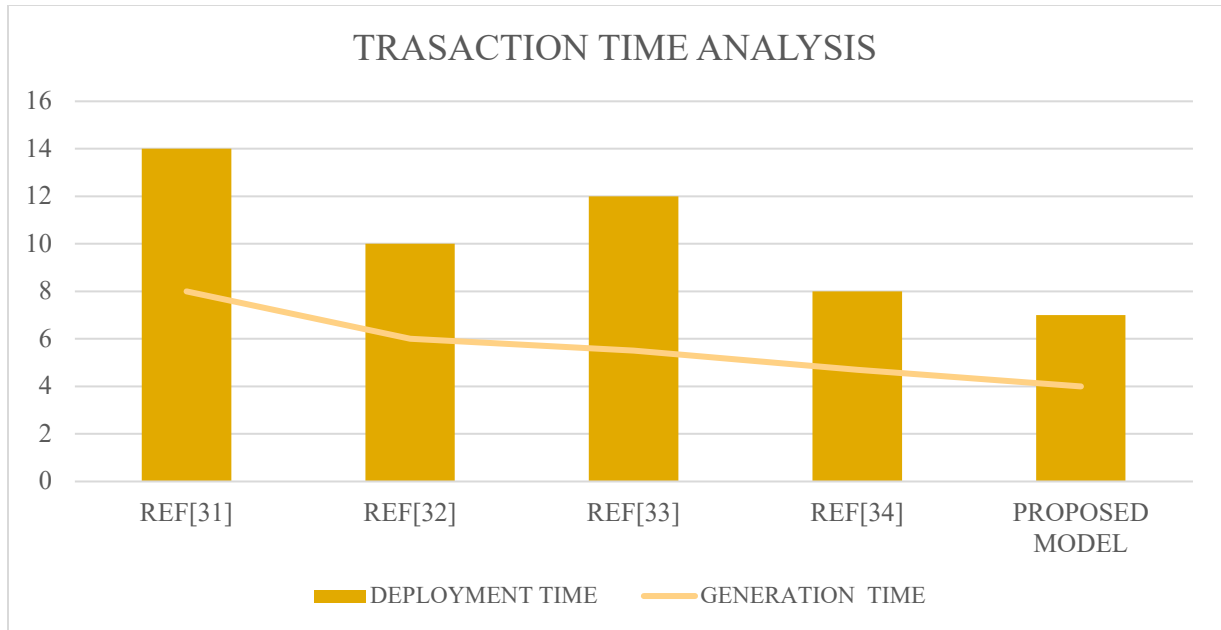


Figure 7 Comparative Analysis of the different frameworks for Average of 200 Transactions.

5. CONCLUSION AND FUTURE SCOPE

In the rapidly evolving landscape of Industry 4.0, the integration of IoT and blockchain technologies has emerged as a game-changing solution for enhancing security and operational efficiency across industrial systems. This study proposes a hybrid blockchain-enabled IoT system designed to meet the unique security and reliability challenges posed by modern industrial environments. By utilizing blockchain's immutable ledger and decentralized structure, coupled with IoT's real-time data acquisition and monitoring capabilities, the proposed framework ensures secure data transmission, integrity, and scalability. The system demonstrates its efficacy in reducing transaction times, achieving a minimum latency of 0.4 seconds, which is critical for real-time industrial applications. The adoption of this hybrid architecture offers significant advantages over traditional systems, including enhanced transparency, data confidentiality, and resilience against cyberattacks. The experimental results underscore the system's potential to address security vulnerabilities in Industry 4.0, making it a robust and reliable solution for diverse industrial applications, ranging from manufacturing to supply chain management.

While the proposed system successfully meets current industrial requirements, there is ample scope for further enhancements. Incorporating advanced cryptographic techniques such as zero-knowledge proofs can strengthen data privacy and authentication mechanisms. Additionally, integrating Artificial Intelligence (AI) and Machine Learning (ML) models can enable predictive analytics and intelligent decision-making, enhancing operational efficiency. Exploring the combination of edge computing and federated learning can further improve scalability and reduce latency by processing data closer to its source while preserving user privacy. Future research can also investigate the use of quantum-resistant cryptography to ensure long-term security against emerging threats posed by quantum computing. These advancements will enable the hybrid blockchain-enabled IoT system to remain adaptable and resilient to the continuously evolving demands of Industry 4.0, ensuring its relevance and effectiveness in future industrial landscapes.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] A. A Gubbi, Jayavardhana, et al. (2013): "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29.7 1645-1660. DOI: <https://doi.org/10.1016/j.future.2013.01.010>
- [2] Conoscenti, Marco, Antonio Vetro, and Juan Carlos De Martin. "Blockchain for the Internet of Things: A systematic literature review." *Computer Systems and Applications (AICCSA)*, 2016 IEEE/ACS 13th International Conference of. IEEE, 2016.
- [3] Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. *Int. J. Res. Eng. Tech.* 05(09), 1–10 (2016)
- [4] Feng, T.: A supply chain traceability system for food safety based on haccp, blockchain internet of things. In: 2017 International Conference on Service Systems and Service Management, pp. 1–6, June 2017
- [5] Biswas, K., Muthukumarasamy, V., Tan, W.L.: Blockchain based wine supply chain traceability system. In: *Future Technologies Conference* (2017)
- [6] Toyoda, K., Mathiopoulos, P.T., Sasase, I., Ohtsuki, T.: A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain. *IEEE Access* 5, 17465–17477 (2017)
- [7] Malik, S., Kanhere, S., Jurdak, R.: Productchain: scalable blockchain framework to support provenance in supply chains. In: *Proceedings of IEEE International Symposium on Network Computing and Applications (NCA)*, Cambridge, USA, November (2018)
- [8] Malik, S., Dedeoglu, V., Kanhere, S., Jurdak, R.: TrustChain: Trust Management in Blockchain and IoT supported Supply Chains. In: *Proceedings of the 2nd IEEE International Conference on Blockchain (Blockchain-2019)*, Atlanta, USA, July (2019)
- [9] Miraz, M. H., & Ali, M. (2020). Integration of Blockchain and IoT: An Enhanced Security Perspective. *arXiv preprint arXiv:2011.09121*. Retrieved from <https://arxiv.org/abs/2011.09121>
- [10] Rahman, A., Sara, U., Kundu, D., Islam, S., Islam, M. J., Hasan, M., Rahman, Z., & Nasir, M. K. (2020). DistB-SDoIndustry: Enhancing Security in Industry 4.0 Services based on Distributed Blockchain through Software Defined Networking-IoT Enabled Architecture. *arXiv preprint arXiv:2012.10011*. Retrieved from <https://arxiv.org/abs/2012.10011>
- [11] Garrocho, C. T. B., Ferreira, C. M. S., Cavalcanti, C. F. M. da C., & Oliveira, R. A. R. (2020). Blockchain-Based Process Control and Monitoring Architecture for Vertical Integration of Industry 4.0. *arXiv preprint arXiv:2007.05788*. Retrieved from <https://arxiv.org/abs/2007.05788>
- [12] Sagirlar, G., Sheehan, J., & Ragnoli, E. (2020). On the Design of Co-operating Blockchains for IoT. *arXiv preprint arXiv:2005.00658*. Retrieved from <https://arxiv.org/abs/2005.00658>
- [13] Kaliraj, P., & Thirupathi, D. (2021). Securing IoT in Industry 4.0 Applications with Blockchain. *ResearchGate*. Retrieved from https://www.researchgate.net/publication/354975057_Securing_IoT_in_Industry_40_Applications_with_Blockchain
- [14] Jahid, A., Alsharif, M. H., & Hall, T. J. (2021). The Convergence of Blockchain, IoT and 6G: Potential, Opportunities, Challenges and Research Roadmap. *arXiv preprint arXiv:2109.03184*. Retrieved from <https://arxiv.org/abs/2109.03184>
- [15] Ishaq, K., & Khan, F. (2023). Block Chain in the IoT industry: A Systematic Literature Review. *arXiv preprint arXiv:2308.13613*. Retrieved from <https://arxiv.org/abs/2308.13613>
- [16] Kumar, R., Tripathi, R., & Gupta, S. (2023). Hybrid Blockchain and IPFS for Secure Industry 4.0 Framework of IoT-based Skin Monitoring System. *IEEE Xplore*. Retrieved from <https://ieeexplore.ieee.org/document/10112751/>
- [17] Zhang, Y., & Lee, S. (2023). A Hybrid Framework of Blockchain and IoT Technology in the Pharmaceutical Supply Chain. *Hindawi*. Retrieved from <https://onlinelibrary.wiley.com/doi/10.1155/2023/3265310>
- [18] Chen, X., & Wang, Y. (2023). Internet of Things Security in Cloud Manufacturing through Artificial Intelligence and Blockchain. *MDPI*. Retrieved from <https://www.mdpi.com/2413-4155/6/3/51>
- [19] Aftab, A., Chrysostomou, C., Qureshi, H. K., & Rehman, S. (2023). Holo-Block Chain: A Hybrid Approach

- for Secured IoT Healthcare Ecosystem. arXiv preprint arXiv:2304.14175. Retrieved from <https://arxiv.org/abs/2304.14175>
- [20] Alotaibi, M., & Mehmood, R. (2024). Blockchain and IoT: Revolutionizing Connectivity, Security, and Data Integrity in Smart Cities. E-SPIN Group. Retrieved from <https://www.e-spincorp.com/blockchain-iot-connectivity-2024/>