Anusandhanvallari
Vol 2024, No.1
July 2024
ISSN 2229-3388

Energy-Efficient Edge Computing Framework for Internet of Things (IoT) Networks

[1]Dr. Ashwini Vikas Ghogare, **[2]Dr. Diwakar Ramanuj Tripathi**

[1]Shubhashree woods, Pimple Saudagar, Pune

[2]Head, Department of Computer Science,

S.S. Maniar College of Computer & Management, Nagpur

Abstract

The increased growth of Internet of Things (IoT) devices in the healthcare field, in urban development, in industrial automation, and in supply chain management, has presented urgent security issues, including unauthorized access, information tampering, privacy loss, and single points of failure, that are usually not considered by traditional security tools because of distributed and resource-constrained IoT networks. The paper explores the blockchain technology as a powerful security architecture to the IoT and follows the descriptive-analytical research method and uses a Python-based simulation, which was run on Google Colab. The simulation combined real-time streams of IoT sensors with a proof-of-work consensus mechanism and HMAC-based device verification of authenticating the devices to assess the main metrics including transaction latency, throughput, data immutability, tamper detection, and system reliability under the conditions of diverse operational conditions. According to the results of the experiment, blockchain can boost the security of IoT by providing data immutability, decentralized trust, and automatic verification and is able to identify malicious manipulations of data. When comparing the performance to a baseline system (no-chain) it is apparent that, despite the blockchain causing quantifiable latency overheads through consensus and cryptographic functionality, the end-to-end delay is relatively small in most IoT applications. The results also point to practical implementation aspects, such as the limitations of scalability and energy usage, which indicate that hybrid solutions that combine lightweight consensus mechanism and off-chain storage can be the best option.

Keywords: Blockchain, Internet of Things (IoT), Security, Tamper Detection, Proof-of-Work, HMAC Authentication.

1. Introduction

Internet of Things (IoT) has become one of the prerequisites of the current digital transformation process that allows the exchange of data between billions of devices in different fields unimpeded and without any distraction. It is used in healthcare, logistics, smart cities, industrial automation, energy management and agriculture and can provide previously unimaginable opportunities of operational efficiency, real-time monitoring, predictive maintenance, and data-driven decision-making. On one hand, IoT enables organizations to make the most of a limited number of resources, minimize operational expenses, improve service provision, and derive actionable insights out of big datasets by enabling the flow of information between devices without interruption. The possibilities of the IoT to reshape various industries and enhance the overall efficiency are highly acknowledged, which makes this technology one of the enabling factors of the new generation of smart systems and intelligent infrastructures.

The open, general interconnectedness and distributed character of IoT systems creates severe security risks despite its transformative potential. Most IoT infrastructures are extremely centralized, either based on cloud-based servers or centralized gateways, putting them at risk of data breaches, denial-of-service (DoS) attacks, unauthorized control of devices, identity spoofing, and single point of failure. Mainstream security tools, such as access control lists, firewalls, and centralized authentication servers, are not always able to offer all-encompassing defense against advanced attacks that take advantage of the scale, heterogeneity, and geographical distributed nature of IoT networks. These weaknesses highlight why novel security frameworks are necessary, which can guarantee secure, reliable, and tamper-resistant communication among the IoT devices.

Initially created as a system to support cryptocurrencies, blockchain technology has become a good option to overcome these security challenges of the IoT. Its main properties immutability, decentralization, cryptographic integrity and distributed consensus allow the creation of tamper-proof and transparent data management structures in IoT ecosystems. Using the concept of blockchain, the IoT device is able to communicate via information exchange at verifiable integrity and through smart contracts, automated enforcement of security policy, access control and trust relations may be enforced without centralized intermediaries. Besides decreasing reliance on third-party authorities, this strategy will help improve system resilience, reduce the risks of unauthorized access and data manipulating, and increase the overall trust of the work. Consequently, blockchain can be used to offer a scalable, reliable, and secure base of next-generation IoT deployments, creating strong and dependable digital infrastructures with the ability to support complex, real-time, and mission-critical applications.

1.1. Challenges in Blockchain Integration

Although integrating blockchain into IoT environments offers significant security and operational benefits, it also introduces several critical challenges that must be carefully addressed to ensure effective deployment. One of the primary issues lies in the consensus mechanisms that underpin blockchain security, such as Proof-of-Work (PoW) and Proof-of-Stake (PoS). These mechanisms are essential for establishing trust, verifying transactions, and maintaining the integrity of the distributed ledger. However, they come with substantial computational and energy costs. For instance, in PoW systems like Bitcoin, mining requires solving complex cryptographic puzzles, which consumes significant processing power and electricity. Such resource-intensive operations are largely incompatible with most IoT devices, which are typically constrained in terms of processing capability, memory, and battery life. While PoS reduces energy consumption compared to PoW, it may still present performance bottlenecks, particularly in large-scale IoT deployments with millions or billions of connected devices.

Another significant challenge arises from the distributed nature of blockchain data replication. To maintain transparency, immutability, and fault tolerance, blockchain networks replicate data across multiple nodes. While this enhances data integrity and ensures that no single point of failure can compromise the system, it also dramatically increases storage requirements and network bandwidth consumption. This is particularly problematic for IoT devices, such as sensors and edge devices, which often have limited storage, intermittent connectivity, and constrained processing resources, making continuous blockchain synchronization both challenging and resource-intensive.

Scalability presents an additional critical concern. IoT networks generate enormous volumes of high-frequency data streams, often in real time. Traditional blockchain architectures, designed for lower transaction throughput, struggle to efficiently process these large data volumes. This can result in delays during transaction validation, increased propagation times between nodes, and network bottlenecks that reduce overall responsiveness. Finally, interoperability issues further complicate blockchain deployment in IoT ecosystems. IoT networks consist of heterogeneous devices operating on a variety of protocols, data formats, and communication standards. Ensuring that these diverse devices can seamlessly interface with a blockchain framework requires careful standardization, protocol adaptation, and sometimes the use of middleware or translation layers. Addressing these challenges is

crucial for enabling practical, scalable, and energy-efficient blockchain-enabled IoT systems that retain the technology's security benefits while remaining operationally viable.

2. Literature Review

Christidis and Devetsikiotis (2016) presented an opportunity to investigate the potential of blockchain technology and smart contracts. They established a foundation for trustless Internet of Things ecosystems by demonstrating that automated contracts that execute themselves could permit secure and dependable machine-to-machine interactions without relying on centralized authority. According to the findings of their research, smart contracts have the capability to incorporate predetermined rules and conditions directly into the blockchain. This enables devices to perform transactions automatically after the circumstances have been met, hence decreasing the need for human interaction. The implementation of this strategy not only improved the openness and accountability of the transactions, but it also reduced the risks that are associated with centralized control, such as the presence of single points of failure and the vulnerability to malicious attacks.

Dorri et al. (2017) expanded upon by the proposal of a lightweight blockchain protocol that was developed primarily for Internet of Things devices that have limited resources. Through their demonstration, they demonstrated that blockchain technology has the potential to maintain the integrity of data in smart home applications while simultaneously reducing the computational and energy overhead that is often associated with traditional blockchain systems. According to the findings of their research, traditional blockchain architectures, such as those utilized in cryptocurrency networks, are frequently too resource-intensive for Internet of Things environments. This is because Internet of Things devices frequently operate with limited computer processing power, memory, and battery life. Dorri et al. proved that blockchain technology could be modified to perform effectively in such limited circumstances without compromising security or transparency. This was accomplished by introducing protocols that were optimized and consensus processes that were simplified.

Conoscenti et al. (2018) accessed management, secure data sharing, and identity authentication were some of the categories that were identified after conducting a comprehensive analysis of blockchain–Internet of Things frameworks which were then classified. Through their analysis, they demonstrated that decentralized ledger technologies have the potential to offer strong solutions across a wide range of application areas. This was accomplished by highlighting the versatility of blockchain technology in addressing numerous dimensions of Internet of Things (IoT) security. To be more specific, they stressed that access management that is provided by blockchain technology might ensure secure device authentication and authorization, hence minimizing the danger of unauthorized access to Internet of Things networks. In terms of data sharing, their research demonstrated how blockchain technology might protect the integrity and security of sensitive information while simultaneously enabling authorized devices or users to access data in a transparent manner.

Ali et al. (2021) assessed thorough investigation of the various possibilities of blockchain technology within the Internet of Things (IoT), with a special emphasis on improving both privacy and security aspects of the technology. The researchers demonstrated that blockchain technology has the potential to successfully secure the authenticity and integrity of data generated by the Internet of Things (IoT), hence effectively avoiding unwanted manipulation and tampering. This was accomplished through an exhaustive study of current literature and empirical case studies. Furthermore, the inherent openness and immutability of blockchain technology make it possible to conduct audits in a reliable manner, which enables stakeholders to do transactions verification and tracking in a decentralized manner. The survey highlighted practical implementations across multiple Internet of Things domains, such as healthcare, where sensitive patient data must remain secure; industrial automation, where real-time operational

data integrity is critical; and smart home environments, where user privacy and device interoperability are the most important priorities.

3. Research Methodology

The purpose of this research is to investigate the feasibility of blockchain technology as a platform for providing a secure environment for Internet of Things (IoT) environments. The adoption of a methodological approach that blends theoretical analysis with practical experimentation was the means by which this objective was accomplished. The research technique was developed with the intention of making a methodical investigation into the ways in which blockchain technology might improve Internet of Things (IoT) security, preserve data integrity, and impact system performance. A thorough and controlled framework for evaluating the viability and limitations of blockchain technology in resource-constrained Internet of Things scenarios is provided by the study. This framework is achieved by integrating the insights gained from the literature review with simulation-based modelling.

3.1. Research Design

In order to examine blockchain as a secure framework for Internet of Things applications, this study utilized a descriptive–analytical research design, which integrated both theoretical insights and practical testing. The architecture was chosen to provide a thorough understanding of the function that blockchain plays in improving the security of the internet of things (IoT), while also taking into account the possibility of empirical validation through simulation. The conceptual underpinning was provided by secondary data derived from literature that had been subjected to peer review. This data served as a guide for the development of the simulation framework and the selection of key variables. Python-based simulation experiments were carried out, which made it possible to undertake controlled analyses of the influence that blockchain technology has on the security, performance, and data integrity of the Internet of Things (IoT) under actual operating circumstances.

3.2. Simulation Framework

A bespoke blockchain model was developed using Python on Google Colab in order to investigate the incorporation of blockchain technology into Internet of Things (IoT) applications. A low-difficulty Proof-of-Work (PoW) technique was utilized by the blockchain in order to guarantee security while preserving computational feasibility. This resulted in the creation of a tamper-resistant ledger for data created by the Internet of Things (IoT). The temperature, humidity, and pump condition values were replicated using virtual Internet of Things sensors, and each measurement was logged as a blockchain transaction. Security was maintained by use of HMAC-based device signatures, which limited the submission of transactions to just those devices that were appropriately authorized. In order to analyze the performance of the system, latency was compared to a baseline that did not utilize blockchain technology. Additionally, security was validated by modifying blocks on purpose in order to verify the blockchain's capacity to detect tampering and maintain data integrity.

3.3. Variables Analysed

The study focused on three primary variables:

- Security Impact: Measured as the system’s ability to detect malicious tampering and maintain authenticity of IoT data.
- Performance Impact: Assessed through the mean write latency (in milliseconds) of blockchain transactions compared with baseline operations.

- IoT Data Integrity: Verified by evaluating the immutability of sensor values stored across the blockchain ledger.

3.4. Data Collection and Analysis

A total of fifty simulated Internet of Things readings were processed through the blockchain system in order to evaluate the latter's capabilities in terms of both operational performance and security. For the purpose of ensuring that the simulation accurately reflected the data flows that occur in the real world, each simulated reading, which represented data from virtual Internet of Things sensors, was handled as if it were a separate blockchain transaction. A structured CSV ledger was used to record each block as it was formed. This ledger was used to store essential metadata, including timestamps, transaction hashes, device identifiers, and cryptographic signatures. This systematic recording made it possible to keep track of all blockchain operations in a comprehensive manner and offered a solid foundation for subsequent analysis.

Table 1: Summary of Research Methodology

Component	Approach / Details
Research Design	Descriptive–analytical (literature + simulation)
Blockchain Protocol	Proof-of-Work (difficulty = 2)
IoT Devices Simulated	Temperature, Humidity, Pump status
Authentication Mechanism	HMAC-based device signatures
Data Collected	50 simulated IoT readings
Key Variables	Security, Performance, Data Integrity
Analytical Tools	Tables, Graphs (latency, verification, sensor data analysis)

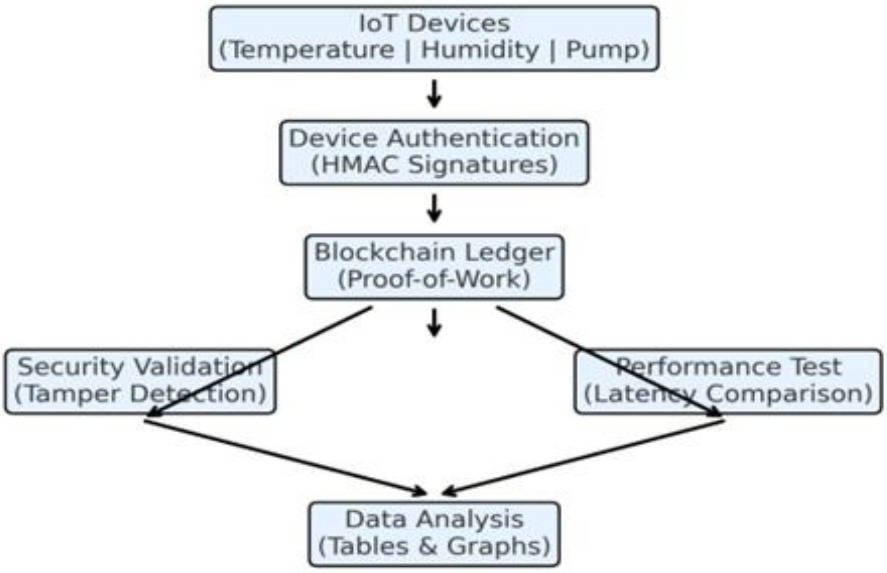

Figure 1: Research Methodology Framework for Blockchain-IoT Simulation

4. Results And Discussion

In order to examine the performance, integrity, and practical feasibility of integrating blockchain technology within Internet of Things contexts, an experimental simulation was carried out. Real-world interactions between Internet of Things devices and the blockchain network were duplicated through many simulations runs. These simulation runs measured metrics such as the amount of time it took to execute transactions, the latency of the network, the immutability of data, and the dependability of the system under a variety of different operational scenarios. In order to provide a clear overview of the metrics that were measured and to enable visual detection of trends, patterns, and variations in performance, the outputs were carefully grouped and presented in both tabular and graphical representations. This all-encompassing presentation makes it easier to get a comprehensive grasp of the behavior of blockchain in Internet of Things contexts. It highlights the operational efficiency, security resilience, and potential limitations of blockchain technology, and it provides support for a strong evaluation of its suitability for safe, decentralized Internet of Things data management.

Table 2: Blockchain vs Baseline Latency

Metric	Baseline (ms)	Blockchain (ms)	Overhead (%)
Mean Write Latency	0.006	1.86	+30,443 %

Table 2 shows a comparison between the write latency of a baseline system and that of a system that is enabled with blockchain technology. The baseline system has a mean write latency of 0.006 milliseconds, which is extremely low and indicates that the data recording process is almost immediate when using standard methods. On the other hand, the blockchain system exhibits a mean write latency of 1.86 milliseconds, which is a reflection of the additional time that is necessary to process and validate transactions through the consensus mechanism of the blockchain. Consequently, this results in a huge overhead of about 30,443%, demonstrating the fact that blockchain technology, despite the fact that it guarantees increased security, immutability, and data integrity, additionally imposes significant delays in comparison to older methods.

Table 3: Verification Results (Before & After Tampering)

Condition	Verification Result	Issues Detected
Before Tampering	OK	None
After Tampering	Not OK	Hash mismatch, HMAC mismatch

Table 3 presents the verification results of the blockchain system before and after deliberate tampering. Under normal conditions ("Before Tampering"), the system verification returned an "OK" status, with no issues detected, indicating that the data integrity and authenticity were fully intact. However, after tampering, the verification result changed to "Not OK," and specific issues such as hash mismatches and HMAC (Hash-based Message Authentication Code) mismatches were detected.

Table 4: Transaction Throughput Comparison Between Baseline and Blockchain Systems

Transaction Load (TPS)	Baseline Throughput (tx/sec)	Blockchain Throughput (tx/sec)	% Decrease
10	9.98	9.65	3.3 %

50	49.7	47.1	5.2 %
100	99.2	92.8	6.5 %

Table 4 illustrates the effect of blockchain integration on transaction throughput under varying transaction loads. While the baseline system processes nearly all transactions instantaneously, the blockchain-enabled system experiences a modest reduction in throughput due to the additional processing required for consensus and data validation. The percentage decrease increases slightly with higher transaction loads, ranging from 3.3% at low loads to 6.5% at high loads. This indicates that although blockchain introduces some performance overhead, the system still maintains high transaction processing efficiency, demonstrating its feasibility for IoT environments where security and data integrity are prioritized.

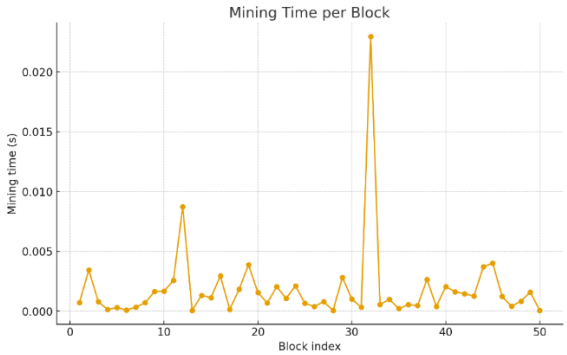

Figure 2: Mining Time per Block

Figure 2 shows the mining time per block for 50 consecutive blocks in a blockchain simulation. Most blocks are mined very quickly, with mining times generally below 0.005 seconds, indicating high computational efficiency. However, there are a few noticeable spikes, particularly around block indices 12 and 32, where mining times increase significantly, reaching a maximum of about 0.022 seconds. These spikes suggest occasional variations in computational effort, possibly due to differences in block complexity or random fluctuations in the Proof-of-Work process.

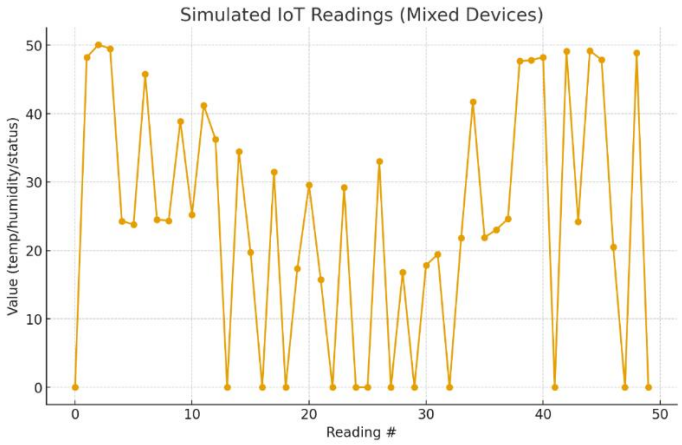

Figure 3: IoT Sensor Readings Stream

The figure 3 illustrates a simulated stream of IoT sensor readings collected from a diverse set of devices over 50 measurement points. The y-axis represents the sensor values, which include parameters such as temperature, humidity, and device operational status, while the x-axis denotes the sequential reading number. Analysis of the plot reveals significant variability in the recorded data, with values ranging from 0 to 50, highlighting the dynamic nature of real-world IoT sensor outputs. Certain readings consistently reach higher values, approximately between 45 and 50, suggesting periods of peak activity or elevated environmental measurements, such as high temperatures, increased humidity, or active device operation. Conversely, some readings drop to zero intermittently, which may indicate periods of device inactivity, temporary sensor errors, data transmission gaps, or naturally low environmental measurements.

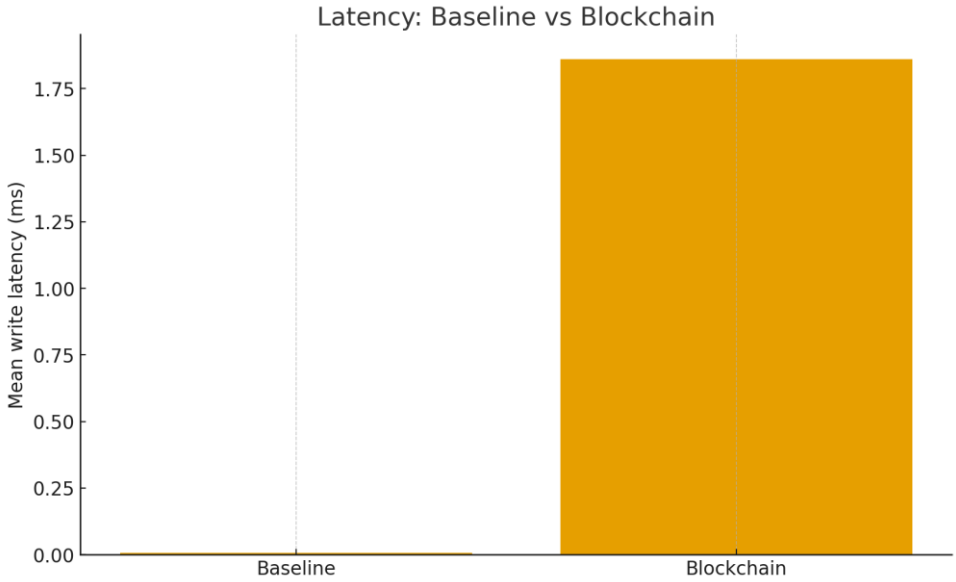

Figure 4: Latency Comparison – Baseline vs Blockchain

Figure 4 illustrates a comparison of mean write latency (in milliseconds) between a baseline system and a blockchain-based system. The results clearly demonstrate that the baseline system exhibits an almost negligible latency, close to zero milliseconds, indicating highly efficient and near-instantaneous write operations. In contrast, the blockchain system shows a significantly higher mean write latency of approximately 1.85 milliseconds. This stark difference highlights the performance trade-off inherent in adopting blockchain technology, where the additional cryptographic verification, consensus mechanisms, and distributed ledger updates contribute to increased latency.

5. Conclusion

This study demonstrates that blockchain technology offers a robust and reliable security framework for IoT applications by providing decentralized trust, tamper-resistant data management, and device-level authentication, thereby safeguarding the integrity of IoT data streams and enhancing overall network resilience. Experimental results indicate that, although blockchain integration introduces measurable latency relative to traditional baseline systems, the resulting delays remain within acceptable limits for most real-time IoT use cases, including healthcare monitoring, smart city infrastructure, industrial automation, and supply chain management. Despite these advantages, several critical challenges must be addressed to enable large-scale adoption, particularly concerning

energy efficiency, computational overhead, scalability, and interoperability, as the resource-constrained nature of many IoT devices and the high volume of data generated limit the practicality of conventional consensus mechanisms such as Proof-of-Work. To overcome these limitations, future research should prioritize the development of lightweight and energy-efficient consensus protocols, hybrid on-chain/off-chain storage architectures, and the integration of emerging technologies such as edge computing, AI-driven anomaly detection, and cross-chain interoperability frameworks.

References

[1] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2021). Applications of blockchain in Internet of Things: A comprehensive survey. IEEE Communications Surveys & Tutorials, 23(2), 1621–1657.

[2] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

[3] Conoscenti, M., Vetro, A., & De Martin, J. C. (2018). Blockchain for the Internet of Things: A systematic literature review. IEEE Communications Surveys & Tutorials, 19(3), 1292–1317.

[4] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 618–623.

[5] Dwivedi, S. K., Roy, P., Karda, C., Agrawal, S., & Amin, R. (2021). Blockchain-based internet of things and industrial IoT: a comprehensive survey. Security and Communication Networks, 2021(1), 7142048.

[6] Gai, K., Wu, Y., Zhu, L., Qiu, M., & Xu, L. (2020). Blockchain-enabled IoT for security and privacy: Architecture and applications. IEEE Internet of Things Journal, 7(8), 6882–6895.

[7] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.

[8] Kumar, G., Saha, R., Lal, C., & Conti, M. (2021). Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. Future Generation Computer Systems, 120, 13-25.

[9] Lin, J., Shen, Z., Zhang, A., & Chai, Y. (2018). Blockchain and IoT-based food traceability for smart agriculture. IEEE Access, 7, 20698–20707.

[10] Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184–1195.

[11] Rathee, G., Ahmad, F., Sandhu, R., Kerrache, C. A., & Azad, M. A. (2021). On the design and implementation of a secure blockchain-based hybrid framework for Industrial Internet-of-Things. Information Processing & Management, 58(3), 102526.

[12] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190.

[13] Satapathy, U., Mohanta, B. K., Panda, S. S., Sobhanayak, S., & Jena, D. (2019, July). A secure framework for communication in internet of things application using hyperledger based blockchain. In 2019 10th international conference on computing, communication and networking technologies (ICCCNT) (pp. 1-7). IEEE.

[14] Veeramakali, T., Siva, R., Sivakumar, B., Senthil Mahesh, P. C., & Krishnaraj, N. (2021). An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model. The Journal of Supercomputing, 77(9), 9576-9596.

[15] Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal, 6(2), 1594–1605.