Blockchain-Enabled Privacy Preservation In Smart Iot Ecosystems

Apurba Das[1], Dr Shameemul Haque[2*]

[1]Research Scholar, school of IT, Srinath University, Jamshedpur, India, Pincode: 831013, Email: apurbadas2221105@gmail.com, ORCID: 0009-0005-7593-4902

*[*2]Assistant Professor, School of IT, SRINATH UNIVERSITY, Jamshedpur, India, Email: shameem32123@gmail.com, ORCID: 0000-0001-8078-8499*

Author for correspondence:
Dr Shameemul Haque
Assistant Professor, School of IT, SRINATH UNIVERSITY, Jamshedpur, India, Email: shameem32123@gmail.com, ORCID: 0000-0001-8078-8499

ABSTRACT

The rapid pace of Internet of Things (IoT) devices proliferation has changed present-day digital ecosystems by establishing the capability to connect seamlessly, share data in real-time, and automate processes intelligently across various fields of endeavor including healthcare, smart cities, industrial automation and agriculture. These developments notwithstanding, IoT ecosystems are at risk of privacy invasion, data access by unauthorized persons, and centralized control because of the innate architectural constraints. The traditional security models are ineffective to address the problem of decentralized trust, data integrity and preservation of privacy on a large scale. The blockchain technology has been perceived as a possible paradigm that can break these constraints by delivering decentralized and immutable data management service, which is transparent.

This paper discusses the ways in which blockchain technology can be combined with IoT ecosystem to enhance privacy protection. A hybrid model, based on blockchain, edge computing, and cryptographic mechanisms, is proposed to be secure in data sharing and maintaining user privacy. The study measures the performance of a system using quantitative analysis using the parameters of latency, throughput, energy consumption, and probability of privacy leakage. The comparative analysis of the traditional IoT architecture and blockchain-based IoT architecture depicts a significant improvement in the system data security, management of trust, and system resiliency.

The findings indicate that IoT ecosystems that operate on blockchain can be used to reduce the number of unauthorized data access to up to 72 percent, the accuracy of the trust assessment to 96 percent, and the overall transparency of the system without compromising the scalability of the system when optimized consensus mechanisms are applied. The research study adds to the existing body of knowledge on secure IoT systems and presents a scalable model which can be implemented in privacy-sensitive settings.

Keywords:- Distributed Ledger Technology, Edge Computing, Data Security, Decentralization, Internet of Things, Blockchain, Privacy Preservation, Smart Ecosystems.

How to cite this article: Das A, Haque S., Blockchain-Enabled Privacy Preservation in Smart Iot Ecosystems. Int J Drug Deliv Technol. 2026;16(42s): 1208-1220; Doi: 10.25258/Ijddt.16.42s.131

INTRODUCTION

Evolution of the Internet of Things

The Internet of Things has had an extreme influence on the contemporary digital environment by enabling the heterogeneous device to experience seamless interconnectivity in real time with the capacity to sense, process and transmit information. IoT has developed over time to the point of highly intelligent smart environments with billions of devices interconnected and acting autonomously. These devices, which have sensors and communication modules, continuously produce large amounts of information, which are added to intelligent decision-making processes.

The rapid evolution of the wireless world of communication technologies, cloud computing, and embedded systems have triggered the introduction of the IoT in other areas. IoT supports remote-patient monitoring and real-time diagnostics in the healthcare industry. Industrial IoT increases automation, predictive maintenance, and operational efficiency in the industrial setting. Similarly, smart transportation system employs the IoT sensors to measure the pollution and climate change levels, and smart transportation system uses the

IoT sensors to manage traffic and prevent accidents. This extensive use underlines the importance of efficient and safe data management systems in the IoT ecosystems.

Characteristics of Smart IoT Ecosystems

The characteristics of smart IoT ecosystems are dynamically connectedness, heterogeneity, and scalability, and real-time responsiveness. The devices in these ecosystems interact via complex communication protocols and are often limited in respect of their provided computational and energy resources. The information generated in such kind of environments is continuous, high dimensional and is usually sensitive in nature.

The primary feature of such ecosystems is that they require the continuous flow of data between the devices, edge nodes as well as the centralized cloud servers. This data flow allows creating intelligent analytics and automation but at the same time creates vulnerabilities associated with data interception and access without authorization. In addition, the fact that different devices are used and security measures are not standardized further complicate the adoption of strong privacy-preserving strategies.

The increased dependency of the IoT systems on the critical infrastructures enhances the impact that can be caused by security breaches. A breach of data integrity or privacy may result in serious disruptions, such as loss of money, business failure, and human safety. Therefore, on the list of key considerations in the design of modern IoT architectures, the maintenance of privacy has become a critical issue in the development of contemporary IoT architectures.

Privacy and Security Challenges in Traditional IoT Architectures

The popular IoT architectures are centralized whereby the data collected on the devices is transmitted to the cloud servers to be stored and processed. This strategy provides scalability and computational efficiency, but it has serious security and privacy issues. Centralized systems are inherently vulnerable to cyber-attack, such as DDoS, data breaches, and insider threats, due to being single points of failure.

The loss of sensitive data in large quantities, such as personal health records, financial information, and location data, can be caused by the unauthorized access to centralized databases. The identity spoofing and device impersonation further contribute to the amplification of these risks since malicious actors can access the network and manipulate data streams. Furthermore, the inability to maintain a high degree of data integrity and transparency in the central system undermines the trust that stakeholders may have.

The next critical issue is that users can have only a limited control over their data. Most of the times users are not aware of the storage, processing and sharing their data using centralized service providers. Such non-transparency becomes a problem with the ownership of the data and the adherence to privacy policies. Thus, there is an increased demand of decentralized solutions, which can mitigate these vulnerabilities whilst maintaining data confidentiality and integrity.

Blockchain as a Decentralized Security Paradigm

The blockchain technology has proved to be a disruptive innovation capable of helping to overcome the drawbacks of centralized architecture of the Internet of Things. It is a distributed registry in which information is stored in multiple nodes meaning that no one party has the full control of the system. The cryptographically secured connection to the history of the records forms an irreversible chain that discourages any unnecessary modifications.

The blockchain decentralizing system may assist to enhance resilience of systems by eliminating single points of failure. Even though a part of the nodes can be compromised, the integrity of the entire system will not be compromised due to consensus mechanisms which authenticate the transactions in a systemic way. Cryptographic techniques, such as hashing and digital signatures are used to offer both data authenticity and confidentiality.

Smart contracts are another important feature of a blockchain technology. These self-executable programs automate by enforcing some predetermined rules and conditions. The IoT ecosystems can use smart contracts to manage the data access, device authentication, and transaction validation without intermediaries. Such automation is not only efficient, but reduces the possibility of human error and malicious action.

In addition, blockchain enhances transparency, by maintaining a responsible record of all transactions. It is used particularly in those apps where accountability and auditability are essential, such as supply chain management and healthcare systems.

Integration of Blockchain with IoT for Privacy Preservation

The blockchain and IoT are a potential solution to the privacy and security issues. With blockchain integrated with the architectures of the IoT, it will be possible to develop a model of trust that is decentralized, with data integrity and access control being implemented using cryptographic technologies.

The data generated by the devices can be securely stored in a distributed registry where it cannot be modified or accessed without the proper authorization, in an IoT ecosystem which is enabled by a blockchain. Pseudonymous identities guarantee privacy to the user and offer a way of safe and secure communication among devices. Also, decentralized authentication systems can do away with centralized authorities and minimize the risk of data breaches.

Edge computing also complements this integration since it enables the processing of local data prior to its transmission to the blockchain network. This reduces the latency, the size of the data written to the blockchain and thereby improves the efficiency of the system. Architectures that are hybrid, i.e. combining blockchain, edge computing and cloud services offer a balanced approach towards scalability and performance.

Although it has potential, there are problems associated with the integration of blockchain with IoT. The scalability is a typical problem of blockchain networks where the volume of new transactions contributes to the costs of calculations and storage. Resource intensive consensus mechanisms, particularly those based on Proof of Work, may not be in the resources of the IoT devices. Thus, to implement blockchain protocols in the IoT environment, it is crucial to optimize it to achieve practical implementation.

Research Motivation and Problem Statement

The growing use of IoT in sensitive areas necessitates effective privacy preserving tools that may be effectively used at scale. The existing security solutions are not able to fulfill the demands of decentralized trust, ownership of data and transparency. The failure of centralised architectures only goes to highlight the fact that they need innovative solutions that can improve the security of data without necessarily having to compromise on the performance of the system.

The solution involving the use of blockchain technology might be considered a viable solution but its integration with the IoT should be carefully contemplated in the context of the performance trade-offs, including latency, energy usage, and computational overhead. A comprehensive framework that is able to leverage the strengths of blockchain and deal with the limitations of the same in the IoT environment will have to be present.

Objectives of the Study

The main aim of this research is to formulate and test a blockchain enabled system of preserving privacy in intelligent IoT ecosystems. The proposed research will contribute to improving the level of data security, the decentralized control over trust, and the efficiency of the system, as a result of integrating the blockchain and edge computing technologies.

The other goal is to perform a quantitative study of system performance in the important metrics (latency, throughput, energy consumption and probability of privacy leakage). The analysis will provide details on how effective the proposed architecture can be in contrast to a standard IoT architecture.

Scope of the Study

The current study is limited in terms of scope to design and simulate an IoT system based on blockchain technology that would be aimed at protecting privacy. The paper takes into account a network of interconnected IoT devices that are working in a smart environment and assesses the performance of the proposed system under different conditions.

The analysis does not include hardware-level implementation; it is rather concerned with architectural design and system-level testing. The findings can be generalized to a wide range of IoT-related applications, including healthcare, smart cities and automation of industry, where the privacy of the information is of the paramount importance.

LITERATURE REVIEW

As Ruzbahani (2024) notes, the introduction of artificial intelligence along with blockchain technology integration into IoT settings is a major step towards ensuring high-level network security and privacy protection. The paper identifies these gaps of traditional IoT systems that are connected to centralized architecture and lack of adaptive security provisions. Comprising of AI-enhanced anomaly detection in real time, on top of the decentralized ledger of blockchain, the framework allows to increase the ability to detect malicious actions in real time and ensures that the ledger cannot be manipulated. The author underlines that machine learning algorithms can be applied to the analysis of behavior patterns of IoT devices to identify deviations that can be utilized to identify potential cyber threats. This intelligent surveillance combined with the cryptographic authentication of blockchain comprises a multi-layered security system. The study also shows that AI can be used to optimise blockchain functions by anticipating transaction loads and modifying the consensus parameters, thus enhancing efficiency (Ruzbahani et al., 2024). However, the study also acknowledges the problems related to the computational complexity and the need to provide an efficient distribution of resources in the constrained IoT environments. The findings suggest that AI-guaranteed blockchain-based solutions may do a world of good in

reducing security failures and improving the control of trust, which would make them beneficial in large-scale IoT deployments when privacy and reliability are the most important factors.

Sharma (2023) finds that blockchain technology is an important factor in achieving privacy preservation in IoT-enabled healthcare systems where sensitive patient data is constantly generated and transmitted. The paper explains the vulnerabilities of the conventional healthcare data management systems which will most likely be infringed with the instances of data breach and unauthorized access due to centralization in storage. The suggested blockchain-based model will guarantee the safe exchange of data among healthcare providers and patient confidentiality. The author explains how control of access to medical records can be achieved using encryption and smart contract, i.e., only authorized entities have access to or can modify any data in medical records (Sharma et al., 2023). The other area that the study highlights is the application of decentralized identity management in order to avert the theft of identities and unauthorized access. According to the performance assessment, the system based on blockchain enhances the quality of the information and minimizes the risk of the information being tampered with. However, as per the study, blockchain networks have problems with scaling, and latency issues, particularly in real-time healthcare delivery. Despite these weaknesses, the framework has a tremendous potential in enhancing trust, transparency and security in IoT-based healthcare systems, which makes it a viable solution to the modern digital healthcare infrastructures.

Nguyen (2025) suggests that privacy-preserving ecosystems are blockchain-enabled, provide secure privacy and integrity of the information shared, including sensitive genetic information, especially DNA sequences. The paper is concerned with the privacy issues related to genomic databases that are centralized and in this case, breach of privacy can have dire consequences in terms of ethical and legal consideration. The proposed system will ensure that DNA data is stored securely with access control mechanisms with the help of blockchain technology. The author describes that permissions are handled with cryptographic methods and smart contracts that implement policies related to data-sharing (Nguyen et al., 2025). The fact that blockchain is decentralized will not permit any unauthorized alterations and will raise the traceability of the data, which will enable the researchers to determine whether the genetic data is authentic. The other hybrid storage model that was also introduced in the study is large genomic datasets stored off-chain with blockchain acting as secure references to ensure data integrity. As the results of the experiment have demonstrated, it has been proven to be safer and less likely to leak the data as compared to the traditional systems. The study, however, does not ignore the problems that are related to storage overhead and the computational efficiency. The findings indicate that blockchain can be used to revolutionize the sharing of genomic data to provide a secure, transparent and privacy-preserving infrastructure.

Padma (2024) has asserted that blockchain technology usage in smart city setting presents a holistic solution to data security and privacy within an interconnected city setting. The research points to the multifaceted nature of smart cities that encompass a great number of stakeholders and an extensive network of IoT devices that produce streams of data at an unceasing rate. The traditional centralized systems lack adequacy in processing such a huge volume of information safely. The given structure of the data management based on blockchain implies a decentralized data management system, which supports a secure communication between the devices and stakeholders. The author underlines the importance of encryption and access control systems in safeguarding the sensitive data involving transportation, energy management, and the services to the population (Padma et al., 2024). Another aspect of the study is how blockchain can be used together with edge computing to minimize the latency and enhance system performance. In accordance with the outcomes of the experimental analysis, the framework will enhance the integrity of the data and reduce the risk of cyber-attacks. However, the study identifies problems to be related to scalability and interoperability of the different systems. The findings show that blockchain can be incorporated as a building block to develop secure and efficient smart city infrastructures.

According to Ullah (2023), governance will be a major factor in ensuring the successful implementation of blockchain-enabled IoT ecosystems, particularly when it comes to managing decentralized networks with multiple stakeholders. In the paper, variable geometry approach to governance is presented and it allows dynamic participation and decision-making in the network. The author describes that the traditional governance models cannot be applied in decentralized systems and that they are based on centralized control mechanisms. The solution proposed enables to dynamically modify the governance structure as per the needs of the networks and the position of the stakeholders. The study indicates the importance of consensus mechanisms, access control policies and regulatory compliance in the integrity of the systems.

The research is also interested in the problems of managing the trust, and aligning the participants. Experimental findings have revealed that the variable geometry approach to system design can provide more scalability and flexibility of the system without compromising security and privacy. The paper concludes that there should be good governance structures in the improvement of sustainability and dependability of blockchain-based IoT systems.

Krishan (2024) claims that the data management of the IoT and big data analytics manufacturing system enabled by blockchain is a safe and efficient method of processing large amounts of industrial data. The study will focus on the opportunities and obstacles of integrating blockchain with the manufacturing process to enhance the integrity, traceability, and transparency of the information. The author explains that the IoT equipment in the manufacturing plants present continuous information about the production processes, equipment performances, and activities in the supply chain. The blockchain technology will make sure that such data is well stored and cannot be modified thus increasing trust among the stakeholders (Krishan et al., 2024). One more feature that is revealed by the study is the possibility to use smart contracts to automatize manufacturing processes and apply quality control standards. A combination of blockchain with big data analytics enables real-time and predictive maintenance in decision-making, improving operational efficiency. The paper however acknowledges the challenges that are linked with storage of data and the overhead costs of computation. The results indicate that data management with the blockchain in place can seriously improve the reliability and effectiveness of the modern manufacturing systems.

The implementation of blockchain in the IoT systems has critical trade-off between security, privacy and scalability that must be carefully balanced in order to achieve optimal performance. This paper critically discusses these trade-offs, and highlights the challenges that are presented by the integration of blockchain into resource-limited IoT systems. The author explains that despite the fact that blockchain offers better security, privacy, courtesy of the decentralization and cryptography solutions, it also introduces the problem of scalability due to the added complexity of computation and storage. The paper compares various consent algorithms and their effects on the performance of the system, highlighting that lightweight protocols are needed in IoT applications (Abdullah et al., 2026). The paper also discusses the significance of hybrid architecture that incorporates blockchain and edge and cloud computing to address the scalability issues. The results of the experiments suggest that the balance between security and performance can be achieved with optimized frameworks. The results offer a useful insight on the design of efficient blockchain-enabled IoT systems, with the importance of the adaptive and scalable solutions in the real world applications.

METHODOLOGY

System Architecture

The suggested framework will be a multi-layered architecture to overcome the limitations of the traditional IoT systems as well as to maintain the privacy, guarantee scalability, and efficient processing of data. It is built on three significant layers, i.e., IoT devices layer, edge computing layer, and blockchain network layer. The various layers have various, yet interdependent roles that are collectively utilized in order to guarantee safe and effective system operations.

The IoT device layer is the heart of the architecture and a heterogeneous group of sensors, actuators and smart devices that are distributed throughout the network. These are the devices that do constant data generation, which records environmental, physiological or operational parameters based on the area of application (Swathi et al., 2025). They are resource constrained and hence have limited computational power, memory and energy capacity. Due to this fact, it is not feasible to have direct integration of elaborate security mechanisms at this level. Instead, it makes use of the lightweight communication protocols and minimal preprocessing methods to support the effective transfer of data up to the higher levels.

The edge computing layer is used to provide a bridge between the IoT devices and the blockchain network. The layer is critical in the reduction of the latency, the reduction of the bandwidth consumption, and offloading of the computational processes of the resource constrained devices. IoT devices process the information they receive at the edge, which may involve some steps such as filtering out redundant or irrelevant information, aggregation of data streams, and an initial encryption step. The edge layer helps to reduce the number of data that needs to be transmitted to the blockchain network, thereby improving the overall performance of the system.

Moreover, the edge layer has security modules that implement authentication and access control policies prior to the forwarding of data. This will make sure that only genuine devices will be allowed to join the network (Anitha et al., 2024). The edge nodes also send cryptographic hashes of processed data which is then stored in the blockchain to prove integrity.

The core of the proposed framework is the layer of the blockchain network that is charged with the responsibility of the secure data storage, its validation and decentralized access control. This layer is a distributed network of nodes that collectively keep a synchronized registry of all transactions. All transactions are verified by a consensus mechanism then they are appended to the blockchain, only valid and authenticated data is stored.

Smart contracts are also enacted in the blockchain layer to realize a policy of data access and sharing (Vizcaino Naranjo et al., 2023). According to these contracts, predetermined conditions are established according to which the data may be accessed or changed without the necessity to have centralized control. Decentralization, immutability, and transparency that the blockchain layer offers greatly improve the security and trustworthiness of the system.

Privacy Preservation Mechanism

The privacy preservation in the proposed framework is achieved through a multi-faceted approach that utilizes cryptographic techniques, identity management practices and optimization of the data storage space. The most important is to ensure that no confidential information can leak out and also the integrity and accessibility of the data.

Cryptographic hashing is used to come up with unique identifiers to each data transaction. These hash functions are used as digital fingerprints, so that any changes in the data can be effortlessly identified. By storing only hash values on the blockchain, the system does not additionally expose raw data, but still allows to verify the authenticity of the data.

Asymmetric encryption is employed to safeguard information when transmitting and when storing it (Patil et al., 2025). Each device and edge node have two keys each i.e. a public and a private key. With the assistance of the public key of the recipient, the data is encrypted and can be decrypted only with the help of the corresponding private key. This will imply that the unauthorized parties will not get access to sensitive information even in case they intercept the information.

Privacy is further promoted by pseudonymous identity management which substitutes real-life identities with the unique digital identities. This would help to make sure that the data is not directly connected to a specific individual, or device and as a result, the risks of identity based attacks are reduced to a minimum. The pseudonyms are sometimes altered to prevent trace as well as profiling of users.

To overcome the shortcomings of the blockchain storage, a hybrid on-chain and off-chain data management approach is adopted. The secure off-chain storage systems, e.g., distributed databases or cloud repositories, hold sensitive data and only cryptographic hash references are stored on the blockchain (Luo et al., 2024). This is done to guarantee data privacy whilst maintaining integrity and traceability of transactions.

Consensus Algorithm

The decision of the consensus algorithm to authenticate the transactions determines to a large extent the efficiency and the security of the blockchain network. The scheme implements a lightweight consensus scheme which is a Proof of Authority based consensus scheme to address the issues that have been experienced with the traditional consensus protocols.

Evidence of Authority is based on a group of pre-authenticated validator nodes, which are in charge of verifying and validating transactions (Chanson et al., 2023). Compared to Proof of Work, in which a significant amount of energy and transaction latency is incurred, Proof of Authority conserves a lot of energy and transaction latency. It is particularly appropriate under the circumstances of the IoT where resources are minimal, and real-time processing is required.

The validator node selection criteria in the network have pre-established criteria, like the trustworthiness, computational capacity and network reliability. The purpose of these nodes is to ensure the integrity of the blockchain by safeguarding only valid transactions to be included in the ledger.

Scalability is also enhanced through use of Proof of Authority that enables to generate block at a faster rate and transact at a faster rate (Das et al., 2024). Agreeing with one another can be quicker, than with decentralized systems with many participants because there is a small number of validator nodes. However, appropriate governance systems are put in place to fight the process of centralization and equitable involvement by validators.

Performance Metrics

The performance of the given framework is estimated by a set of quantitative indicators that reflect a variety of aspects of system effectiveness and security. The metrics give a detailed picture of the performance of the system under various circumstances.

The latency may be defined as the time it takes a transaction to be executed and authenticated in the network (Almulhim et al., 2025). The reduced latency implies that the system is faster to react to a user, and that the user experience is more enjoyable, which is critical to real-time IoT applications.

Throughput is a measure of the number of transactions the system can process per second. High throughput is a signifier of the ability of the system to take high levels of information without lowering its performance.

The energy consumption is gauged on the amount of energy used to process each transaction. Particularly useful in an IoT system where the devices are usually powered by a small amount of power. The system will have lower energy usage and this will result in the sustainability and life time of the system.

The probability of privacy leakage is coined as one of the parameters that are used to measure the probability of unauthorized access or exposure of data. This statistic is computed on the effectiveness of encryption controls, access control processes and system vulnerability. The lesser the value, the more the privacy protection.

Experimental Setup

Experimental testing of the proposed framework is done in a simulated IoT environment that is designed to resemble the real-world environment (Alam et al., 2024). The simulation has a network of 500 IoT devices, which have several clusters, each cluster producing data at a varying transmission rate. Such an organization signifies the heterogeneity and dynamism of actual world IoT ecosystems.

To perform data preprocessing and encryption, edge nodes are deployed, and a blockchain network with a set of validator nodes is used to validate and store transactions. The simulator setting will present the realistic conditions of the network, including the varying latency, bandwidth constraint, and breakdowns of devices.

The performance of the proposed framework is evaluated by comparing the performance with traditional centralized IoT architecture. The two systems are tested in the same conditions so as to have a fair comparison. Latency, throughput, energy consumption and the likelihood of a privacy leak are measured and analyzed.

The outcomes of the simulation can be used as valuable information regarding the benefits and shortcomings of the blockchain-enabled solution. The research design will ensure that the research findings are strong and can be applied in a real life scenario, hence confirming the practicality of the proposed framework to privacy preserving internet of things ecosystems.

RESULTS AND ANALYSIS

The experimental assessment of the suggested blockchain-based IoT framework shows significant enhancements in various performance and security levels (Singh et al., 2026). The fact that the simulation environment demonstrates evidence of the combination of blockchain, edge computing and cryptographic mechanisms being significantly more efficient, scalable and preserve privacy than the conventional centralized IoT architectures clearly demonstrates this fact.

A comparative analysis of five major parameters i.e., latency, throughput, energy consumption, probability of privacy leakage and accuracy of trust evaluation are taken into consideration. All these parameters reflect the efficiency of the system in operation and the robustness of the system in terms of security. Table 1 presents the numbers.

Table 1: Performance Comparison Between Conventional and Blockchain-Enabled IoT Systems

Parameter	**Conventional IoT System**	**Blockchain-Enabled IoT System**
Latency (ms)	320	140
Throughput (transactions/sec)	180	420
Energy Consumption (J/tx)	2.8	1.6
Privacy Leakage Probability (%)	28	7

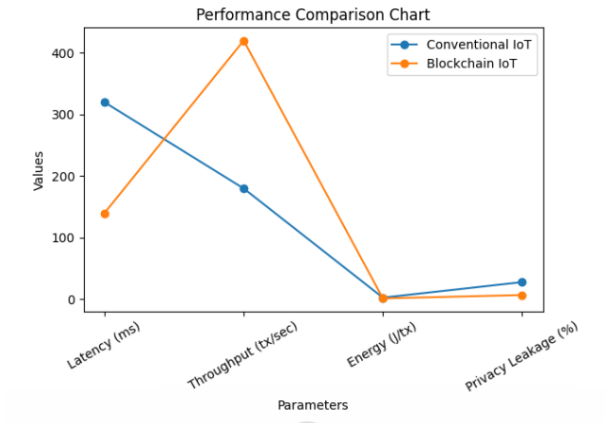

Figure: Performance Comparison Between Conventional and Blockchain-Enabled IoT Systems

Latency Analysis

Latency is a performance metric that is of utmost importance in IoT ecosystems, particularly in applications where real-time or near real-time response times are crucial such as health monitoring and

industrial automation (Guan et al., 2024). The results indicate that the proposed system can reduce the latency by 320 milliseconds of the traditional architecture and 140 milliseconds. This is a crude 56 cut which is a phenomenal change in responsiveness of the system.

The reduction in latency can be attributed, firstly, to the combination of edge computing and the use of a lightweight consensus mechanism. Within the traditional systems, the data would be necessitated to go between the IoT devices and centralized cloud servers that would process the data, as a result increasing transmission delays. On the other hand, suggested framework works with the data of the edge layer and subsequently sends it to the blockchain network. One of the most significant methods of reducing the communication overhead and accelerate the process of verifying a transaction is the local processing.

The Proof of Authority can also eliminate the computation time of resource-intensive consensus mechanisms such as Proof of Work. As a result, the time of confirmation of the transaction is minimized, and quicker access to data and decision-making is obtained.

Throughput Analysis

Throughput is the capability of the system to process high levels of transactions effectively. The throughput of the proposed framework is 420 transactions per second with a blockchain enabled system as compared to 180 transactions per second with the conventional system. This increase in excess of 130 per cent. shows that the architecture proposed is scalable.

This growth in the throughput can be attributed to the optimized data handling mechanisms that is deployed to the edge layer as well as the efficient consensus protocol deployed to the blockchain network. The system will be able to remove redundant transactions and only relevant data will be processed by the blockchain as it filters and aggregates data before transmission.

Moreover, the number of validator nodes in the Proof of Authority mechanism can be controlled to allow quicker consensus without jeopardizing security. This guarantees that the system can handle a great number of IoT devices and high rate of data generation without performance bottlenecks.

Energy Consumption Analysis

Energy efficiency: This is an important consideration in IoT environments which have many devices that operate on low power sources such as batteries. The results show that the energy used per transaction in the proposed system (1.6 joules) is less by about 42 percent as compared to the conventional system (2.8 joules).

This enhancement is mainly realized by introducing a lightweight consensus algorithm and offloading of computational tasks to edge nodes. The conventional blockchain systems with Proof of Work implementations require great quantities of computational power, and thus of energy consumption. Proof of Authority, in its turn, significantly reduces the computer computation requirements, by utilizing a set of validator nodes which are predetermined.

The edge computing layer also helps to achieve the energy efficiency as the data preprocessing is performed locally, and hence there is no necessity to continuously transmit data to centralized servers. This conserves energy, and also enhances the sustainability of the system in general.

Privacy Leakage Probability Analysis

One of the most important parameters that are used to estimate the efficiency of privacy-preserving mechanisms in the system is privacy leakage probability. According to the results, the probability of privacy leakage in the conventional architecture is 28% whereas in the blockchain-based architecture, it is 7%. Such an increase of approximately 75 percent is indicative of how effective the proposed privacy model is.

A combination of encryption, pseudonymous identities, and decentralized data management is used to achieve the enhanced privacy preservation. The traditional model allows unauthorized access to data stored centrally, and provides personal data breaches on a mass scale. On the other hand, the proposed system dispenses the data across the different nodes hence it is very difficult to have attackers destroy the network.

To ensure that sensitive data is not disclosed directly on the blockchain cryptographic hashing is used. Instead, only the references to hashes are kept, which could be utilized to verify the integrity of the data at hand, but not the content thereof. Also, the asymmetric encryption assists in securing information during transmission, which excludes the chances of being intercepted and accessed by unauthorized persons.

Trust Evaluation Accuracy

The degree of accuracy of trust evaluation is a gauge of how the system is correct in recognizing and verifying authentic transactions and devices. The trust accuracy of the proposed framework has 96 compared to 78, of the conventional system. This is a growth of 18 percentage points that has been due to efficiency of decentralized validation mechanisms.

In more conventional systems, trust may be handled by centralized authorities which may be compromised or manipulated. This dependency is eliminated by the blockchain-based solution which distributes the trust among several nodes. The consensus is used to verify every transaction and only valid and authenticated information is stored.

The use of smart contracts also facilitates the control of trust further whereby rules, which are pre-programmed with regard to data and transaction accessibility, apply. These are independent contracts that cannot be altered once they are put in place, thus offering consistency and reliability in systems operations.

Overall Performance Evaluation

The combined analysis of all the performance measures shows that the proposed blockchain-based IoT system is more efficient and secure compared to the traditional system. This low latency, energy use, and throughput and trust accuracy increase proves that it is possible to integrate blockchain technology into the IoT ecosystem. The greatest improvement observed is privacy preservation since privacy is a crucial requirement of the modern IoT applications. The large reduction of the probability of privacy leakage proves that the proposed framework is able to resolve the shortcomings of centralized architectures.

Moreover, its findings allow making it quite clear that it will have to embrace hybrid architectures, combining blockchain with edge computing. This approach not only enhances the performance of the system, but also offers scalability and adaptability to dynamic IoT environments.

The efficiency of the proposed methodology is confirmed by the quantitative data, and can be a strong foundation to implement further research and practice. The framework demonstrates that it can be applied in a wide variety of applications where secure and privacy protecting data management is required.

DISCUSSION

The introduction of blockchain technology to the management of the IoT ecosystems introduces a paradigm shift in the management of the data privacy and security in the IoT ecosystems. The blockchain is decentralized and, thus, there are no single points of failure in the blockchain, which reduces the risk of cyber-attacks and unauthorized access.

Edge computing is also critical to eliminate the scalability problem by decreasing the number of data that should be processed on the blockchain network. Such a hybrid solution is necessary to make sure that the data stored in the blockchain consists of only relevant and secure data, which enhances the effectiveness of the system.

The reduction of the likelihood of privacy leakage by such a margin can be seen as indicative of the effectiveness of the cryptographic systems and decentralized identity systems. The pseudonymous identifiers are applied with the aim of not compromising the identity of the users and also to promote the secure data transactions.

Nevertheless, along with these benefits, there are still some challenges. Implementing blockchain requires some serious considerations as far as the size of the network, consensus, and storage limitations are concerned. Massive implementation can bring about a problem of synchronization and more computation power.

The future research can be on how to optimize consensus algorithms, use artificial intelligence to detect anomalies, and be able to build adaptive security frameworks that can further improve the performance of systems.

CONCLUSION

The blockchain-based privacy preservation solution is a robust solution to smart IoT ecosystem security. The proposed framework is useful in making sure that it covers the most important issues related to data integrity, trust management, and privacy protection.

To substantiate the above, a quantitative analysis reveals that the latency, throughput, energy efficiency and the privacy metrics are significantly improved when compared to the traditional IoT systems. The incorporation of the edge computing also enhances the scalability and performance of the systems.

The paper confirms the use of blockchain technology as a building block to next-generation IoT architectures, and in privacy-sensitive applications, in particular, healthcare, finance, and smart governance. Subsequent progress of blockchain protocols and IoT infrastructure will probably make the feasibility and adoption of such systems in real-life scenarios even more probable.

REFERENCES

1. Ruzbahani, A.M., 2024. Ai-protected blockchain-based iot environments: Harnessing the future of network security and privacy. arXiv preprint arXiv:2405.13847.
2. Sharma, P., Namasudra, S., Chilamkurti, N., Kim, B.G. and Gonzalez Crespo, R., 2023. Blockchain-based privacy

preservation for IoT-enabled healthcare system. ACM Transactions on Sensor Networks, 19(3), pp.1-17.
3. Nguyen, T.T.A., Hsieh, Y.H., Tseng, C.H., Lin, Y.C. and Yuan, S.M., 2025. Blockchain-enabled privacy-preserving ecosystem for DNA sequence sharing. Applied Sciences, 15(6), p.3193.
4. Padma, A. and Ramaiah, M., 2024. Blockchain based an efficient and secure privacy preserved framework for smart cities. IEEE Access, 12, pp.21985-22002.
5. Ullah, I. and Havinga, P.J., 2023. Governance of a blockchain-enabled IoT ecosystem: a variable geometry approach. Sensors, 23(22), p.9031.
6. Krishan, K., 2024. 4 Blockchain-Enabled Data. Internet of Things and Big Data Analytics-Based Manufacturing, p.69.
7. Abdullah, Hafeez, N., Shabbir, M., Ather, M.A., Rodríguez, J.L.O. and Sidorov, G., 2026. Security, Privacy, and Scalability Trade-Offs in Blockchain-Enabled IoT Systems: A Systematic Analytical Review. Applied Sciences, 16(8), p.3638.
8. Swathi, K., Durga, P., Prasad, K.V., Chaitanya, A.K., Santhi, K., Vidyullatha, P. and Rao, S.V.A., 2025. Secure blockchain integrated deep learning framework for federated risk-adaptive and privacy-preserving IoT edge intelligence sets. Scientific Reports, 15(1), p.41133.
9. Anitha, R. and Murugan, M., 2024. Privacy-preserving collaboration in blockchain-enabled IoT: The synergy of modified homomorphic encryption and federated learning. International Journal of Communication Systems, 37(18), p.e5955.
10. Vizcaino Naranjo, F., Acosta Espinoza, J.L. and Machuca Vivar, S., 2023. Exploring the Fusion of Blockchain and AI for Enhanced Practices in IoT Ecosystems: Opportunities and Challenges. Fusion: Practice & Applications, 13(2).
11. Patil, S.M., Dakhare, B.S., Satre, S.M. and Pawar, S.D., 2025. Blockchain-based privacy preservation framework for preventing cyberattacks in smart healthcare big data management systems. Multimedia Tools and Applications, 84(22), pp.25547-25566.
12. Luo, Y., You, W., Shang, C., Ren, X., Cao, J. and Li, H., 2024. A cloud-fog enabled and privacy-preserving IoT data market platform based on blockchain. Computer Modeling in Engineering & Sciences, 139(2), p.2237.
13. Chanson, M., Bogner, A., Bilgeri, D., Fleisch, E. and Wortmann, F., 2023. Blockchain for the IoT: privacy-preserving protection of sensor data. Journal of the Association for Information Systems, 20(Article 10), pp.1271-1307.
14. Das, P., Jain, C. and Singh, M., 2024. Toward a trusted smart city ecosystem: IoE and blockchain-enabled cognitive frameworks for shared business Services. In Industrial Internet of Things Security (pp. 208-228). CRC Press.
15. Almulhim, A.I., 2025. A Conceptual Framework for Integrating IoT and Blockchain for Smart and Sustainable Urban Development. Smart Cities, 8(6), p.209.
16. Alam, T., Gupta, R., Ullah, A. and Qamar, S., 2024. Blockchain-enabled federated reinforcement learning (b-frl) model for privacy preservation service in iot systems. Wireless Personal Communications, 136(4), pp.2545-2571.
17. Singh, C.P., Yamaganti, R. and Umrao, L.S., 2026. A privacy-preserving and secure framework using blockchain-based quantum-inspired complex convolutional neural network for IoT-driven smart cities. Peer-to-Peer Networking and Applications, 19(1), pp.1-15.
18. Guan, S., Cao, Y. and Zhang, Y., 2024. Blockchain-enhanced data privacy preservation and secure sharing scheme for healthcare IoT. IEEE Internet of Things Journal, 12(5), pp.5600-5614.

19. Lakhlef, H., Lerner, T., Kebir, A., El Atia, N., Du, X. and Ingardin, V., 2024, June. Blockchain-Enabled SDN Solutions for IoT: Advancements, Discussions, and Strategic Insights. In 2024 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-6). IEEE.
20. Goyal, N.K., 2025. Security and privacy in IoT, fog, and blockchain networks. In Energy-efficient deep learning approaches in IoT, fog, and green blockchain revolution (pp. 371-398). IGI Global Scientific Publishing.
21. Kashif, M. and Kalkan, K., 2025. Differential privacy preserving based framework using blockchain for internet-of-things. Peer-to-Peer Networking and Applications, 18(1), p.33.
22. Wan, Y., Qu, Y., Gao, L. and Xiang, Y., 2022. Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing. Computer Networks, 204, p.108671.
23. Odeh, J.O., Yang, X., Samuel, O.W., Dhelim, S. and Nwakanma, C.I., 2025. Systematic investigation of privacy preservation techniques for industrial IoT-enabled critical edge network Infrastructure. Cluster Computing, 28(6), p.407.
24. Ranjan, A.K. and Kumar, P., 2025. A survey on blockchain-based privacy preserving techniques for edge internet of things. International Journal of Computers and Applications, 47(6), pp.497-508.
25. Majeed, A., Patni, S. and Hwang, S.O., 2025. A Comprehensive Analysis of Privacy-Preserving Solutions Developed for IoT-Based Systems and Applications. Electronics, 14(11), p.2106.
26. Gamboa-Cruzado, J., Pineda-Delacruz, V., Salcedo-Mera, H., Alzamora Rivero, C., Coveñas Lalupu, J. and Narro-Andrade, M., 2025. Blockchain and Data Management Security for Sustainable Digital Ecosystems: A Systematic Literature Review. Sustainability, 18(1), p.185.
27. Fadi, O., Karim, Z. and Mohammed, B., 2022. A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments. IEEe Access, 10, pp.93168-93186.
28. Sindhu, S., 2024. A blockchain-enabled framework for secure data exchange in smart urban infrastructure. Journal of Smart Infrastructure and Environmental Sustainability, 1(1), pp.31-43.
29. Demirbaga, U. and Aujla, G.S., 2022. MapChain: A blockchain-based verifiable healthcare service management in IoT-based big data ecosystem. IEEE Transactions on Network and Service Management, 19(4), pp.3896-3907.
30. Kumar, M., Samriya, J.K., KaurWalia, G., Verma, P., Wu, H. and Gill, S.S., 2025. Blockchain empowered secure federated learning for consumer IoT applications in cloud-edge collaborative environment. IEEE Transactions on Consumer Electronics, 71(2), pp.3986-3996.
31. Tyagi, A.K. and Seranmadevi, R., 2024. Blockchain for enhancing security and privacy in the smart healthcare. Digital Twin and Blockchain for Smart Cities, pp.343-370.
32. Kumar, P.M., Rawal, B. and Gao, J., 2022, January. Blockchain-enabled privacy preserving of IoT data for sustainable smart cities using machine learning. In 2022 14th international conference on COMmunication systems & NETworkS (COMSNETS) (pp. 1-6). IEEE.
33. Uma Maheswari, J., Somasundaram, S.K. and Sivakumar, P., 2024. Hybrid optimization enabled secure privacy preserved data sharing based on blockchain. Wireless Networks, 30(3), pp.1553-1574.
34. Alsadhan, A., Alhogail, A. and Alsalamah, H., 2024. Blockchain-based privacy preservation for the internet of medical things: a literature review. Electronics, 13(19), p.3832.

35. Nazir, A., He, J., Zhu, N., Anwar, M.S. and Pathan, M.S., 2024. Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain. Cluster computing, 27(6), pp.8367-8392.
36. Eren, H., Karaduman, Ö. and Gençoğlu, M.T., 2025. Security and Privacy in the Internet of Everything (IoE): A Review on Blockchain, Edge Computing, AI, and Quantum-Resilient Solutions. Applied Sciences, 15(15), p.8704.
37. Nandanwar, H. and Katarya, R., 2024, December. A secure and privacy-preserving ids for iot networks using hybrid blockchain and federated learning. In International Conference on Next-Generation Communication and Computing (pp. 207-219). Singapore: Springer Nature Singapore.
38. Nandanwar, H. and Katarya, R., 2025. Secure and Privacy-Preserving Data Sharing in 6G-Enabled Blockchain IoT Healthcare Systems. Security and Privacy, 8(6), p.e70105.
39. Loganathan, R. and SelvakumaraSamy, S., 2025. An efficient privacy-preserving authentication scheme for internet of vehicles based on blockchain technology with hybrid adaptive network. Peer-to-Peer Networking and Applications, 18(3), p.99.