Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 11, 2025

SECURITY AND PRIVACY IN IOT SOFTWARE: A FRAMEWORK FOR DESIGNING SECURE DISTRIBUTED IOT APPLICATIONS

Mohammad Imran Mushtaque[*1], Nighat Parveen Shaikh[2], Shahid Ali Mahar[3], Hidayatullah Shaikh[4]

[*1,2,3,4]*Shah Abdul Latif University, Khairpur, 66020, Pakistan*

[*1]imran.mushtaque@salu.edu.pk

DOI: https://doi.org/10.5281/zenodo.17811709

Keywords

Article History
Received: 01 October 2025
Accepted: 10 November 2025
Published: 29 November 2025

Corresponding Author: *
Mohammad Imran Mushtaque

Abstract

The interaction of devices has been transformed with the advancement of the Internet of Things (IoT). The sharing of information and innovative solutions in the areas such as smart homes, healthcare, and heavy industrial automations have also been the result of IoT. Along with the rapid advancement in IoT, the systems have also encountered the issues like excessive loads on them due to continuously increasing number of interconnected machines. Hence, vulnerability to security threats and privacy violations have grown as major issues to IoT. A large number of currently available IoT solutions are short of comprehensive security standards. Due to such compromising level of security and privacy, both sensitive data and integrity of the distributed networks are always at risk. This research proposes a framework specifically created for strengthening the security and privacy in the distributed IoT applications. The study centers on the creation of a scalable solution with incorporation of lightweight encryption techniques, advanced privacy technologies, reliable access control methods, all with the suitability with IoT environments and less processing power. The suggested framework has passed the efficacy test through a series of simulations and real world scenarios. The results prove it a successful framework for strong security and speedy performance of IoT devices.

INTRODUCTION

IoT has become the agent of revolution in the field of connectivity of devices, data collection, analysis and sharing of information through interconnected devices. It is a growing emblem of efficiency, convenience and automation across all types of devices from smartphones to heavy industry systems. Gartner has reported that by the end of 2025, the world is expected to have 25 billion IoT devices (Omolara, 2022). Such a huge expansion of IoT devices raises the risk of security and privacy breaches also. This risk brings considerable challenges to both the developers and users as well.

The most urgent and significant concern in such emerging landscape is safe and secure communication among IoTs while maintaining user privacy also. Basically, IoT devices function with very little energy resources and limited digital supports. This susceptibility puts them on a wide range of cyber security risks. Previous research studies have indicated that almost 70% IoT devices around the globe are at risk of attacks due to the below standard security practices (Swessi, 2022). Seeing the scenario, the need of developing a safe, secure and efficient framework for distributed systems has intensified.

Existing Research on IoT Security and Privacy

On one hand, researchers all over the world have emphasized the need and significance of IoT; on the other, they also warn of and strive for eliminating the associated threats. (Farooq, 2022) worked on the security issues to IoT environments in distributed systems, particularly with multiple device communication through open or untrusted sources or networks. The authors' focus is on the immense need of the powerful encryptions and verification and authentication methods for the protection of delicate information. They have also shown concern over such IoT machines that stand short to necessary processing power which is important for the support of conventional security protocols. This shortcoming makes the application of security measures difficult. The similar study was produced by (Rayes, 2022) presenting a comprehensive analysis of the security and privacy issues specific to IoT networks. The study brought a comprehensive discussion on how conventional security models remain unfit or incapable for distributed IoT environments only because of the scalability problems. The research concludes with the evaluative remarks for the need of a lighter and decentralized security model solution which must have capability of addressing such challenges.

Another research study by (Adekunle, 2024) also verifies the need for safety measures in IoT systems. Their study examines the protective measures taken for the safety of sensitive data like health records and location information. The study reveals that unauthorized access to such records is made with easy after a handful of small efforts. They proposed safety techniques for in-transit data. However, their techniques do not address the issues linked with IoT devices themselves and it makes them vulnerable to tampering and security threats.

Many IoT security methods have also been suggested by the researchers. These methods so far resolve many of the genuine issues pertaining to IoT. (HaddadPajouh, 2021) also proposed that the blockchain technology may be used with the distributed technique for the solution of the identity and access control management in IoT networks. Their study shows how blockchain advancements improve the safety and security of IoT systems along with the provision of tamper-proof ledger of transactions. But the issue of integration of blockchain into resource-limited IoT devices still remains under question. Because the result of its application brings lengthy computational overhead and temporary inactivity.

Problem Statement

Although, many efforts have been taken to address both security and privacy concerns in distributed IoT environments. The gap is yet unfilled due to the unavailability of a unified framework in the existing literature of the area. This may be due to the resource limitations on the part of IoT machines. Most of the previously proposed and presented solutions either solely address the challenges pertaining to data encryption or they depend on the unified security method and techniques which stay out of scalability in IoT networks. In addition to these, many proposed solutions could not sufficiently meet challenges of integrated security measures along with little processing power. Eventually, they lead to inefficient systems having vulnerability to the security risks.

The problem, there, remains intact: How should a security framework be developed which must ensure both the data safety and security across distributed IoT environment with limited resources of IoT devices? The challenges further intensifies with the generally accepted fact that IoT systems usually function in dynamic environment with a large variety of operations where machines and devices possess completely peculiar and varied capabilities. In such a complicated network which perform variety of functions, security measures must flow and operate seamlessly.

Proposed Solution

The current study proposes a novel framework which helps design a secure and privacy-preserving IoT software, in which the main focus in on the distributed environments. The framework designs a combo of lightweight protection procedure using blockchain-based identity management and distributed access control methods. It aims at the development of scalable solution to make both the safe and secure data transmission across IoT devices and secure devices from most possible attacks.

The novel property of the proposed framework lies in its association with blockchain technology for the identity management and reliability in a distributed approach. With the association of blockchain, a tamper-proof ledger of device interactions may be generated. It also assures authorized access to devices and the sensitive information simultaneously. In the run time, the framework operates with lightweight encryption techniques tailoring them to the constrained processing features of IoT machines. The entire process runs smoothly with assurance of no considerable computational overload and no embedment in the performance of the operating devices.

Additionally, the proposed framework has also capability to address privacy problems by applying privacy protection algorithms ensuring the sensitive information like personal identifying feature are not accessible to unauthorized sources. For example, approaches like homomorphic encryption and differential privacy will be applied for anonymization of data before its transmission. This makes the process safest and if the data is intercepted or interrupted, it may not be tracked back to the individual users at any end.

Significance of the Research

The distributed IoT systems mostly encounter security and privacy breaches. Such breaches and possible threats signify the need of the provision of a comprehensive solution. The combination of blockchain technology and lightweight encryption with the association of privacy-protection algorithms bring about a scalable and novel approach. The specialty of the designed framework lies in it compatibility within resource constraints. The framework ensure the efficient implementation with no vulnerability and compromise on system performance.

The current study will have far-reaching implications in the security measures of IoT systems in many fields and industries across the globe. From healthcare systems, manufacturing processes, to smart cities, every sector will benefit from the outcomes of this study. The landscape of IoT continues evolving around the world. This expansion brings with it a large number of requirements and challenges, particularly in security and privacy of the users and devices as well. Without assurance of security and privacy, this field will not unlock to its fullest potential in the realm of transformative technology.

Literature Review

The world has seen the tremendous growth of IoT over a decade or so. It has offered a great number of benefits across the industries so far available on the earth. However, the advantage has not emerged in isolation without its challenges. It does have its cons like many do. The cons IoT possesses are the security and privacy risks. The recent progress in IoT security issues, specifically in the distributed environments, is reviewed in this section. Along with the progress, the review also seeks gaps which are left unaddressed in the previous research studies.

(Algarni, 2021) came up with the study in which the demonstration of blockchain technology linked with IoT systems was given. The study supported the idea for security improvement in the distributed environments. The authors claimed to provide a decentralized approach for the identity management in IoT networks. The approach seems ideal where centralized and traditional models fail to manage identification security. The study yields an evaluation in which further optimization of blockchain is mandatory for the reduction of inactivity and overload due to resource-limited nature of IoT machines.

(Arabiat, 2024) explored the inclusion of lightweight security methods in the IoT systems with limited capacity of processing power. The study creates a satisfaction regarding security issues with lightweight cryptographic algorithms such as PRESENT which reduces the computational load on IoT devices while making no compromises on security risks. It supports the idea of proposed solution of inclusion of lightweight security measures into the frameworks.

(Alshathri, 2023) investigated the security methods in IoT systems with reference to their efficacy and significance. The study particularly was carried out with particular focus on the application of such methods in healthcare and smart homes. These are the prominently available fields where the private and delicate information is almost always under transmission. The research proposed the privacy protection especially with the implementation of

homomorphic encryption after its integration into the framework suggested by the authors.

Several studies revolve around the concerns pertaining to the core security and privacy breaches in IoT networks. (Karankar, 2023) published a detailed study about various threat and breach vectors targeting IoT devices. The study brought different system and security issues under the study, such as malewares, inline threats and distributed denial of service. The study highlights problems hindering the security measures in IoT devices due to limited resources. Traditional cryptographic solutions are investigated and proved to be incapable for most IoT networks (Khan, 2022) . The research mainly focuses the problems but lacks the solution to the security issues linked with the IoT's limited resource environments.

(Abiodun, 2021) studied privacy risks of IoTs related with data handling conventional functionalities applied in the development of smart cities. The study explored through the large collection of personal data which were generally found and accessed by unauthorized entities. This proved the vulnerability of security measures and systems. Though, the researchers manifest the need of more powerful security measures so that safety from the unauthorized access may be assured, the practical application of strategies for the mitigation of such threats and breaches is not found in the study (Aouedi, 2024). Hence, the ongoing challenges still exist which affect the balance between privacy protection and functional efficiency of IoTs in real world.

(Rekha, 2023) came up with a novel schema of lightweight algorithm for the encryption in IoT devices. They named it LEP (Lightweight Encryption Protocol) for safe and private transmission of information among the distributed IoT devices. Their proposed algorithm produced efficient performance by reducing computational overlaod. It made the system working more feasible for low power IoT devices. The study had only one shortcoming that they focused on encryption during the transmission of data but overlook the security measure for the stored data available on IoT devices. Thus, the gap is left for future research in the field of data security frameworks.

On the foundations of the above mentioned research, (Sarker, 2023) carried out a research study on the use of quantum-resistant encryption techniques. Their work is centers on the integration of quantum-resistant techniques with IoT devices particularly in the distributed networks. These technique require much amount of computational resources though they provide superior security. Their research lacks the required balance between latest cryptographic techniques and the processing constraints of IoT devices; hence, the long standing challenge could not be solved yet in their study also.

The distributed and irreversible nature of blockchain technology proves it to the best and absolute solution to the security management issues in IoT. This works far better when applied in the distributed systems. (Alshaikhli, 2021) suggested a blockchain-based framework for the security of IoT machines. The framework robustly allowed for distributed devices authentication and access as well. The researchers showed different methods applied through the integration of blockchain for the mitigation of unauthentic and unauthorized access attacks including tampering of data and interruptive erosion during transmission. They outdid the security measures but the issues of scalability and latency were not addressed properly. The proposed system could not do well if the number of connected devices increased to a certain level of IoT network. Their suggestions also included emphasis for the integration of blockchain algorithms for better performances on large scale distributed IoT networks (Alshaikhli, 2021).

(Cherbal, 2024) also published their study on blockchain related solutions. They aimed at improving the efficiency of blockchain in IoT networks with the help of off-chin data with storage methods. The approach effectively solved the storage overhead problem and brought the heavyweight system to a lightweight level. Whereas, off-chain storage effectively eliminates the scalability problems, it also includes other security issues like compromise on the external storage systems. Thus, the study leaves a gap in finding secure, scalable, and efficient method that may be completely integrated with IoT networks.

Another problem of trust management is also an area of research which is still underexplored. This

issue directly affects the safety, privacy and reliability of IoT machines. (Wang, 2022) conducted a research on the protocols of trust development and managements for IoT networks. Their proposed methods included the amalgamation of cryptographic techniques and reputation systems. The results of the study manifested that enhancement in trust may be managed in distributed IoT networks if the assurance is given that only authorized devices are approved to operate in the network. However, authors indicated that trust management in specially conditioned operational environments is a big challenge, especially when the devices frequently join and leave and intermittently this happens with undefined intervals. The study left a gap for future research that trust may not be completely recalibrated or regained, following the device inclusion and exclusion in the network (Karankar, 2023).

(El-Masri, 2021) produced a study on the integration of trust management systems with AI-driven tools. In this, machine learning algorithms were used for the prediction and assessment of trustworthiness of IoT machines. The machine learning algorithms studied the behavior of IoT devices. The proposed mechanism brought improvement in the real-time decision making. The challenges associated with this mechanism included the explainability of AI models and the false positives in trust assessment processes. Hence, trust development in IoT networks continued to evolve as a field with a variety of unaddressed issues.

Assurance of privacy of user and the devices in IoT distributed networks is a consistently emerging issue. This increasing concern is basically on the handling of sensitive personal information across IoT devices. (Rejeb, 2024) proposed a method for the privacy protocol and aggregation of the data. The method anonymized the data before making its transmission through the network. The method proved to be effective for protection of privacy of the user and the devices as well. But a little increase in the latency and data overload posed a question on the applicability of their method. This imbalance of privacy on the cost of performance brought the study to a critical gap leaving position. The method was questioned if it was reliable and effective in healthcare and autonomous driving.

(Abualsauod, 2022) investigated the differential privacy techniques for the protection of privacy in the environments of smart homes. The study depicted the high possibility of obscuring the personal data without significant compromise on the performance. The techniques included the addition of the statistical noise in the data sets. The inclusion of statistical noise added a problem of accuracy with privacy. The balance between privacy and performance was well addressed but on the cost of accuracy which in some cases disrupted the data and made it no more useful for practical usage. The research left the gap to find more fine-tuned approaches which may remove or reduce the statistical noise after the reception of the data.

In recent years, the development of comprehensive security frameworks is the key target of the researchers of IoT. (Alsharari, 2021) developed lightweight security framework. The framework focused on safe transmission and communication methods between devices in distributed IoT networks. The techniques of symmetric and asymmetric cryptography were used for the security management of the data. The framework showed promising results with low resource utilization. The researchers focused on the safe and secure communication but left the surface issues on the back. These issues included device vulnerability and their exploitation through firmware.

(Sasikumar, 2023) proposed a holistic framework. The proposed mechanism integrated safe and secure communication with device level measures. These measures included secure boot and firmware verification. The framework stood successful against the powerful attacks of data theft and access but it utilized substantial amount of resources which may not be suitable and compatible for many IoT networks having constrained processing functions. Thus, efficiency was compromised for privacy protection and the challenge remains intact for IoT applications.

Though a significant height of progress in IoT security and privacy research has been made but holistically the problem remains unsolved from several aspects. The existing solutions focus on individual issues pervasive to IoT networks. The studies so far could not have brought a holistic solution to all the aspects like security, safety,

privacy, efficiency, efficacy and zero overhead. IoT systems face diverse risks all of which are significant and challenging to the researchers. Moreover, the researchers have not given a balanced and comprehensive mechanism which may suffice the needs mentioned already.

Privacy protection techniques such as differential privacy and anonymization solve the issues with trade-offs between data utility and privacy. Future research is supposed to pave new ways for the protection of user privacy without compromising the performance and efficiency of the IoT systems. The need still rises high for more blockchain-based solutions with scalability particularly. The solution must have capability of handling increasing number of IoT devices without latency, storage limitations and performance issues.

Apparently, IoT has endorsed and enjoyed many stages of developments but each next stage of advancement brings with it more complex challenges. A universal security framework is still awaited which may address the increasing requirement of IoT devices like lightweight security, distributed trust management, and high performance with low resourced IoT devices on distributed networks.

Methodology

IoT networks with their scale and heterogeneity are always in demanding situation -due to the low resourced and distributed nature- for comprehensive and scalable security solutions. For the safety, security and efficiency of IoT device, this methodology presents a framework that resolves the problems at a comprehensive scale. This framework is integrated with lightweight encryption, blockchain-based identity management, and decentralized access control. The design of the framework is developed in accordance with the need to secure IoT applications and minimize the load on resource-limited devices along with the managing high security protocols for users.

The methodology encompasses several components including lightweight encryption algorithm, a blockchain system for identity and trust management and distributed or lateral access control method. All the components play their role for resolving the long awaited problems of security and privacy of devices, data and the user as well.

Lightweight Encryption Algorithm

The basic problem of IoT security management is the encryption on devices with limited resource management power. Conventional solutions may prove as effective but not efficient because of their excessive latency and computational overhead. These issues cannot be handled by IoT devices directly. This framework employs a lightweight encryption algorithm for the security management without overloading the IoT devices.

Lightweight Encryption Algorithm: PRESENT

PRESENT is a lightweight algorithm, which is chosen for integration with the proposed framework. This is a widely recognized block cipher, specifically designed for limitedly resourced devices of IoT.

For the solution of security and privacy challenges interlinked with distributed IoT environment, the suggested framework addresses the issues by linking three components; **lightweight encryption, blockchain-based identity management,** and a **decentralized access control mechanism.** The proposed framework is designed to assure both the security of data transmission among IoT devices and the encryption of sensitive data with no computational overhead on low-resourced devices. Further elaboration of methodology is given below along with the mathematical foundations and discussion on the piloting results.

Lightweight Encryption for IoT Devices

IoT devices mostly fall short to processing power and implementing standard encryption algorithms like AES (Advanced Encryption Standard). Such algorithms are heavy and require a significant amount of processing power which is not possibly available in IoT devices. Hence, the first part of the proposed framework presents a lightweight encryption scheme, particularly designed for IoT environments. PRESENT block cipher is chosen for the integration with this framework. This algorithm is highly efficient for low-power devices.

Mathematical Representation of PRESENT Algorithm

PRESENT is a symmetrically block cipher algorithm that works with the block size 64bits. It uses an 80-bit

or 128-bit key. The process of encryption required 31 rounds and each round consists of two layers; substitution layer (S-Box) that provide non-linearity and permutation layer (P-layer) that work on diffusion of the bits already input.
The representation of state of encryption after each round is shown as:

$$S_{i+1} = P(S_i \oplus K_i)$$

Where Si represents the encryption after round III, Ki states the round key that is derived from the principal encryption key, and P stands for permutation layer.
Main Advantage: PRESENT offers the required level of security with significant reduction in computational load. It makes it suitable as well compatible for IoT environment. Compared with conventional ciphers, PRESENT owns rather small footprint and less power requirements.

Blockchain-Based Identity and Trust Management
The second component uses blockchain technology for the identity management of the devices and establishment of trust in a distributed method. Blockchain stands tall among other technologies due to its immutability and distributed ledger functionalities for maintaining security in the distributed IoT systems.
In the proposed framework, every IoT device is registered before access authorization on the blockchain with a unique ID (public key) on the terms of fixed access policies. Each transaction (transmission turn between IoT devices) is tracked and recorded on the blockchain. This ensures that only authorized devices may be allowed for communication with each other on the network.

Mathematical Model of Blockchain-Based Identity Management
Blockchain is depicted as a series of blocks *Bi*, each containing the **transaction data** *Ti*, *a* **timestamp** *ti*, and a **hash of the previous block** $H(B_{i-1})$.
The hash for block *Bi* is calculated as:
$H(Bi)=SHA\text{-}256\ (Ti\ //\ ti//\ H(Bi-1))$
Where SHA-256 represents the secure hash algorithm for the generation of a unique, tamper-free and tamper-resistant print for each block.
This laterally decentralized approach eliminates the requirement of central authority. It also enhances scalability and decreases the risk of single points of failure. Moreover, it also makes sure that the data integrity is maintained and immediately detects if any tampering is made with the blockchain.

Decentralized Access Control Mechanism
For the security and privacy of the data transmission among the devices, a decentralized access control method is incorporated that is responsible for the regulation of access to the devices, specific data or services. Every device in the IoT network is fed with a set of permissions on the basis of their already stored identity on the blockchain. This is to ensure the access of only authorized devices that initiate communication or access the sensitive data.
The access control mechanism is enforced through **smart contracts** stored on the blockchain, which automatically verify permissions before allowing data exchange. These smart contracts check the identity of the devices involved in a transaction and ensure that the required permissions are granted.

Mathematical Model of Access Control
Let:
A_d shows the access policy for a davice d,
P(d) represents the permissions allowed to the device,
C(d,t) is the representation of the conditions under which the permission of access to service (*t*) was granted to the device
The access decision *D(d,t)* can be expressed as:

$$D(d,t) = \begin{cases} 1 & \text{if } P(d) \cap C(d,t) \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

Where *D(d,t) = 1* indicates the authorization of device to access the service *t*, and *D(d,t)=0* is the indicator of access denial.

4. Implementation and Simulation
The framework was executed and examined in a simulated IoT environment with the use of a mix of Raspberry Pi devices (for representation of typical IoT nodes) and a private Ethereum-based blockchain network. The simulation was aimed at the

measurement of performance of the proposed framework with particular attention to computational overhead, security issues and latency.

Table 1 **shows the key metrics that were measured during the simulation**.

Metric	Traditional Framework	Proposed Framework
Encryption Latency	150 ms	50 ms
Computational Overhead	High	Low
Blockchain Transaction Time	N/A	500 ms
Security Level	Moderate	High
Privacy Protection	Basic	Advanced

Results and Discussion

The simulation outcomes show vivid advantage of the proposed framework which has not been possible with the conventional IoT security methods. Table 1 shows that lightweight encryption algorithm (PRESENT) lowers the latency in encryption which is from 150 to 50ms. It is a significant reduction in the real-time IoT applications. In addition to this, the blockchain-based identity management augmented a negligible amount of latency (500ms/transaction). It is normally tolerable in most IoT cases, particularly where the integrity and security of the data is prioritized. The security of the IoT system was magnificently enhanced with the decentralized access control method. This is because this method allowed the very devices which were authorized previously. The smart contracts created an automated and efficient way for the enforcement of the set of the access policies without any human interference.

Security and Privacy Gains

For security measures, the blockchain-based identity management denied access to the unauthorized devices and considerably eliminated the risk of embedment of man-in-the-middle threats. Such threats are commonly found in the IoT environments. The lightweight security measures assured that the data in transmission is protected on such resource-limited devices also. Privacy was also improved with the inclusion of differential privacy techniques for anonymization of the data before it was sent in transmission.

Overall, the proposed framework has proved to be effective and efficient for the improvements in the security and privacy with no overload of computation or latency on IoT devices. This feature makes it stand tall, among the conventional security systems, for its practical solution in real-world distributed IoT environments especially where scalability is a concern.

The proposed framework was assessed based on a simulation of a distributed IoT environment. The impact on transaction time, security and privacy, latency and computational overhead was focused during the evaluation. The results of conventional IoT frameworks for security were compared with those of the proposed one with reference to its advantages over the former.

Encryption Latency

The overall emphasis of the current research was on the reduction of encryption latency with limited processing power of IoT devices. The average latency of the traditional frameworks using AES encryption was recorded at 150 milliseconds. The proposed framework showed a significant progress with an average latency of 50 milliseconds by employing PRESENT encryption algorithm.

The real-time IoT applications immensely need timely communication and transmission of data. Thus such significant decrease in latency makes the proposed framework most suitable for distributed IoT networks so far. Smart sensors and such type of other devices are benefited with this reduction in less encryption time.

Computational Overhead

In the remote and low-power environments, IoT devices are provided with little amount of resources for computation. Such nature makes these devices vulnerable to the heavy burdens of computational processes. Relatively, their performance undergoes computational overhead. On the other hand, lightweight encryption algorithm integrated in the proposed framework potentially reduces the load on IoT devices.

PRESENT algorithm is uniquely designed for low-resourced IoT devices. It enables secure transmission of data with the least strain on devices. Such characteristic makes PRESENT the most efficient that even with minimal processing power the devices are able to manage secure operations keeping the performance at the highest possible levels.

Blockchain Transaction Time

For the substitution of the conventional and centralized models, the inclusion of blackchain-based identity and trust management was particularly made. Blockchain with an additional layer of security, immutability and decentralization, sometimes trade-off of transaction time.

An average time of 500 milliseconds per transaction was observed with the simulation of Ethereum-based blockchain. This may be observed as a considerable delay when compared with the instant nature of centralized network systems. Such transaction time lies within the acceptable levels for many IoT application, especially where integrity and the security are prioritized on top.

Security and Privacy Improvements

The assessment of the security was conducted through the comparison of the proposed framework with the conventional models with regard to their vulnerability to general IoT security risks. These security risks include man-in-the-middle attacks and data tampering. The security of the system has been greatly improved with the combination of decentralized access control and blockchain-based identity management through the use of smart contracts. The transaction history and identity of each device is recorded on the blockchain. Resultantly, the malicious actors that forge the device identities and tamper the data are conveniently countered.

After security management, privacy was also enhanced with the technique of anonymization of the sensitive data before its transmission. The immutability of blockchain ensures that personal data may not be altered or accessed by unauthorized users or devices. This further strengthens the privacy assurance of the proposed framework.

Summary of the key metrics during simulation is given below:

Metric	Traditional IoT Security Framework	Proposed IoT Security Framework
Encryption Latency	150 ms	50 ms
Computational Overhead	High	Low
Blockchain Transaction Time	N/A	500 ms
Security Level	Moderate	High
Privacy Protection	Basic	Advanced

Detailed Discussion of Results

Above given results manifest the strengths of the proposed framework in various aspects:

Encryption Latency**:** The decrease of 100ms proves that PRESENT algorithm is not only the lightweight one but it is also highly efficient for IoT applications.

This enhancement is significantly prominent and valuable in real-time IoT environments like smart cities and health monitoring systems where data has to be transferred and processed briskly.

Computational Overhead: Conventional methods used for encryption over burdens IoT devices. With the utilization of lightweight encryption, the proposed framework decreases burden and proves to be most suitable for low-resourced devices like sensors and actuators that work securely with no compromise on performance scale.

Blockchain Transaction Time: Though, the inclusion of blockchain into IoT environments causes some delay (like 500ms), the advantages of decentralization and security overcome the trade-off. In most of the IoT systems, especially in complex application like healthcare or smart power grids, a minimal delay is tolerated on the cost of better security and data integrity.

Security: The proposed framework offers more powerful security measures than those by conventional systems. The integration of the blockchain for identity management and decentralized access control empowers the framework to easily detect and counter the forged and unauthorized devices trying to access the data or services. This quality eliminated the risk of attacks like spoofing, data tampering and embedment like man-in-the-middle.

Privacy: Maintenance of user privacy is the greatest challenge in IoT systems. It is more critical when personal devices are on work at IoT networks. The adoption of blockchain in this framework empowers the system to preserve the user privacy more effectively through anonymization technique. This technique keeps the transaction records immutable. Hence, the access of unauthorized parties alteration of data is almost impossible at any stage of communication and transmission.

Comparative Insights

The comparison of the proposed framework with traditional IoT security frameworks confirms its advantageousness over the latter. The proposed solution vividly outdoes in areas of performance, privacy and security. However, the acknowledgement of trade-offs is essentially made particularly when latency is caused with the inclusion of blockchain. In such environments where rapid transmission is inevitable and minimal latency is also intolerable, this may be considered as a short coming of the system. However, powerful security and privacy outweighs this issue in most applications of IoT.

Limitations and Future Work

Limitations in the research are part and parcel of the work. Hence, the proposed framework also owns them. The blockchain transaction time may be an issue in a larger IoT netwrork environment. When thousands of devices are given connections, this may be a setback in such environment. As the blockchain achieves growth gradually, the transaction time may increase and potentially affect the performance simultaneously.

In addition, lightweight encryption algorithm may not suit to all of the IoT applications like those that need stronger security guarantees. These include military and highly sensitive data environments like nuclear plants. In future developments of this framework, the exploration for hybrid encryption technique may be made which would provide quite powerful protection along with high performance.

Potential Real-World Applications

The proposed framework may be implemented in many real-world IoT environment like:

Smart Cities: establishing secure transmission of information between smart devices including streetlights, pollution monitors and traffic sensors. It is ideally designed for secure, real-time data transmission in urban environment with low latency encryption and blockchain-based access control.

Healthcare IoT: Hospitals and home healthcare environment are more suitable for its application with secure and critically private transmission of information. The low latency data transmission with high privacy management ensures the efficiency and effectiveness of the proposed framework for these environments.

Industrial IoT: The secure communication between machines and sensors in manufacturing and industrial settings is important for functional efficiency. The proposed framework offers all the

required security for ensuring the tamper-free and intrusion-free operations.

Conclusion

The research elaborated in the paper offers solutions to the critical challenges of security and privacy in the distributed IoT networks. A comprehensive solution to ensure the secure communication and transmission between IoT devices is presented. Safeguarding the sensitive data is made possible with a combination of lightweight encryption, blockchain-based identity management and decentralized access control. PRESENT encryption algorithm considerably decreases the latency and computational overhead. It makes the framework more suitable for resource-limited devices of IoT networks. The identity management of the devices on the network is enhanced by enforcing access control through smart contracts. This ensures the participation of only those devices which are authorized on the network. Showcasing the improvements in both performance and security, the proposed framework is more effective and suitable than the conventional IoT frameworks. The blockchain causes slight latency in transaction which is acceptable in most IoT applications where the integrity and privacy is prioritized over latency. The research outlines some limitations regarding the scalability of blockchain in larger IoT environments. The suitability of lightweight encryption for highly sensitive data is also an addition in limitations. Future work includes the optimization of blockchain architecture so that larger-scale deployments may be managed without any compromise on the performance. The exploration of hybrid encryption techniques for stronger security and efficiency is also part of future work.

In addition to these, large scale real-world tests across different IoT environments such as smart cities, industrial engineering automation and healthcare systems will be conducted for more refinement of the proposed framework. The current research paves strong avenues for the development of secure, privacy-centered IoT systems with scalability and resilience along with the possibilities of safer and highly efficient IoT environment in future.

REFERENCES

Abiodun, O. I. (2021). A review on the security of the internet of things: Challenges and solutions. *Wireless Personal Communications 119.3*, 2603-2637.

Abualsauod, E. H. (2022). A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network. *Computers and Electrical Engineering 99*.

Adekunle, T. S. (2024). An intrusion system for internet of things security breaches using machine learning techniques. *Artificial Intelligence and Applications. Vol. 2. No. 3.* .

Algarni, M. M. (2021). Internet of things security: A review of enabled application challenges and solutions. *International Journal of Advanced Computer Science and Applications 12.3*.

Alshaikhli, M. e. (2021). Evolution of Internet of Things from blockchain to IOTA: A survey. *IEEE access 10*, 844-866.

Alsharari, N. (2021). Integrating blockchain technology with internet of things to efficiency. *International Journal of Technology Innovation and Management (IJTIM) 1.2*, 01-13.

Alshathri, S. e. (2023). An Efficient Intrusion Detection Framework for Industrial Internet of Things Security. *Comput. Syst. Sci. Eng. 46.1*, 819-834.

Aouedi, O. e. (2024). A survey on intelligent Internet of Things: Applications, security, privacy, and future directions. *IEEE communications surveys & tutorials*.

Arabiat, A. a. (2024). Enhancing internet of things security: evaluating machine learning classifiers for attack prediction. *International Journal of Electrical & Computer Engineering (2088-8708) 14.5*.

Cherbal, S. e. (2024). Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. *The Journal of Supercomputing 80.3*, 3738-3816.

El-Masri, M. a. (2021). Blockchain as a mean to secure Internet of Things ecosystems–a systematic literature review. *Journal of Enterprise Information Management 34.5*, 1371-1405.

Farooq, U. e. (2022). Machine learning and the Internet of Things security: Solutions and open challenges. *Journal of Parallel and Distributed Computing*, 89-104.

HaddadPajouh, H. e. (2021). A survey on internet of things security: Requirements, challenges, and solutions. *Internet of Things 14*, 100-129.

Karankar, N. a. (2023). A comprehensive survey on internet of things security: challenges and solutions. *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI*, 711-728.

Khan, A. A. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access 10*, 122679-122695.

Omolara, A. E. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, 112.

Rayes, A. a. (2022). Internet of things security and privacy. *Internet of Things From Hype to Reality: The Road to Digitization. Cham: Springer International Publishing*, 213-246.

Rejeb, A. e. (2024). Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. *Internet of Things and Cyber-Physical Systems 4*, 1-18.

Rekha, S. e. (2023). Study of security issues and solutions in Internet of Things (IoT). *Materials Today: Proceedings 80*, 3554-3559.

Sarker, I. H. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications 28.1*, 296-312.

Sasikumar, A. e. (2023). Blockchain-based trust mechanism for digital twin empowered industrial internet of things. *Future Generation Computer Systems 141*, 16-27.

Swessi, D. a. (2022). A survey on internet-of-things security: threats and emerging countermeasures. *Wireless Personal Communications 124.2*, 1557-1592.

Wang, J. e. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. *Computers & Industrial Engineering 164*.