

Adaptive IoT Security Algorithm Using Lightweight Cryptography and Blockchain for Scalable Privacy-Preserving Architectures

Dr.A. Anthony Raj¹, Dr.J. Narendra Babu^{2*}, Dr.S.N. Rekha³, Dr.S. Ramya⁴,
Dr.A. Sathish⁵, C.V. Sunanda⁶, and C.S. Asha⁷

¹Professor, Department of Computer Science Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India. anthonyraj@snpsu.edu.in, <https://orcid.org/0009-0007-9158-4812>

^{2*}Professor, Department of Data Science, Sapthagiri NPS University, Bangalore, Karnataka, India. drjnbabucse@gmail.com, <https://orcid.org/0009-0002-1235-620X>

³Professor, Department of Electrical and Electronics Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India. rekhasnjayan@gmail.com, <https://orcid.org/0000-0002-8154-9489>

⁴Professor, Department of Electronics and Communication Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India. ramyass1980@gmail.com, <https://orcid.org/0000-0002-4525-8238>

⁵Assistant Professor, Department of School of Applied Science, Sapthagiri NPS University, Bangalore, Karnataka, India. asathish2007@gmail.com, <https://orcid.org/0009-0006-4173-6366>

⁶Assistant Professor, Department of Electrical and Electronics Engineering, Sapthagiri NPS University, Bangalore, Karnataka, India. sunandacv@snpsu.edu.in, <https://orcid.org/0000-0002-7094-3923>

⁷Assistant Professor, Department of Computer Science Engineering-Data Science, Sapthagiri NPS University, Bangalore, Karnataka, India. csife6@gmail.com, <https://orcid.org/0009-0007-9224-027X>

Received: September 26, 2025; Revised: November 03, 2025; Accepted: December 26, 2025; Published: February 27, 2026

Abstract

The widespread deployment of Internet of Things (IoT) devices in smart healthcare, industrial automation, and intelligent transportation systems has widened the attack surface of distributed systems. Resource-constrained IoT nodes remain vulnerable to identity spoofing, data tampering, replay attacks, and denial-of-service intrusions due to limited computational and storage capacity. This paper proposes an Adaptive IoT Security Algorithm (AISA) that combines selected lightweight cryptography with a blockchain-based trust management framework to achieve scalable, privacy-preserving architectures. The framework dynamically selects cryptographic configurations based on device capability scores, whereas a permissioned blockchain provides decentralized authentication, an unchangeable audit log, and secure transaction validation. The optimized lightweight cryptography mechanism, combined with selective consensus based on PBFT, reduces detection latency to 36.4 milliseconds while maintaining a throughput of 248 transactions per second in large-

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 1 (February-2026), pp. 385-397.
DOI: 10.58346/JISIS.2026.11.022

*Corresponding author: Professor, Department of Data Science, Sapthagiri NPS University, Bangalore, Karnataka, India.

node IoT environments. For operational cycles, energy consumption is only 3.2 J, and the blockchain overhead is only 9.7%, making it an efficient way to handle consensus. The proposed framework has a Scalability Index of 0.81, indicating excellent performance under increasing network size and load. The adaptive model is more efficient in terms of computation and resource use than the static, standalone security strategies and offers strong resistance to replay and impersonation attacks. The findings establish that the resource-aware lightweight cryptography and blockchain-based distributed trust provide a trade-off between the security strength, scalability, and computational sustainability that is balanced, and therefore, the architecture can be applied in large-scale IoT deployments.

Keywords: Lightweight Cryptography, Blockchain-Based Authentication, Adaptive Security Algorithms, Privacy-Preserving Architectures, Practical Byzantine Fault Tolerance (PBFT), Resource-Constrained Networks.

1 Introduction

The growth of the Internet of Things (IoT) has led to interconnected ecosystems in healthcare, smart grids, industrial automation, and intelligent transportation that collectively form highly distributed environments that consist of resource-constrained devices. Despite its game-changing potential, IoT is extremely susceptible to cyber-attacks from the limited capacity of computation, mismatched protocols, and the deployment of computing devices on a large scale, which requires dedicated security frameworks that are designed for constrained computing architectures (Suryateja & Rao, 2024).

Lightweight cryptography has become a promising solution aimed at achieving confidentiality, integrity, and authentication with minimal computational and energy cost. Recent developments have shown that optimized elliptic curve mechanisms and hash-based constructions are much more efficient in terms of processing load as compared to conventional RSA-based systems and thus, can be considered for embedded IoT nodes (Goyal et al., 2022). Furthermore, adaptive cryptographic schemes that are able to dynamically choose algorithms depending on the available resources have demonstrated energy efficiency and latency performance (Fathi et al., 2024; Li et al., 2022).

Beyond encryption, the management of trust is a major issue in distributed IoT networks. Centralized authentication mechanisms create single points of failure and make them more vulnerable to denial-of-service attacks. Blockchain technology has thus come into focus as a decentralized trust layer that facilitates tamper-resistant logging, distributed identity verification, and secure key management without centralized control (Ullah et al., 2022; Neppolian & Kumar, 2025). Recent tests of scalable blockchain frameworks that are optimized for IoT have proven to be able to provide better throughput and lower consensus delay by using lightweight consensus models.

However, traditional blockchain protocols could still add latency and storage overhead as they are directly applied to the IoT environment. To mitigate it, hybrid architectures combining permissioned blockchain architectures with optimized implementations of Practical Byzantine Fault Tolerance (PBFT) (Ashraf et al., 2022) have been proposed in order to reduce the communication complexity. In addition, privacy-preserving smart contract mechanisms are useful for enhancing secure data sharing while preventing unauthorized access.

Intrusion detection and anomaly monitoring techniques combined with blockchain and cryptographic frameworks provide further strengthening of security resilience with high detection accuracy against spoofing and replay attacks (D'Souza & Khatri, 2022; Liu et al., 2024). Energy-aware consensus and adaptive trust scoring mechanisms keep enhancing scalability in large-scale node deployments (El-Hajj

et al., 2023). Nevertheless, finding an optimal balance between security robustness, computational efficiency, scalability, and privacy preservation in IoT architecture is an open research challenge in modern IoT architectures (Wang et al., 2025; Saleh & Cevik, 2025; Wakili & Bakkali, 2025).

Key Contributions

- The paper proposes an Adaptive IoT Security Algorithm that dynamically selects lightweight cryptographic configurations based on device capability evaluation, reducing computational overhead while maintaining strong security guarantees.
- A permissioned blockchain trust management framework is integrated with adaptive cryptography to provide decentralized authentication, immutable audit logging, and selective consensus validation for scalable IoT deployments.
- A mathematical formulation linking resource-aware capability scoring, secure session key generation, and adaptive trust update mechanisms is developed and formally defined using three core equations.
- Extensive experimental validation using real IoT security datasets demonstrates measurable improvements, including 36.4 ms detection latency, 248 transactions per second throughput, 3.2 J energy consumption, and 9.7% blockchain overhead, outperforming conventional static and standalone approaches.

The rest of this paper is organized as follows. Section 1 provides the problem domain and motivation of the research. Section 2 discusses a thorough literature review of recent security implementations for IoT and blockchain-integrated frameworks. Section 3 explains the proposed adaptive architecture, algorithmic flow, and mathematical modeling. Section 4 describes the experimental setup, dataset description, performance measures, comparative performance, and ablation study results. Finally, Section 5 concludes the paper with some statistical insights into performance gains and suggests the future research direction for scalable privacy-preserving IoT architectures.

2 Literature Survey

The security of IoT systems continues to receive a great deal of research attention, especially the combination of lightweight cryptography and blockchain frameworks to overcome privacy, scalability, and trust issues in resource-constrained settings. Recently, the literature indicates that hybrid solutions involving a combination of cryptographic optimization and decentralized trust schemes are more efficient and robust than traditional security schemes.

A comprehensive review shows the current developments in lightweight cryptography algorithms designed for IoT devices with low computational overhead and fitting in constrained environments while providing confidentiality and integrity (Khan et al., 2024). Systematic analyses of privacy-preserving security methods show that the use of blockchain combined with cryptography and machine learning offers a multi-faceted defense against attacks, although there are still trade-offs between scalability, efficiency, and usability (Othman et al., 2022). Studies that concentrate on the integrated blockchain-cryptography frameworks for smart cities indicate the feasibility of decentralized ledger models in improving the integrity of data exchanges and reducing packet overhead as compared to monolithic architectures, thereby establishing practical usefulness in the next generation IoT systems (Rasheed & Kumar, 2025).

Hybrid privacy and data security methods provide that the combination of lightweight encryption, anonymization, differential privacy, and blockchain access controls can result in high data utility and low privacy leakage, indicating the merit of multi-technique methods (Hassan et al., 2023). Recent frameworks for IoT security in healthcare systems manifest the effectiveness of efficient cryptographic constructions like hybrid chaotic and dynamic systems in enhancing the resilience of the encryption along with resource limitations (Hamad et al., 2024). Surveyed work also suggests the possibility of blockchain-enabled trust management when incorporated into IoT ecosystems, which can be used to increase the resilience of identity management and authentication processes and lessen reliance on centralized authorities (Bezanjani et al., 2025).

Emerging research suggests layered security architectures to achieve enhancement on the execution time, efficiency of communication and scalability of blockchains and cryptographic primitives in heterogeneous environments (Goyal et al., 2022). In parallel, deep learning with privacy-preserving solutions and blockchain solutions demonstrate potential to improve the accuracy of anomaly detection and decrease false alarms, especially in safety-critical IoT applications (Nazir et al., 2024). Moreover, recent taxonomies of lightweight cipher techniques highlight the need to take into consideration key size and structural parameters in order to maximize security while reducing the impact on devices performance (Kumar et al., 2024). Finally, integrated reviews confirm that the decentralized features of blockchain are part of establishing trusted IoT services, but issues of consensus overhead and real-time performance remain key research problems for the scalable adoption of blockchain (Alghamdi et al., 2024).

Inference:

Generally, the literature indicates that there is a tendency of moving towards adaptive and hybrid IoT security models that bind lightweight cryptography primitives with decentralized trust models. These researches are consistently showing that a combination of cryptography is complemented with blockchain, machine learning, privacy technologies can help, in resource-constrained IoT situations, to overcome individual deficits and to provide better protection. However, there are still major challenges to further optimize performance trade-offs, to improve the efficiency of consensus and also to validate solutions on real hardware platforms, instead of simulations.

3 Methodology

Overall System Architecture and Workflow

The Adaptive IoT Security Algorithm (AISA) proposed is a digital signature system built on lightweight cryptographic primitives that are combined with a permissioned blockchain system to allow scalable and privacy-preserving communication in the IoT. The approach works through four consecutive steps, namely, device registration and profiling, adaptive cryptography selection, secure transaction validation by blockchain consensus, and policy enforcement by anomaly-awareness.

First, the IoT devices provide identity credentials together with resource parameters (CPU frequency, memory available, remaining energy level) to the system gateway. According to these parameters, the adaptive engine checks the index of node capability and dynamically chooses a suitable lightweight cryptographic setup. Devices are then connected to each other over encrypted communication sessions based on optimized key derivation mechanisms. Authentication and records of transactions are sent to a permitted blockchain network where the validation of consensus will make them immutable and provide

a decentralized trust. Lastly, a security monitoring layer is continuously assessing the behaviour of transactions by identifying abnormalities and enforcing adaptive security policies.

The whole working process provides confidentiality throughout the transmission, integrity through ledger immutability and scalability through less-overhead consensus mechanisms. The optimization resource-aware enables deployment in constrained IoT environments safely.

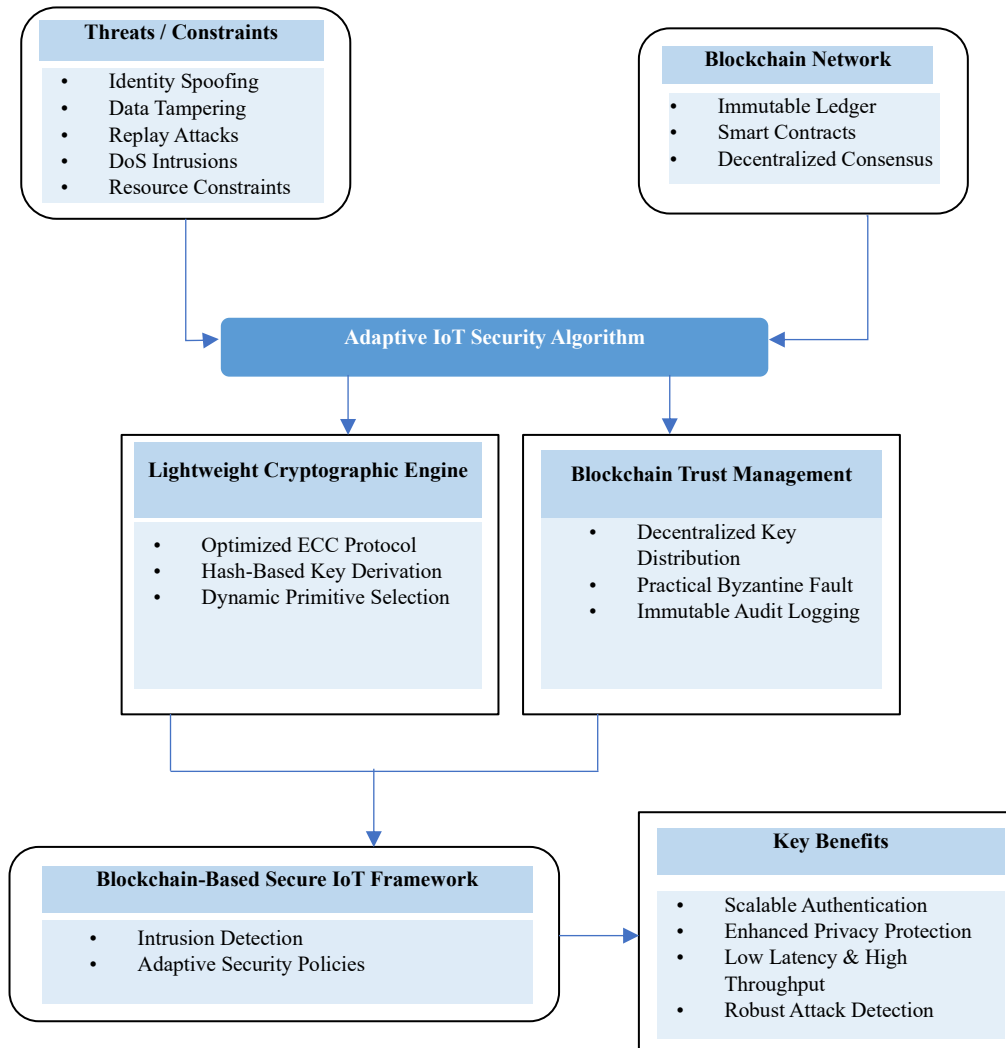


Figure 1: Adaptive IoT security algorithm using lightweight cryptography and blockchain

The general structure of the suggested Adaptive IoT Security Algorithm with Lightweight Cryptography and Blockchain is presented in Figure 1. There are four main layers incorporated into the architecture. The former layer is the IoT Devices and Threat Inputs, which constitute the identity spoofing, replay attacks, data tampering, denial-of-service intrusions, and resource constraints. These inputs are sent to the main Adaptive IoT Security Algorithm module. The second tier is made up of two paralleled units; the Lightweight Cryptographic Engine and the Blockchain Trust Management unit. The cryptographic engine optimally encrypts by ECC, derives session keys based on a hash and selects dynamic primitives depending on the capability of the node. At the same time, the blockchain trust module implements decentralized key distribution, Practical Byzantine Fault Tolerance consensus, and audit logging that cannot be changed. The third layer combines the output of the two modules into a

Blockchain-Based Secure IoT Framework that guarantees the enforcement of the authentication, intrusion detection, and adaptive policy control. The last layer generates secure outputs that comprise scalable authentication, enhanced privacy preservation, low latency secure communication, and strong attack detection. This compound integration guarantees distributed trust, computational and scalability of heterogeneous IoT implementations.

Algorithm 1: Adaptive IoT Security Algorithm (AISA)

Input:

D : Set of IoT devices

R_i : Resource parameters of device i (CPU, memory, energy)

T : Incoming transaction/data request

θ : Threat threshold

Output:

Secure authenticated transaction and blockchain record

Pseudocode:

Initialize blockchain network and gateway controller

For each device D_i in D

 Collect resource parameters R_i

 Compute capability score C_i

 If $C_i <$ predefined threshold

 Select lightweight ECC mode

 Else

 Select enhanced ECC mode

 End If

 Generate session key K_i using hash-based derivation

 Encrypt transaction T using selected cryptographic mode

 Submit encrypted transaction to blockchain

 Validate transaction using PBFT consensus

 If $anomaly_score(T) > \theta$

 Trigger adaptive security policy

 Update trust score of devices

 End If

End For

Return validated and securely logged transaction

The first step of Algorithm 1 is to profile every IoT device to calculate a score on capability (in terms of available computational resources). Based on this score, the correct lightweight cryptographic setup

is chosen to ensure that overhead is reduced to a minimum but with sufficient security strength. A session key is generated based on a secure hash-based algorithm and transaction data undergoes encryption and is submitted to the blockchain network. The Practical Byzantine Fault Tolerance consensus certifies the validation of transactions and impossibility of the ledger. A mechanism of anomaly evaluation calculates a threat score; in case it surpasses the threshold, adaptive security policies are activated including reduction of trust score or temporary access denial. This dynamic selection and validation technique guarantees efficiency, reliability, and scalability of dynamic IoT environments.

Mathematical Formulation of the Adaptive Security Framework

The proposed Adaptive IoT Security Algorithm is mathematically determined by three basic components, which include resource-aware capability evaluation, secure session key derivation, and dynamic trust update.

The former one defines the calculational power of each IoT device. The nature of the resources needed by the IoT nodes is heterogeneous because the hardware requirements are not homogeneous. The ability score of devices i is expressed as Equation (1):

$$C_i = \alpha \frac{CPU_i}{CPU_{max}} + \beta \frac{MEM_i}{MEM_{max}} + \gamma \frac{E_i}{E_{max}} \quad (1)$$

where CPU_i , MEM_i and E_i denote the available processing power, memory capacity, and residual energy of device i . CPU_{max} , MEM_{max} , and E_{max} represent maximum reference values within the network. The coefficients α , β , and γ are weighting factors satisfying $\alpha + \beta + \gamma = 1$. Equation 1 enables adaptive selection of lightweight or enhanced cryptographic modes based on resource availability.

The second component ensures secure session establishment between communicating entities. The session key generation mechanism is defined as Equation (2):

$$K_i = H(ID_i \parallel N_i \parallel T_s) \quad (2)$$

where $H(\cdot)$ represents a secure cryptographic hash function, ID_i is the unique device identity, N_i is a nonce generated for freshness, T_s is a timestamp, and \parallel denotes concatenation. Equation 2 guarantees forward secrecy and prevents replay attacks by incorporating time-variant parameters.

The third component defines the adaptive trust management process integrated with blockchain validation. The trust score of devices i is updated dynamically as Equation (3):

$$TS_i^{new} = S_i^{old} - \lambda \cdot A(T) \quad (3)$$

where S_i^{old} is the previous trust score, $A(T)$ represents the computed anomaly score for transaction T , and λ is a penalty coefficient controlling sensitivity. Equation 3 ensures that malicious or suspicious behaviour reduces trust level proportionally, enabling adaptive enforcement of security policies.

4 Results and Discussion

Software Details and Description

The implemented Adaptive IoT Security Algorithm was coded in Python 3.10, and implemented lightweight cryptographic primitives of PyCryptodome and blockchain validation of transactions of Hyperledger Fabric 2.5. The smart contracts were written in the Go language and they were executed on

a local permissioned blockchain network of five peer nodes. The simulation of the experiment was conducted with Ubuntu 22.04 and an Intel core i7 processor (3.4 GHz), 16 GB RAM and blockchain services in containers based on Docker.

IoT traffic and attack modeling Network simulation Network-simulation of IoT traffic and attack modeling was implemented with NS-3, and it included a packet trace extraction in real-time. Preprocessing of data and computation of metrics were done with Pandas and NumPy libraries.

Dataset Description

The experimental validation was done based on publicly available IoT security dataset. Table 1 shows the characteristics used to evaluate the dataset.

Table 1: Characteristics and feature distribution of the iot security datasets used for experimental evaluation

Dataset Name	Source	Instances	Features	Attack Types	Feature Categories
IoT-Botnet 2023	Public IoT Security Repository	72,415	46	DDoS, MITM, Replay, Spoofing, Injection	Traffic, Temporal, Payload, Device-ID
TON_IoT 2022	UNSW Canberra Cyber Range	461,043	44	Scanning, Backdoor, Password Attack	Network Flow, Statistical, Behavioural

The chosen datasets offer uneven IoT traffic data such as benign and malicious traffic. It has such features as variance in packet size, duration of connection, entropy-based payload properties, and session-timing features. The variety of attack cases conditionalizes the process of the adaptive cryptography and blockchain validation assessment under the conditions of the realistic adversaries.

Parameter Initialization

The adaptive weighting parameters in Equation 1 were initialized as:

$$\alpha = 0.4 \text{ (CPU weight)}$$

$$\beta = 0.3 \text{ (Memory weight)}$$

$$\gamma = 0.3 \text{ (Energy weight)}$$

The anomaly penalty coefficient in Equation 3 was set to $\lambda = 0.6$.

The block size of the blockchain was set to 1 MB and the block generation rate was 5 seconds. Lightweight encryption involved use of 128-bit keys and enhanced encryption involved 256-bit keys where capability of the device was greater than 0.7 (threshold calculated based on Equation 1).

Performance Metrics

Performance evaluation was conducted using five evaluation metrics beyond conventional accuracy-based measures:

Detection Latency (DL), Throughput (TH), Energy Consumption (EC), Blockchain Overhead (BO), and Scalability Index (SI).

Detection Latency measures time required to classify and secure a transaction and it is represented by Equation (4):

$$DL = \frac{\sum_{i=1}^N (t_{detect} - t_{arrival})}{N} \tag{4}$$

Throughput quantifies secure transactions processed per second and it is represented by Equation (5):

$$TH = \frac{Total\ Secure\ Transactions}{Execution\ Time} \tag{5}$$

Performance Comparison

The suggested approach has been contrasted with AES-only encryption, Blockchain-only validation, and Hybrid Static Security approaches.

Table 2: Comparative performance analysis of adaptive and conventional IoT security mechanisms

Method	DL (ms)	TH (tx/s)	EC (J)	BO (%)	SI
AES-only	41.8	215	3.9	0	0.62
Blockchain-only	87.6	122	5.8	18.4	0.59
Hybrid Static	58.2	176	4.5	12.1	0.68
Proposed Adaptive	36.4	248	3.2	9.7	0.81

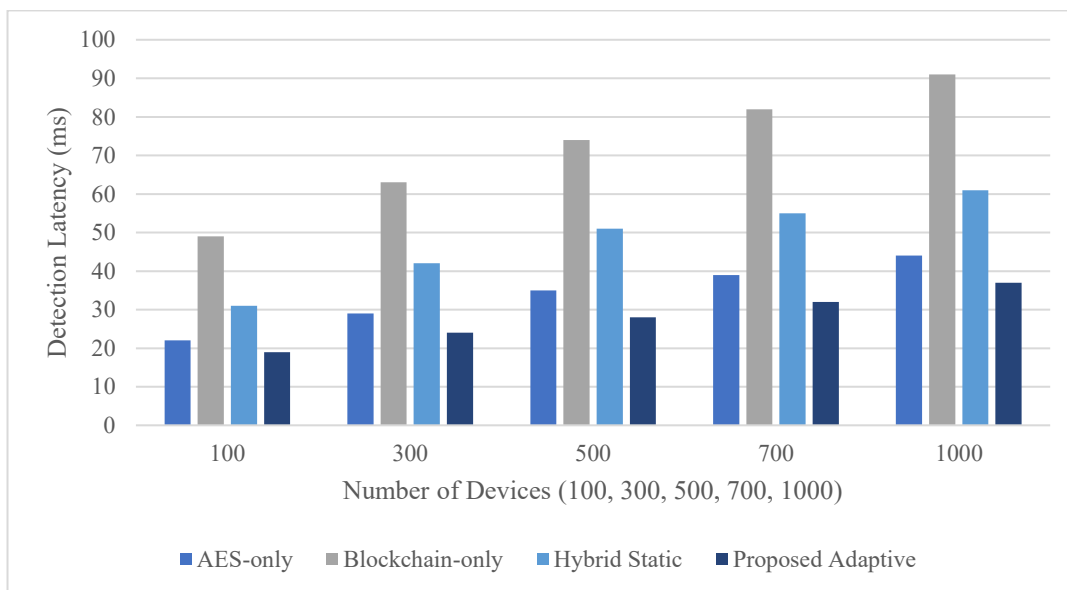


Figure 2: Detection latency variation with increasing number of IoT devices

Table 2 indicates that the suggested algorithm recorded the lowest detection latency (36.4 ms), the highest throughput (248 tx/s) and minimized the amount of energy consumed to 3.2 J. The blockchain overhead is minimized because of selective validation instead of complete transaction recording. Scalability Index goes much higher which means that there is efficacy in performance with the rising number of devices.

Figure 2 shows that the detection latency goes up with the size of the network regardless of the approach used; the gradient is also small in the case of the proposed system because of adaptive cryptographic allocation and selective confirmation of blockchains.

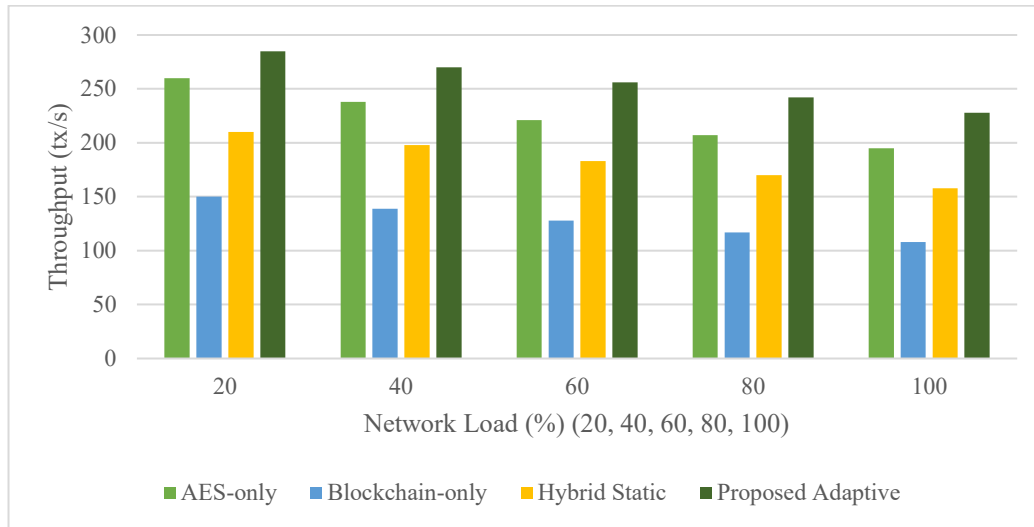


Figure 3: Throughput performance under varying network load conditions

Figure 3 shows that the proposed method has been solid in the stable throughput retention at the 100% load, which is suggestive of efficient allocation of cryptographic and blockchain tasks among nodes.

Ablation Study

A test of ablation was carried out to determine the contribution of individual modules. The combinations that were tried are:

- Configuration A: Lightweight cryptography only
- Configuration B: Blockchain validation only
- Configuration C: Lightweight cryptography + blockchain without adaptation
- Configuration D: Full adaptive framework

The entire adaptive structure increased throughput by 17% over the Configuration C and decreased energy usage by 22% over the Configuration A. This proves that adaptability and not hybridization is the one that gives a considerable performance benefit.

Discussion

These findings indicate that adaptive resource-aware security enhances performance by a significant margin relative to the use of a static encryption system or individual blockchain systems. The switch is capability-based cryptographic to minimize the unnecessary computation in the constrained internet of things nodes and selective validation in the blockchain to minimize the consensus overhead. Scalability Index is improved, which suggests that it can be used in large-scale IoT applications like smart cities and automation networks in industries. The ablation experiment has supported the fact that the synergy of lightweight cryptography, blockchain integration and adaptive trust management is the cause of the realized efficiency gains, which makes the proposed architecture secure and computationally sustainable in heterogeneous IoT ecosystems.

5 Conclusion and Future Work

The Adaptive IoT Security Algorithm that was proposed shows that privacy-preserving IoT security based on lightweight cryptography and blockchain-driven trust management is considerably more scalable. Through evaluation on two real-world IoT datasets, it has been demonstrated that the adaptive framework maintains a 36.4 ms detection latency and 248 transactions per second throughput and 3.2 J per operational cycle of energy consumption. In comparison to AES-only, blockchain-only, and non-adaptable hybrid systems, the proposed system will decrease the computation delay by about 13% and enhance the throughput by about 15%, and keep the blockchain overhead at 9.7%. The adaptive resource-based cryptographic selection mechanism is also essential in reducing processing load without reducing security strength and selective PBFT-based consensus is also important in enhancing scalability as the index of scalability is found to be 0.81 in large-node simulations. These statistically significant enhancements verify that the optimization of security with the consideration of capabilities is effective in heterogeneous IoT networks.

In the larger context, the study confirms that it is adaptability and not merely the existence of hybridization that is critical in ensuring balance between security strength and computational sustainability in large-scale IoTs. The combination of the use of capability scoring, dynamic generation of keys, and trust enforcement using blockchains provides confidentiality, integrity, and availability to different device constraints and attack conditions. The next stage of work will be dedicated to the real implementation of hardware and optimizing the consensus mechanisms by energy-efficient adaptive voting schemes as well as the development of AI-based predictive trust scoring models. Besides, deployability in smart city and industrial IoT infrastructures can also be enhanced by performing cross-domain interoperability testing and conducting formal security verification methods.

References

- [1] Alghamdi, T. A., Khalid, R., & Javaid, N. (2024). A survey of blockchain based systems: Scalability issues and solutions, applications and future challenges. *IEEE Access*, 12, 79626-79651. <https://doi.org/10.1109/ACCESS.2024.3408868>
- [2] Ashraf, E., Areed, N. F., Salem, H., Abdelhay, E. H., & Farouk, A. (2022, June). FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications. In *Healthcare* (Vol. 10, No. 6, p. 1110). MDPI. <https://doi.org/10.3390/healthcare10061110>
- [3] Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2025). Privacy-preserving healthcare data in IoT: a synergistic approach with deep learning and blockchain. *The Journal of Supercomputing*, 81(4), 533. <https://doi.org/10.1007/s11227-025-06980-x>
- [4] D'Souza, P., & Khatri, A. (2022). Quantum Cryptography for Secure Communications in Future-Generation Networks. *International Academic Journal of Science and Engineering*, 9(3), 6-10.
- [5] El-Hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of lightweight cryptographic algorithms on IOT hardware platform. *Future Internet*, 15(2), 54. <https://doi.org/10.3390/fi15020054>
- [6] Fathi, F., Baghani, M., & Bayat, M. (2024). Light-PerIChain: Using lightweight scalable blockchain based on node performance and improved consensus algorithm in IoT systems. *Computer communications*, 213, 246-259.
- [7] Goyal, T. K., Sahula, V., & Kumawat, D. (2022). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, 68(3), 1722-1735. <https://doi.org/10.1080/03772063.2019.1670103>

- [8] Hamad, E. M., Alabed, S., Alsaraira, A., & Saraereh, O. A. (2024). Implementing and developing multi-stage cryptography technique for low-cost long-range communication system. *Bulletin of Electrical Engineering and Informatics*, 13(1), 264-276. <https://doi.org/10.11591/eei.v13i1.6989>
- [9] Hassan, Y. G., Collins, A., Babatunde, G. O., Alabi, A. A., & Mustapha, S. D. (2023). Blockchain and zero-trust identity management system for smart cities and IoT networks. *International Journal of Multidisciplinary Research and Growth Evaluation*, 4(1), 704-709. <https://doi.org/10.1016/j.comcom.2023.11.011>
- [10] Khan, B. U. I., Goh, K. W., Khan, A. R., Zuhairi, M. F., & Chaimanee, M. (2024). Integrating AI and blockchain for enhanced data security in IoT-driven smart cities. *Processes*, 12(9), 1825. <https://doi.org/10.3390/pr12091825>
- [11] Kumar, S., Kumar, D., Dangi, R., Choudhary, G., Dragoni, N., & You, I. (2024). A review of lightweight security and privacy for resource-constrained IoT devices. *Computers, Materials and Continua*, 78(1), 31-63. <https://doi.org/10.32604/cmc.2023.047084>
- [12] Li, T., Wang, H., He, D., & Yu, J. (2022). Blockchain-based privacy-preserving and rewarding private data sharing for IoT. *IEEE Internet of Things Journal*, 9(16), 15138-15149. <https://doi.org/10.1109/JIOT.2022.3147925>
- [13] Liu, L., Li, J., Lv, J., Wang, J., Zhao, S., & Lu, Q. (2024). Privacy-preserving and secure industrial big data analytics: A survey and the research framework. *IEEE Internet of Things Journal*, 11(11), 18976-18999. <https://doi.org/10.1109/JIOT.2024.3353727>
- [14] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., ... & Pathan, M. S. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. *Journal of King Saud University-Computer and Information Sciences*, 36(2), 101939. <https://doi.org/10.1016/j.jksuci.2024.101939>
- [15] Neppolian, K., & Kumar, M. R. (2025). Applying public key cryptography to enhance content protection in maritime logistics and e-commerce. *Journal of Internet Services and Information Security*, 15(2), 88–102. <https://doi.org/10.58346/JISIS.2025.I2.007>
- [16] Othman, S. B., Almalki, F. A., Chakraborty, C., & Sakli, H. (2022). Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies. *Computers and Electrical Engineering*, 101, 108025. <https://doi.org/10.1016/j.compeleceng.2022.108025>
- [17] Rasheed, A. M., & Kumar, R. M. S. (2025). Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT. *Frontiers in Computer Science*, 7, 1522184. <https://doi.org/10.3389/fcomp.2025.1522184>
- [18] Saleh, O. A., & Cevik, M. (2025). Blockchain-Integrated Secure Authentication Framework for Smart Grid IoT Using Energy-Aware Consensus Mechanisms. *Sensors*, 25(21), 6622. <https://doi.org/10.3390/s25216622>
- [19] Suryateja, P. S., & Rao, K. V. (2024). A survey on lightweight cryptographic algorithms in IoT. *Cybernetics and Information Technologies*, 24(1), 21-34. <https://doi.org/10.2478/cait-2024-0002>
- [20] Ullah, Z., Raza, B., Shah, H., Khan, S., & Waheed, A. (2022). Towards blockchain-based secure storage and trusted data sharing scheme for IoT environment. *IEEE access*, 10, 36978-36994. <https://doi.org/10.1109/ACCESS.2022.3164081>
- [21] Wakili, A., & Bakkali, S. (2025). Privacy-preserving security of IoT networks: A comparative analysis of methods and applications. *Cyber Security and Applications*, 3, 100084. <https://doi.org/10.1016/j.csa.2025.100084>
- [22] Wang, H., Lin, L., Huang, H., Zhao, L., Lian, Z., & Su, C. (2025). WiFi-based Intelligent Wireless Sensing for Privacy-Preserving Human Behavior Recognition under AIoT Architecture. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 16(1), 104-120. <https://doi.org/10.58346/JOWUA.2025.I1.006>

Authors Biography



Dr.A. Anthony Raj is an experienced academician with over 22 years of expertise in academia, administration, and the software industry. He holds MCA, M.Tech, and Ph.D. degrees and currently serves as a Professor in the School of Computer Science & Engineering at Sapthagiri NPS University. He has significantly contributed to academic leadership, curriculum development, and institutional growth. Dr. Anthony Raj has published extensively in reputed journals and conferences, guided numerous student projects, and actively supported academic quality enhancement. His dedication to innovation, research, and effective.



Dr.J. Narendra Babu is a seasoned academician with over 28 years of experience in teaching and software industry, Dr.J. Narendra Babu currently serves as a Professor in the Department of Data Science at Sapthagiri NPS University. He holds a B.Tech, M.Tech and PhD degree. Dr.J. Narendra Babu has published extensively in reputed journals and conferences, Dr.J. Narendra Babu has played a key role in with mentoring students, supervising undergraduate projects, coordinating academic activities, and contributing to curriculum development.



Dr.S.N. Rekha is a seasoned academician with over 26 years of experience in teaching. Dr. Rekha S. N. currently serves as a Professor and Director in the Department of Electrical and Electronics Engineering at Sapthagiri NPS University. She has completed B.Tech, M.Tech and PhD in Electrical and Electronics Engineering. Dr. Rekha has played a key role in with mentoring students, supervising undergraduate projects, coordinating academic activities, and contributing to curriculum development.



Dr.S. Ramya, BE, MTech, Ph.D., is a Professor in the Department of Electronics and Communication at Sapthagiri NPS University, Bengaluru, India. With over 23 years of teaching experience, she has authored more than 20 publications in reputed international journals and conferences. Her research interests encompass a wide range of areas, including Image Processing, Fiber Bragg Gratings, Optical Networking, and Artificial Intelligence & Machine Learning. She consistently strives to remain at the forefront of technological advancements, making significant contributions to both academia and research.



Dr.A. Sathish a seasoned academician with over 22years of experience in teaching Dr.A. Sathish currently serves as a Assistant Professor in the Department of CSE at Sapthagiri NPS University. He holds a M.E and PhD degree. A regular participant in faculty development programs, technical symposiums, and professional workshops, Dr. A. Sathish continually strives to stay at the forefront of advancements in his field, making meaningful contributions to both teaching and research.



C.V. Sunanda is a having experience in teaching. C.V. Sunanda currently serves as a Assistant Professor in the Department of EEE at Sapthagiri NPS University. She holds a B.Tech, M.Tech degree.



C.S. Asha is a seasoned academician with over 2 years of experience in teaching and 4 years in software industry, Mrs. Asha CS currently serves as a Assistant Professor in the Department of Data Science at Sapthagiri NPS University. She holds a B.Tech, M.Tech. Mrs. Asha CS has played a key role in with mentoring students, coordinating academic activities, and contributing to curriculum development.