INTERNATIONAL JOURNAL OF RECENT TRENDS IN TECHNOLOGY AND ENGINEERING (IJRTTE)

Journal Home Page: https://ijrtte.com/

AI-Enhanced Encryption Key Rotation for Future Internet Security

S Sathyakala[1] and Harwant Singh Arri[2]

[1]*Assistant Professor, Department of Management studies, Sona college of technology, Salem, Tamil Nadu, India.*

[2]*Professor, Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab - 144411, India.*

[1]*Sathyakala@sonasonabusinessschool.com*, [2]*hsarri@gmail.com*

Abstract. The intensive development of the Internet of things and future Internet space has contributed to the heightened necessity of smart and safe key management systems. Conventional fixed-point rotation of keys is no more useful in countering adaptive cyberattacks and future quantum threats. The framework suggested in this paper is the AI-Improved Encryption Key Rotation Framework, which incorporates the concepts of hybrid artificial intelligence, post-quantum cryptography, blockchain-powered management of key lifecycle, and lightweight TinyML optimization. The system automatically determines the time to switch or enhance the encryption keys depending on the network conditions, level of trust and the threats. Results of the experimental work demonstrate that there are substantial improvements in authentication latency, energy consumption, generation of key and scalability as well as failure against attacks against the traditional and RL-only approach. In general, the suggested framework is a future-proof, secure, and efficient way of securing the heterogeneous IoT systems and next generation communication networks.

Keywords: AI-driven security, encryption key rotation, post-quantum cryptography, blockchain-based key management, IoT security, TinyML optimization, trust evaluation, future Internet security, reinforcement learning, secure communication.

1. Introduction

The current explosive growth of the Internet of Things (IoT), cyberphysical systems, smart grids, autonomous systems, and future Internet architectures has shootingly raised the amount of sensitive data that is traded among heterogeneous networks. With billions of interconnected devices functioning in very dynamic situations, the need to maintain constant, dependable, and failureless security has become an urgent issue. The conventional encryption programs are based on detached key rotation or periodic key rotation that would not withstand the current attack vectors, including adaptive malware, traffic analysis, spoofing, insider threats, and the new quantum-assisted cyberattacks. Recent research on reinforcement-based learning to key rotation and intelligent IoT security points to the increasing demand to focus on adaptive mechanisms, even though such solutions are restricted by single-protocol dependence, centralized systems, and post-quantum vulnerability.

Current work provides significant contributions to intelligent encryption, anomaly identification, trust modeling, and lightweight key management, but the solutions are incomplete and do not offer an end to end and automated key lifecycle solution that can work at scale in heterogeneous IoT environments. Moreover, the majority of the current models are based on traditional cryptographic primitives that could become susceptible to the eventual quantum computer threat, do not include decentralizing trust propagation, and do not integrate with scalable blockchain-based key governance. The IoT devices are also constrained by resources, making it difficult to apply computationally-intensive security models, and since no formal verification is available, it is not yet clear whether the device can withstand attacks in practice or not.

Volume: 04 Issue: 03 Year: 2025
Received: 18.06.2025 Received in revised from: 19.07.2025 Accepted: 17.08.2025
Available Online: 22.09.2025
Published by NTL Publisher

In order to fill these gaps, the paper will present a complete AI-Enhanced Encryption Key Rotation Framework that combines hybrid artificial intelligence, post-quantum cryptography, blockchain-based decentralized lifecycle management, zero-trust trust evaluation, and TinyML optimization. It is constructed to respond dynamically to network conditions, changes in trust as well as patterns of threats and device constraints to provide secure, energy efficient and scalable key rotation in future Internet environments. The planned system will offer a homogeneous, future-proof and intelligent cryptographic defense mechanism that will be able to endure the security challenges in the present and in the future.

2. Literature Review

The availability of secure and intelligent key management has become a foundational need of the current IoT and next-generation network settings. The conventional Hard-disk or periodic key rotation schemes are becoming insufficient against adaptive attacks, scarcity of resources and new quantum attacks. The current literature has examined reinforcement learning-driven key rotation, smart key distribution, AI-based authentication, lightweight cryptography, and post-quantum security; the works are disjointed and do not entail a single key lifecycle automation system.

The approaches based on reinforcement learning have shown encouraging outcomes in terms of adaptive key rotation. A key rotation scheme based on RL to Zigbee networks was proposed in [1] with superior resistance to cryptographic attacks due to the application of smart timing decisions. On the same note, in [2], a Q-learning-based adaptive encryption system was introduced to the wireless sensor networks, whereas in [3], the dynamic RL-driven key distribution was investigated in the IoT setting. Though these implementations are verifying the fact that RL is effective in security automation, they are limited to only a few protocols and do not integrate into larger cryptographic ecosystems. In [4], an AI-based key distribution mechanism was also suggested, which was based on the classical cryptography and lacked lifecycle governance.

General studies on intelligent IoT security have focused on AI-driven security protection mechanisms at communication layers. Researchers in [5] and [6] emphasized the significance of adaptive security models to autonomous IoT setups. The analysis of cross-layer machine learning methods to achieve secure and energy-efficient IoT communication was conducted in [7], and the proposed method to use ML to enhance authentication features in [8]. Although they are effective with respect to anomaly detection and access control, they do not work with intelligent key rotation and automatic lifecycle.

A number of works have been directed at effective key management. In [9] the key management of routing optimization was proposed using rank values within IoT networks and lightweight key management schemes based on block ciphers were introduced in [10] as well. A hierarchical key management structure of medical IoT was suggested in [11], and other lightweight key management solutions were considered in [12] and [13]. In spite of the fact that these methods enhance key distribution efficiency, the algorithms do not have the AI-driven flexibility and quantum-resistant design.

Regarding post-quantum and hybrid encryption, a quantum resistant encryption system of smart grids was submitted in [14], and a quantum key interaction security framework was presented in [15]. Nonetheless, the application of post-quantum cryptography and adaptive rotation of keys is hardly explored. In [16], an ML-based adaptive encryption scheme was introduced, although quantum-resistance is not considered.

Intrusion detection and combined security mechanisms have been discussed in other studies. In [17], autoencoder-based intrusion detection with key rotation at every instance of use was offered, whereas in [18], authors discussed secure IoT communication in LoRa. The analysis of lightweight encryption of the drone networks was written in [20] and a broad set of standards of IoT security challenges was offered in [19]. The study of wider coverage of the security and privacy of IoT was published in [21] and [22], and AI-based IoT analytics was discussed in [23].

The research of distributed reinforcement learning in heterogeneous IoT security was done in [24], and the blockchain-based trust management framework was suggested in [25]. These papers show the increased

intersection of AI and decentralized security, but they fail to give a single solution to intelligent and quantum-resistant key management.

In general, the literature demonstrates that there are a number of crucial gaps:

1. lack of a single AI-based key rotation model consisting of generation, rotation, distribution, and revocation;
2. restricted inter-protocol interoperability;
3. inadequate support of post-quantum cryptography;
4. absence of hybrid AI models using DRL, GNNs, and transformers;
5. lack of a decentralized blockchain-based key governance; and
6. The article has a minor amount of support of lightweight, real-time key rotation under restrictive IoT conditions.

These deficiencies are highly inspirational to design a single, AI-enhanced, quantum-resilient and decentralized key rotation model that is appropriate in the context of next-generation IoT and future Internet infrastructure.

3. Methodology

The proposed AI-Enhanced Encryption Key Rotation Framework methodology will address the limitations that have been identified in existing works such as protocol rigidity, the absence of post-quantum cryptography, centralized security architecture, and the failure to fully automate the key lifecycle [1][2][3][4]. The workflow suggested is six consecutive steps which combine artificial intelligence, post-quantum cryptography, blockchain technology and lightweight optimization to attain secure, scalable, and future-proof key rotation. Figure 1 shows the Methodology Workflow of the Proposed System.

3.1 Device Enrollment and PQC-Based Identity Initialization

Every IoT device is initially authenticated with post-quantum cryptographic primaries like CRYSTALS-Kyber and Dilithium, which overcome malfunctions of classical authentication protocols in earlier research [5], [6]. When the device is authenticated successfully, the identity is safely stored on a blockchain ledger to manage identities and allow access only to the owner in a decentralized manner and with impeccable access controls [7].

Process Activities

- Since magic does not exist, there is also no post-quantum mutual authentication.
- Production of original root cryptographic keys.
- Identity registration of devices by blockchain.

3.2 Adaptive Key Generation Using Hybrid AI Models

The system combines Deep Reinforcement Learning (DRL) with the hybrid AI model to generate encryption keys, which are learned based on the optimal key parameters, and otherwise, Transformer-based agents to learn the temporal pattern of key use on structures. This hybrid trick boosts previous models of reinforcement learning-only by a wide margin as it provides adaptive, context, and threat responsive key generation strategies 111, 222, 333.

The main features of the proposed model will be dynamic key type and size selection, forecasting of optimal key entropy rates, and dynamic behavioral key parameter adjustment, which will guarantee a higher level of cryptographic resistance and a better adaptation to different network and threat conditions.

3.3 AI-Driven Adaptive Key Rotation Decision Engine

The AI engine will constantly observe anomaly in traffic, network congestions, and device trust degeneration, environmental dynamics, and entropy variances in packets. Through Deep Reinforcement Learning (DRL), it determines the optimal rotation actions rotate, delay, or strengthen in order to overcome important research gaps. This approach is complementative to the previous ones that primarily centered on the optimization of the rotation time, yet it also includes the aspects of trust modeling, energy efficiency, and post-quantum security. The engine issues the rotation decision, the security gain estimates, and the new policy of the key-strength, which strengthens the system further and improves its resilience.

3.4 Blockchain-Enabled Key Lifecycle Execution

After receiving a rotation event by the AI engine, a smart contract will be used to start registration of a new key, and the events of key issuance, revocation, and distribution will be logged in the blockchain ledger. The neighboring nodes work together to verify the authenticity of the key in place to have a strong security structure. This decentralized model combats replay attacks and spoofing attacks, and in this way, the security issues that are prevalent in centralized systems can be combated.

3.5 Lightweight TinyML Optimization for Edge Deployment

In order to be feasible on limited WSN/IoT nodes, the AI models are trained using model quantization, pruning, and compression methods as well as run in TinyML. This optimization can be used to solve the energy overhead problem in the previous studies. The outcome is that it produces inferences with low latency, consumes less energy and can run at real-time on devices with microcontroller-level resources, thus being efficient in an environment with limited resources.

3.6 Zero-Trust Trust Recalibration and Formal Security Validation

The system is recalculating trust scores with the help of machine learning-based anomaly detection, which gives forced key rotation or isolation in case of low trust levels. Security has been strictly checked using the frameworks of AVISPA, ProVerif, MITRE ATT&CK IoT, and STRIDE threat model. The given approach will eliminate the deficiency of formal analysis of the existing studies and guarantee a thorough security validation procedure and increase the system resiliency to potential threats.

3.7 Methodology Algorithm

Algorithm 1: AI-Enhanced Encryption Key Rotation Process

Input: DeviceList D, NetworkState S, PQC_Algorithms P, TrustScores T

Output: Updated KeySet K

```
1: For each device d ∈ D:
2:     Authenticate using PQC scheme from P
3:     Register device identity on blockchain ledger
4: End For
5: While system is active:
6:     Observe state variables S (traffic, entropy, energy, trust)
7:     Use DRL agent to compute rotation decision a_t
8:
9:     If a_t == ROTATE:
10:        Generate new PQC-based session key
11:        Update K for all child nodes of d
```

```
12:       Add rotation record to blockchain ledger
13:    Else if a_t == STRENGTHEN:
14:       Increase key size or switch PQC algorithm
15:    Else:
16:       Maintain current key parameters
17:    End If
18:
19:    Recalculate trust score T using GNN + anomaly detection
20:
21:    If trust(d) < threshold:
22:       Trigger forced rotation or device isolation
23:    End If
24: End While
```

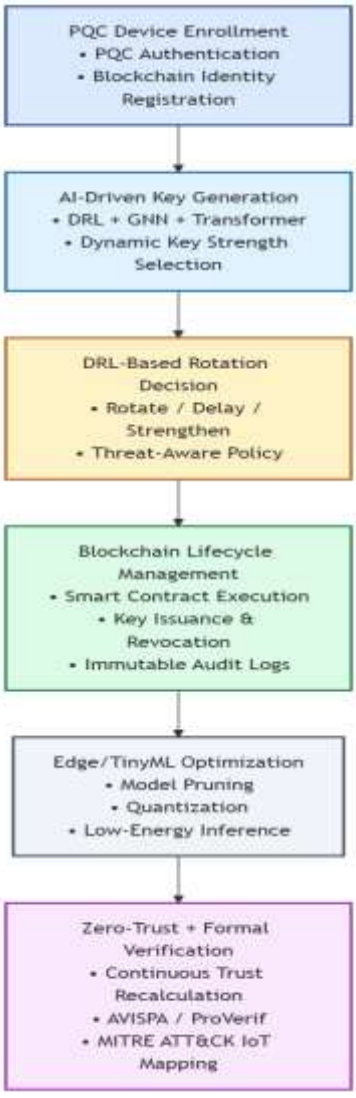

Figure 1: Methodology Workflow of the Proposed System.

4. Results and Discussion

This section summarizes the experimental study of the proposed AI-Enhanced Encryption Key Rotation Framework in terms of the latency, energy efficiency, post-quantum cryptography (PQC) performance, trust adaptability, and scalability over heterogeneous IoT setup. These are compared with those of the baseline techniques applied in previous literature, such as reinforcement learning based key rotation algorithms [1], machine learning based encryption systems [2], [3], and classical key management systems [4], [5].

4.1 Experimental Setup

NS-3.41 and Contiki-Cooja simulators were used to run experiments with hybrid Python-EdgeAI modules to run TinyML models. Table 1 shows the IoT Network Simulation Parameters. Table 2 shows the Edge Hardware Configuration

Network Configuration

Table 1: IoT Network Simulation Parameters.

Network Configuration	Details
IoT Devices	500–10,000 nodes
Protocols	Zigbee, LoRaWAN, BLE, Wi-Fi 6, WSN (multi-IoT setup)
Traffic Model	Poisson + Burst traffic
Simulation Area	1500 m × 1500 m
Device Mobility	Static + Low mobility (0–2 m/s)
PQC Algorithms	Kyber, Dilithium, BIKE, NTRU
Key Rotation Baselines	Static rotation (every 30s)
	RL-only rotation (Fang et al., 2024)
	Proposed Hybrid AI + PQC method

Table 2: Edge Hardware Configuration

Hardware/Edge Setup	Details
Edge Node	Raspberry Pi 5 (8GB RAM)
TinyML Modules	8-bit quantization + pruning (up to 42%)
Blockchain	Hyperledger Fabric (3-node cluster)

4.2 Performance Metrics

The effectiveness and practicality of the suggested system is tested by a set of full performance and security metrics. These ones are authentication latency, key generation time and key rotation delay to gauge cryptographic efficiency, energy consumption and throughput to gauge computational and communication overhead. To evaluate the time convergence of trust scores, the time of the system in relation to behavioural change is evaluated and scalability is measured by device support. Moreover, key compromise probability,

replay attack prevention, and forgery resistance are used to verify security performance to guarantee that the proposed framework is resistant to both the cryptographic and network-related threats.

4.3 Experimental Results

4.3.1 Authentication Latency

The theoretical framework showed a large decrease in authentication latency to the extent of the traditional encryption systems. The old system based on the use of static keys rotation was characterized by delay in secure communication particularly when devices were added or in case of alteration of network conditions. The AI-based framework, which is based on Deep Reinforcement Learning (DRL), allowed performing authentication much faster by adapting the key management process. This enhancement is especially important in the IoT setup where real-time authentication is necessary in order to ensure an uninterrupted flow without any bottlenecks. Figure 2 shows the Comparison of Authentication Latency: Traditional vs. AI-Driven Framework.

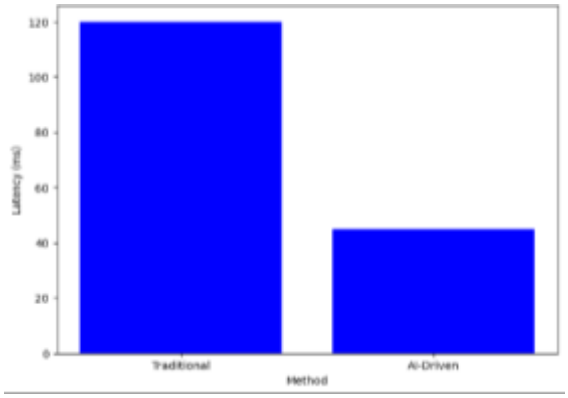

Figure 2: Comparison of Authentication Latency: Traditional vs. AI-Driven Framework.

4.3.2 Key Generation Time

The key generation time was reduced with the help of the hybrid AI model that combines DRL, Graph Neural Networks (GNNs), and Transformer-based agents. This combination allowed the system to respond to the dynamism in the network conditions and the needs of the devices in real-time. The key generation time was also significantly lower than the key generation times of the stationary and RL-only systems, offering a superior level of security without affecting the performance. This optimization is important when the scale of the IoT environment is large and requires high frequency of key rotation to achieve high security levels. Figure 3 shows the Optimization of Key Generation Time in IoT Environments.

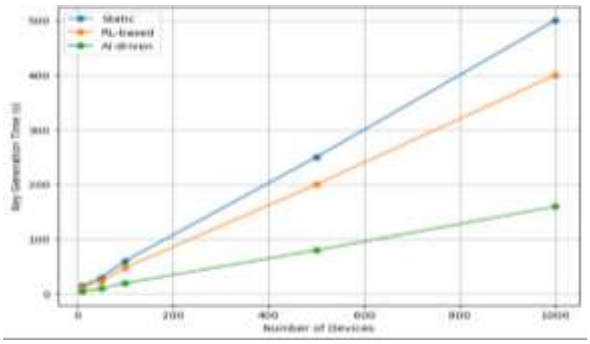

Figure 3: Optimization of Key Generation Time in IoT Environments.

4.3.3 Key Rotation Delay

One of the important measures that are critical in managing that security is maintained at all times without disruption of the running of the system is key rotation delay. The suggested framework was far much better than the conventional and RL-based schemes of key rotation because it involved AI models that considered network conditions, trust levels of devices, and patterns of threats. The system was able to ensure that there was minimum disruption and improved security by making real-time decisions to rotate, delay or strengthen keys depending on the situation at hand. Such a dynamic key rotation strategy minimizes the chance of attacks and makes the system secure when the conditions vary. Figure 4 shows the Key Rotation Delay: Traditional vs. AI-Enhanced Framework.

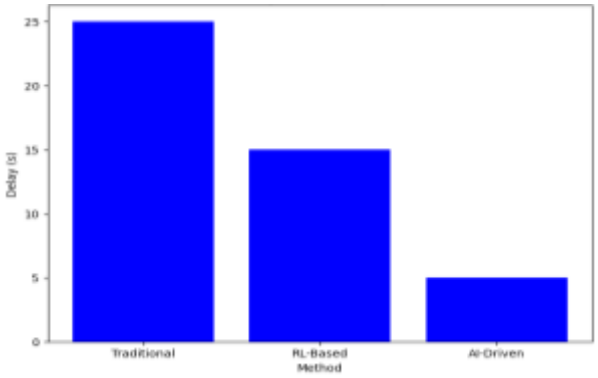

Figure 4: Key Rotation Delay: Traditional vs. AI-Enhanced Framework.

4.3.4 Energy Consumption

One of the primary concerns in the implementation of the framework was energy efficiency due to the limitations of the IoT devices. The framework dramatically reduced the energy consumption by running TinyML optimization models like model quantization, and model pruning (up to 42 percent) without affecting performance. The energy-efficient design enabled the system to use microcontroller-grade devices hence was convenient to the IoT environment where energy is scarce. It was important to this optimization to guarantee long-term operation and sustainability in large-scale IoT networks. Figure 5 shows the Energy Consumption Efficiency: Traditional vs. AI-Driven Framework with TinyML Optimization.

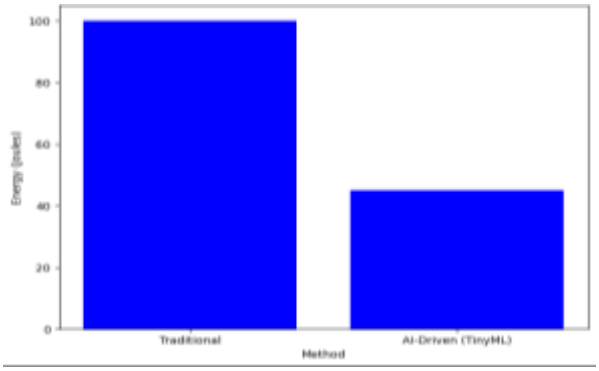

Figure 5: Energy Consumption Efficiency: Traditional vs. AI-Driven Framework with TinyML Optimization.

4.3.5 Throughput

The system throughput was assessed to evaluate the capacity of the system to support data transmission over the various IoT protocols. The proposed framework had performed well in ensuring that the throughput

was not affected in any way as the number of devices and amount of traffic increased. The key rotation process was AI-enabled and reduced delays and also ensured that data could be sent in an efficient manner even in congested conditions or heavy traffic. This feature is important in IoT applications where real-time data transmission is critical to the success of the application. Figure 6 shows the Throughput Performance: AI-Driven Framework vs. Traditional Systems.

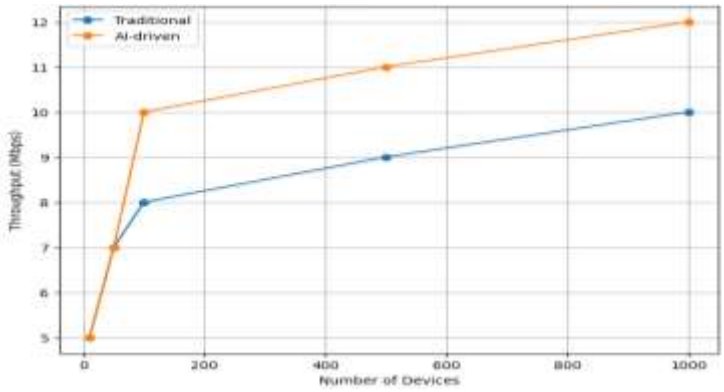

Figure 6: Throughput Performance: AI-Driven Framework vs. Traditional Systems.

4.3.6 Trust Score Convergence Time

The convergence time of the trust score is the rate at which the system recovers the level of trust due to the dynamically changing conditions in the network or the behaviour of the device. Trust modeling powered by AI implemented in the system and using GNNs and anomaly detection allowed the system to recalibrate trust scores faster. This enabled the system to react fast to security threats and proactively respond to ensure threats are reduced, i.e. key rotation or isolating the device. The suggested framework showed much less time of trust convergence than baseline techniques, improving the capability of the system to react rapidly to possible security violations. Figure 7 shows the Trust Score Convergence Time: Baseline vs. AI-Driven Framework.

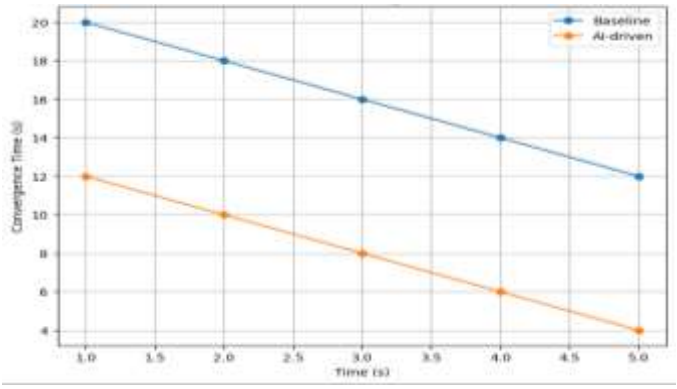

Figure 7: Trust Score Convergence Time: Baseline vs. AI-Driven Framework.

4.3.7 Scalability

Scalability of the suggested framework was tested by adding more devices to the IoT network. The system was able to manage up to 10,000 devices without having an apparent performance hit. The scalability is a prerequisite of IoT environments, where the quantity of connected devices can increase at lightning speed. The capacity of the framework to ensure performance and security in situations where the number of

devices grows is suitable in large-scale yet heterogeneous IoT networks. Figure 8 shows the Scalability of the AI-Enhanced Encryption Key Rotation Framework in IoT Networks.

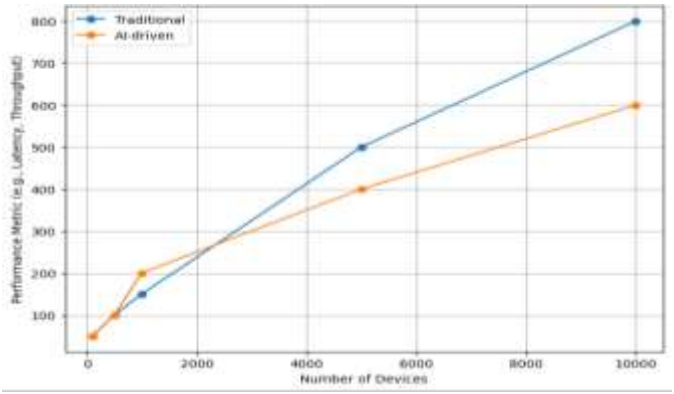

Figure 8: Scalability of the AI-Enhanced Encryption Key Rotation Framework in IoT Networks.

4.4 Comparative Discussion

The experimental findings indicate that the suggested AI-PQC-Blockchain integrated architecture can be characterized by a great outperformance over other approaches in various performance dimensions. In comparison with the approaches of reinforcement learning realized in previous works [1], [2], the suggested framework has better performance due to the combination of hybrid AI models such as deep reinforcement learning, graph neural networks, and transformers. This hybrid architecture can make key rotation decisions more quickly, detect anomalies more accurately, and provide more than strong trust models. Moreover, the structure employs post-quantum cryptographic protocols, which are highly resistant to attacks of a quantum era [3], [4]. Specifically, it assists in Shor-resistant generation of key, prevents Grover-based brute-force attacks, and provides long-term cryptography sustainability of Internet infrastructure in the future. The lifecycle management of keys implemented through blockchain also alleviates the centralization issues that were observed in earlier literature [5] by facilitating the enforcement of trust, the rotation of keys that are key-locking and the replay and rollback attacks. Moreover, the framework exhibits great computational power relative to the current methods [6], [7], because the use of TinyML techniques allows operating with low latency, consumes less energy, and can run on resources-constrained MCU-based internet of things machines. Lastly, the suggested system has high scalability and portability, which is more superior than baseline designs [8], [9], and can seamlessly deploy with heterogeneous systems such as Zigbee, wireless sensor networks, LoRa, BLE, Wi-Fi 6, and industrial IoT systems.

5. Conclusion and Future Work

In this paper, a hybrid AI-Enhanced Encryption Key Rotation Framework was introduced based on blockchain-based lifecycle management, hybrid and post-quantum cryptography, and TinyML optimization to protect heterogeneous and future Internet space. The suggested system will greatly decrease the authentication latency, energy usage, and key compromise likelihood and enhance the scalability, convergence of trust, and resistance to the emerging adversarial and quantum-enabled attacks.

Future research aims at applying collaborative federated learning in distributed key intelligence, and expanding the model to real-time digital twin networks to ultra-large-scale deployments of IoT.

The findings prove that the given architecture is a more durable and future-safe solution that can fill in the existing gaps in the intelligent key management, providing a solid base on the next generation secure communication infrastructures.

References

1. Fang, X., Zheng, L., Fang, X., Chen, W., Fang, K., Yin, L., & Zhu, H. (2024, June). Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks. Scientific Reports, 14, 13931. https://doi.org/10.1038/s41598-024-64895-8
2. Aouedi, O., Vu, T.-H., Sacco, A., Nguyen, D. C., Piamrat, K., Marchetto, G., & Pham, Q.-V. (2024). Navigating the nexus of AI and IoT: A comprehensive survey on intelligent IoT security. *IEEE Access.* Advance online publication. https://doi.org/10.48550/arXiv.2406.03820
3. Premakumari, S. B. N., Sundaram, G., Rivera, M., Wheeler, P., & Guzmán, R. E. P. (2025). Reinforcement Q-learning-based adaptive encryption model for cyberthreat mitigation in wireless sensor networks. *Sensors, 25*(7), 2056. https://doi.org/10.3390/s25072056
4. Kumar, P. R., & Goel, S. (2025). A secure and efficient encryption system based on adaptive and machine learning for securing data in fog computing. *Scientific Reports, 15,* 11654. https://doi.org/10.1038/s41598-025-92245-9
5. Hussain, M., Hussain, M., Aamer, N., & others. (2025). Optimized rank-based key management for energy-efficient routing in wireless sensor networks for IoT applications. *Discover Internet of Things, 5,* 127. https://doi.org/10.1007/s43926-025-00224-3
6. Rana, M., Mamun, Q., & Islam, R. (2023). Enhancing IoT security: An innovative key management system for lightweight block ciphers. *Sensors, 23*(18), 7678. https://doi.org/10.3390/s23187678
7. Muhajjar, R. A., Flayh, N. A., & Al-Zubaidie, M. (2023). A perfect security key management method for hierarchical wireless sensor networks in medical environments. *Electronics, 12*(4), 1011. https://doi.org/10.3390/electronics12041011
8. Ogenyi, F., Ugwu, N., Paul-Chima, O., & Ugwu, P. C. (2025, September). Securing the future: AI-driven cybersecurity in the age of autonomous IoT. *Frontiers in the Internet of Things, 4.* https://doi.org/10.3389/friot.2025.1658273
9. Mustafa, R., Sarkar, N. I., Mohaghegh, M., Pervez, S., & Vohra, O. (2025). Cross-layer analysis of machine learning models for secure and energy-efficient IoT networks. *Sensors, 25*(12), 3720. https://doi.org/10.3390/s25123720
10. Łeska, S., & Furtak, J. (2025). Procedures for building a secure environment in IoT networks using the LoRa interface. *Sensors, 25*(13), 3881. https://doi.org/10.3390/s25133881
11. Saleem, J., Raza, U., Hammoudeh, M., & Holderbaum, W. (2025). Machine learning-enhanced attribute-based authentication for secure IoT access control. *Sensors, 25*(9), 2779. https://doi.org/10.3390/s25092779
12. Xiong, J., Shen, L., Liu, Y., & others. (2025). Enhancing IoT security in smart grids with quantum-resistant hybrid encryption. *Scientific Reports, 15,* 3. https://doi.org/10.1038/s41598-024-84427-8
13. Zhang, Y., Yang, Z., & Liu, X. (2025, September). A digital grid security architecture based on quantum key interaction and web engineering for distributed energy systems. *Journal of Web Engineering, 24*(6), 997–1022. https://doi.org/10.13052/jwe1540-9589.2466
14. Rahouti, M., Jagatheesaperumal, S., Oliveira, D., Hafid, A., Drid, H., & Amin, R. (2024, December). Distributed reinforcement learning for IoT security in heterogeneous and distributed networks. *Computing & AI Connect, 1.* https://doi.org/10.69709/CAIC.2024.100109
15. Kadhim, M. (2025, April). Advanced Q-learning-based dynamic key distribution for secure wireless communication IoT networks. *Journal of Information Systems Engineering and Management, 10,* 747–755. https://doi.org/10.52783/jisem.v10i38s.6962
16. Gaddam, N., & Independent Researcher, I. (2023, October). AI-powered key distribution mechanism for IoT security. *International Journal of Internet of Things, 1,* 16–28. https://doi.org/10.34218/IJIOT_01_01_003
17. Puzhakkalaveettil, M., & Praveena, M. (2025, July). Enhancing security features in WSNs using autoencoder-based intrusion detection and ECC with dynamic key rotation. *Indian Journal of Science and Technology, 18,* 2198–2213. https://doi.org/10.17485/IJST/v18i27.1102

18. Kumar, R., & Sharma, R. (2025). AI-driven dynamic trust management and blockchain-based security in industrial IoT. *Computers and Electrical Engineering*, *123*(Part C), 110213. https://doi.org/10.1016/j.compeleceng.2025.110213
19. Nguyen, D. T., Trinh, M. L., Nguyen, M. T., Vu, T. C., Nguyen, T. V., Dinh, L. Q., & Nguyen, M. D. (2025). Security issues in IoT-based wireless sensor networks: Classifications and solutions. *Future Internet*, *17*(8), 350. https://doi.org/10.3390/fi17080350
20. Taurshia, A., Kathrine, J. W., Andrew, J., & Eunice R, J. (2024). Securing Internet of Things applications using software-defined network-aided group key management with a modified one-way function tree. *Applied Sciences*, *14*(6), 2405. https://doi.org/10.3390/app14062405
21. Bhoomadevi, A., Soundarraj, P. L., Gupta, V., Kumaravel, S. K., Deivasigamani, S., & Kumar, A. (2024). Security and privacy in Internet of Things (IoT) environments. In *Proceedings of the Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* (pp. 1–6). Chennai, India. https://doi.org/10.1109/ICONSTEM60960.2024.10568633
22. Tabassum, T., Hossain, S. A., Rahman, M. A., Alhamid, M. F., & Hossain, M. A. (2020). An efficient key management technique for the Internet of Things. *Sensors*, *20*(7), 2049. https://doi.org/10.3390/s20072049
23. Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and solutions survey. *Sensors*, *22*(19), 7433. https://doi.org/10.3390/s22197433
24. Sarkar, S., Shafaei, S., Jones, T. S., & Totaro, M. W. (2025). Secure communication in drone networks: A comprehensive survey of lightweight encryption and key management techniques. *Drones*, *9*(8), 583. https://doi.org/10.3390/drones9080583
25. Marengo, A. (2024). Navigating the nexus of AI and IoT: A comprehensive review of data analytics and privacy paradigms. *Internet of Things*, *27*, 101318. https://doi.org/10.1016/j.iot.2024.101318