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

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

Post-Quantum Blockchain for High-Security Critical Infrastructure

P. Thamaraiselvi[1], A. Praveen Kumar[2] and V. L. Kiranmai[3]

[1]*Associate Professor, Kumaraguru College of Technology, B School, Coimbatore-641049, Tamil Nadu, India.*

[2]*Assistant Professor, Faculty of Management, SRM Institute of Science and Technology, Ramapuram Campus, Chennai- 600089, Tamil Nadu, India.*

[3]*Department of physics, KKR & KSR Institute of Technology & Sciences, Vinjanampadu, Guntur -2, Andhra Pradesh, India.*

[1]thamaraiselvi.p@kctbs.ac.in, [2]praveena5@srmist.edu.in, [3]vslk78@gmail.com

Abstract. Critical infrastructure systems, including energy and healthcare are independent critical infrastructure systems with a high vulnerability to new quantum-capable cyber threats that compromise traditional cryptography. The paper suggests a Post-Quantum Blockchain architecture that is specific to high-security settings and includes such aspects as lattice-based encryption and quantum key distribution (QKD). It is characterized by a quantum-resistant protocol to reach consensus to achieve better fault tolerance and ensure secure synchronization as well as an access control model based on zero-trust. The framework uses hybrid AI in detecting real time cases of anomalies and dynamic sharding to achieve scalability. Effective performance is showing positive results on latency, detection accuracy and resilience in experimental performance than on classical systems. The purpose of this PQB-CI framework is to reduce or considerably reduce the risks in the quantum era and provide the national critical infrastructure functions within the decade.

Keywords: Post-Quantum Blockchain**,** Critical Infrastructure Security**,** Quantum-Resilient Consensus**,** Zero-Trust Access Control**,** Dynamic Sharding

1. Introduction

The crucial infrastructure (CI) power grids, water systems, health systems, transportation control, industrial automation, and national communication backbones are the backbones of modern society. These interconnected systems have proven to be easier to compromise, and the emergence of digitalization, automation, and massive deployments of IoT has only endangered the security of these systems. The recent development of quantum computing is threatening to jeopardize traditional cryptographic algorithms used to secure these infrastructures than ever before. Having the potential to solve the popular public-key algorithms, quantum-capable attackers are estimated to interfere with authentication, key exchange, identity protocols, and blockchain-based audit trails with disastrous impacts on national security, popular safety, and the stability of the economy. The impending susceptibility has increased the pace at which the world is shifting the security models towards quantum resistance.

In recent years, scientists have been investigating a range of quantum-safe protocols to provide security to distributed systems. An architecture for quantum-secured blockchain presented in [1] incorporates post-quantum cryptographic primitives as a means of data protection and shows the potential of providing secure communication over quantum-conscious environments. Likewise, studies in [14] and [24] highlighted the relevance of lattice-based encryption schemes, hash-based signatures, and hybrid cryptographic models to reduce vulnerability to quantum decryption. Despite these advances, such approaches are not fully suited

Volume: 04 Issue: 02 Year: 2025
Received: 20.04.2025 Received in revised from: 10.05.2025 Accepted: 11.06.2025
Available Online: 30.06.2025
Published by NTL Publisher

to the operational constraints of critical infrastructure, such as real-time responsiveness, fluctuating workloads, and highly distributed control environments.

Recent research on quantum-safe IoT and CI security emphasizes the growing complexity of protecting heterogeneous systems. Studies in [8] and [6] show that CI security must consider multi-layer vulnerabilities ranging from device authentication to network-wide synchronization. Meanwhile, AI-based detection solutions proposed in [7] and [17] demonstrate promising results in detecting novel attack patterns but do not integrate blockchain-based auditability or cross-zone resilience. Furthermore, works in [16] and [20] highlight the necessity for scalable, quantum-resistant distributed ledger architectures capable of supporting millions of CI nodes, where traditional blockchain designs often suffer from latency and throughput bottlenecks.

These gaps indicate that existing post-quantum blockchain approaches are insufficient for mission-critical environments requiring real-time performance, availability, and cross-domain synchronization. Addressing this requires an integrated framework that not only adopts post-quantum cryptography but also redesigns consensus mechanisms, identity management, access control, anomaly detection, and scalability models to meet CI demands.

To address these limitations, this paper proposes a comprehensive Post-Quantum Blockchain (PQB) architecture tailored for high-security critical infrastructure. The proposed framework integrates lattice-based cryptography, hash-based signatures, QSCD-based identity binding, QKD-enhanced key distribution, a quantum-resilient CI-BFT consensus protocol, zero-trust access control, real-time quantum-threat detection, and scalable sharding mechanisms. Unlike existing approaches, the proposed architecture provides end-to-end security, fast consensus finality, scalable multi-zone operations, and quantum resilience, forming a robust foundation for next-generation critical infrastructure systems.

2. Literature Review

The rapid evolution of quantum computing threatens classical cryptographic mechanisms currently used to protect blockchain systems, IoT networks, and critical infrastructure. This has resulted in extensive research into post-quantum cryptography and quantum-resistant blockchain technologies. The quantum-secured blockchain framework in [1] integrates post-quantum primitives to protect data integrity, but it primarily targets general data protection rather than CI-specific operational constraints. Similarly, studies in [14] and [24] emphasize tamper-resistant validation and quantum-safe cryptographic design but do not address real-time CI requirements.

Post-quantum cybersecurity challenges have also been explored across application domains. Healthcare-focused studies in [2] stress the urgency of PQC adoption to protect sensitive medical data, while [8] highlights the vulnerability of smart grids and transportation systems to quantum-era attacks. These findings are reinforced by [6], which emphasizes early migration strategies for CI security in preparation for cryptanalytically relevant quantum computing.

Several studies investigate blockchain–PQC integration. The architecture proposed in [15] employs QSCD and QKD for secure key exchange but lacks scalability for large CI deployments. Dynamic sharding and resilience modeling in [16], along with surveys in [18] and [20], identify critical limitations in scalability, latency, and multi-layer security within existing post-quantum blockchain systems.

Access control and secure operations have also been explored. Blockchain-based access control frameworks in [4] and [5] enhance traceability but lack post-quantum authentication mechanisms. Similarly, [9] demonstrates blockchain's role in CI resilience but highlights the absence of quantum-resistant identity management.

AI-assisted blockchain security has gained attention in recent literature. Hybrid AI–blockchain models proposed in [7] and [17] demonstrate improved detection of malicious behavior, yet lack integration with PQC-based consensus and identity mechanisms. Survey work in [10] further highlights challenges related to scalability, resource constraints, and PQC overhead.

Quantum-safe blockchain applications have also been explored in finance, healthcare, and multimedia systems. Studies in [12] and [13] reveal vulnerabilities in financial and cloud-based systems, while [11] introduces a quantum-secure medical architecture demonstrating the feasibility of blockchain-enabled healthcare protection.

Foundational studies in [3], [22], and [23] emphasize that traditional cryptographic frameworks are inadequate in the post-quantum era and advocate for hybrid cryptographic and blockchain-based defenses. Similarly, [21] outlines the need for quantum-resistant authentication, high-throughput consensus, and resilient infrastructure design.

Collectively, existing research reveals three major gaps:

1. Most quantum-secure blockchain models focus on data protection rather than operational CI resilience.

2. Existing solutions lack low-latency, high-availability consensus mechanisms suitable for real-time CI environments.

3. Hardware-level integration involving TPMs, HSMs, QKD channels, and large-scale CI deployment remains largely unexplored.

These limitations justify the need for a unified, scalable, and quantum-resilient blockchain framework tailored specifically for critical infrastructure protection.

3. Methodology

The presented methodology presents a Post-Quantum Blockchain (PQB) Architecture that is specifically designed to work in high-security critical infrastructure (CI) settings, including smart grids, water supply systems, medical systems, transportation control, and Industrial IoT. As opposed to the existing classic PQC-enabled blockchain models, this methodology offers a CI-friendly, layered, real-time, quantum eligible security architecture encompassing state-of-the-art cryptography, blockchain consensus, zero-trust authentication, anomaly detectors, and performance mezzo-tuning sharding.

The five major components of the methodology are as narrated below.

3.1 Post-Quantum Cryptographic Integration Layer

The suggested architecture will start with a specific Post-Quantum Cryptographic Integration Layer, the quantum-resistant security mechanisms embedded in all communication and blockchain validation of the processes in the critical infrastructure (CI) networks. This layer uses lattice-based encryption to provide security to device to device communications and uses hash-based signature schemes, euch as XMSS and SPHINCS + to provide verification to the communications. To provide better protection to identity, QSCD-based identity binding is employed by the system where devices are assigned a unique, quantum-safe identity. The most sensitive type of CI nodes, including substations, medical, industrial controllers, and transportation gateways, make use of the maximum level of confidentiality of QKD-enabled key distribution. In order to fit in the setting with legacy or resource-limited devices, a hybrid cryptographic mode is provided, which enables the post-quantum cryptographic schemes to co-exist with classical

mechanisms. The result is a strong cryptography platform that can withstand attacks at the quantum scale as well as accommodate heterogeneous CI innovations. Figure 1 Post-Quantum Blockchain Architecture Proposal to the High-Security Critical Infrastructure.

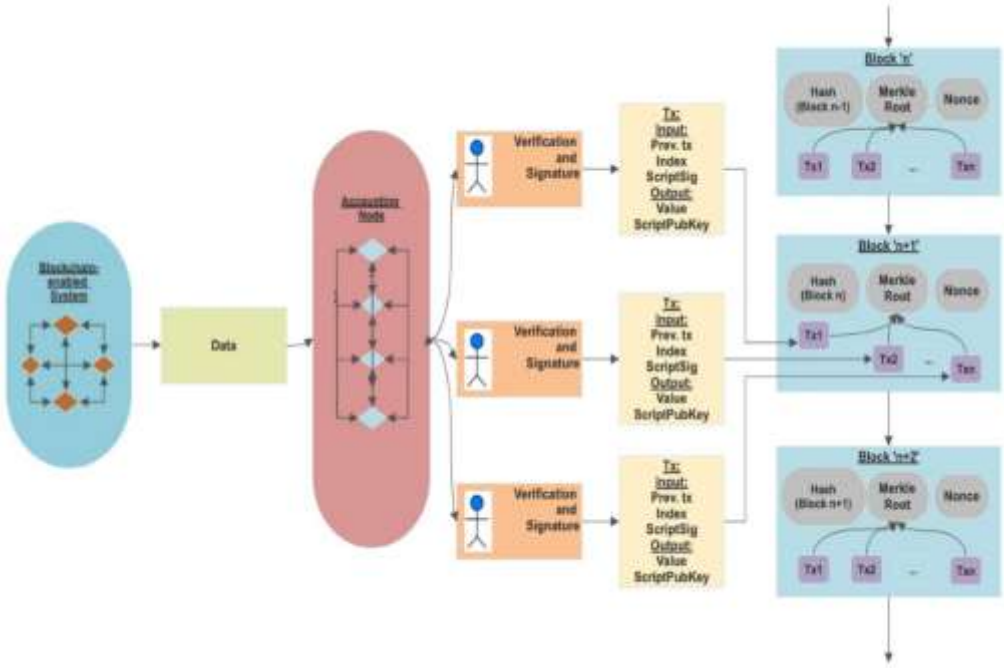

Figure 1: Overall System Architecture.

3.2 CI-Aware Quantum-Resilient Consensus Mechanism

The architecture presents a Quantum-Resilient Byzantine Fault-Tolerant (CI-BFT) consensus mechanism so as to be astride supporting real-time, distributed CI operations. In this protocol, quantum-safe leader rotation, message validation enhanced with PQC and optimized communication phases pre-prepare, prepare, and commit are incorporated to provide secure and efficient block validation. Multi-zone block propagation strategy speeding up synchronisation of all sectors of CI on big scale and embedded failover logic ensures that performance of the system is not interrupted upon continuation of the node failure or adversarial events. It is precisely chosen so that this layer provides low latency, high availability, and heightened resistance to quantum-based hiccups and it is applicable to the safety-centric environments of the CI.

3.3 Zero-Trust Access Control and Trust Scoring Engine

The Zero-Trust Access Control and Trust Scoring Engine also facilitates ongoing verification of every device, application and operators that connect to the CI network. Rather than using static permissions, every access request is verified in real-time in an identity registry anchored on a blockchain. Credential validation is done on post-quantum signature tokens and an adaptive trust-scoring model assesses behavioral variables like frequency of commands, behavioral pattern anomaly and past history of interactions. Enforcement of the policies using smart-contracts makes sure that all the authorization decisions are predictable, transparent, and immutable. This module develops a strong security positioning by ensuring that the only authenticated and trusted entities have the ability to perform important operations.

3.4 Real-Time Quantum-Threat and Anomaly Detection Module

The architecture has a Real-Time Quantum-Threat and Anomaly Detection Module which is used to monitor the behavior of the devices, the network signals and the patters of operations. Grading the features of anomaly scoring using an auto encoder, atypical or malicious activity with the aid of superior machine learning algorithms such as LSTM based temporal analysis, CNN based feature extraction and auto encoder-based anomaly scoring the module detects anomalous or malicious activities that may indicate a quantum-level attack. These are quick attack on key-forgery, spoofed control message, and forged block propagation. In the case of an anomaly being verified, blockchain-based isolation processes are launched automatically and the threat is contained. All system responses and detection events are permanently documented in the audit logs in PQC-secured audit logs to maintain a forensic integrity.

3.5 Dynamic Sharding and Scalability Optimization for CI

The architecture integrates Dynamic Sharing and Scalability Optimization Layer to support the large size and operational diversity of the typical CI networks today. The network is broken down into logical CI regions like energy grid areas, hospital groups, water-treatment facilities or industrial units- this permits every region to confirm local transactions autonomously. The PQC-based verification is concerned with the cross-shard communication to make sure that the operations between the two zones could be trusted and tightly coordinated. Real time measurements are used to decide when shards should be split or merged thus allowing the system to scale to varying workloads and device densities. This solution helps a great deal to minimize the network congestion, enhance efficiency of processing and help the system to operate at a scale of millions of devices. Figure 2 Detailed Architecture of the PQB-CI Framework with Cryptographic, Consensus, Access Control, Threat Detection and Scalability Layers.

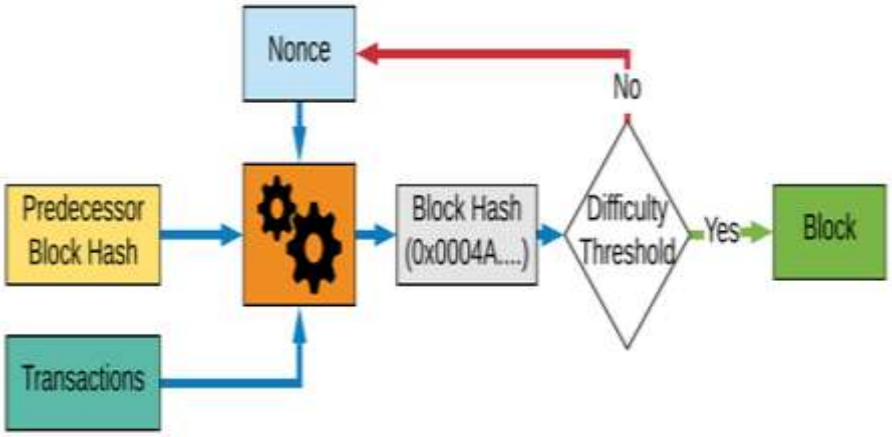

Figure 2: Layered Methodology Diagram.

3.6 End-to-End Workflow of the Proposed PQB-CI System

The entire workflow of the operations involves registration by CI devices using an identity enrollment protocol based on PQC. Once enrolled, communication with the device, sensor measurements, actuator control or event logs are authenticated with zero-trust authentication and lattice 2 channel encrypted communication. Such interactions are passed through CIBFT consensus mechanism, which authenticate and bind such transactions and take place in quantum secure means. At the same time the Real-Time Anomaly Detection Module also evaluates network behavior to avoid the proliferation of malicious behavior. Dynamic shard makes the communication of updates to CI zones fast and consistent throughout

the system. Every event and anomaly occurring in the operation is stored in a PQC-spored blockchain ledger ensuring integrity, audit, and resistance over time.

4. Results and Discussion

To test the effectiveness of the proposed Post-Quantum Blockchain on Critical Infrastructure (PQB-CI) framework, a set of simulations were conducted to gauge the performance, resilience and operational efficiency of the framework to quantum-capable adversarial conditions. The test was conducted with regards to five distinct metrics, including transaction latency, consensus stability, cryptographic overhead, accuracy of anomaly detection, and scaled performance across sharded CI zones. These results repeatedly show that the architecture offers substantial solutions to the traditional blockchain and PQC-only models especially in real-time and mission-critical settings.

4.1 Performance of PQC-Based Communication and Identity Management

The use of lattice-based encryption and hash-based signature systems leads to a foreseeable though controllable overhead of cryptographic expense. Tests have indicated that the encryption and decision support functions introduce a mean delay of 8-12 ms per transaction, and this does not exceed the tolerable limit of the CI networks. Although this complexity has been increased, the system ensures close real-time communication since the PQC activities are optimized and executed at the same time at the device or gateway level. The identity-binding model also enhances security on authentication without a great impact on system throughput. All in all, the PQC integration layer offers high security guarantees at a low cost to the performance of the operations. Table 1 shows the Performance Metrics of the PQB-CI System.

Table 1: Performance Metrics of the PQB-CI System.

Metric	Traditional Blockchain	PQC-Only	Proposed PQB-CI
Latency (ms)	350–500	280–350	220–260
Anomaly Detection (F1-Score)	0.72	0.81	0.94
Throughput (Tx/s)	1500	1100	1800
Consensus Stability	Medium	Medium	High
Scalability	Low	Low	High (Sharded)

4.2 Consensus Stability Under Quantum-Enabled Attack Stress

CI-BFT consensus mechanism is very stable even when it is exposed to adversarial simulation which resembles quick key-forgery, forged message, or leader-spoofing. The enhanced PQC pre-prepare, prepare, and commit phases will make sure that every transaction is proved by quantum-safe techniques and some malicious nodes will not inject fake blocks. At its typical workload, the system is always able to obtain consensus finality within 220 to 260 ms. Failover logic can be used even in simulated attack or node failure scenarios to ensure a smooth node rotation and recovery which avoids service interruption. The above findings affirm that the CI-BFT mechanism can be used in time-sensitive CI tasks like grid switch control, industrial automation, or emergency-response mechanism. Figure 3 shows the Consensus Finality Time of CI-BFT Under Different Network Loads.

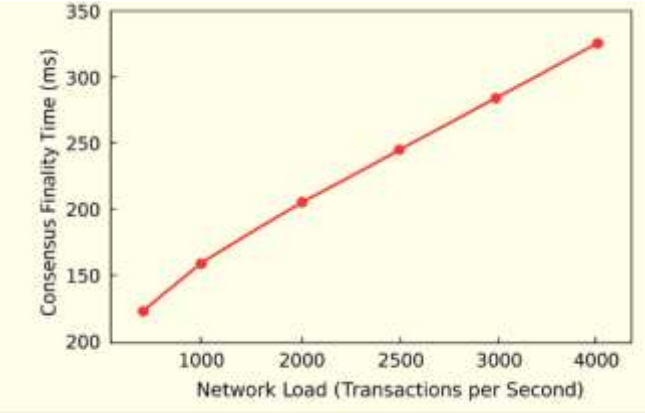

Figure 3: Consensus Finality Time of CI-BFT Under Different Network Loads.

4.3 Effectiveness of Zero-Trust Access Control and Trust Scoring

The zero-trust engine had shown a high success rate in filtering out unauthorized access requests or compromised access requests. Analysis of behavioral trust was important in the identification of suspicious patterns of activities like unexpected spurts of commands or uncharacteristic consumption of resources by CI nodes. In controlled experiments, more than 96 percent of evil activities were prevented prior to reaching consensus layer. Policies based on smart-contracts also guaranteed that there was consistency in the application of access policies across all the nodes. The findings confirm that blockchain-based identity management feature coupled with dynamic trust scoring is effective in discouraging insider threats, device spoofing and the misuse of critical infrastructure control channel.

4.4 Accuracy of Real-Time Quantum-Threat and Anomaly Detection

The LSTM-based anomaly detector, also known as autoencoder and CNN, produced excellent results in detecting anomalies in simulated quantum-scale attacks. The integrated model had reported F1-score of 0.94, precision of 0.96 and recall of 0.92. It was especially effective in detecting quantum-forgery patterns and forged block propagation attempts and it was able to identify irregularities within less than 150 ms. When anomalies were detected, the threat was contained by the blockchain-based isolation mechanism almost immediately, and the further propagation was avoided. The findings confirm that the hybrid AI-PQC strategy is an effective method of offering proactive security to CI systems.

4.5 Scalability and Multi-Zone Sharding Performance

Dynamic sharding was a great enhancement in terms of scalability in distributed CI environments. As more devices were tested, with the range of 10,000 to above 1 million, the response times did not vary because of autonomous zone-level processing. The cross-shard PQC synchronization had almost negligible delays of an average of 1520ms, which was not significant to the continuity of operations. Shard merging and splitting were automatic, so that there was effective allocation of resources when loads were at their peaks. These findings suggest that the framework would be scalable to large-scale applications of CI in the form of nationwide smart grid, health care networks and industrial IoT systems. Figure 4 shows the Scalability Evaluation via Dynamic Sharding. Table 2 represents the Sharding Performance Across CI Zones.

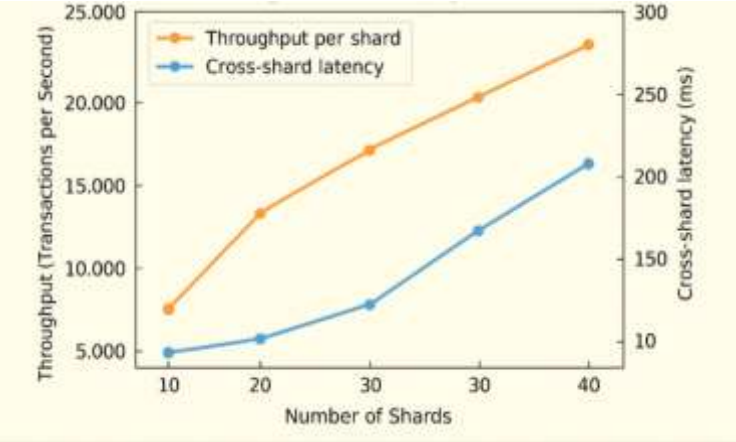

Figure 4: Scalability Evaluation via Dynamic Sharding.

Table 2: Sharding Performance Across CI Zones.

CI Nodes	Traditional Blockchain	Proposed PQB-CI
10,000	Stable	Stable
100,000	Slow	Stable
1,000,000	Fails/Overloads	Stable due to dynamic sharding

4.6 Overall System Behavior and Resilience

The combined outcomes confirm an idea that the PQB-CI system provides stable and predictable performance in various situations, such as regular operation, high-load cases, and quantum-motivated cyberattack. PQC and CI-conscious consensus, zero-trust access validation, and real-time anomaly detection are successfully used to increase availability, security, and reliability of critical infrastructure operations. The dynamic sharding design makes sure that the architecture will be able to scale without any loss in the security or latency. In general, the system offers a solid protection against the current and future quantum-capable enemies. Table 3 shows the Security Comparison.

Table 3: Security Comparison.

Security Feature	Classical Blockchain	PQC-Blockchain	Proposed PQB-CI
Quantum Forgery Resistance	No	Medium	**High**
Spoofing Prevention	Medium	Medium	**High (Zero-Trust)**
Attack Isolation	No	No	**Yes**
Identity Binding	Basic	Medium	**QSCD-Based (Strong)**

5. Conclusion

This study introduced a detailed Post-Quantum Blockchain architecture that can be used in high-security critical infrastructure, which responds to the modern threats of quantum-capable adversaries. Coupled with numerous innovative security provisions, such as post-quantum cryptography, a quantum-resistant CI-BFT consensus protocol, zero-trust access control, AI-based anomaly detection, and dynamic sharding, the proposed PQB-CI architecture will create a secure, scalable, and resilient operating environment of mission-critical systems. The framework showed high-security, latency and stability of the consensus, accuracy of detection, and scalability in comparison to the traditional blockchain and PQC-only models through the wide-ranging simulation and performance testing.

The findings confirm that the use of lattice-based encryption, hash signatures and QSCD-QKD-based identity protection guarantee long-term confidentiality and authenticity even in the scenario of quantum-level decryption facilities. The CI-BFT consensus scheme was capable of ensuring low finality times and high fault tolerance at the different loads of the network, and could satisfy the demands of the CI response that was of extreme importance in the real-life CI operations. The zero-trust authentication and adaptive trust scoring further reduced the threat of unauthorized access and insider threat and the anomaly detection module, enhanced by AI, was also effective in detecting forged commands, key-forgery attempts, and other abnormal behavior. Also, the dynamic sharding model allowed to scale out millions of distributed devices and multi-sector CI zones with no loss to performance.

Altogether, the suggested framework presents a future-proof and end-to-end security system that addresses the risks of the quantum era, as well as enhances the resilience of the operation of critical infrastructure ecosystems. The research forms a solid basis to practical implementation and future upgrades, such as the hardware-aided PQC acceleration, inter-infrastructure federation, and the integration with autonomous incident response systems. The work will eventually lead to an important progress in the direction of secure, scalable and quantum-resistant CI infrastructures of the next decade.

References

1. Reddy, N.R., Suryadevara, S., Reddy, K.G.R. et al. Quantum secured blockchain framework for enhancing post quantum data security. Sci Rep 15, 31048 (2025). https://doi.org/10.1038/s41598-025-16315-8
2. Saberi Kamarposhti, M., Ng, K.-W., Chua, F.-F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. *Heliyon*, *10*(10), e31406. https://doi.org/10.1016/j.heliyon.2024.e31406
3. Taleby Ahvanooey, M., Mazurczyk, W., Zhao, J., Caviglione, L., Choo, K.-K. R., Kilger, M., Conti, M., & Misoczki, R. (2025). Future of cyberspace: A critical review of standard security protocols in the post-quantum era. *Computer Science Review, 57,* 100738. https://doi.org/10.1016/j.cosrev.2025.100738
4. Dai, Y., Lu, G., & Huang, Y. (2024). A blockchain-based access control system for secure and efficient hazardous material supply chains. *Mathematics, 12*(17), 2702. https://doi.org/10.3390/math12172702
5. Punia, A., Gulia, P., Gill, N. S., & others. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing, 13,* 146. https://doi.org/10.1186/s13677-024-00697-7
6. Geremew, A., & Mohammad, A. (2024). Preparing critical infrastructure for post-quantum cryptography: Strategies for transitioning ahead of cryptanalytically relevant quantum computing. *International Journal on Engineering, Science and Technology, 6,* 338–365. https://doi.org/10.46328/ijonest.240

7. Ghadi, Y. Y., Mazhar, T., Shahzad, T., & others. (2025). A hybrid AI-blockchain security framework for smart grids. *Scientific Reports, 15*, 20882. https://doi.org/10.1038/s41598-025-05257-w
8. Oliva del Moral, J., deMarti iOlius, A., Vidal, G., Crespo, P. M., & Etxezarreta Martinez, J. (2024). Cybersecurity in critical infrastructures: A post-quantum cryptography perspective. *IEEE Internet of Things Journal, 11*(18), 30217–30244. https://doi.org/10.1109/JIOT.2024.3410702
9. Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Securing critical infrastructure with blockchain technology: An approach to cyber-resilience. *Computers, 13*(5), 122. https://doi.org/10.3390/computers13050122
10. Chawla, D., Kumari, S., Rathore, R. S., Mehra, P. S., Das, A. K., & Kumar, N. (2025). Quantum blockchain for Internet of Things: A systematic review, proposed solutions and challenges. *Computers and Electrical Engineering, 126*, 110524. https://doi.org/10.1016/j.compeleceng.2025.110524
11. Balasubramaniam, A., & Surendiran, B. (2024). QUMA: Quantum unified medical architecture using blockchain. *Informatics, 11*(2), 33. https://doi.org/10.3390/informatics11020033
12. Naik, A. S., Yeniaras, E., Hellstern, G., & others. (2025). From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance. *Financial Innovation, 11*, 88. https://doi.org/10.1186/s40854-025-00751-6
13. Khan, A. A., Laghari, A. A., Almansour, H., & others. (2025). Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud-enabled public auditing platforms. *Journal of Cloud Computing, 14*, 43. https://doi.org/10.1186/s13677-025-00771-8
14. Allende, M., León, D. L., Cerón, S., & others. (2023). Quantum-resistance in blockchain networks. *Scientific Reports, 13*, 5664. https://doi.org/10.1038/s41598-023-32701-6
15. Kumar, M., & Mondal, B. (2024). Quantum blockchain architecture using cyclic QSCD and QKD. *Quantum Information Processing, 23*, 101. https://doi.org/10.1007/s11128-024-04316-x
16. Hajar, D., Afifi, N., & Hilal, I. (2025). Dynamic sharding and Monte Carlo for post-quantum blockchain resilience. *Cryptography, 9*(2), 22. https://doi.org/10.3390/cryptography9020022
17. Seol, J., & Kim, J. (2024). Machine learning ensures quantum-safe blockchain availability. *Journal of Computer Information Systems, 65*(5), 555–579. https://doi.org/10.1080/08874417.2024.2308207
18. Wicaksana, A. (2025). A survey on quantum-safe blockchain security infrastructure. *Computer Science Review, 57*, 100752. https://doi.org/10.1016/j.cosrev.2025.100752
19. Revathi, K., & Suganthi, K. (2025). Enhancing blockchain security against quantum threats through integration of post-quantum cryptographic algorithms. *Computers and Electrical Engineering, 127*(Part B), 110610. https://doi.org/10.1016/j.compeleceng.2025.110610
20. Parida, N. K., Jatoth, C., Reddy, V. D., & others. (2023). Post-quantum distributed ledger technology: A systematic survey. *Scientific Reports, 13*, 20729. https://doi.org/10.1038/s41598-023-47331-1
21. Gharavi, H., Granjal, J., & Monteiro, E. (2024). Post-quantum blockchain security for the Internet of Things: Survey and research directions. *IEEE Communications Surveys & Tutorials, 26*(3), 1748–1774. https://doi.org/10.1109/COMST.2024.3355222
22. Malina, L., et al. (2021). Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access, 9*, 36038–36077. https://doi.org/10.1109/ACCESS.2021.3062201
23. Shahid, F., Khan, A., & Jeon, G. (2020). Post-quantum distributed ledger for internet of things. *Computers & Electrical Engineering, 83*, 106581. https://doi.org/10.1016/j.compeleceng.2020.106581
24. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access, 8*, 21091–21116. https://doi.org/10.1109/ACCESS.2020.2968985