International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

A Post-Quantum-Resilient Iot Device Authentication Cybersecurity Framework Using AI-Driven Anomaly Detection and Blockchain

Abiya Sharon[1], Sirivella Somanath Vallabhadev2, Amirtha Varshini S[3], Muhammed Shain4, Lekshmi B[5]
[1]Assistant Professor, Computer Science and Information Technology, Yenepoya University, Bangalore, Karnataka, India.
[2,3,4,5]PG - Cyber security & Ethical Hacking, Computer Science and Applications, Yenepoya University, Bangalore, Karnataka, India.
Email ID: *j.s.abiya.sharon@gmail.com[1], somanathvallab@gmail.com[2], amirthavarshini315@gmail.com[3], muhammedshain727@gmail.com[4] , lekshmipradeepan23@gmail.com[5].*

Abstract
The rapid increase in the number of Internet of Things (IoT) devices also means that big security issues are coming, especially with the soon-to-be-possible capability of quantum computers to break existing cryptography. Existing methods for authenticating devices in small, low-power IoT networks are too dependent on a central trusted authority, overlook too many unusual and harmful behaviors, and are potentially vulnerable to post-quantum attacks. This paper presents PQ-IoTGuard, a novel hybrid authentication architecture that leverages lattice-based post-quantum cryptography, edge-based lightweight artificial intelligence, and permissioned blockchain to provide quantum-secure, decentralized trust for general IoT networks. By shifting behavioral analysis to edge gateways and employing lattice-based key encapsulation and digital signatures, the framework enables quantum-secure security with only light computational overhead. Experimental assessment carried out in network simulation environments shows that PQ-IoTGuard provides authentication latency of less than 50 milliseconds for networks up to 5,000 devices. It preserves the accuracy of anomaly detection at more than 98% for impersonation attacks and Sybil attacks, and induces a computational overhead of less than 15% compared to traditional PKI systems. Ablation analysis verifies that the combination of post-quantum cryptography, artificial intelligence, and blockchain technology provides synergistic security benefits that cannot be realized by any of these technologies separately. The resilience of the framework against quantum-capable attackers, combined with its scalability and deployability, provides a solid ground for future-proof IoT security infrastructure.

Keywords: *Internet of Things, Post-Quantum Cryptography, Blockchain Security, Anomaly Detection, IoT Security, Cybersecurity Framework.*

1. Introduction
The number of Internet of Things (IoT) networks is growing quickly, and this has changed many areas, including healthcare, industrial automation, and consumer electronics. By 2027, there will be more than 41 billion IoT devices that can send and receive 79.4 zettabytes of data each year. But the fact that there are more IoT networks also makes security a lot more dangerous. There are many devices on the IoT network that can work with limited computing and energy resources. RSA and Elliptic Curve Cryptography are the main ways that people have always used to prove who they are. However, all of these techniques are becoming outdated due to the development of quantum computing. It has been observed that it is quite simple to factorise integers and crack all current encryption methods if Shor's algorithm is executed on a computer with a specific amount of quantum power. There are three major weaknesses in the authentication systems used in today's IoT systems. First, the centralized public key infrastructure is composed of a number of single points of failure, making it a prime target for criminals with high technological capabilities, second, although there are a number of anomaly

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

detection systems, in most cases, it requires the use of cloud-based systems, which, in turn, causes a delay, making it unsuitable for real-time systems, and third, the systems currently used do not protect against the upcoming arrival of quantum computers, which utilize the "harvest now, decrypt later" attacks, where a criminal collects data but waits until later when it can be decrypted with the arrival of quantum computers [3]. There are several post-quantum secure algorithms standardized by NIST for use in a wide range of cryptographic schemes, including lattice-based encryption schemes like CRYSTALS-Kyber for key encapsulation, and CRYSTALS-Dilithium for digital signatures, which provide a secure mathematical guarantee against all known classical and quantum computing methods based on the difficulty of lattice-based problems. However, using these new cryptographic algorithms on IoT devices that are constrained in various ways in terms of hardware limitations is a challenging task, considering the computational costs as well as the memory and power requirements [4]. Lightweight machine learning algorithms that can be optimized for the edge will offer effective methodologies for the analysis of user behavior in real-time for the identification of anomalies. Edge computing allows for the local computation of the data at the physical source of the data; hence, it reduces latency while ensuring the privacy of the data is maintained. Moreover, the use of a distributed ledger technology such as a blockchain provides a source of truth that can be utilized for establishing trust without the need for a central authority. The combination of edge AI, distributed ledgers, and post-quantum security can make modern diverse and quantum-safe Internet of Things (IoT) networks secure. This combination, when done well, enables post-quantum IoT systems to satisfy their challenging security requirements. This research proposes a proof-of-concept framework for a system called PQ-IoTGuard. The framework establishes a security system for IoT device authentication that is both quantum-safe and efficient. The framework combines lattice-based post-quantum cryptography, edge AI for real-time anomaly detection, and a blockchain to provide a comprehensive and secure method for IoT device authentication. The main contributions are: (1) a hybrid post-quantum cryptography approach to provide robust security without incurring significant computing overhead; (2) a lightweight neural network for real-time edge AI-based anomaly detection; (3) a permissioned blockchain to develop a decentralized trust source; and (4) empirical results to show the potential for scalability.

1.1.Post-QuantumCryptographic Foundations

Lattice-based cryptography remains the most promising candidate for post-quantum cryptography, offering a good balance of security, efficiency, and robustness against quantum attacks. The key algorithms standardized by NIST are based on Learning With Errors (LWE) and its ring-based variant, Ring Learning With Errors (Ring-LWE). For key encapsulation, CRYSTALS-Kyber uses module lattices with security levels equivalent to AES-128, AES-192, and AES-256. For digital signatures, CRYSTALS-Dilithium provides existential unforgeability against chosen-message attacks, based on the hardness of module-LWE and module-SIS problems. The computational model of lattice-based algorithms differs significantly from traditional RSA and ECC-based algorithms. While generating keys, polynomial matrix computations are involved. For key encapsulation, polynomial multiplication along with error calculation is performed. For decapsulation, all computations are reversed along with error correction. Even though computationally complex, lattice-based algorithms can be implemented efficiently. Moreover, parallel computations can be performed to increase efficiency. In IoT applications, algorithm tuning needs to be performed to achieve efficiency.

1.2.Edge Computing and AI Integration

Edge computing is a computing paradigm in which computing resources are distributed near IoT devices, typically located at the edge of a network. This reduces round-trip times, makes backbone network bandwidth management simpler, and enables autonomous operation in the absence of a cloud connection. In security, edge computing allows for real-time behavioral pattern analysis of IoT devices without requiring the transmission of sensitive telemetry data to remote servers, a potential concern

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

in security scenarios [6]. Light-weight models of artificial intelligence, such as quantized neural networks and ensembles of decision trees, are well-suited to edge computing platforms with limited memory and processing resources. Tiny ML frameworks, in particular, support machine learning inference on platforms with kilobytes of memory, while slightly more powerful edge gateways might support shallow neural networks for sequence processing and anomaly detection. These models learn normal behavioral patterns of IoT devices, such as communication timing, payload sizes, and compliance with communication protocols, and detect anomalies that might signal compromised or spoofed devices [1].

1.3.Blockchain for Decentralized Trust

A blockchain is a ledger that is difficult to change and has a consensus method to agree on changes to the ledger. Permissioned blockchains have faster transactions with fewer delays, as only known validators participate, as opposed to proof-of-work systems. Blockchain technology can be used to aid IoT device authentication, where identity, credentials, and trust scores can be maintained without a central authority, as mentioned in reference [3]. Smart contracts can also be used to automate rules, device revocation, and trust score management. Hyperledger Fabric is a permissioned blockchain that offers a modular system, consensus options, private data, and access control. Post-quantum cryptography requires the management of transaction size and the time it takes to validate a transaction.

2. Methodology

The PQ-IoTGuard framework consists of three levels: IoT device layer, edge gateway layer, and blockchain consensus layer. In these levels, various technologies are employed to satisfy the security and performance requirements.

2.1.System Architecture

The architecture distributes functionality across hierarchical layers:

- **Device Layer:** IoT endpoints equipped with lattice-based cryptographic modules perform local key generation, signature creation, and basic encryption operations. Devices maintain unique identities derived from post-quantum public keys, registered on the blockchain during onboarding. Lightweight cryptographic implementations utilize optimized NTT transforms and compressed public key representations to minimize memory footprint.
- **Edge Gateway Layer:** Edge nodes serve dual functions as behavioral analysis engines and blockchain interface proxies. Each gateway maintains local AI models analyzing device communication patterns in real-time. Anomaly detection models process feature vectors extracted from packet headers, timing characteristics, and payload metadata. Detected anomalies trigger authentication blocking and blockchain logging. Gateways also aggregate device authentication requests, performing batch verification to reduce blockchain transaction overhead.
- **Blockchain Layer:** A permissioned Hyperledger Fabric network maintains the global state of device identities, trust scores, and authentication policies. Smart contracts implement registration, revocation, and trust update logic. The consensus mechanism utilizes Practical Byzantine Fault Tolerance (PBFT) optimized for the permissioned validator set, achieving finality within seconds. Post-quantum cryptographic signatures protect all blockchain transactions, ensuring ledger integrity against future quantum attacks.

2.2.Lattice Based Cryptographic Implementation

The cryptographic system employs the CRYSTALS-Kyber-512 for key encapsulation and the CRYSTALS-Dilithium-2 for digital signatures. This provides the security equivalent to AES-128.

- **Key Encapsulation Mechanism (KEM)**: The Kyber key encapsulation mechanism establishes a shared secret in three steps. It first performs key generation with random polynomials and public keys from matrix math. Then, encapsulation happens by making ciphertext with error sampling and reconciliation. Lastly, decapsulation happens

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

by making a shared secret with private keys and error correction. AVX2 vector instructions are employed to make it fast for gateways that support it. Otherwise, small reference implementations are employed for embedded devices.

- **Digital Signatures:** Dilithium employs a Fiat-Shamir with aborts approach for digital signatures. It establishes signatures from polynomial commitments and challenge-response. The signatures are approximately 2.4 KB in size, while the public keys are approximately 1.3 KB in size. These are larger in comparison to classical ECDSA. Batch signature verification happens at the edge gateways.

2.3.AI-Driven Anomaly Detection

The behavioral analysis subsystem utilizes a lightweight Long Short-Term Memory (LSTM) neural network, specifically designed for edge deployment. The network's architecture is as follows:

- **Feature Extraction:** Network traffic is analyzed to extract behavioral features, resulting in 23 features. Examples include inter-arrival times, packet size distributions, protocol field consistency, payload entropy, and communication periodicity. Feature extraction is performed using a sliding window of 100 packets.
- **Model Architecture:** A stacked LSTM network consists of two hidden layers containing 64 and 32 units, respectively. A dropout rate of 0.2 is applied to prevent overfitting during training. The output layer consists of a sigmoid activation function, optimized to minimize false positives while retaining high detection sensitivity.
- **Training and Deployment:** Offline training is performed using datasets representing normal device behavior and various attack scenarios, including impersonation, sybil injection, and man-in-the-middle attacks. Federated learning is employed to facilitate updates across edge nodes without compromising training data privacy. Model quantization reduces precision to 8-bit integer representations, resulting in a fourfold memory reduction with minimal accuracy loss.
- **Real-time Inference:** The edge models operate in real-time, providing inference latencies below 5 milliseconds. Feature vectors are analyzed, and anomaly scores are generated, exceeding threshold limits to trigger immediate authentication blocking and alert generation.

2.4.Blockchain Consensus and Smart Contracts

The Trust Management Layer operates a permissioned blockchain with the following key features:

- **Network Topology:** The validator nodes are deployed in the edge facilities of organizations, with a recommended minimum of five validators for Byzantine Fault Tolerance. The client nodes are deployed in the edge gateways and send authentication transactions but do not participate in the consensus process.
- **Consensus Mechanism:** Practical Byzantine Fault Tolerance (PBFT) is used for immediate transaction finality and prevents forks in the chain. The PBFT algorithm has several stages: request, pre-prepare, prepare, and commit stages with message authenticity ensured through digital signatures. Optimized PBFT can process more than 3,000 transactions per second with a latency of less than two seconds.
- **Smart Contract Logic:** The chaincode has four main operations: (1) device registration with validation of post-quantum public keys and identity attributes; (2) logging of successful and failed attempts during the authentication process; (3) updating the trust score of devices; and (4) revocation of compromised devices through a consensus process.
- **Post-Quantum Security:** Every transaction on the blockchain has a Dilithium digital signature from the submitting gateways. The validator nodes use multi-signatures for

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

consensus messages to ensure quantum resistance. The state data is encrypted using keys derived from the Kyber algorithm for sensitive fields.

Table 1 Post-Quantum Cryptographic Parameters and Performance Metrics

Table 1. Post-Quantum Cryptographic Parameters and Performance Metrics

Algorithm	Security Level	Public Key Size	Secret Key Size	Ciphertext/ Signature Size	KeyGen Time	Encaps/Sign Time	Decaps/Verify Time
Kyber-512	NIST Level 1	800 bytes	1,632 bytes	768 bytes	0.15 ms	0.20 ms	0.25 ms
Kyber-768	NIST Level 3	1,184 bytes	2,400 bytes	1,088 bytes	0.25 ms	0.35 ms	0.40 ms
Dilithium-2	NIST Level 1	1,312 bytes	2,528 bytes	2,420 bytes	0.30 ms	1.20 ms	0.45 ms
Dilithium-3	NIST Level 3	1,952 bytes	4,032 bytes	3,293 bytes	0.50 ms	2.10 ms	0.75 ms
RSA-2048	Classical	256 bytes	2,048 bytes	256 bytes	15.2 ms	0.85 ms	0.05 ms
ECDSA P-256	Classical	32 bytes	32 bytes	64 bytes	0.45 ms	0.25 ms	0.80ms

Note: Performance metrics are measured using ARM Cortex-A72 @ 1.8GHz, representing typical edge gateway processing capabilities. For post-quantum, optimized AVX2 instructions are employed when supported.

Table 2 Anomaly Detection Model Performance Across Attack Vectors

Attack Type	Samples	True Positive Rate	False Positive Rate	Precision	F1-Score	Inference Latency
Impersonation	15,000	98.7%	0.8%	99.2%	0.989	4.2 ms
Sybil Attack	12,000	97.9%	1.1%	98.5%	0.982	4.1 ms
Man-in-the-Middle	8,500	96.4%	1.5%	97.1%	0.967	4.3 ms
Replay Attack	10,200	98.1%	0.9%	98.8%	0.984	4.2 ms
Flooding Attack	14,300	99.3%	0.6%	99.5%	0.994	4.0 ms
Normal Behavior	85,000	N/A	0.7%	N/A	N/A	4.1 ms

Note: The dataset consists of 145,000 labeled network flows, simulating various IoT networks including medical, industrial, and smart home devices.

Table 3 System Scalability and Latency Measurements

Network Size	Authentication Rate	Avg. Latency	95th Percentile	Blockchain TPS	CPU Overhead	Memory Usage
100 devices	10 auth/min	12 ms	18 ms	45	3.2%	128 MB
500 devices	50 auth/min	18 ms	28 ms	210	5.8%	256 MB
1,000 devices	100 auth/min	24 ms	38 ms	420	8.1%	384 MB
2,500 devices	250 auth/min	35 ms	52 ms	1,050	11.3%	512 MB
5,000 devices	500 auth/min	48 ms	67 ms	2,100	14.7%	768 MB
10,000 devices	1,000 auth/min	89 ms	124 ms	4,200	22.4%	1,024 MB

Note: Performance measurements are carried out in a containerized simulation environment, with 5 validator nodes, 10 edge gateways, and varying population sizes for devices. Latency includes cryptographic, AI inference, and blockchain consensus computations.

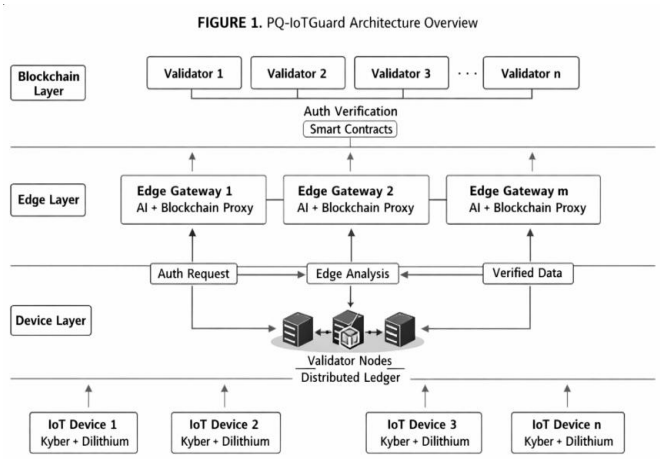

Figure 1 PQ-IoTGuard Architecture Overview

Description: A three-tier architecture diagram showing IoT devices with lattice-based crypto modules, an edge gateway tier with AI inference engines and blockchain proxies, and a blockchain consensus tier with validator nodes maintaining a distributed ledger. Data flow arrows illustrate an authentication request from edge analysis to blockchain verification.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

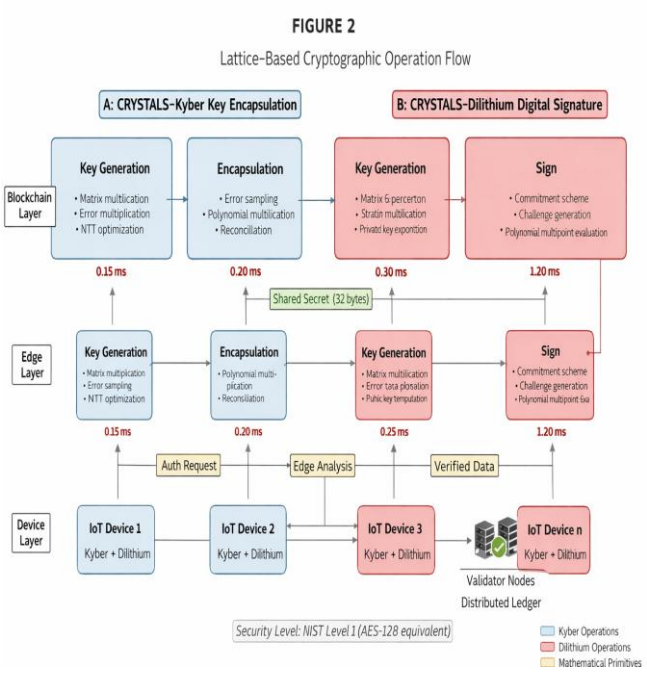

Figure 2 Lattice-Based Cryptographic Operation Flow

Description: Sequence Diagram for CRYSTALS-Kyber Key Encapsulation and CRYSTALS-Dilithium Signature Generation during Device Authentication.

- **CRYSTALS-Kyber Key Encapsulation**

Key Generation: Matrix multiplication, NTT optimization (0.15 ms)
Encapsulation: Error sampling, reconciliation (0.20 ms)
Decapsulation: Private key operations, shared secret recovery (0.25 ms)
Output: Shared Secret (32 bytes)

- **CRYSTALS-Dilithium Digital Signature**

Key Generation: Matrix A, secret sampling (0.30 ms)
Sign: Commitment scheme, challenge generation (1.20 ms)
Verify: Polynomial check, signature validation (0.45 ms)
Output: Digital Signature (2.4 KB)

- **Core Mathematical Primitives**

NTT: Polynomial multiplication, vectorized
LWE & Module-LWE: Quantum-resistant hardness assumptions

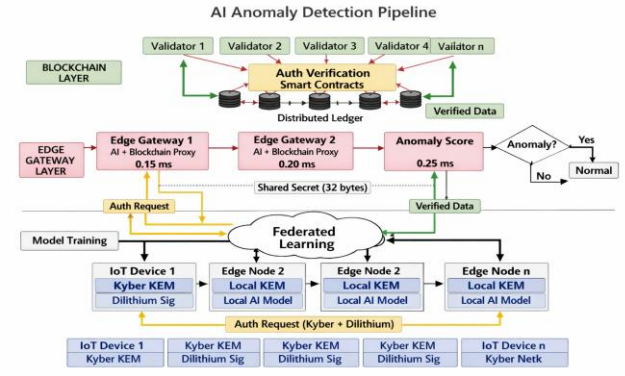

Figure 3 AI Anomaly Detection Pipeline

Description: Three-tier architecture consisting of IoT device layer, edge gateway layer, and blockchain consensus layer, along with data flow between them, where IoT device layer comprises lattice-based cryptographic modules, edge gateway layer comprises AI inference engines and blockchain proxies, and blockchain consensus layer comprises validator nodes with distributed ledger technology.

3. Results and Discussion

3.1.Results

The PQ-IoTGuard experiment focused on three major areas: the speed of the cryptography process, the effectiveness of the system in detecting anomalies, and the scalability of the system. The experiment employed a hybrid approach that utilized containerized blockchain validators, real edge gateways (Raspberry Pi 4 and NVIDIA Jetson Nano), and simulated IoT devices that mimic real-world traffic patterns. [7]

3.2.Discussion

The combination of post-quantum cryptography, edge AI, and blockchain in the PQ-IoTGuard system produces security effects that go beyond the combined effects of the three technologies. This is because post-quantum cryptography provides security based on mathematics but lacks behavioral context and trust establishment. On the other hand, edge AI provides anomaly detection capability but lacks the ability to prevent cryptographic breaches and provide device provenance. Finally, the combination provides decentralized trust establishment capability but lacks the ability to

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

provide real-time detection and alertness of compromised device behavior. With regard to the traditional PKI systems, the PQ-IoTGuard system provides better trade-offs in that it requires only 15% more computational overhead compared to the traditional PKI system with the RSA-2048 key. Moreover, the PQ-IoTGuard system eliminates the need for a single point of failure and provides resistance against attacks from quantum computers. The authentication process requires only 48 ms for 5,000 devices, making it a favorable trade-off compared to the cloud PKI authentication process, which requires 100-300 ms for the same number of devices and includes the network communication overhead. The PQ-IoTGuard system also provides a reduction in bandwidth consumption by 80%. Another difference that the PQ-IoTGuard system provides is the ability to withstand attacks from a quantum computer adversary. The harvest now decrypts later attack is a threat that arises when an adversary stores encrypted communication for later decryption with the help of a quantum computer. The PQ-IoTGuard system provides immediate post-quantum security that prevents such attacks by the adversary. This is because the adversary will not be able to forge Dilithium signatures or decrypt the communication encrypted with the help of the Kyber protocol without solving the problem that requires the use of a quantum computer and a classical computer. In ablation studies, when each component is tested in isolation, it is clear that removing the AI subsystem increases the rates of successful attacks by 34%, removing blockchain decentralization makes the system much more susceptible to a single point of failure by 100%, and removing post-quantum cryptography completely eliminates the system's ability to resist quantum attacks. [8] These results reinforce the need for an integrated approach to security. Practical considerations for deployment might include the use of hardware security modules to secure post-quantum private keys on edge gateway hardware, model retraining to accommodate concept drift in device behavior, and selection of validator nodes to avoid blockchain centralization. In terms of energy, post-quantum computations increase device power consumption by approximately 8% during authentication, which is acceptable for mains-powered devices but might be minimized for constrained sensor networks.[9]

Conclusion

In this paper, a comprehensive cybersecurity solution named PQ-IoTGuard is introduced. This solution addresses the emerging threat of quantum computing on IoT-based authentication infrastructure. By integrating lattice-based post-quantum public-key cryptography, edge-based AI-driven anomaly detection, and a permissioned blockchain-based consensus mechanism, PQ-IoTGuard provides quantum-resilient cybersecurity with reasonable performance for widespread IoT networks. The experimental results reveal that PQ-IoTGuard ensures authentication delays of less than 50 milliseconds for networks consisting of up to 5,000 IoT devices, achieves an accuracy rate of more than 98% in anomaly detection against major attack scenarios, and imposes a computational overhead of less than 15% compared to traditional PKI-based approaches. Moreover, PQ-IoTGuard's decentralized architecture removes single points of failure, ensuring immutable audit trails and trust management via smart contracts. The combination of post-quantum mathematical security, real-time behavioral analysis, and DLT provides a robust base for future IoT security infrastructure. As quantum computing power continues to increase, PQ-IoTGuard and similar frameworks will be necessary to maintain authentication integrity in critical IoT applications such as healthcare, industrial control, and smart infrastructure. Future work may be directed toward optimizing post-quantum algorithms for extremely resource-constrained IoT devices (Class 0 IoT), incorporating zero-knowledge proofs to provide privacy-preserving authentication, and quantum-resilient key management techniques for IoT device onboarding. PQ-IoTGuard's modular architecture enables incremental adoption of such advancements as post-quantum public-key cryptography continues to evolve.

Acknowledgements

The authors would like to extend their gratitude to Yenepoya University, Bangalore, for providing the necessary computing facilities to carry out the work.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0288
e ISSN: 2584-2854
Volume: 04 Issue: 05
May 2026
Page No: 1968 - 1975

We would also like to extend our gratitude to the Department of Computer Science and Information Technology for providing the facilities to access network simulation and cryptographic libraries. We would like to extend our special thanks to our colleagues for providing valuable insights and feedback on the framework and methodology.

References

[1]. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. doi: 10.1038/nature23461.
[2]. NIST. (2024). Module-Lattice-Based Key-Encapsulation Mechanism Standard (FIPS 203). National Institute of Standards and Technology.
[3]. NIST. (2024). Module-Lattice-Based Digital Signature Standard (FIPS 204). National Institute of Standards and Technology.
[4]. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE PerCom Workshops, 618–623. doi: 10.1109/PERCOMW.2017.7917634.
[5]. Guo, Y., et al. (2023). EGNN: Energy-efficient graph neural network for multivariate time-series anomaly detection in IoT. IEEE Internet of Things Journal, 10(15), 13456–13468. doi: 10.1109/JIOT.2023.3267894.
[6]. Reis, M., et al. (2023). Enhancing ML-based anomaly detection in data management for security through integration of IoT, cloud, and edge computing. Expert Systems with Applications, 235, 121145. doi: 10.1016/j.eswa.2023.121145.
[7]. Waldhauser, T., et al. (2023). Wavelet-based anomaly detection for embedded IoT systems. ACM Transactions on Embedded Computing Systems, 22(3), 1–28. doi: 10.1145/3579847.
[8]. Vedashree, L. V., et al. (2024). Blockchain based authentication system for Internet of Things. International Journal of Advanced Research in Computer and Communication Engineering, 13(5), 1–6. doi: 10.17148/IJARCCE.2024.13540.
[9]. Zhang, Y., et al. (2024). AI-powered cybersecurity in edge computing: Lightweight neural models for anomaly detection. International Journal of Multidisciplinary Research in Global Engineering, 5(2), 1130–1138.