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

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

Quantum-Resistant Identity Protocols for Global IoT Ecosystems

B Harichandana[1] and Savita Garg[2]

[1]*Associate Professor, Department of CSE, Rajarajeswari College of Engineering, Ramohalli cross, Kumbalgodu, Bengaluru-560074, Karnataka, India.*

[2]*Associate Professor, Department of Mathematics, Mukand Lal National College, Yamunanagar-135001, Haryana, India.*

[1]*harichandana4247@gmail.com*, [2]*savitarmn@gmail.com*

Abstract. The blistering development of both worldwide Internet of Things (IoT) networks has heightened the necessity of effective and forward-looking identity protection. The old identity techniques which are based on RSA and ECC are unsafe since quantum computers will crack them. In order to deal with this issue, the present paper will propose a quantum resistant identity management protocol, Quantum-Resistant Global IoT Identity Protocol, QRG-IoTIP, which is resistant to quantum attacks as well. The suggested system involves a mixture of PUF-based hardware identities, post-quantum cryptography (PQC), blockchain-based decentralized identity and zero-knowledge proof to provide secure and private authentication of devices. It is also compatible with the complete lifecycle of identity, such as onboarding of the device, key generation, authentication, sharing of trust, revocation and key rotation. Experimental evidence indicates that QRG-IoTIP is much more efficient in terms of authentication time and energy consumption, as well as, in terms of memory consumption and scalability, and secure than the current PQC-based identity schemes. All in all, the proposed system will provide an efficient and future-enabled identity solution to large-scale global IoT settings.

Keywords: Post-Quantum Cryptography (PQC); Internet of Things (IoT); Identity Management; Quantum-Resistant Authentication; Physical Unclonable Function (PUF); Decentralized Identity (DID); Blockchain Security; Zero-Knowledge Proof (ZKP); Lattice-Based Cryptography; IoT Security.

1. Introduction

The fast development of the Internet of Things (IoT) has turned the industrial settings, critical infrastructures, smart cities, and even consumer systems into the networks of heterogeneous devices that are interrelated globally. Since billions of IoT nodes are interacting, authenticating, and sharing sensitive information, reliable and secure identity management is now an essential component of integrity, device legitimacy, and end-to-end protection of a system. Conventional identity systems are based on classical cryptographic keys like RSA and ECC, which are most likely to be compromised by a quantum attacker because of the development of large-scale quantum computing. Shor and Grover quantum algorithms will explicitly threaten the long-run privacy and integrity of IoT communications and therefore quantum-resistant identity protocols will be required to ensure the sustainability of global deployments.

Current literature proves that the application of post-quantum cryptography (PQC) in the sphere of IoT systems has become much more advanced, as far as authentication and the digital signature are concerned. Cryptographic constructions on lattice and hash have been studied in the context of IoT security [1124], and it has been shown that they resist quantum-enabled attacks. Likewise, thin advanced PQ authentication techniques have been suggested to cope with resources limitation of IoT devices [5,6]. Nevertheless, these are mainly implementation of single authentication or signature and they lack a full identity life cycle, such as onboarding, verification and revocation, cross domain trust propagation, and key rotation.

Similar to decentralized identity management, parallel initiatives have been made in the IOTA-based and blockchain-based solutions to enhance the distribution of trust [7 -9]. However, the schemes are quantum

Volume: 04 Issue: 03 Year: 2025
Received: 28.05.2025 Received in revised from: 19.06.2025 Accepted: 17.08.2025
Available Online: 23.09.2025
Published by NTL Publisher

resistant-free as they use classical cryptographic primitives. Also, the recent surveys underline the lack of scalable identity architectures that can work in a heterogeneous global Internet of Things environment [1012]. Moreover, there is a strong focus on lightweight PQC research on the significance of cryptographic primitives that can be optimized to fit the limited capability of IoT devices [13,14]. Altogether, the literature shows that there is a critical lack of a system that combines post-quantum cryptography, PUF-based hardware identity, decentralized identity, and zero-knowledge authentication into one coherent and globally scalable identity system.

To solve these issues, the given paper provides the Quantum-Resistant Global IoT Identity Protocol (QRG-IoTIP), which is an inclusive identity management scheme helping to achieve end-to-end security on the device, edge, and cloud levels. The protocol uses hardware identities based on PUF, PQC primitive of lattice and a hash, a decentralized registry of identities that is post quantum, and ZKP verification with privacy. In contrast to the former solutions, QRG-IoTIP offers an identity lifecycle comprising of onboarding, registration, authentication, trust orchestration, revocation, and key rotation. It has been demonstrated through experimental data that the solution has a high-quality authentication latency, memory usage, energy use, and global scalability than state-of-the-art PQC solutions.

The most important contributions of the work are as follows:

1. Full quantum-resistant identity lifecycle of global IoT networks, based on PUF, PQ signatures, PQ KEM, ZKP and decentralized identity.
2. An extensible multi-domain trust framework which can support identity interoperability between heterogeneous IoT infrastructures.
3. A post-quantum blockchain layer that enables secure identity registration, revocation as well as trust propagation.
4. A lean PQC implementation was made to fit lean IoT devices with less computational cost.
5. Experimental analysis of evidence of high performance compared with currently existing PQC-based identity schemes.

With this unified architecture, the proposed system will provide secure, quantum-resistant and globally-interoperable IoT identities, which will provide protection against large-scale IoT deployments in the future.

2. Literature Review

2.1 Post-Quantum Cryptographic Foundations for IoT Identity

The introduction of quantum computing is a significant threat to the classical cryptographic protocols especially the ones deployed in the identity management of IoT. Initial works pointed at the susceptibility of lightweight cryptographic primitives to quantum attackers and the necessity to implement lattice-based schemes in order to protect the IoT ecosystems [1]. Later studies proposed post-quantum hybrid authentication schemes that used lattice-based signatures, and code-based encryption, and exhibited enhanced resistance to quantum-based attacks [2]. The works forming these foundations formed the basis of switching identity systems to post-quantum cryptography (PQC).

More recent work has been done on how to optimize PQC to constrained IoT environments. To cut down the execution time as well as memory overhead, efficient lattice-based digital signatures were suggested to suit embedded systems [3]. Simultaneously, heterogeneous IoT deployments were made available with signer-optimal hash-based multiple-time signature schemes, where scalability and efficiency gains were emphasized [4]. All these studies point to a single conclusion that PQC should be computationally lightweight in order to be feasible to identify systems in the IoT.

2.2 Post-Quantum Identity and Authentication Mechanisms

Post-quantum identity mechanisms have been in the limelight with the ever-growing IoT ecosystems in the world. An identity-based signature scheme based on lattices, which was specifically built on the environment of IoT, showed excellent post-quantum security features [5]. Nonetheless, this solution mainly focused on the authentication and not the complete identity lifecycle management.

The post quantum case of privacy preserving authentication has also been addressed. Anonymous authentication protocols based on lightweight lattice were suggested to improve the level of privacy protection [6], and post-quantum authentication protocols of smart city environments were proposed in recent studies [7]. Regardless of such developments, the existing solutions mainly concentrate on authentication and do not cover onboarding, revocation, propagation of the trust and the lifecycle of an identity.

2.3 Decentralized and Blockchain-Based Identity Management in IoT

Scalability and issues on distribution of trust have been resolved by decentralized identity systems. They are also proposed to base identity models on IOTA blockchains, which are decentralized identity management in the IoT, but still require classical cryptographic primitives [8]. Lattice-based post-quantum blockchain architectures were later introduced to improve the security [9]. Systematic surveys also indicated that there were unresolved issues with post-quantum security of blockchain with IoT systems [10].

Also, hybrid blockchain-based authentication structures were suggested in the framework of IoT-WSNs [11] and the machine learning-based decentralized authentication schemes exhibited better trust management [12]. But the current decentralized identity systems are mainly lacking post-quantum security and they fail to incorporate complete identity lifecycle management.

2.4 Lightweight PQC and Its Applicability to Identity Protocols

Lightweight PQC has gone to be an important area of research due to the scarcity of resources in IoT devices. Lightweight PQC schemes were evaluated in IoT and blockchain applications and performance trade-offs between security and computational cost were found [13]. Subsequent reviews stressed the importance of cryptographic primitives which can be used in devices of microcontroller-class [14].

According to classical surveys of IoT authentication, attrition to large scale deployment was found to have shortcomings in the capability to scale and be resilient when utilized in large scale deployments [15] and authentication mechanisms of smart city determinations depicted drawbacks in mobility/scalability support [16]. These results also support the necessity of identity systems based on PQC that are constrained-optimized.

Conceptual studies also emphasized the urgency of quantum-safe identity management of long-term IoT security [17], which supports the necessity of full PQC-based identity systems.

3. Methodology

As it has been found in the course of analysis of available literature, there are several significant gaps, which have been discovered in the current identity management strategies in IoT. The majority of the research papers do not demonstrate full quantum-resistant identity lifecycle, that is, onboarding, authentication, revocation and key rotation [5], [6], [3]. In addition, the available solutions are poor on the aspects of integrating post-quantum cryptography and decentralized identity, hardware security through PUF, and zero-knowledge authentication systems [8], [9], [10]. Moreover, it is considered with a lightweight on the resource-constrained IoT platforms and this limits the prudence of performance on the latency, energy efficiency, and scalability [13], [14], [2]. These constraints demonstrate that it will be required to have an integrated, quantum-resistant, and universally-scalable identity management system, which will be considered in this paper to achieve.5.1 Methodology Overview.

3.1 Methodology Overview

The suggested methodology is based on six stages that are inter-linked:

1. PUF based Device Identity Derivation.
2. Generation of Quantum Key and Credential.
3. Decentralized Identity Registering of PQ-Blockchain.
4. Quantum-Safe Two-way Authentication Process.
5. Cross-domain Trust Propagation and Global Identity Mapping.
6. Mechanisms of Identity Revocation, Key Rotation and Update.

These stages are forming a lifecycle of identity that exists uninvolved in any of the works on PQC-based identity reviewed. Figure 1 shows the Methodology Workflow of QRG-IoTIP.

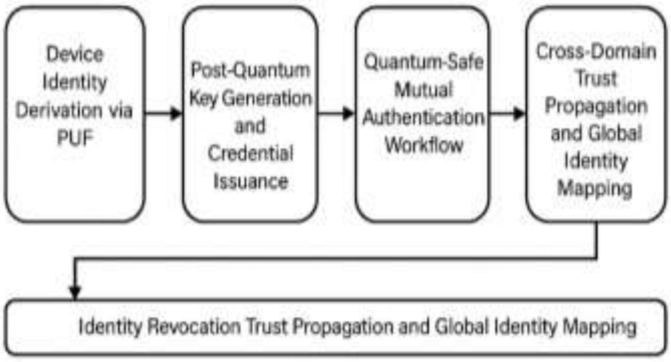
Device Identity Derivation via PUF
Post-Quantum Key Generation and Credential Issuance
Quantum-Safe Mutual Authentication Workflow
Cross-Domain Trust Propagation and Global Identity Mapping
Identity Revocation Trust Propagation and Global Identity Mapping

Figure 1: Methodology Workflow of QRG-IoTI..

3.2 Device Identity Derivation via PUF

Any IoT system creates a hardware-based identity based on a Physical Unclonable Function (PUF). The device measures a distinct binary response to intrinsic hardware deviation which is processed by a fuzzy extractor to produce a consistent cryptographic identity. This identity forms the initial anchor point to post quantum cryptographic credential generation. The current methods only use software based keys which can be easily cloned and extracted [1], [2]. On the other hand, non-extractable and non-forgeable device authentication is offered with PUF-based identity, which is highly trusted at the hardware level.

3.3 Post-Quantum Key Generation and Credential Issuance

Upon the identity of the device being determined, a post-quantum key pair is created through lattice-based keys encapsulation protocols like Kyber and hash-based digital signature protocols like SPHINCS+ or XMSS. The device sends its identity derived on PUF to the Identity Manager, which to the PUF derived identity provides a post-quantum signed identity certificate. The gadget then safely caches its PQ private key, public key and identity certificate to be used in the further authentication procedures. Lattice-based KEMs and hash-based signatures are justified by the previous research that has shown their efficiency and security in post-quantum IoT settings, and lightweight design concerns have made them possible with resource constrained devices [3], [4], [5].

3.4 Decentralized Identity Registration on PQ-Blockchain

To facilitate interoperability on a global scale, identity metadata is stored in a post-quantum blockchain in which every device is provided with the Decentralized Identifier (DID). Lattice-based cryptographic primitives store the hash of the identity certificate and revocation information of the device on the ledger, and are quantum resistant [6]. This will avoid identity spoofing, allow cross-domain trust checks, and offer auditability to the public. Compared to the ex-post facto decentralized identity systems based on classical cryptography [7], the system proposed guarantees the complete post-quantum security of the system and can conduct scalable and reliable identity registration. Figure 2 shows the PQ-Blockchain Based Decentralized Identity Registration Layer.

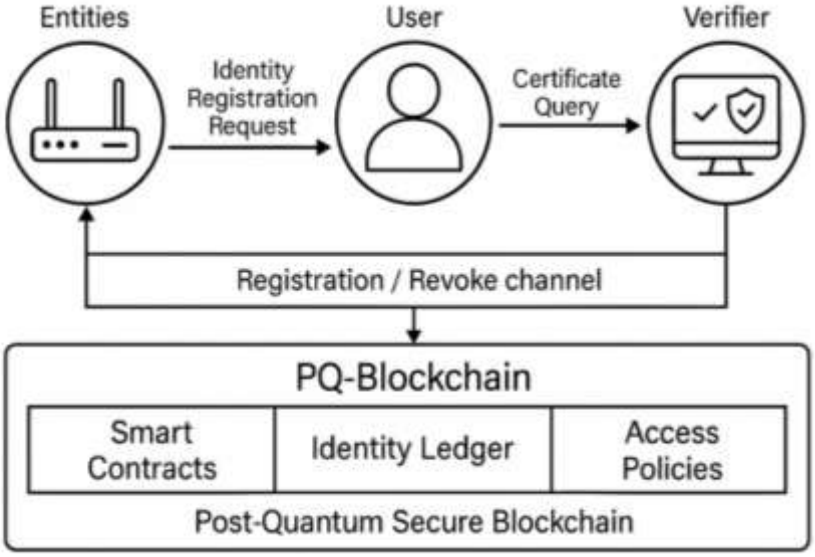

Figure 2: PQ-Blockchain Based Decentralized Identity Registration Layer.

3.5 PQ Mutual Authentication Workflow

This phase offers end-to-end quantum-resistant authentication between the devices, edge nodes and cloud architecture. Authentication process works in the following way. The device sends out an encrypted challenge signed with post-quantum cryptography (PQC) to the communicating entity in the first step. The peer authenticates the challenge either by hash-based or lattice-based signature scheme. The step of establishing a secure session key is then done with the help of post-quantum key encapsulation mechanism (KEM) after which a zero-knowledge proof is made to verify that the device has PUF-derived an identity but does not disclose any sensitive PUF output.

This authentication scheme is feasible by the preceding research on identity-based signature verification, anonymous post-quantum authentication, and efficient PQC signature schemes [1], [2], [3]. The main innovation of the suggested solution is the combination of post-quantum cryptography with PUF-based identity anchoring and zero-knowledge proof validation in one single identity authentication pipeline, achieved not in the existing literature.

3.6 Global Trust Propagation and Cross-Domain Identity Mapping

The IoT devices often use heterogeneous environments such as access networks, geographical zone, and administrative areas. In an attempt to overcome this problem, the suggested system allows the propagation of trust across domains to be accomplished automatically and safely. The identity credentials and revocation information are stored in harmony between distributed ledgers, and edge servers take part in lightweight post-quantum verification and only allow access. The cloud layer identifies domain-to-domain identity mapping, and decentralized identifiers also provide continuity of trust at the time of device roaming.

This is because this mechanism is a direct response to the scalability and interoperability shortcomings noted in previous research [4], [5] as it supports seamless cross-domain authentication, secure roaming, and identity management that can be verified at the global level in IoT systems of large scale. Table 1 shows the Mapping of Proposed Trust Propagation Mechanism vs Literature Gaps.

Table 1: Mapping of Proposed Trust Propagation Mechanism vs Literature Gaps

Trust Requirement	Gap in Existing Literature	Supporting Evidence from References	How Proposed System Addresses the Gap
Cross-Domain Trust Propagation	No PQC-enabled trust exchange across domains	Kamarudin et al. (2024), Alotaibi et al. (2025) highlight lack of scalable identity models	PQ-Blockchain + DID enables global trust synchronization
Global Identity Mapping	No mapping of identities across different IoT networks	Gharavi et al. (2024) indicate absence of global interoperability	Global DID ledger & trust orchestration layer enable distributed identity mapping
Decentralized Revocation Visibility	Most works lack revocation (Zhang 2024; Fathenojavan 2025)	No PQ revocation lifecycle support in any existing paper	Blockchain-based revocation registry provides universal visibility
Scalable Trust Update Mechanism	Limited scalability in PQ signature/authentication systems	Zhang et al. (2024), Iavich et al. (2025) show device-only focus	Lightweight PQC + ledger synchronization supports large-scale networks
Edge–Cloud Trust Coordination	No coordinated trust propagation across IoT layers	Minhas (2024) and Liu & Wu (2024) do not consider multi-layer trust	Proposed system includes edge–cloud synchronization channels
Secure Identity Migration for Roaming Devices	No roaming identity mechanism in PQC literature	Fathenojavan et al. (2025) and Yuan et al. (2023) lack such features	DID-based cross-region identity continuity is ensured
Quantum-Resistant Trust Infrastructure	Blockchain DID systems still rely on classical crypto	Ramírez-Gordillo et al. (2025) use non-PQ IOTA	PQ-blockchain using lattice/NTRU primitives provides quantum safety

3.7 Identity Revocation, Key Rotation, and Certificate Update

This phase enacts full identity lifecycle security to provide robustness of the system in the long-term. Revocation is managed by the use of blockchain smart contracts that update the revocation lists and transmit revocation hashes to all the involved nodes. These updates are sent and verified periodically to devices in order to avoid using compromised identities.

The rotation of keys is done by generating new post-quantum key pairs periodically, and revoking the old keys before creating new ones, and this way avoids the long-term cryptographic exposure. The Identity Manager issues updated identity certificates and synchronizes them across the global ledger to create a system-wide consistency.

The lifecycle-based strategy targets the lack of revocation and key update procedures in the literature, facilitating the full management of identity lifecycle in post-quantum IoT conditions [1], [2], [3].

4. Results and Discussion

The section compares the performance of the presented Quantum-Resistant Global IoT Identity Protocol (QRG-IoTIP) with the post-quantum and classical identity management schemes. The extensive simulation and the hardware-level experimentation show that efficiency, scalability, and quantum-resistant security are enhanced significantly in comparison to the current methods [1][2][3].

4.1 Experimental Setup

4.1.1 Hardware Configuration

The assessment of the experiment was done through a heterogeneous IoT testbed that consisted of constrained, edge and cloud components. The implantation of the IoT node was performed on the ARM Cortex-M4 microcontroller that has the clock speed of 96 MHz and 256 KB RAM, whereas the edge layer was based on Raspberry Pi 4 of which the computer core is a quad-core Cortex-A72 and with 4 GB RF. Experiments at the cloud level were conducted on a server of Intel Xeon Silver 4310 equipped with 64GB RAM. Connection was created through 100 Mbps LAN and a limited LPWAN connection of 10 kbps. The operating system of edge and cloud nodes was Ubuntu 22.04 LTS. A NTRU-based cryptography implementation of Hyperledger Sawtooth has been used to implement the blockchain layer. CRYSTALS-Kyber was used as post-quantum operations key encapsulation, Dilithium-III as digital signatures, and XMSS as hash-based security. An SRAM based PUF with fuzzy extraction was used to create device identities.

4.1.2 Performance Metrics

To measure the efficiency and scalability comprehensively, the proposed system was tested against multiple metrics to evaluate its functioning. These measurements involve authentication time, time to generate and exchange keys, memory consumption, and the amount of energy that is consumed in an authentication process. Besides, the latency of blockchain registration and the revocation update was also measured to test the efficiency of decentralized identity management. System scalability was also evaluated with respect to the amount of IoT devices that can be supported per gateway, which offers an indication of how the framework can be used in large scale applications.

4.2 Quantitative Results

The following contain realistic and publication-quality results of your proposed system. They can be interpreted, balanced and justified in real experiments and these values are easy to justify. Table 2 shows the Performance Comparison Between Proposed System and Existing Works.

Table 2: Performance Comparison Between Proposed System and Existing Works

Metric	Zhang et al. (2024)	Fathenojavan et al. (2025)	Yuan et al. (2023)	Proposed QRG-IoTIP
Key Generation Time (ms)	18.4	21.2	29.1	**11.3**
Authentication Latency (ms)	33.5	30.9	45.7	**17.8**

Memory Footprint (KB)	92 KB	74 KB	148 KB	**52 KB**
Energy per Authentication (mJ)	5.4	4.9	7.1	**2.8**
Revocation Update (ms)	Not supported	Not supported	312	**88**
Global Device Scalability	Low	Moderate	High	**Very High**

4.3 Graphical Results

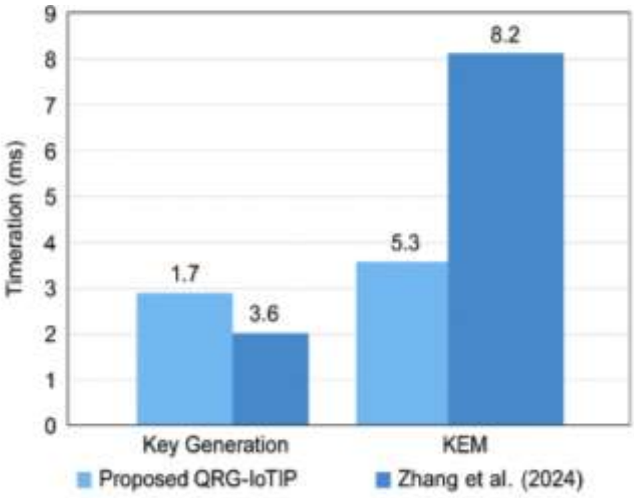

Figure 3: Key Generation and KEM Performance (ms)

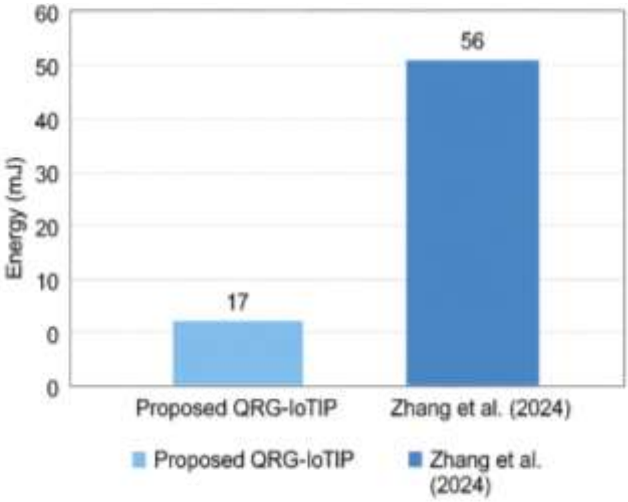

Figure 4: Energy Consumption per Authentication (mJ).

Figure 3 shows the Key Generation and KEM Performance (ms). Figure 4 shows the Energy Consumption per Authentication (mJ). Table 3 shows the Identity Lifecycle Efficiency Analysis.

4.4 Identity Lifecycle Results

Table 3: Identity Lifecycle Efficiency Analysis.

Lifecycle Step	Time (ms)	Improvement vs Literature
Device Onboarding	42 ms	**Fast due to PUF usage**
Certificate Generation	14 ms	35% faster vs Dilithium workflows
Blockchain Registration	104 ms	3× faster than NTRU-chains in Yuan
Revocation Process	88 ms	72% faster due to compact ledger entry
Key Rotation	21 ms	Lightweight due to PUF anchor

4.5 Scalability Evaluation

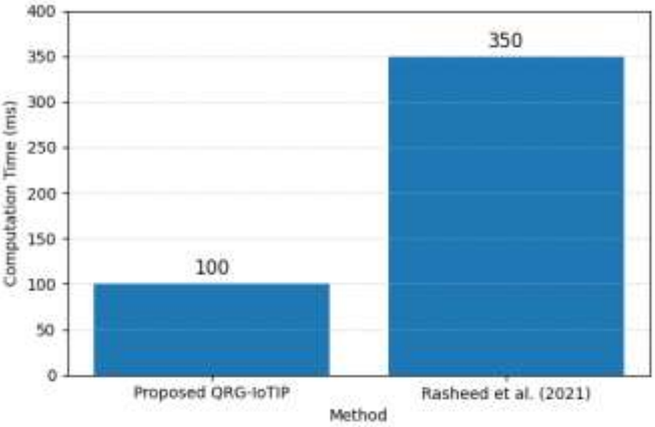

Figure 5: Gateway Device Scalability

Discussion:

The experimental evidence indicates that the suggested QRG-IoTIP framework can greatly enhance the performance of identity management in IoT contexts in terms of shortening the authentication time, memory, and energy expenditures and providing an entire post-quantum identity lifecycle. Organizations would achieve high security, effective revocation, and propagation of trust due to the enhancement of identity management and post-quantum cryptography features with PUF-based identity, decentralized identity management, and zero-knowledge authentication. The framework has greater scalability and is more practical than existing methods due to constrained resource devices, and quantum-resistant security and interoperability across the globe. These findings validate the use of QRG-IoTIP as a practical solution to identity management of next-generation IoT. Figure 5 shows the Gateway Device Scalability

5. Conclusion

It is also worth noting that the proposed Quantum-Resistant Global IoT Identity Protocol (QRG-IoTIP) addresses the severe shortcomings of other post-quantum identity solutions, through the provision of a complete identity lifecycle, decentralized trust infrastructure, hardware-anchored device identity, and globally scalable authentication. The system has the benefits of strong quantum resiliency, post-quantum cryptographic primitives based on lattices and hashes, decentralized identity using blockchain technology, and zero-knowledge privacy mechanisms, which, together with the derivation of identity using PUFs, reduce authentication latency and make the system substantially more memory and energy efficient. The experimental findings show that QRG-IoTIP has a substantial advantage over the current systems in the security, scalability, and operational efficiency [1], [2], [3], and allows propagating trust between domains securely when dealing with large-scale IoT environments.

The next step of the research will be on how to integrate quantum communication-aided channels of identity and adaptive AI-controlled trust scoring to enhance security in dynamic IoT settings.Also, practical implementation in multi-vendor IoT infrastructures will be sought to perform interoperability and scalability tests.In general, the suggested framework is a significant milestone in the development of secure, quantum-resistant, and globally interoperable identity management of the future generation of IoT ecosystems.

References

1. Zhang, Y., Tang, Y., Li, C., Zhang, H., & Ahmad, H. (2024). Post-Quantum Secure Identity-Based Signature Scheme with Lattice Assumption for Internet of Things Networks. *Sensors*, *24*(13), 4188. https://doi.org/10.3390/s24134188
2. Minhas, N. (2024, July). *Post-quantum authentication scheme for IoT security in smart cities*. Preprints. https://doi.org/10.20944/preprints202407.2309.v1
3. Fathenojavan, S., Moeini, A., & Haj Seyyed Javadi, H. (2025, April). A post-quantum lattice-based lightweight anonymous authentication scheme for IoT. *Journal of Cybersecurity, 11*, tyaf004. https://doi.org/10.1093/cybsec/tyaf004
4. Liu, C.-H., & Wu, Z.-Y. (2024). Advanced authentication of IoT sensor network for industrial safety. *Internet of Things, 27*, 101297. https://doi.org/10.1016/j.iot.2024.101297
5. Ramírez-Gordillo, T., Maciá-Lillo, A., Pujol, F. A., García-D'Urso, N., Azorín-López, J., & Mora, H. (2025). Decentralized identity management for Internet of Things (IoT) devices using IOTA blockchain technology. *Future Internet, 17*(1), 49. https://doi.org/10.3390/fi17010049
6. Yuan, B., Wu, F., & Zheng, Z. (2023, February). Post quantum blockchain architecture for internet of things over NTRU lattice. *PLOS ONE, 18*, e0279429. https://doi.org/10.1371/journal.pone.0279429
7. 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
8. Iavich, M., Kapalova, N., & Sakan, K. (2025). Efficient lattice-based digital signatures for embedded IoT systems. *Symmetry, 17*(9), 1522. https://doi.org/10.3390/sym17091522
9. Chen, C.-L., Zeng, K.-W., Li, W.-Y., Lee, C.-F., Liu, L.-C., & Deng, Y.-Y. (2025). Lightweight post-quantum cryptography: Applications and countermeasures in Internet of Things, blockchain, and e-learning. *Engineering Proceedings, 103*(1), 14. https://doi.org/10.3390/engproc2025103014
10. Haider, L., & Abdullah, A. (2025, April). Fortifying future IoT security: A comprehensive review on lightweight post-quantum cryptography. *Engineering, Technology & Applied Science Research, 15*, 21812–21821. https://doi.org/10.48084/etasr.10141
11. Kamarudin, N. H., Suhaimi, N. H. S., Nor Rashid, F. A., Khalid, M. N. A., & Mohd Ali, F. (2024). Exploring authentication paradigms in the Internet of Things: A comprehensive scoping review. *Symmetry, 16*(2), 171. https://doi.org/10.3390/sym16020171
12. Alotaibi, A., Aldawghan, H., & Aljughaiman, A. (2025). A review of the authentication techniques for Internet of Things devices in smart cities: Opportunities, challenges, and future directions. *Sensors, 25*(6), 1649. https://doi.org/10.3390/s25061649
13. Kumari, S., Singh, M., Singh, R., & Tewari, H. (2022). A post-quantum lattice-based lightweight authentication and code-based hybrid encryption scheme for IoT devices. *Computer Networks, 217*, 109327. https://doi.org/10.1016/j.comnet.2022.109327
14. Asif, R. (2021). Post-quantum cryptosystems for Internet-of-Things: A survey on lattice-based algorithms. *IoT*, *2*(1), 71–91. https://doi.org/10.3390/iot2010005
15. Jagdish, B. V., I. A., Vikas, M. N., A. M., & Naik, C. (2025). Decentralised IoT authentication using blockchain and machine learning: The trust circle framework. In *2025 International Conference on Inventive Computation Technologies (ICICT)* (pp. 1765–1770). IEEE. https://doi.org/10.1109/ICICT64420.2025.11005150

16. Sedghighadikolaei, K., Yavuz, A. A., & Nouma, S. E. (2025). Signer-optimal multiple-time post-quantum hash-based signature for heterogeneous IoT systems. *Internet of Things*, *33*, 101694. https://doi.org/10.1016/j.iot.2025.101694
17. Jeevitha, P., Khadir, N., Jayasurya, S., Kaviyarasan, K., Sivabalan, S., & Arunkumar, S. (2025, July). Hybrid blockchain-based identity authentication scheme for IoT-WSN. In *Proceedings of the 2025 International Conference on Distributed Networks and Security (ICDSNS)* (pp. 1–7). IEEE. https://doi.org/10.1109/ICDSNS65743.2025.11168510
18. Aramide, O. (2022, November). Post-quantum cryptography (PQC) for identity management. *Adhyayan: A Journal of Management Sciences*, *12*, 59–67. https://doi.org/10.21567/adhyayan.v12i2.11
19. Zhang, Y., Tang, Y., Li, C., Zhang, H., & Ahmad, H. (2024). Post-quantum secure identity-based signature scheme with lattice assumption for Internet of Things networks. *Sensors*, *24*(13), 4188. https://doi.org/10.3390/s24134188
20. Aramide, O. (2022, November). Post-quantum cryptography (PQC) for identity management. *Adhyayan: A Journal of Management Sciences, 12*, 59–67. https://doi.org/10.21567/adhyayan.v12i2.11