International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

Secure And Privacy Preserving IoT Cybersecurity With A Blockchain Based Zero Trust Model

Younus Ahmed Jaleeli[1], Dr. Md Zainlabuddin[2]
[1]PG Scholar, Department Of Computer Science & Engineering ISL Engineering College, Hyderabad, India.
[2]Associate Professor; Department Of Computer Science & Engineering ISL Engineering College, Hyderabad, India
Corresponding Author Email: younus.jaleeli2000@gmail.com

Abstract
This research proposes a Unified Quantum-Resilient Blockchain–Zero-Knowledge Proof Privacy Authentication Framework (QBC-ZKPAF) designed to strengthen security, privacy, and authentication in Internet of Things (IoT) environments. The proposed framework combines blockchain technology, Zero Trust Architecture (ZTA), post-quantum cryptography, and Zero-Knowledge Proofs (ZKPs) to provide secure communication, privacy-preserving authentication, and effective access control. A hybrid Reinforcement-Lattice Blockchain Key Generation mechanism is employed to generate quantum-resistant cryptographic keys, while a Deep Q-Network Multi-Factor Secure Key (DQN-MFSK) mechanism dynamically selects secure keys based on authentication requirements and network conditions. Zero-Knowledge Proof-based signatures further protect sensitive information by enabling authentication without revealing confidential data.
The immutable blockchain ledger records device interactions, access requests, and data transactions in a tamper-resistant manner, thereby improving transparency, traceability, auditability, and post-event forensic analysis. In the event of suspicious activity or security breaches, the framework supports accurate source identification through a tracing key maintained by the audit server within the Zero Trust Architecture. By decentralizing identity management and incorporating multi-factor authentication, QBC-ZKPAF provides enhanced protection against conventional cyber threats as well as emerging quantum-based attacks. Experimental evaluation demonstrates promising performance, achieving 98% privacy preservation, 700 transactions per second (TPS), a quantum resilience score of 0.98, and 96% access control effectiveness. These results indicate that the proposed framework is a reliable and efficient solution for securing modern IoT and blockchain-based applications.

Keywords: *Internet of Things (IoT), Blockchain, Zero-Knowledge Proofs, Zero Trust Architecture, Post-Quantum Cryptography, Quantum-Resilient Security, Privacy-Preserving Authentication, Multi-Factor Authentication, Deep Q-Network, Access Control.*

1. Introduction

The Internet of Things (IoT) has become an important component of modern digital infrastructure, connecting sensors, smart devices, industrial equipment, healthcare systems, vehicles, and other resource-constrained endpoints to communication networks and cloud services. The rapid expansion of these interconnected environments has created substantial security challenges because IoT devices frequently operate with limited computational resources, heterogeneous communication protocols, and diverse security capabilities. A compromise of one device can potentially provide an attacker with an entry point into other connected components, making identity verification, access control, privacy protection, and continuous security monitoring essential requirements for dependable IoT environments [15].

Received: *14-06-2026*
Revised: *21-07-2026*
Accepted: *11-08-2026*
Published: *20-08-2026*
Citation: *" Secure And Privacy Preserving IoT Cybersecurity With A Blockchain Based Zero Trust Model", ijaicn, vol. 2, no. 3, pp. 86–98, August. 2026,*

Conventional perimeter-based security models are increasingly inadequate for highly distributed IoT infrastructures. Devices, users, applications, and services may communicate across organizational and geographical boundaries, while resources can be accessed through cloud, edge, wireless, and peer-to-peer environments. Zero Trust Architecture (ZTA) addresses this limitation by removing the assumption that a device or user should automatically be trusted because of its network location. Instead, access decisions are continuously evaluated according to identity, authorization, device status, context, and security policies [1].

Blockchain technology provides another promising mechanism for strengthening trust in distributed IoT environments. Its decentralized ledger can maintain records of authentication events, transactions, device activities, and access decisions without depending exclusively on a centralized authority. The tamper-resistant nature of blockchain records can improve accountability and make unauthorized modifications more difficult. Research on blockchain adoption in IoT has consequently identified decentralized ledgers as a potential mechanism for addressing identity, trust, security, and data-management challenges [9].

Authentication represents a particularly important component of IoT security because large-scale deployments may contain thousands or millions of heterogeneous devices. A compromised identity can allow an attacker to impersonate a legitimate device and obtain unauthorized access to protected resources. Blockchain-based authentication mechanisms can provide decentralized identity management while maintaining verifiable records of authentication activities [3]. However, authentication mechanisms must also minimize the disclosure of sensitive device and user information, particularly in applications where identity or transaction metadata itself may reveal confidential information.

Privacy preservation is therefore closely associated with secure authentication. Conventional authentication protocols may require the disclosure of credentials or identity-related information to an authenticating authority. Zero-Knowledge Proofs (ZKPs) provide an alternative cryptographic principle in which one party can demonstrate possession of valid information without directly revealing the information itself. Privacy-preserving verification mechanisms can consequently reduce unnecessary exposure of sensitive credentials while still allowing an access-control system to determine whether a request satisfies the required conditions [23].

The combination of Zero Trust principles and blockchain can further strengthen access control by providing continuous verification together with decentralized and auditable security records. Existing research has explored blockchain-inspired attribute-based access-control mechanisms for Zero Trust IoT systems, demonstrating the potential of combining distributed ledgers with policy-driven authorization [22]. Such an approach is particularly relevant to IoT environments in which access privileges may depend on device identity, user role, operational context, and current security conditions.

Another challenge arises from the evolving nature of cyber threats. IoT devices are exposed to malware, unauthorized access, credential theft, spoofing, denial-of-service attacks, and other forms of malicious activity. In smart-city environments, the large number of connected devices and their interaction with critical services further increase the potential consequences of a security compromise [11]. Similarly, smart healthcare environments require proactive security mechanisms because compromised devices can affect both sensitive information and critical healthcare operations [15].

Network segmentation can provide an additional layer of protection by restricting the movement of compromised devices or unauthorized users. Micro-segmentation approaches based on technologies such as VLAN and VxLAN can divide network resources into controlled security zones and limit unnecessary communication between components [5]. When integrated with Zero Trust policies, such segmentation can help ensure that successful compromise of one endpoint does not automatically result in unrestricted access to the wider IoT infrastructure.

Identity and trust management also require careful consideration in decentralized environments. Luecking et al. investigated decentralized identity and trust management for IoT environments, demonstrating the relevance of distributed approaches to establishing relationships between devices and services [20]. Similarly, research on Zero Trust architectures for peer-to-peer communication has examined the use of blockchain and hardware-oriented security mechanisms to strengthen trust among distributed participants [16]. These studies indicate that decentralized identity management can complement Zero Trust principles in environments where conventional centralized trust models may become bottlenecks or single points of failure.

Based on these considerations, this research proposes a **Unified Quantum-Resilient Blockchain–Zero-Knowledge Proof Privacy Authentication Framework (QBC-ZKPAF)** for secure IoT environments. The proposed framework integrates Blockchain, Zero Trust Architecture, Zero-Knowledge Proofs, post-quantum cryptographic principles, and adaptive key-management mechanisms within a unified security

architecture. The framework is designed to provide privacy-preserving authentication while maintaining auditable records of device interactions and access activities.

A hybrid Reinforcement-Lattice Blockchain Key Generation mechanism is incorporated to support quantum-resilient key generation, while the proposed Deep Q-Network Multi-Factor Secure Key mechanism dynamically selects security keys according to authentication requirements and changing network conditions. ZKP-based authentication is used to minimize direct disclosure of sensitive credentials, while the blockchain ledger provides tamper-resistant records for auditing and forensic investigation. The framework additionally incorporates a tracing mechanism so that suspicious activities can be investigated without compromising the privacy of legitimate participants.

The primary objective of the study is to develop and evaluate an integrated security framework capable of addressing authentication, privacy, access control, trust management, and emerging quantum-related security risks in IoT environments. The experimental evaluation considers privacy preservation, transaction throughput, quantum resilience, and access-control effectiveness. The reported results indicate promising performance, with the proposed framework achieving 98% privacy preservation, 700 transactions per second, a quantum resilience score of 0.98, and 96% access-control effectiveness.

2. Literature Review

2.1 Zero Trust Architecture for IoT Security

The National Institute of Standards and Technology (NIST) established a formal foundation for Zero Trust Architecture through Special Publication 800-207. The Zero Trust model moves away from implicit trust and requires explicit verification before granting access to protected resources. This principle is highly relevant to IoT because devices and users may operate across multiple networks and security domains. Continuous verification, least-privilege access, and policy-driven authorization provide a stronger security foundation for distributed IoT infrastructures than conventional perimeter-based protection [1].

Muhammad, Munir, Munir, and Zafar examined the integration of Zero Trust with layered security mechanisms for resilient digital systems. Their work emphasizes that security should not depend on a single defensive mechanism but should involve multiple complementary controls. This principle supports the proposed framework's combination of identity verification, blockchain records, access control, cryptographic protection, and privacy-preserving authentication as interconnected security layers [24].

Niraula investigated Zero Trust architecture for peer-to-peer communication using blockchain and hardware-oriented security mechanisms. The research demonstrates the relevance of combining decentralized trust management with hardware-supported security in distributed communication environments. Such an approach is particularly applicable to IoT systems, where devices may need to establish secure relationships without relying on a single centralized trust authority [16].

2.2 Blockchain-Based Authentication and Trust Management

Al Hwaitat, Almaiah, Ali, Al-Otaibi, Shishakly, Lutfi, and Alrawad investigated a blockchain-based authentication framework for IoT networks. Their research demonstrates how blockchain can be used to improve authentication by providing decentralized records and reducing dependence on conventional centralized identity mechanisms. The study provides direct support for using blockchain as part of an IoT authentication architecture, although additional privacy-preserving mechanisms are required when authentication itself involves sensitive information [3].

Uddin, Stranieri, Gondal, and Balasubramanian reviewed blockchain adoption in IoT and examined challenges, applications, and possible solutions. Their analysis highlights the potential of blockchain for decentralized trust, authentication, data integrity, and secure interaction among IoT devices. At the same time, the authors identify practical considerations associated with blockchain deployment, including resource limitations and scalability. These considerations motivate the need for a framework that balances security improvements with transaction-processing efficiency [9].

Luecking, Fries, Lamberti, and Stork proposed a decentralized framework for identity and trust management in IoT environments. Their work demonstrates that distributed identity mechanisms can support trust relationships between heterogeneous IoT participants without depending entirely on centralized authorities. The concept is relevant to QBC-ZKPAF because the proposed framework similarly seeks to decentralize identity-related operations while maintaining verifiable records of device activities [20].

2.3 Privacy-Preserving Authentication

Bian, Zhang, and Shao investigated identity-based privacy-preserving remote data-integrity verification using a designated verifier. Their work addresses the challenge of verifying data integrity while controlling who can validate the verification evidence. This privacy-oriented perspective is relevant to IoT environments because authentication

and integrity verification should not unnecessarily expose sensitive information to unauthorized parties. The proposed framework extends this principle toward privacy-preserving device authentication through Zero-Knowledge Proof mechanisms [23].

Yuen, Esgin, Liu, Au, and Ding examined efficient generic constructions for ring-signature schemes. Ring signatures provide a mechanism for signing information while concealing the specific identity of the signer within an authorized group. Although ring signatures and Zero-Knowledge Proofs are distinct cryptographic techniques, both demonstrate the broader research direction toward authentication mechanisms that provide security without unnecessary disclosure of identity information [7].

Awan, Azad, Arshad, Waheed, and Sharif proposed a blockchain-inspired attribute-based access-control approach for Zero Trust IoT systems. Their work demonstrates how authorization can be associated with attributes and policy conditions rather than relying solely on static identity credentials. This approach is relevant to the proposed framework because IoT access decisions may need to consider multiple factors, including device identity, user permissions, network conditions, and security status [22].

2.4 IoT Cybersecurity and Network Protection

Alnahari and Quasim examined privacy challenges and cyberattacks affecting IoT devices in smart-city environments. Their study highlights the broad attack surface created by interconnected smart devices and emphasizes the importance of protecting both device operations and sensitive information. The findings reinforce the requirement for security architectures that address authentication, privacy, communication security, and access management together rather than treating each concern independently [11].

Marshal, Gobinath, and Rao examined proactive cybersecurity strategies for IoT-enabled smart healthcare systems. Their work highlights the need for preventive security mechanisms in healthcare environments, where compromised IoT devices may expose sensitive information or interfere with critical services. The study supports the broader motivation for proactive and continuously evaluated security architectures in IoT deployments [15].

Li, Yang, Yu, Duan, and Yang examined micro-segmentation using VLAN and VxLAN mapping as a mechanism for improving network security. Their research demonstrates how dividing network infrastructure into controlled segments can restrict unauthorized movement between resources. When combined with Zero Trust access policies, micro-segmentation can provide an additional containment mechanism by limiting the communication privileges available to compromised or suspicious IoT devices [5].

Bast and Yeh examined emerging authentication methods that support Zero Trust security in IoT. Their work demonstrates the continuing evolution of authentication mechanisms required for IoT environments and emphasizes the importance of stronger identity verification under Zero Trust principles. The findings provide additional motivation for integrating advanced authentication and privacy mechanisms into IoT security frameworks [13].

2.5 Research Gap and Motivation

The reviewed literature demonstrates that blockchain, Zero Trust, privacy-preserving authentication, and decentralized identity management have each received considerable research attention. However, these technologies are frequently examined as separate security mechanisms or as combinations addressing only selected aspects of IoT protection. Blockchain can provide integrity and auditability, while Zero Trust can strengthen access decisions; however, privacy-preserving authentication and protection against future cryptographic threats require additional mechanisms [3], [9], [22].

The proposed QBC-ZKPAF framework attempts to address this gap by bringing these security dimensions together within a unified architecture. Blockchain provides a tamper-resistant trust and audit layer, Zero Trust establishes continuous verification and least-privilege access, and Zero-Knowledge Proofs reduce the need to disclose sensitive authentication information. The framework additionally introduces quantum-resilient key-generation and adaptive key-selection mechanisms to address the possibility of future cryptographic threats.

The literature also indicates that practical IoT security solutions must consider both protection and performance. A security architecture that provides strong cryptographic protection but introduces excessive communication overhead may be difficult to deploy in large-scale IoT environments. Consequently, the present research evaluates the proposed framework using privacy preservation, transaction throughput, quantum resilience, and access-control effectiveness. This combination of security and performance measures provides a basis for determining whether the proposed architecture can provide practical protection for modern blockchain-enabled IoT environments.

3. Methodology

Figure 2 illustrates the overall methodology of the proposed security framework. The methodology integrates IoT security mechanisms, Zero Trust principles, blockchain-based trust management,

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

privacy-preserving techniques, secure communication, and continuous threat detection into a unified architecture. Each IoT device is initially registered with a unique identity and cryptographic credentials. The identity information is protected, and relevant verification records are maintained in a tamper-evident manner using blockchain technology.

Before a device, user, or application can access a resource, the framework performs authentication and security verification. The Zero Trust policy engine evaluates every request independently and does not automatically trust an entity based on its network location. Access decisions are determined according to identity, device status, requested resource, contextual information, and security risk. Least-privilege principles are applied to ensure that entities receive only the permissions required for their authorized operations. The framework continuously monitors device behavior, network traffic, access requests, and security events. Anomaly detection mechanisms identify unusual activities and dynamically update the risk associated with users or devices. When suspicious behavior is detected, the system can initiate additional authentication, restrict permissions, or revoke access automatically. The proposed framework is evaluated using security, privacy, latency, computational overhead, network overhead, detection performance, and scalability metrics.

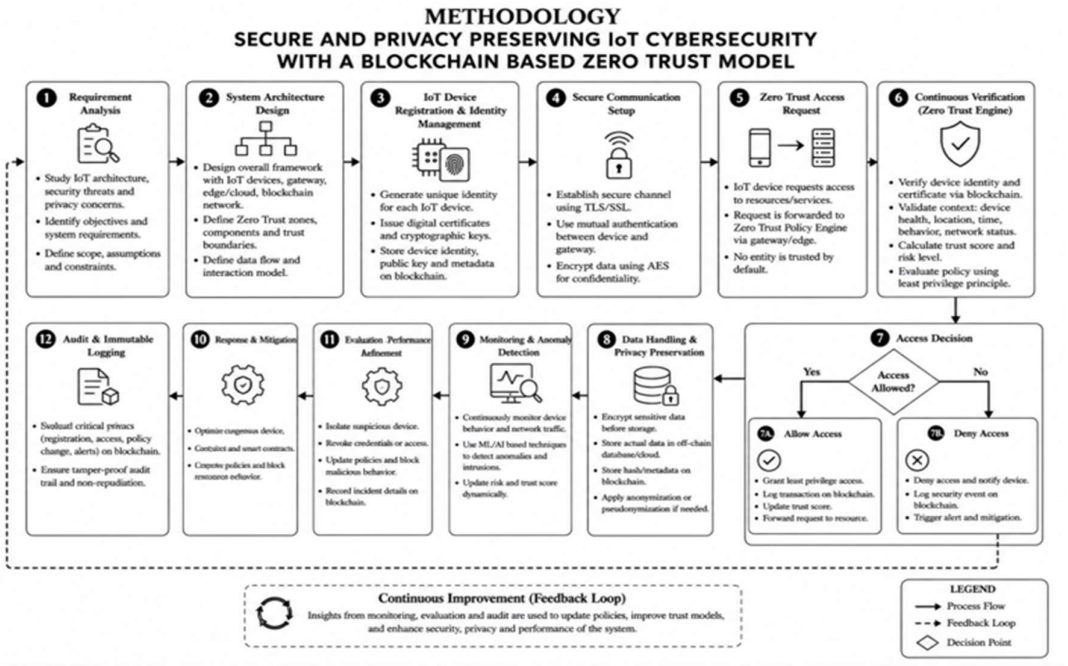

Fig. 1: QBC-ZKPAF Framework

Figure 3 presents the proposed **Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF)**. The framework is designed to provide a comprehensive and future-oriented security architecture for IoT environments by combining Zero Trust Architecture, blockchain, post-quantum cryptography, adaptive key management, and privacy-preserving authentication.

The QBC-ZKPAF framework employs a Reinforcement-Lattice Blockchain Key Generation mechanism to generate cryptographic keys designed to improve resistance against emerging quantum computing threats. In addition, a Deep Q-Network Multi-Factor Secure Key (DQN-MFSK) mechanism supports adaptive and intelligent management of authentication and security keys. This enables the framework to respond dynamically to changing security conditions. The Zero Trust component continuously evaluates access requests and security context throughout system operation. No device or user receives permanent trust, and access permissions can be modified according to changing risk conditions. When normal behavior is observed, access may be permitted according to predefined privileges. Suspicious activity can trigger additional verification, while high-risk behavior can result in immediate access restriction or revocation.

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (Qbc-Zkpaf)

The proposed Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF) combines post-quantum cryptography, blockchain-based auditing, Zero-Knowledge Proofs, adaptive key management, and Zero Trust access control. The framework involves four principal entities: the Client, Policy Administrator, Server Administrator, and Audit Server. Together, these components establish a decentralized and privacy-aware mechanism for secure registration, authentication, file protection, authorization, and forensic auditing. The framework uses cryptographic primitives including secure hashing, authenticated symmetric encryption, key-derivation functions, post-quantum Key Encapsulation Mechanisms, digital signatures, and Zero-Knowledge Proofs. Sensitive files are encrypted using AES-based authenticated encryption, while post-quantum mechanisms protect key establishment. Blockchain-style ledger records maintain the history of important operations and provide tamper-evident auditability.

Algorithm 1: Privacy-Preserving User Registration

The registration process creates a protected representation of the user's identity instead of exposing unnecessary personal information during authentication. The client generates a secret value and cryptographic key material and computes a commitment associated with the registered attributes. The server verifies the registration information, stores the required public credentials and commitment, and records a cryptographically protected registration event in the ledger. This process establishes a verifiable identity foundation while reducing direct exposure of sensitive user information.

Input: User identity attributes and registration credentials.

Output: Privacy-preserving commitment, public credentials, and ledger record.

Algorithm 2: Hybrid Quantum-Resilient Key Generation

During file upload, the framework calculates a cryptographic hash of the original file and generates a unique symmetric encryption key. The file is then protected using authenticated encryption. A post-quantum key-generation mechanism creates cryptographic material for secure key encapsulation, while a key-derivation function derives the required key-encryption material. The symmetric file key is securely wrapped, and sensitive private key material remains protected at rest. File metadata, encrypted key information, and integrity references are subsequently recorded for secure storage and auditing.

Input: Uploaded file and authenticated uploader information.

Output: Encrypted file, integrity hash, protected key material, and ledger entry.

Algorithm 3: Dqn-Mfsk Dynamic Key Selection

The Deep Q-Network Multi-Factor Secure Key (DQN-MFSK) mechanism dynamically selects an appropriate security configuration according to the operational environment. The decision process considers factors such as device trust level, network latency, estimated threat level, available processing capability, and energy resources. Based on these conditions, the trained model can select an appropriate post-quantum mechanism, lightweight protection mode, or immediate key rotation. The objective is to maintain a balance between security strength, response time, and resource consumption.

Algorithm 4: Zero-Knowledge Privacy-Preserving Ticket Issuance

The authentication mechanism enables a client to demonstrate authorization without unnecessarily disclosing identity information. A valid credential is transformed into a privacy-preserving authentication representation, and a Zero-Knowledge Proof demonstrates that the required security conditions are satisfied. The Policy Administrator verifies the proof and, when authorization requirements are fulfilled, issues a designated access ticket. Only minimal security references are recorded in the audit ledger, thereby supporting data minimization and privacy protection.

Requirements Engineering

The requirements engineering process defines the functional, security, privacy, performance, and deployment expectations of the proposed QBC-ZKPAF system. The framework is designed to support secure interaction among clients, policy administrators, server administrators, and audit authorities. Its primary objective is to provide

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

decentralized, privacy-aware, and traceable authentication and access control for IoT and distributed computing environments.

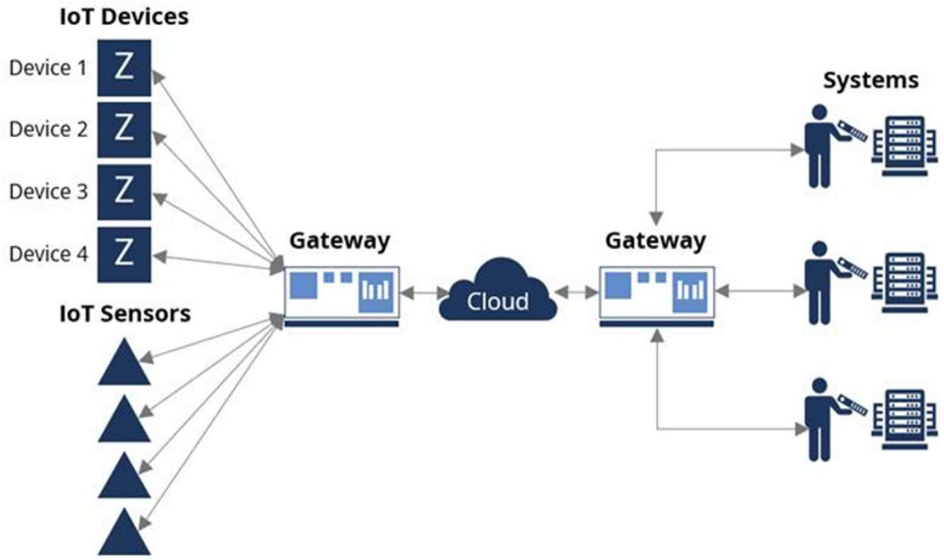

Fig. 2: IoT in a Zero Trust World

Figure 4 illustrates the security concept of IoT operation within a Zero Trust environment. Unlike conventional architectures, devices and users are not permanently trusted after initial authentication. Every important access request is evaluated continuously according to identity, authorization, context, security condition, and risk.

Hardware Requirements

The proposed framework can be developed and tested using a standard computing environment with an Intel Core i3 processor or higher, at least 4 GB of DDR4 RAM, approximately 100 GB of storage, and a standard display and input devices. Additional hardware resources may be required when deploying large-scale blockchain nodes, machine-learning services, or extensive IoT infrastructures.

Software Requirements

The prototype can be implemented using Java EE technologies, including JSP and Servlets, with MySQL for database management. The application may operate on Windows 10 or Windows 11 and can be deployed through Apache Tomcat. Eclipse IDE or IntelliJ IDEA may be used for development, while modern browsers such as Chrome or Firefox can provide user access to the application. Conventional IoT security systems often depend on centralized authentication servers, perimeter-based protection, firewalls, and static access-control mechanisms. Such architectures may create single points of failure and can allow compromised devices to retain access after successful authentication. Security logs stored centrally may also be vulnerable to manipulation. These limitations become increasingly significant as IoT environments grow in size and complexity.

4. Design Engineering

The QBC-ZKPAF system is designed as a modular and layered cybersecurity architecture for secure and privacy-preserving resource access. The design separates user interaction, application processing, and data management to improve maintainability, security, and scalability. The presentation layer provides interfaces for clients, providers, administrators, and auditors. The business layer manages registration, authentication, Zero-Knowledge Proof processing, access policies, encryption, quantum-resilient key management, blockchain logging, and security analytics. The data layer maintains encrypted resources, metadata, cryptographic references, ledger records, and audit information.

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

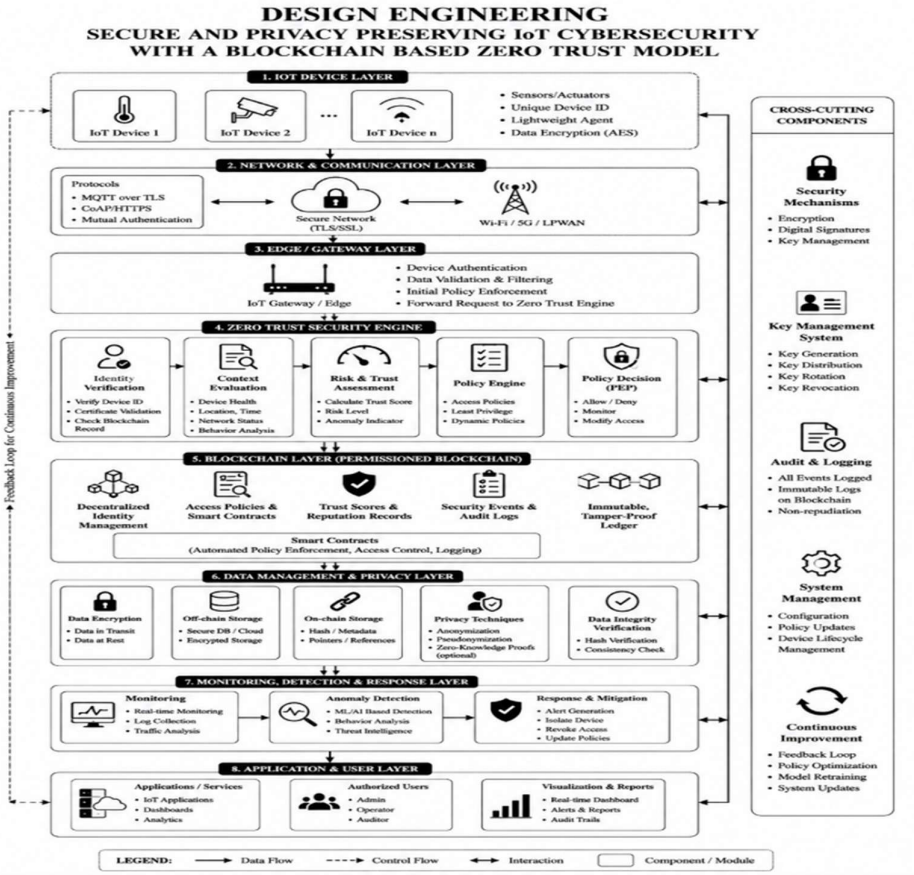

Fig. 3: Design Engineering

Figure 5 presents the overall design engineering architecture of the proposed QBC-ZKPAF system. The architecture illustrates the interaction among users, authentication services, policy components, quantum-resilient key mechanisms, blockchain-based records, secure storage, and auditing services. The design protects sensitive resources through authenticated encryption and protected cryptographic key management. Post-quantum techniques strengthen key establishment, while blockchain-based records provide tamper-evident evidence of important system activities. Zero-Knowledge Proof mechanisms reduce unnecessary disclosure of confidential information during authentication and authorization.

The access-control process follows Zero Trust principles by continuously evaluating security conditions rather than granting permanent trust after an initial login. Authorized actions are recorded for accountability, while suspicious behavior can trigger additional verification or access restriction. The audit component validates important security events and supports controlled investigation when necessary.

The modular nature of the design enables future enhancement without requiring complete redevelopment of the system. Additional post-quantum algorithms, distributed ledger platforms, anomaly-detection models, identity technologies, and analytics components can be incorporated as the security environment evolves. Overall, the proposed design provides an integrated foundation for confidentiality, integrity, authentication, privacy, accountability, and future resilience in IoT and distributed environments.

System Architecture

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

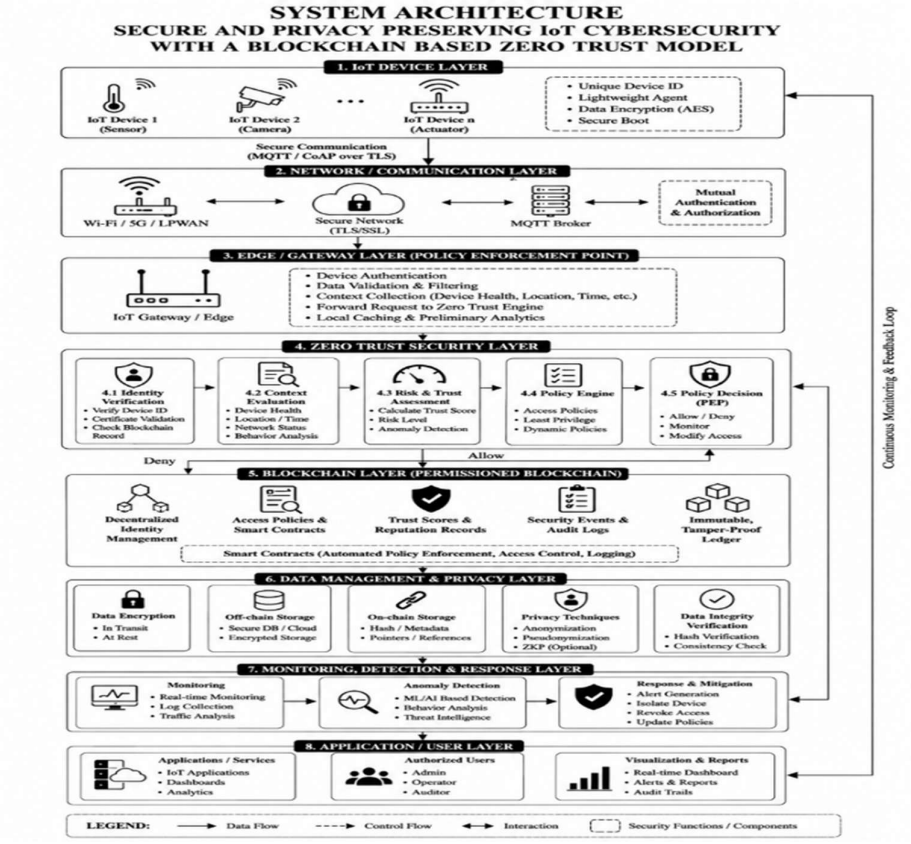

Fig. 4 : System Architecture

The proposed QBC-ZKPAF architecture integrates Zero Trust Architecture (ZTA), blockchain, zero-knowledge proofs, and quantum-resilient cryptography to provide secure and privacy-aware authentication for IoT environments. As illustrated in Fig. 6, the framework is organized around the control plane, data plane, and identity management infrastructure. The control plane contains the Policy Administrator and Policy Engine, which continuously evaluate authentication requests and enforce access policies. The data plane manages authorized interactions between clients and protected resources. The identity management layer supports device and user registration, certification, key generation, authentication, and auditing. Privacy is preserved through cryptographic commitments and zero-knowledge proofs, allowing users to demonstrate authorization without unnecessarily revealing sensitive identity information.

Architectural Framework

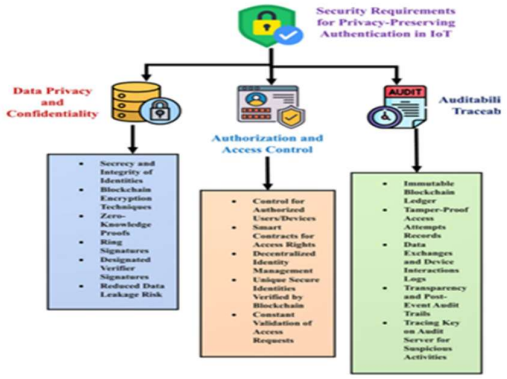

Fig. 5: Architecture

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

The overall architecture establishes a secure interaction among clients, policy services, resource servers, and audit components. Each access request is verified according to Zero Trust principles rather than relying on network location or previous authentication alone. Blockchain-based records provide tamper-evident logging, while quantum-resistant key mechanisms strengthen protection against future cryptographic threats. The architecture therefore combines continuous verification, decentralized auditing, secure key management, and privacy-preserving authentication into a unified security framework.

5. Snapshots

The proposed system is implemented as a web-based application using Java technologies for application processing and server-side communication. Web interfaces are designed using JSP and related web technologies, while CSS is used to provide a clear and responsive presentation layer. The snapshots demonstrate the major functional modules of the proposed framework.

Various Snapshots

The graphical interfaces presented in this chapter illustrate the practical implementation of the framework:

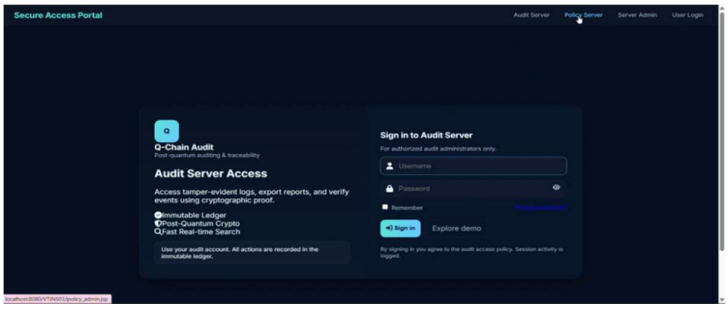

Fig. 6: Audit Server Home Page

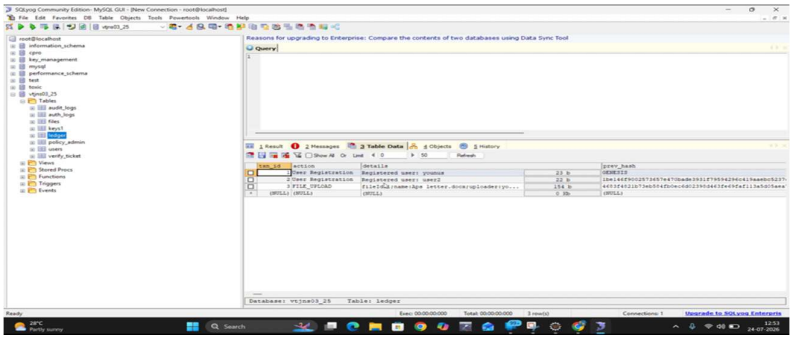

Fig. 7: Blockchain Ledger

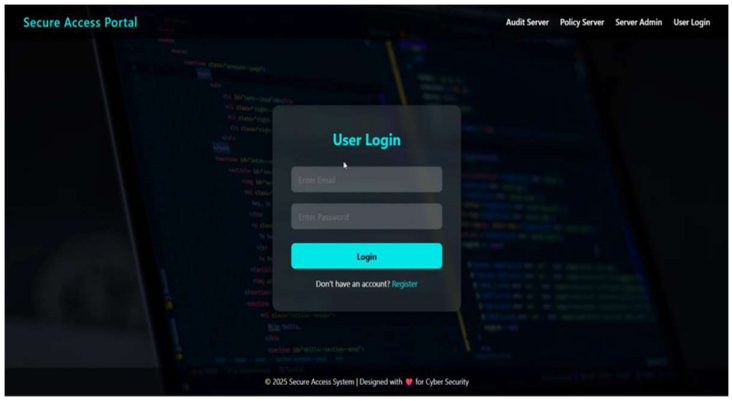

Fig. 8: User Login

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 03, July-September 2026, pp: 86-98
ISSN: 3071-3358

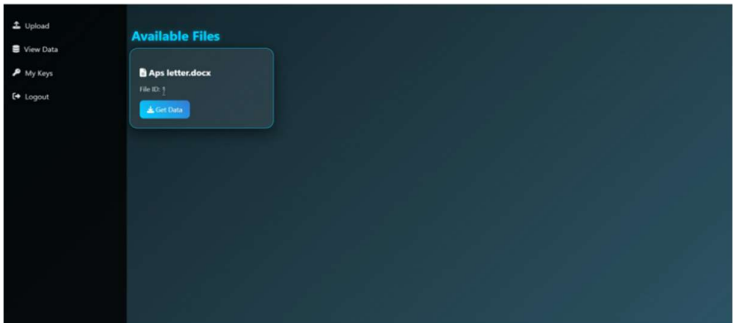

Fig. 9: Data Viewing Interface

These interfaces demonstrate the operational workflow of registration, authentication, key generation, encrypted storage, policy verification, ledger maintenance, auditing, and secure data access.

Software Testing

Software testing is performed to verify that the developed QBC-ZKPAF application operates according to its specified functional and security requirements. Testing focuses on identifying implementation defects and validating the behavior of individual modules and the integrated system. Particular attention is given to user authentication, file encryption, quantum-resilient key operations, ticket verification, access authorization, ledger integrity, and audit functionality.

Testing Methodology

A systematic testing methodology is adopted to evaluate the application under different functional conditions and user interactions. The process begins with a test plan based on the defined system requirements, followed by the verification of individual modules and integrated workflows. Input validation, authentication outcomes, file operations, access decisions, database transactions, and ledger consistency are examined to identify errors or unexpected behavior. The testing process helps ensure that the proposed framework provides reliable, secure, and consistent operation before deployment.

6. Conclusion

The rapid growth of IoT applications has created an urgent requirement for security mechanisms capable of protecting distributed devices, sensitive information, and digital services from increasingly sophisticated threats. Conventional perimeter-oriented approaches are no longer sufficient because IoT environments are highly dynamic, heterogeneous, and vulnerable to unauthorized access, device compromise, and data manipulation. This work presents the Quantum-Resilient Blockchain–Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF), which combines Zero Trust principles, blockchain-based auditing, privacy-preserving authentication, and post-quantum cryptographic techniques. The framework continuously verifies access requests, applies least-privilege authorization, protects sensitive files through encryption, and maintains tamper-evident records of important system activities.

As illustrated in **Fig. 12**, the proposed framework establishes secure interaction among users, administrators, policy services, resource servers, and audit components. Zero-Knowledge Proof mechanisms enable authentication and authorization without unnecessary disclosure of user information, while blockchain-based ledger mechanisms improve traceability, integrity, and accountability.

-sensitive applications such as Industrial IoT, smart healthcare, smart cities, intelligent transportation, cloud services, and critical infrastructure. Nevertheless, issues including computational overhead, blockchain scalability, latency, interoperability, and energy consumption require further investigation. Future work can focus on lightweight consensus mechanisms, edge-assisted processing, AI-based threat detection and trust evaluation, optimized Zero-Knowledge Proof protocols, and standardized post-quantum cryptographic implementations.

References

1. NIST, *Zero Trust Architecture*, Special Publication 800-207, National Institute of Standards and Technology, 2020.

2. Sannidhanam, A. H. (2025). Autonomous AI Agents for Cloud Infrastructure Operations. *Journal of Contemporary Science and Technology Management, 1*(01), 83–100.
3. A. K. Al Hwaitat, M. A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, "Blockchain-based authentication framework for improving security in Internet of Things networks," *Electronics*, vol. 12, no. 17, p. 3618, 2023.
4. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali, "*Smartphone Security and Protection Practices*," *International Journal of Engineering and Applied Computer Science (IJEACS)*; ISBN: 9798799755577, Volume: 03, Issue: 01, December 2021 (International Journal, U.K.), Pages 1–6.
5. D. Li, Z. Yang, S. Yu, M. Duan, and S. Yang, "Micro-segmentation using VLAN and VxLAN mapping for enhanced network security," *Future Internet*, vol. 16, no. 9, p. 320, 2024.
6. Sannidhanam, A. H. (2021). Real-Time Claims Processing Using Event-Driven Architectures. *International Journal of Technology, Management and Humanities, 7*(01), 36–50. doi:10.21590/07.01.02
7. T. H. Yuen, M. F. Esgin, J. K. Liu, M. H. Au, and Z. Ding, "DualRing: Efficient generic constructions for ring signature schemes," in *Proc. Annual International Cryptology Conference*, Springer, 2021, pp. 251–281.
8. Anjani Haritha Sannidhanam. (2024). Guardrails and Safety Mechanisms for LLM-Powered Enterprise Applications. *International Journal of Engineering Science & Humanities, 14*(3), 273–285.
9. M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "Blockchain adoption in IoT: A survey of challenges, applications, and possible solutions," *Blockchain: Research and Applications*, vol. 2, no. 2, Art. no. 100006, 2021.
10. Ijteba Sultana, Dr. Mohd Abdul Bari, Dr. Sanjay, "*Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes*," *International Journal of Intelligent Systems and Applications in Engineering*, ISSN No.: 2147-6799, IJISAE, vol. 12, issue 3, 2024, Nov. 2023.
11. W. Alnahari and M. T. Quasim, "Privacy challenges and cyberattacks affecting IoT devices in smart city environments," in *Proc. International Congress on Advanced Technology and Engineering*, 2021, pp. 1–5.
12. Anjani Haritha Sannidhanam. (2023). Zero-Downtime AI Model Updates in Real-Time Inference Systems. *International Journal of Engineering Science & Humanities, 13*(2), 70–78.
13. C. Bast and K.-H. Yeh, "Emerging authentication methods supporting Zero Trust security in the Internet of Things," *Symmetry*, vol. 16, no. 8, p. 993, 2024.
14. Sannidhanam, A. H. (2020). Comparative Analysis of Cloud Computing Architectures for Enterprise Applications. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12*(02), 169–180. doi:10.18090//samriddhi.v12i02.16
15. R. Marshal, K. Gobinath, and V. V. Rao, "Proactive cybersecurity strategies for mitigating security threats in IoT-enabled smart healthcare systems," in *Proc. IEEE Int. IoT, Electronics and Mechatronics Conf. (IEMTRONICS)*, 2021, pp. 1–4.
16. A. Niraula, *Zero Trust Architecture for Peer-to-Peer Communication Using Blockchain and Hardware-Oriented Security*, University of Toledo, Ohio, USA, 2021.
17. Distributed Data Processing Frameworks for Large-Scale Healthcare Analytics. (2019). *International Journal of Advance Industrial Engineering, 7*(04), 1–10. doi:10.14741/ijaie/v.7.4.01
18. Z. Ruan, "Blockchain approaches for addressing security challenges in Internet of Things systems," in *Proc. International Conference on Computer Simulation, Modeling and Information Security*, 2023, pp. 572–580.
19. Anjani Haritha Sannidhanam. (2024). Prompt Engineering Patterns for Reliable LLM Outputs in Production Environments. *Journal of Multidisciplinary Knowledge, 4*(1), 29–39.
20. M. Luecking, C. Fries, R. Lamberti, and W. Stork, "A decentralized framework for identity and trust management in IoT environments," in *Proc. IEEE International Conference on Blockchain and Cryptocurrency*, 2020, pp. 1–9.
21. **Mohammed Abdul Bari**, Arul Raj Natraj Rajgopal, Dr. P. Swetha, "*Analysing AWS DevOps CI/CD Serverless Pipeline Lambda Function's Throughput in Relation to Other Solution*," *International Journal of Intelligent Systems and Applications in*

Engineering, IJISAE, ISSN: 2147-6799, Nov. 2023, 12(4s), 519–526.
22. S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, "A blockchain-inspired attribute-based access control approach for Zero Trust IoT systems," *Information*, vol. 14, no. 2, p. 129, 2023.
23. G. Bian, R. Zhang, and B. Shao, "Identity-based privacy-preserving remote data integrity verification with a designated verifier," *IEEE Access*, vol. 10, pp. 40556–40570, 2022.
24. T. Muhammad, M. T. Munir, M. Z. Munir, and M. W. Zafar, "Integrating Zero Trust and layered security mechanisms for resilient digital systems," *International Journal of Computer Science and Technology*, vol. 6, no. 4, pp. 99–135, 2022.
25. R. Saxena, D. Arora, V. Nagar, and S. Mahapatra, "Bitcoin and the development of decentralized digital currency systems," in *Intelligent Systems Reference Library*, Springer, 2021, pp. 13–28.
26. Sannidhanam, A. H., & Alladi, S. (2017). Cloud-Based Healthcare CRM Systems for Improved Patient Engagement. *International Journal of Technology, Management and Humanities, 3*(01), 32–44. doi:10.21590/ijtmh.3.03.4

About Author:

Younus Ahmed Jaleeli is currently pursuing a Master of Technology in Computer Science and Engineering at ISL Engineering College, affiliated to Osmania University, Hyderabad, India. He completed his Bachelor of Engineering in Information Technology from ISL Engineering College, affiliated to Osmania University, from 2020 to 2024.