IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

A Blockchain Based Zero Trust Model for Privacy Centric IoT Cybersecurity

B.Ratnamala
Assistant Professor, Department of CSE
Guru Nanak Institute of Technology, Hyderabad, Telangana, India
https://orcid.org/0009-0004-5360-7540
K.Sri Bharath Eshwar, K.Raja Lokesh Reddy, Munjala Tharun Kumar
Students, Department of CSE
Guru Nanak Institute of Technology, Hyderabad,Telangana, India

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.12/Issue04/ISAP26.ISAP10083
Research Article | Open Access | Double-Blind Peer-Reviewed| ArticleID: IJIRAE/RS/Vol.12/Issue04/ISAP26.ISAP10083
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijiris.com/volumes/Vol12/iss-04/04.ISAP26.ISAP10083.pdf
Article Citation:Ratnamala,Sri,Raja,Munjala(2026),A Blockchain Based Zero Trust Model for Privacy Centric IoT Cybersecurity.IJIRIS: International Journal of Innovative Research in Information Security, Volume 12, Issue 04 of 2026 pages 280-286 **Doi:>** https://doi.org/10.26562/ijiris.2026.v1204.04 **BibTeX Key: Ratnamala@2026Blockchain**
IJIRIS papers should be cited as IJIRIS(International Journal of Innovative Research in Information Security, AM Publications, India 2026, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2026.v1204.04 The journal's official abbreviation is IJIRIS. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: This research proposes a Unified Quantum-Resilient Blockchain and Zero-Knowledge Proof-based Privacy Authentication Framework (QBC-ZKPAF) to enhance security in Internet of Things (IoT) environments. The framework integrates blockchain technology, Zero Trust Architecture (ZTA), and post-quantum cryptography to enable secure and privacy-preserving authentication and access control. It utilizes hybrid reinforcement-lattice blockchain key generation for quantum-resilient key creation and a Deep Q-Network-based Multi-Factor Secure Key (DQN-MFSK) mechanism for dynamic key selection. Zero-Knowledge Proofs (ZKP) is employed to ensure authentication without revealing sensitive information. The proposed system provides decentralized identity management, tamper-proof transaction logging, and secure communication. Blockchain ensures transparency, auditability, and traceability, while Zero Trust Architecture enforces continuous verification. Experimental results demonstrate high performance, achieving 98% privacy preservation, 700 transactions per second throughput, 0.98 quantum resilience, and 96% access control effectiveness. The framework offers a robust and scalable solution for securing modern IoT systems against evolving cyber threats, including quantum attacks.

Keywords: Internet of Things (IoT), Blockchain, Zero Trust Architecture (ZTA), Zero-Knowledge Proofs (ZKP), Post-Quantum Cryptography, Decentralized Identity, Smart Contracts, Secure Authentication.

I. INTRODUCTION

The Internet of Things (IoT) has rapidly transformed modern digital infrastructure by enabling seamless connectivity among devices in domains such as healthcare, smart cities, industrial automation, and transportation systems. Despite its numerous advantages, IoT environments are highly vulnerable to cyber threats due to their decentralized architecture, heterogeneous devices, and limited computational resources. Traditional security mechanisms, which rely on perimeter-based protection, are no longer sufficient to safeguard IoT networks against evolving attacks such as data breaches, denial-of-service (DoS), and malware infiltration. To address these challenges, Zero Trust Architecture (ZTA) has emerged as a promising security model based on the principle of "never trust, always verify." ZTA enforces continuous authentication, strict identity verification, and least-privilege access control. However, its continuous monitoring approach introduces privacy concerns due to frequent data validation and exposure of sensitive information. Blockchain technology further enhances IoT security by providing decentralization, immutability, and tamper-proof data storage through distributed ledger mechanisms. It eliminates single points of failure and ensures transparency in system operations. However, blockchain alone faces limitations such as scalability issues, computational overhead, and privacy exposure due to transparent data structures. To overcome these limitations, this paper proposes a Unified Quantum-Resilient Blockchain and Zero-Knowledge Proof-based Privacy Authentication Framework (QBC-ZKPAF). The framework integrates blockchain, ZTA, and post-quantum cryptography to provide a secure, scalable, and privacy-preserving solution for IoT environments. It incorporates advanced techniques such as reinforcement-lattice-based key generation, Deep Q-Network-based multi-factor authentication, and Zero-Knowledge Proofs to ensure secure authentication without revealing sensitive user information. The proposed architecture aims to strengthen IoT security by ensuring data confidentiality, integrity, auditability, and resistance against both classical and quantum cyber threats.

II. LITERATURE SURVEY

A Micro-segmentation Method Based on VLAN–VxLAN Mapping Technology (D. Li, Z. Yang, S. Yu, M. Duan, and S. Yang, 2025) proposes a network-level micro-segmentation approach for cloud data centers using VLAN and VxLAN mapping.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

the method strengthens zero trust implementation by enforcing strict traffic isolation and continuous auditing. it provides a cost-effective and standardized solution for improving security without modifying existing infrastructure; however, it faces limitations in large-scale iot environments due to scalability constraints. Emerging Authentication Technologies for Zero Trust on the Internet of Things (C. Bast and K.-H. Yeh, 2025) discusses authentication mechanisms for iot-based zero trust systems. the study emphasizes lightweight cryptography, mutual authentication, and blockchain-based key management to ensure secure communication in resource-constrained devices. it also identifies challenges such as efficient key management, latency reduction, and scalability in iot networks.

Securing the Metaverse: A Blockchain-enabled Zero-Trust Architecture for Virtual Environments (I.U. Din, K.H. Khan, A. Almogren, M. Zareei, and J.A.P. Díaz, 2025) presents a blockchain-integrated zero trust framework that improves intrusion detection and system resilience. simulation results show improved threat detection rates and reduced response time compared to traditional systems. The study demonstrates that blockchain enhances transparency, trust, and scalability in decentralized security environments. Blockchain-aware Decentralized Identity Management and Access Control System (A. A. Agarkar, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L. Kulkarni, 2024) introduces a self-sovereign identity management system using blockchain. the framework eliminates single points of failure and enables cross-organizational authentication without centralized authorities. it improves transparency, interoperability, and secure identity verification in distributed systems. Securing Smart Manufacturing by Integrating Anomaly Detection with Zero-Knowledge Proofs (A. Salam, M. Abrar, F. Amin, F. Ullah, I. A. Khan, B. F. Alkhamees, and H. AlSalman, 2025) combines anomaly detection techniques with zero-knowledge proofs (zkp) to enhance privacy-preserving verification. the model achieves high detection accuracy while ensuring confidential validation of sensitive industrial data, significantly improving security in smart manufacturing systems.

III. EXISTING SYSTEM

The existing IoT security systems mainly rely on traditional perimeter-based security approaches such as firewalls, intrusion detection systems, and centralized authentication servers. These methods assume that internal network devices are trustworthy, which is not suitable for the dynamic and distributed nature of IoT environments. Some advanced solutions use Zero Trust Architecture (ZTA) and blockchain technology separately to improve security. ZTA enables continuous authentication and strict access control, while blockchain provides decentralized identity management and tamper-proof logging. However, ZTA introduces latency due to continuous verification, and blockchain suffers from scalability and computational overhead issues. Additionally, most existing systems lack strong privacy-preserving mechanisms and are not designed to handle emerging threats such as quantum computing attacks. Therefore, they are unable to provide a complete solution for secure, scalable, and privacy-preserving IoT environments.

Existing System Disadvantages

- IoT devices introduce vulnerabilities and increase security workload.
- Advanced cryptographic methods need high computation, unsuitable for low-power devices.
- Continuous authentication in ZTA causes latency issues.
- Lack of standardization affects integration and scalability.
- Centralized systems create single points of failure and reduce security.

Proposed System

The proposed system enables secure access to IoT environments using blockchain-based smart contracts that automatically enforce access control policies. It implements decentralized identity management, allowing users to maintain secure and verifiable identities without relying on a central authority. Blockchain-based access tokens are used to grant authorized access to system resources, improving security and transparency. To enhance privacy, the system integrates Zero-Knowledge Proofs (ZKP), enabling users to prove their identity without revealing sensitive information. This approach reduces vulnerabilities associated with centralized identity systems, improves data confidentiality, and eliminates single points of failure. Overall, the proposed framework ensures secure, scalable, and privacy-preserving authentication in IoT environments.

Proposed System Advantages:

- Strong access control ensures high accuracy in authorizing only legitimate users.
- Quantum-resilient design protects against future quantum computing threats.
- Zero-Knowledge Proofs (ZKP) ensure privacy-preserving authentication without data exposure.
- Decentralized identity management reduces single points of failure and improves trust.
- Smart contracts enforce secure and transparent access control policies.
- Dynamic key management improves flexibility and strengthens cryptographic security.
- Multi-layer security combines blockchain, ZTA, and post-quantum cryptography for robust protection.

IV. SYSTEM ARCHITECTURE

The proposed system follows a hybrid architecture that integrates IoT devices, blockchain technology, Zero Trust Architecture (ZTA), and post-quantum cryptography to ensure secure and privacy-preserving communication. Users first register by providing their credentials, which are verified using Zero-Knowledge Proofs (ZKP) and securely stored in the database, while the registration details are recorded in the blockchain for transparency and traceability. After successful login, a secure session is created with role-based access control.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

When a user uploads a file, it is encrypted using AES along with quantum-resistant keys generated through a secure key management mechanism. All system activities, including file uploads, access requests, and approvals, are immutably stored in the blockchain ledger to ensure data integrity. An audit server continuously verifies transactions and detects any inconsistencies or tampering attempts. Access control is enforced through a request–approval mechanism, where authorized users are granted secure file access and decryption rights. The admin monitors the entire system through a dashboard that provides statistical analysis and graphical visualization of system activities, ensuring transparency, security, and efficient management.

Methodology

Modules Names:

- User Authentication Module
- File Upload & Quantum Encryption Module
- Blockchain Ledger Module
- Audit Server Module
- File Integrity Verification Module
- Utilizer Access Module
- Admin Control Panel Module
- User Authentication Module – Manages user registration, login, and secure access by validating credentials and ensuring safe authentication using Zero-Knowledge Proofs (ZKP) and session management.
- File Upload & Quantum Encryption Module – Handles secure file uploading, performs integrity checking using hashing, and encrypts files using AES along with quantum-resistant key techniques.
- Blockchain Ledger Module – Records all system activities such as registration, file upload, and access requests in a tamper-proof blockchain ledger to ensure transparency and immutability.
- Audit Server Module – Continuously monitors and verifies blockchain records to detect tampering or inconsistencies and ensures system integrity through validation processes.
- File Integrity Verification Module – Ensures that uploaded and stored files remain unchanged by verifying their hash values during upload and retrieval.
- Utilizer Access Module – Manages file access requests, approvals, and secure authorization to ensure that only permitted users can access protected resources.
- Admin Control Panel Module – Provides a centralized dashboard for administrators to monitor users, file transactions, system logs, and overall system performance.

V. IMPLEMENTATION

The implementation phase converts the proposed QBC-ZKPAF (Quantum-Resilient Blockchain Zero-Knowledge Proof Authentication Framework) into a fully functional IoT security system. This stage involves setting up the development environment, integrating blockchain with Zero Trust Architecture, implementing cryptographic modules, and developing secure authentication and access control mechanisms. The system is designed in a modular structure, separating authentication, encryption, blockchain ledger, and monitoring components to ensure scalability, security, and efficient performance.

Algorithm Used

Existing Algorithm

The existing IoT security systems primarily rely on traditional authentication mechanisms such as password-based login systems, centralized identity management, and standard encryption techniques like AES and RSA. These systems validate users through a central server, where credentials are stored and verified. Blockchain or Zero Trust Architecture, if used, is typically implemented independently without deep integration. While these approaches provide basic security, they suffer from limitations such as single points of failure, lack of privacy preservation, high latency in continuous verification, and vulnerability to advanced cyberattacks. Additionally, conventional systems are not designed to handle quantum computing threats or ensure scalable, decentralized authentication in large IoT networks.

Proposed Algorithm

The proposed QBC-ZKPAF framework integrates blockchain technology, Zero Trust Architecture (ZTA), post-quantum cryptography, and Zero-Knowledge Proofs (ZKP) to provide a secure and privacy-preserving IoT authentication system. User authentication is performed through decentralized identity verification, where credentials are validated without revealing sensitive information using ZKP. Access control is enforced using blockchain-based smart contracts, ensuring that only authorized users can access IoT resources. Quantum-resistant cryptographic techniques are used for secure key generation and encryption, enhancing protection against future quantum attacks. A hybrid Deep Q-Network-based key management system dynamically selects secure keys for communication, improving adaptability and security. All system activities, including login attempts, file access, and transactions, are recorded in an immutable blockchain ledger for transparency and auditability. This integrated approach ensures high security, privacy preservation, scalability, and resilience against evolving cyber threats in IoT environments.

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

V. EXPERIMENTAL RESULTS

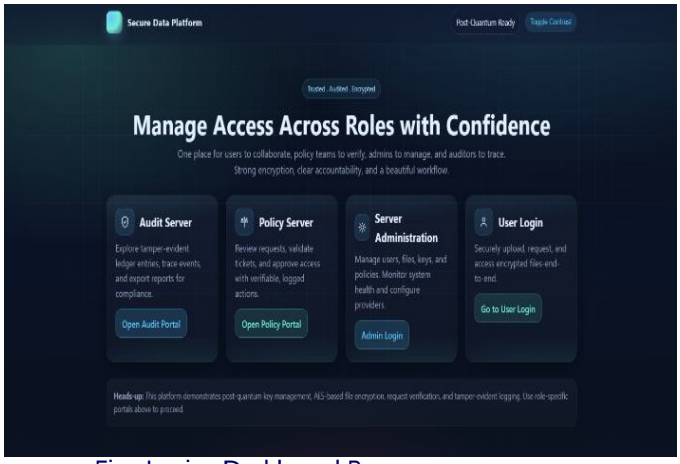

Fig : Logins Dashboard Page

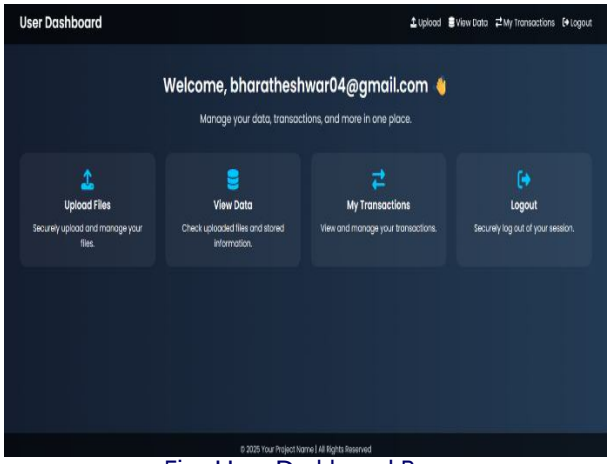

Fig : User Dashboard Page

The Logins Dashboard serves as the main entry point to the system, providing access to different user roles such as Admin, Policy Server, Audit Server, and User Login. It offers a secure interface where users can navigate to their respective portals based on their roles. The dashboard highlights key features such as secure data handling, encrypted file access, and system monitoring. It ensures controlled access and guides users to perform operations like login, request management, and auditing through dedicated modules The User Dashboard provides a centralized interface for authenticated users to manage their activities within the system. It allows users to securely upload files, view stored data, track their transactions, and log out of the system. The dashboard offers easy navigation and ensures that users can perform operations efficiently while maintaining data security and privacy.

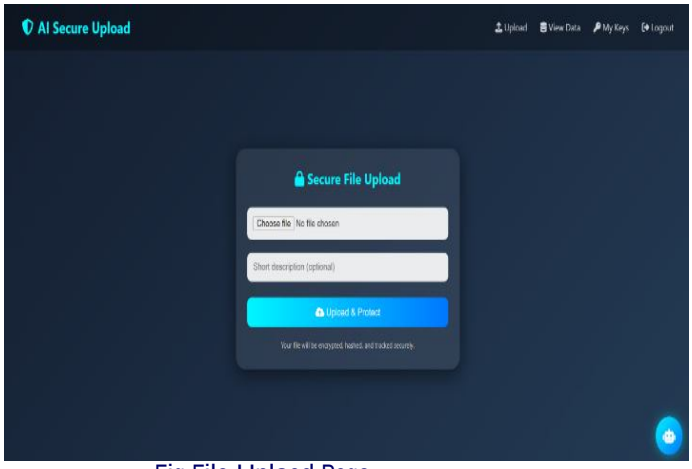

Fig File Upload Page

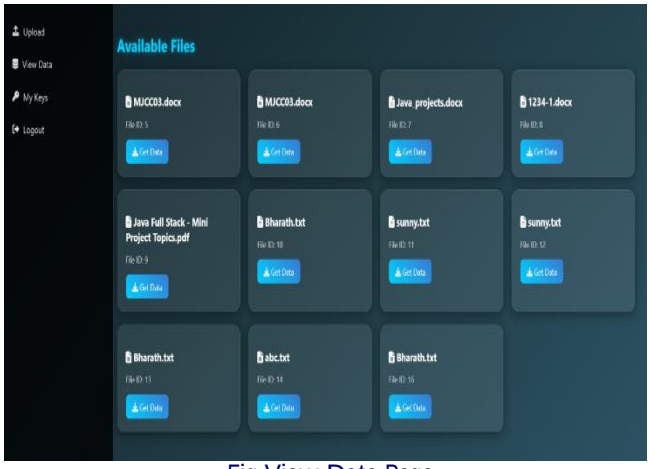

Fig View Data Page

The Secure File Upload interface allows users to upload files into the system in a protected manner. Users can select a file from their local system and optionally provide a description before uploading.

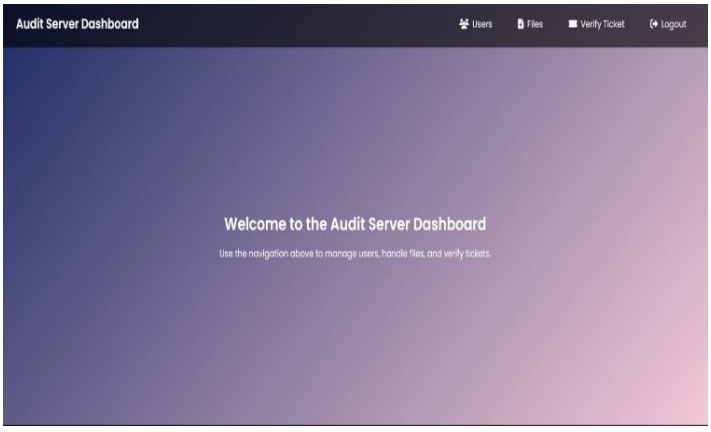

Fig Audit Dashboard Page

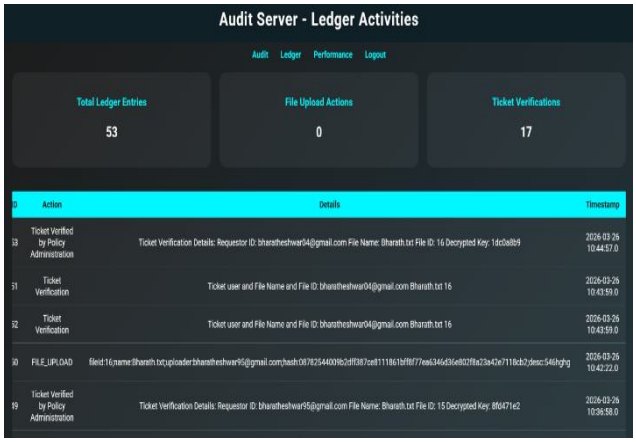

Fig Ledgers Page

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

Once submitted, the system ensures security by encrypting the file, generating hash values, and securely storing it. This module guarantees confidentiality and integrity of the uploaded data while tracking the process within the system. The Available Files view provides a grid-based directory of all documents stored on the platform, ranging from text files to project PDFs. Each entry displays the file name and its unique File ID, accompanied by a "Get Data" button for retrieval. The side navigation menu allows users to quickly toggle between uploading, viewing data, and managing their security keys. The Audit Server Dashboard features a minimalist, gradient-themed landing page that welcomes the administrator to the system. It provides a clear directive to use the top navigation bar for managing users, handling files, and verifying tickets. The clean interface ensures that auditors can easily transition between different administrative modules. The Audit Server Ledger Activities dashboard displays a summary of system operations, showing 53 total ledger entries and 17 ticket verifications. A detailed table logs recent actions like "Ticket Verified" and "FILE_UPLOAD," including specific file IDs and decrypted keys. Each entry is timestamped to maintain a tamper-evident audit trail for system transparency.

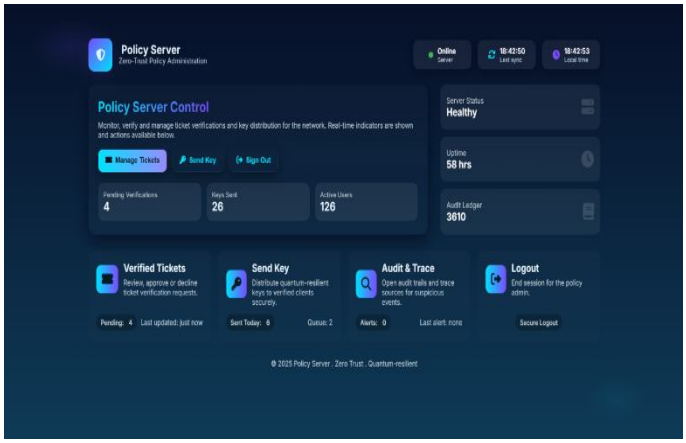

Fig Policy Dashboard Page

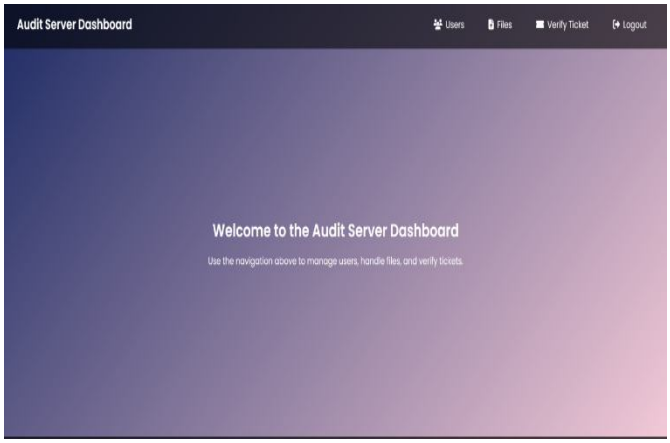

Fig Server Administration Page

The Policy Server Control dashboard provides a real-time overview of the zero-trust environment, indicating a "Healthy" server status and 58 hours of uptime. It tracks key metrics such as 4 pending verifications, 26 keys sent, and 126 active users. Navigation buttons allow administrators to manage tickets, distribute quantum-resilient keys, and trace audit logs. The image features the Audit Server Dashboard, a centralized web interface designed for administrative oversight and system management. Users can navigate through key functional areas including Users, Files, and Verify Ticket using the links at the top right of the screen. The primary purpose of this tool is to provide a streamlined environment for managing user permissions, handling server files, and processing tickets

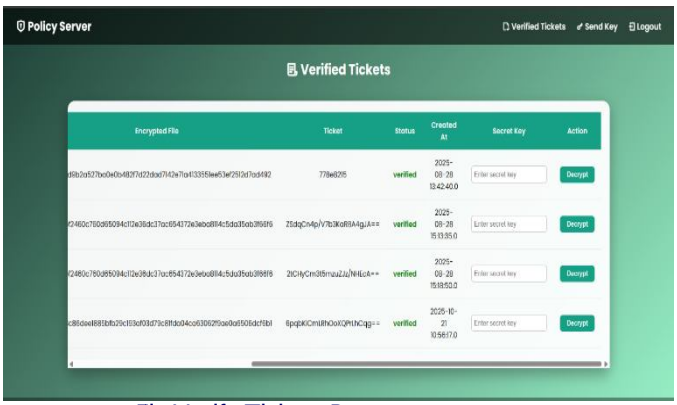

Fig Verify Tickets Page

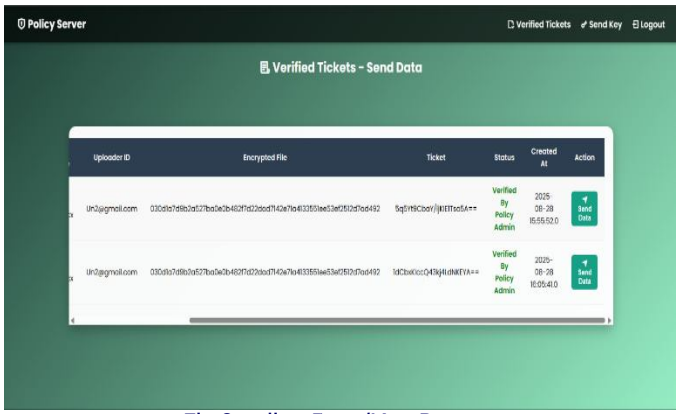

Fig Sending Data/Key Page

The Verified Tickets screen lists various file decryption requests that have reached the "verified" status. It provides fields for administrators to manually "Enter secret key" next to specific encrypted file hashes and tickets. Once the key is entered, the "Decrypt" button enables the final processing of the secure data request. The Verified Tickets – Send Data interface on the Policy Server displays a list of requests that have been "Verified By Policy Admin." It shows the uploader's ID alongside the encrypted file string and the specific ticket associated with the request. Action buttons labeled "Send Data" allow the administrator to finalize the distribution of keys to the users.

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

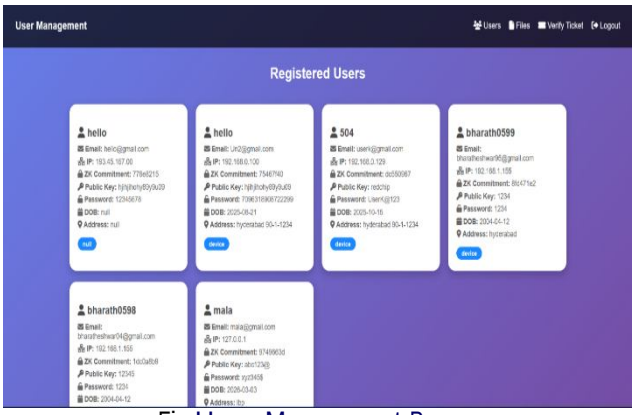

Fig Users Management Page

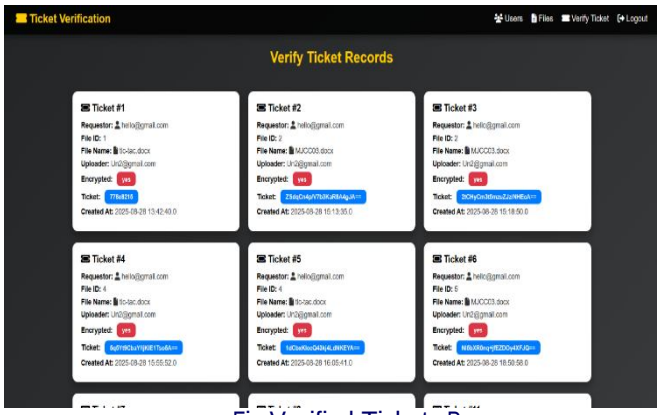

Fig Verified Tickets Page

The User Management page displays a collection of "Registered Users" shown as individual profile cards. Each card lists sensitive technical details such as IP addresses, ZK (Zero-Knowledge) Commitments, Public Keys, and encoded passwords. This view allows administrators to monitor the identities and security credentials of everyone registered on the server. The Verified Tickets screen lists various file decryption requests that have reached the "verified" status. It provides fields for administrators to manually "Enter secret key" next to specific encrypted file hashes and tickets. Once the key is entered, the "Decrypt" button enables the final processing of the secure data request.

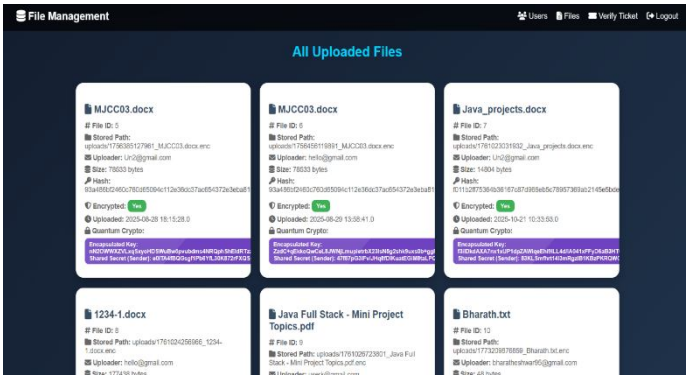

Fig File Management Page

Fig Ledger Graph

The File Management screen displays a grid of "All Uploaded Files," showing various documents like .docx and .pdf files with their respective metadata. Each file card details the unique File ID, uploader email, file size, and encryption status. Notably, the UI highlights "Quantum Crypto" features, including encapsulated keys and shared secrets for enhanced security. The Ledger Action Statistics page features a bar chart titled "Action Distribution" that visualizes system activity by category. "Ticket Verification" and "FILE_UPLOAD" represent the highest volume of actions, followed by "User Registration." This graphical interface allows administrators to quickly assess workload distribution across the secure platform.

VI. CONCLUSION

In conclusion, the proposed QBC-ZKPAF framework demonstrates a robust, privacy-preserving, and quantum-resilient approach for secure file access and identity management in blockchain-based systems. By integrating blockchain technology with Zero-Knowledge Proofs and post-quantum cryptography, the system ensures secure authentication, traceability, and tamper-proof logging while maintaining user privacy. The experimental results indicate that the framework achieves high performance, low authentication latency, strong access control, and scalability suitable for real-world IoT and blockchain applications. For our project, this reinforces the reliability, integrity, and security of file uploads, quantum encryption, access approvals, and auditing mechanisms, providing a secure environment for researchers, providers, and utilizers.

VII. FUTURE ENHANCEMENT

Future enhancements could focus on optimizing the framework for specific use cases within our project, such as integrating advanced quantum-resistant algorithms for key generation, improving energy efficiency during encryption and decryption processes, and incorporating AI-driven anomaly detection for real-time auditing. Additionally, expanding interoperability with other blockchain networks and cloud platforms could further enhance scalability, while developing mobile-friendly dashboards and automated analytics could improve usability for all user roles. These improvements would ensure the system remains future-proof and capable of handling emerging threats in privacy-sensitive, high-security environments.

E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.04

ACKNOWLEDGMENT

The successful completion of this project would not have been possible without the support and guidance of many individuals. We express our sincere gratitude to our project guide for providing valuable suggestions, continuous encouragement, and technical support throughout the development of the QBC-ZKPAF framework. We also thank the faculty members of the department for their assistance and motivation during the course of this work. Finally, we extend our appreciation to our friends and family for their constant support and encouragement.

REFERENCES

1. M.A.Aleisa,"Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments," IEEE Access, vol. 13, pp. 18660–18676, Jan. 2025.
2. A.Sharma,S.Rani,and W.Boulila,"Blockchain-based zero trust networks with federated transfer learning for IoT security in Industry 5.0," PLoS ONE, vol. 20, no. 6, e0323241, Jun. 2025.
3. T.Singh et al.,"Enhancing IoT security with zero-trust architecture: A model leveraging blockchain and AI capabilities," Journal of Cybersecurity Research, vol. 14, no. 3, pp. 112–129, Jul. 2025.
4. M.Khan,"Blockchain-integrated IoT systems: A secure framework for decentralized data management," Frontiers in Engineering and Technology, vol. 1, no. 2, pp. 4–8, Jul. 2025.
5. R.Martin,"The importance of the zero trust IEEE standard: Draft standard for zero trust security (P3409™/D6)," IEEE Computer Society, Feb. 2025.
6. J.Doe and S.Lee,"Zero trust architecture for IoT device ecosystems: Design and implementation," International Journal of Basic and Applied Sciences, vol. 14, no. 4, pp. 818–825, Aug. 2025.
7. A.R.Pathak and P.Kumar,"Decentralized identity and access management in smart cities using blockchain and zero-trust," Sustainable Cities and Society, vol. 102, 105123, Mar. 2025.
8. S.V.Belavadi and K.G.Srinivasa,"A blockchain-inspired zero-trust framework for secure healthcare monitoring," Journal of Medical Systems, vol. 49, no. 1, p. 12, Jan. 2025.
9. L.Zhang,"Blockchain and zero-trust identity management system for smart cities and IoT networks," International Journal of Multidisciplinary Research, vol. 4, no. 1, pp. 704–709, Jan. 2025.
10. H.Kim and T.Park,"Post-quantum cryptographic integration in blockchain-based zero trust for 6G IoT," IEEE Transactions on Industrial Informatics, vol. 21, no. 2, pp. 1450–1462, Feb. 2025.
11. Joshi,Y.,Totad,S.G.,Geeta,R.B.,& Prasad Reddy,P.V.G.D.(2018).Mobile agent-based frequent pattern mining for distributed databases. In S. Bhalla, V. Bhateja, A. Chandavale, A. Hiwale, & S. Satapathy (Eds.), Intelligent computing and information and communication (Vol. 673). Springer. https://doi.org/10.1007/978-981-10-7245-1_9
12. Bharamagoudar,G.R.,Totad,S.G.,Prasad Reddy,P.,&Shobha,R.B.(2015).Zealous leadership paradigms. International Journal of Globalisation and Small Business, 7(1), 92–106. https://doi.org/10.1504/IJGSB.2015.069033
13. Geeta,R.B.,Totad,S.G.,Prasad Reddy,P.,&Shobha,R.B.(2015).Big data structure and usage mining coalition. International Journal of Services Technology and Management, 21(4/5/6), 252–271. https://doi.org/10.1504/IJSTM.2015.073930](https://doi.org/10.1504/IJSTM.2015.073930