AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

PRIVACY-PRESERVING SECURE FILE SHARING USING QUANTUM CRYPTOGRAPHY, BLOCKCHAIN, AND ZERO-KNOWLEDGE AUTHENTICATION

Uzma Shereen[1], Lubna Nausheen[2]
[1]PG Scholar, Department of AI&DS, Shadan Women's College of Engineering and Technology, Hyderabad, uzma.shereen22@gmail.com
[2]Asst Professor, Department of CSE, Shadan Women's College of Engineering and Technology lubnanausheen07@gmail.com

ABSTRACT:
This research introduces a novel Unified Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF) aimed at enhancing security in IoT environments. The system combines post-quantum cryptography, blockchain technology, and Zero Trust Architecture (ZTA) to provide secure communication, access management, and privacy-preserving authentication. It uses a Deep Q-Network Multi-Factor safe Key (DQN-MFSK) for dynamic key selection, a hybrid Reinforcement-Lattice Blockchain Key Generation for quantum-resilient key creation, and Zero-Knowledge Proofs for privacy-preserving signatures to ensure a safe Internet of Things environment. Data privacy, secrecy, auditability, traceability, and resistance to changing threats, such as quantum attacks, are all guaranteed by this architecture. Transparency and thorough post-event audit trails are supported by the blockchain ledger's immutability, which records all access attempts, data exchanges, and device interactions in an unchangeable way. Through a tracing key kept on the audit server within the Zero Trust Architecture, the architecture allows accurate source tracing in the event of suspicious activity or breaches. QBC-ZKPAF provides strong security and privacy solutions for Internet of Things networks by adopting multi-factor authentication and decentralizing identity management. The framework's efficacy is confirmed by experimental results, which show 98% privacy preservation, 700 TPS throughput, 0.98 quantum resilience, and 96% access control effectiveness, making it ideal for contemporary blockchain and IoT applications.

KEYWORDS IoT security, data confidentiality, user authentication, decentralization, blockchain technology, zero trust architecture, quantum resilience, access control, privacy protection, and secure communication

1. INTRODUCTION

IoT is one of the key technologies and bridging devices in smart cities, industrial automation, and healthcare these days. As the number of IoT devices increases, so do the inherent limitations in their processing and security capabilities, making cybersecurity a major concern. IoT ecosystems are typically highly dynamic and decentralized. Such an ecosystem is a prime target for assaults such denial of service (DoS) attacks, malware incursion, and data breaches due to the continuous flow of sensitive data across connected devices. Because it is frequently very difficult to define any specific perimeter within which these devices will operate when they are in distributed, cloud-based, or edge environments, traditional security models, especially those that rely on the idea of a secured perimeter, are not applicable to IoT networks [2]. This calls for improved security architectures created to more successfully handle the unique risks of IoT devices. ZTA has been identified as a promising solution as a result. According to the zero-trust security concept, no entity—internal or external to the network—should be trusted by default. Even if it originates from inside the trusted network perimeter, every request for access or communication is regarded as potentially dangerous and requires ongoing authentication and authorization based on stringent identity verification. Furthermore, no device, user, or application will be trusted by default, whether they are inside or outside the network perimeter, according to ZTA's basic tenet of "never trust, always verify." Enforcing the least privilege principle continuously verifies each access request, which is considered potentially dangerous. It has been demonstrated that ZTA was successful in preventing attackers from moving laterally and securing the network in general. ZTA does increase security, but it also presents new difficulties, especially when it comes to protecting privacy. ZTA's ongoing authentication and access control procedures may unintentionally reveal private user information or device characteristics, creating privacy issues. Because of its decentralization and tamper-resistance features, blockchain has garnered a lot of attention lately. These features promise to assist address a wide range of security and privacy issues in Internet of Things contexts. Blockchain is a decentralized, distributed digital ledger technology that maintains security, transparency, and immutability while recording transactions across numerous computers. To prevent fraud and manipulation, it employs consensus techniques such as Proof of Work (PoW) or Proof of Stake (PoS) to validate and add new data blocks. Additionally, blockchain functions as a distributed ledger with numerous nodes storing data. This guarantees the integrity of the data and prevents the emergence of a single point of failure. Blockchain-based cryptographic approaches make data unchangeable and verifiable, making them ideal for secure Internet of Things networks [8]. However, because sensitive data may leak across all nodes due to blockchain's transparency and immutability, there is

a privacy risk [9]. IoT devices with limited computational capacity are concerned about blockchain's scalability and resource constraints [10]. Given these constraints, a hybrid strategy that capitalizes on ZTA's benefits while utilizing blockchain's decentralized and tamper-resistant features is required. It proposes a blockchain-enabled ZTA to solve privacy and security issues in Internet of Things settings. In this situation, decentralized identity management offers safe blockchain-based storage of IoT device identities, preventing any central authority from controlling or compromising user data. This eliminates all risks related to central identity repositories, including insider attacks and data breaches. Along with ring signatures and designated verifier signatures, it would also make use of advanced cryptographic techniques. These cryptographic techniques enhance communication and authentication privacy protection. Verifier signatures allow for selective disclosure of the signer's identity; that is, only the authorized verifier may confirm the signer's legitimacy. Therefore, even if the system may detect and record risky activity when it counts, these strategies guarantee that user privacy prevails under normal conditions. Furthermore, the ZTA architecture incorporates MFA, which strengthens access constraints. MFA mandates that users authenticate themselves using at least one additional independent authentication factor, such as something they possess, something they know, or something they are. In the event that one factor has been compromised, this restricts even unwanted access [14]. The MFA credentials will be saved and validated with tamper-proof authenticity that cannot be obtained by phishing or credential stuffing assaults due to the decentralized nature of blockchain [15]. Thus, this paper aims to introduce a novel cybersecurity mechanism for IoT settings by integrating blockchain with ZTA and MFA through providing decentralized, and tamper-proof cre dential storage with enhanced quantum resilience. Quantum Resilience refers to the ability of a system or protocol to remain secure in the face of potential threats from quantum computers. Quantum computers have the potential to break current cryptographic algorithms, like RSA and ECC, which rely on the difficulty of factoring large numbers or solving discrete logarithms. Developing cryptographic methods (quantum-safe or post-quantum cryptography) that may survive the processing power of quantum machines is known as quantum resilience. Even in the event that one component is compromised, this combination reduces the possibility of unwanted access. Additionally, it successfully defends against credential stuffing and phishing assaults. For delicate IoT situations, it guarantees both improved access control and privacy protection. Smart cities for improved traffic and energy management [17], smart healthcare systems for secure patient data management [16], and industrial IoT networks for reliable device authentication and threat detection [18] are just a few of the IoT environments that can benefit from this blockchain-enabled zero-trust architecture. Blockchain's intrinsic decentralization, immutability, and transparency make it especially well suited to the QBC-ZKPAF design. In IoT networks, these characteristics are crucial for safe identity management and privacy protection. In contrast to other distributed ledger technologies (DLTs), blockchain offers tamper-proof records and guarantees that all recorded data, including identity verification logs and access rights, cannot be altered once added to the ledger. Furthermore, a central authority is not necessary due to its decentralized structure. In large-scale, dispersed IoT contexts, it is crucial to decrease single points of failure and boost system resiliency.

2. STIMULATING

The system, known as the Unified Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication system (QBC-ZKPAF), focuses on resolving the particular issues brought about by the intersection of emerging quantum computing threats with the Internet of Things. With quantum-resilient key generation via Reinforcement-Lattice Blockchain Key Generation and dynamic key selection driven by a Deep Q-Network Multi-Factor Secure Key (DQN-MFSK) technique, it integrates hybrid mechanisms for key generation and authentication. By utilizing Zero-Knowledge Proofs (ZKPs) for safe, anonymous interactions and providing complete traceability through immutable blockchain records, the project guarantees strong, privacy-preserving authentication. The framework's practicality in real-world IoT applications is demonstrated by the experimental validation of its efficacy, which includes metrics like 98% privacy preservation, 700 TPS throughput, and 96% access control effectiveness.

3. OBJECTIVE

The project offers a quantum-resilient solution for safe key generation, verification, and authentication by combining blockchain technology, Zero Trust Architecture (ZTA), and post-quantum cryptographic techniques. The framework strengthens the overall security posture of IoT networks by providing an adaptable and dynamic approach to key selection and management through a hybrid Deep Q-Network (DQN) in conjunction with multi-factor authentication. The goal is to create a future-proof architecture that can provide unmatched privacy, transparency, and auditability for IoT systems in a variety of applications while withstanding increasing security concerns, such as quantum assaults.

3.1 What The Project Is About

Because IoT environments are decentralized and dynamic, traditional security solutions suffer, leaving devices open to threats like malware and data leaks.

Zero Trust Architecture (ZTA) creates privacy concerns since it exposes sensitive data during authentication, even while it increases security by validating each access request. Blockchain's decentralized, tamper-proof design can improve security, but its resource requirements are difficult for IoT devices, and its transparency may jeopardize privacy. By combining the advantages of blockchain and ZTA, this project seeks to provide a hybrid security framework that efficiently addresses security and privacy issues while guaranteeing robust authentication, privacy protection, and secure identity management for IoT systems.

4. EXISTING SYSTEM:

- The swift expansion of IoT technology, which links gadgets in smart cities, healthcare, and industrial automation, poses serious cybersecurity risks.
- IoT ecosystems are by their very nature decentralized and dynamic, with many devices constantly sharing sensitive data.
- They are therefore easy targets for cyberattacks such denial of service (DoS) attacks, malware invasions, and data breaches.
- Because IoT devices frequently function in distributed, cloud-based, or edge contexts without a fixed boundary, traditional security methods that rely on a well-defined secure perimeter are inadequate in these kinds of networks.
- Because of this, current security strategies are unable to defend IoT systems from new threats.

4.1 Existing System Disadvantages:

- Every new gadget raises the demand for current security protocols and creates possible vulnerabilities.
- Insufficient Standardization

4.2 THE PROPOSED SYSTEM

- The suggested solution uses smart contracts on a blockchain to enforce access restriction, allowing authorized people or devices to safely access the IoT environment.
- Access rights and policies are automatically defined and enforced by these smart contracts.
- Blockchain-based access tokens provide allowed access to resources, while decentralized identity management guarantees that users maintain distinct and secure identities validated by the blockchain.
- This decentralized strategy improves data privacy by safeguarding confidentiality, increases security by lowering attack vulnerabilities, and improves speed by increasing throughput.
- The solution avoids the dangers of centralized identity management, such as single points of failure, by giving users the ability to maintain their own identities.
- To further protect user data during authentication, the framework employs Zero-Knowledge Proofs (ZKP), allowing users to prove their identity without revealing sensitive information, thus preserving privacy while ensuring secure access in IoT environments.
- The framework uses Zero-Knowledge Proofs (ZKP) to further protect user data during authentication. By enabling users to verify their identity without disclosing sensitive information, ZKP ensures secure access in IoT contexts while protecting privacy.

4.2.1 Proposed System Advantage

- High Performance
- Quantum-Resilient: Guards against potential risks from quantum computing

5.METHODOLOGIES

1. Design of User Interfaces

For every user interacting with the system, including devices, suppliers, and utilizers, this module oversees the identity verification procedure. It has features for managing sessions, logging in, and registering users. User credentials, device details, and IP address are collected and safely kept during registration. Additionally, the module creates a Zero-Knowledge Proof (ZKP) promise to guarantee authenticity without disclosing personal information. After authentication, a legitimate session is established, allowing safe access to other system features.**2. User1**

Uploading files or sensitive data into the system is the responsibility of the User1 module. To guarantee integrity and stop unwanted changes, the data is transformed into hash values after uploading. The data is subsequently secured by the system using Quantum Cryptography techniques. A Base64 Secret and Quantum Private Key For safe access and sharing, keys are created. Lastly, for safe administration, the encrypted data is kept in the ledger.

3. Audit Server

Every action taken within the system is tracked and monitored by the Audit Server. It keeps ledger records with user actions and transaction information. Audit records are categorized by the server to facilitate analysis and verification. It verifies ticket information and determines if operations adhere to security guidelines. Additionally, graphical analysis is produced to assist managers in keeping an eye on system performance and identifying questionable activity.

4. Policy Server

Authorization and access control policies are managed by the Policy Server. By verifying user requests with Base64 secret keys and pre-established security criteria, it manages tickets. The server checks to see if users are authorized to access the requested data. It safely transmits access keys to authorized users following successful validation. Only authorized users will be able to access protected data thanks to this module.**5. User2**

The data requester or recipient is the User2 module. Using the supplied ZK (Zero-Knowledge) key, users

can explore the accessible files and make access requests. Until the Policy Server grants approval, the system puts the request in a pending state. The necessary access key is given to the user after approval. The user can safely download and view the requested data with this key.

6.TECHNIQUE ALGORITHM USED

6.1 Proposed Algorithm

- **Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF)**

An sophisticated security solution called the Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF) was created to improve the privacy and authentication processes in Internet of Things environments. To provide strong defense against new dangers, like as quantum attacks, it combines blockchain technology with post-quantum cryptography and Zero Trust Architecture (ZTA). QBC-ZKPAF employs Deep Q-Network Multi-Factor Secure Keys (DQN-MFSK) for dynamic key selection in addition to a hybrid Reinforcement-Lattice Blockchain Key Generation (KeyGen) for quantum-resilient key production. Sensitive data is never revealed thanks to the use of Zero-Knowledge Proofs (ZKP), which enable privacy-preserving authentication. The system supports auditability and transparency in decentralized IoT networks by providing traceable, unchangeable logs via the blockchain in addition to securing data exchange and device interactions.

A safe authentication framework created for Internet of Things settings is called Quantum-Resilient Blockchain-Zero Knowledge Proofs Privacy Authentication Framework (QBC-ZKPAF). To offer robust security and anonymity, it integrates blockchain technology, Zero-Knowledge Proofs (ZKP), and quantum-resistant encryption. While ZKP allows users to authenticate their identity without disclosing sensitive information, Blockchain is used to safely preserve authentication data and prevent unwanted alterations. By employing cutting-edge cryptographic methods, the system also guards against potential risks from quantum computing in the future. All things considered, QBC-ZKPAF offers IoT devices and users dependable, private, and safe authentication and access management.

6.2 EXISTING SYSTEM

- **Zero-Knowledge Proofs (ZKP)**

A cryptographic technique called Zero-Knowledge Proofs (ZKP) enables one person, referred to as the prover, to demonstrate to another, referred to as the verifier, that they are aware of a certain piece of information without disclosing the knowledge itself. The fundamental idea of ZKPs is that no real data is transferred or revealed while the verifier gets confidence that the prover has the knowledge or secret. This technique is very useful in applications that are sensitive to privacy, including secure transactions or authentication, where disclosing the underlying data could pose security problems. Because they guarantee identification and verification without revealing sensitive data, ZKPs are frequently employed in blockchain and IoT systems to safeguard user privacy while maintaining integrity and trust. ZKPs' main benefit is their capacity to maintain anonymity, which makes them perfect for decentralized and privacy-preserving settings.

A cryptographic approach called Zero-Knowledge Proofs (ZKP) enables a person to demonstrate that they possess specific knowledge without disclosing the information itself. ZKP allows users to confirm their identity in authentication systems without disclosing private keys, passwords, or other private information. This method lessens the possibility of data leaking during communication and enhances privacy. However, deploying standard ZKP solutions on resource-constrained IoT devices and large-scale networks might be difficult due to their high processing time and computing resource requirements.

7.SYSTEM ARCHITECTURE

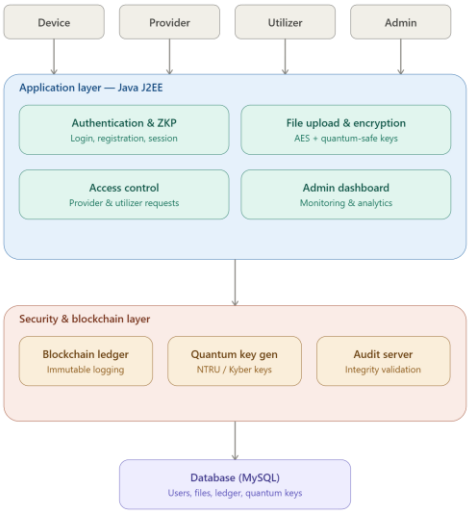
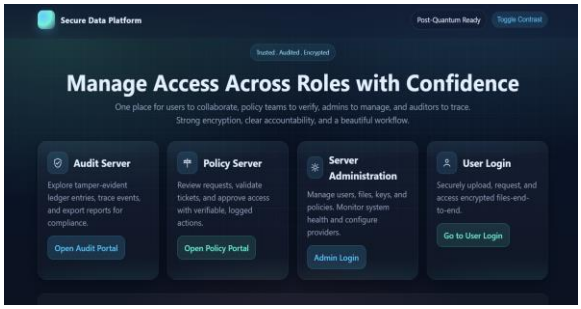


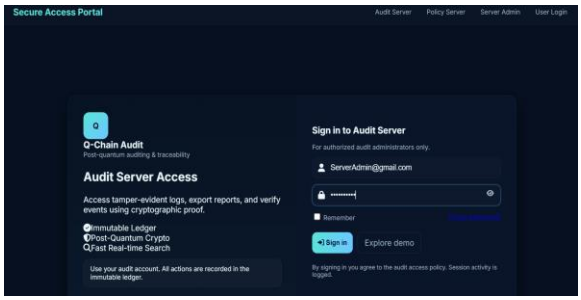
FIG: 7 System Architecture

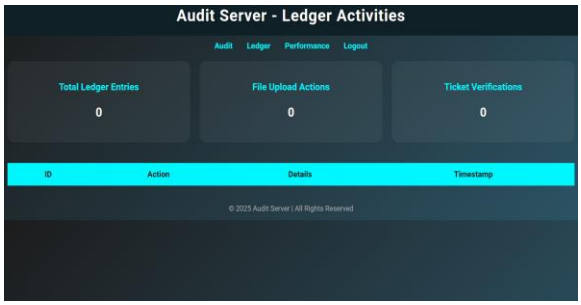
Users, data controllers, servers, and blockchain networks are all integrated into the system architecture, which is a decentralized blockchain-based tracking and tracing framework. Through secure web or application interfaces, users and data controllers may access the system at the client layer for tasks including file upload, registration, login, search, and download. Core modules including file management, access control, authentication, and decision-making logic are found at the application layer. The server serves as a middleman, coordinating communication between entities, enforcing permissions, and validating requests. The file management module processes uploaded files and

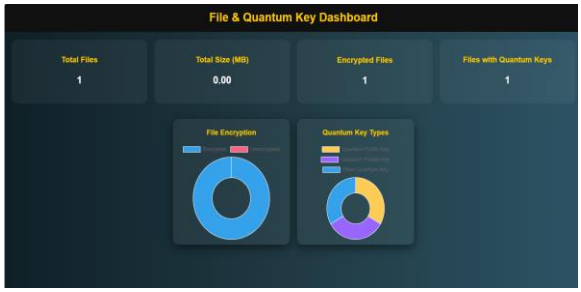
creates cryptographic hashes and information. Without the need for human involvement, smart contracts automate access control and enforce predetermined restrictions. The Picture Fuzzy COCOSO model-based decision-making engine assesses system performance in the face of ambiguity. The confidentiality and integrity of shared data are guaranteed via cryptographic key management. Network nodes use consensus techniques to validate transactions. Blocks of verified transactions are added to the blockchain. Admin modules keep an eye on and authorize system users. Scalability, transparency, security, and dependability are all guaranteed by this tiered design.

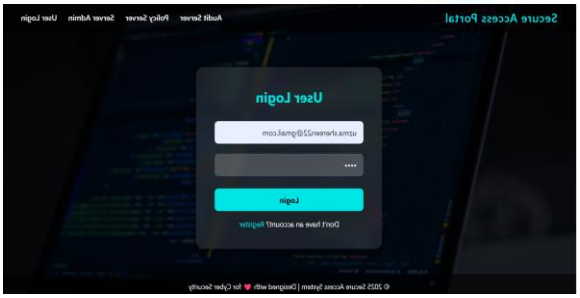
8.RESULTS

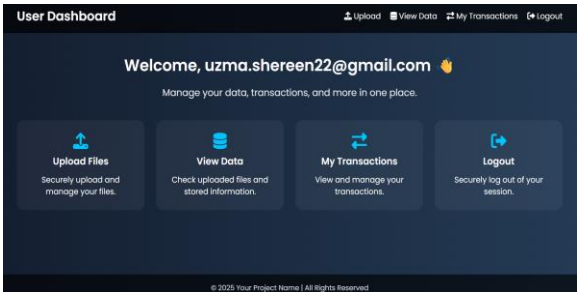












9. CONCLUSION

To sum up, the suggested QBC-ZKPAF framework shows a reliable, quantum-resilient, and privacy-preserving method for safe file access and identity management in blockchain-based systems. The system guarantees secure authentication, traceability, and tamper-proof logging while protecting user privacy by combining blockchain technology with Zero-Knowledge Proofs and post-quantum cryptography. The framework delivers high performance, low authentication latency, robust access control, and scalability appropriate for real-world blockchain and IoT applications, according to the experimental results. This strengthens the dependability, integrity, and security of file uploads, quantum encryption, access permissions, and auditing procedures for our project, offering a safe environment for users, suppliers, and researchers.

10. FUTURE ENHANCEMENT

Future improvements might concentrate on optimizing the framework for particular use cases within our project, like adding AI-driven anomaly detection for real-time auditing, enhancing energy efficiency during encryption and decryption processes, and integrating sophisticated quantum-resistant algorithms for key generation. Developing mobile-friendly dashboards and automated analytics could increase usability for all user roles, and increasing compatibility with other blockchain networks and cloud systems could further boost scalability. These enhancements would guarantee that the system is future-proof and able to manage new threats in high-security, privacy-sensitive settings.

REFERENCES

[1] R. Marshal, K. Gobinath, and V. V. Rao, "Proactive measures to mitigate cybersecurity challenges in IoT based smart health care networks,"

in Proc. IEEE Int. IoT, Electron. Mechatronics Conf. (IEMTRONICS), Apr. 2021, pp. 1–4.
[2] A. K. Al Hwaitat, M. A. Almaiah, A. Ali, S. Al-Otaibi, R. Shishakly, A. Lutfi, and M. Alrawad, ‘‘A new block chain-based authentication frame work for secure IoT networks,’’ Electronics, vol. 12, no. 17, p. 3618, Aug. 2023.
[3] T. Muhammad, M. T. Munir, M. Z. Munir, and M. W. Zafar, ‘‘Integrative cybersecurity: Merging zero trust, layered defense, and global standards for a resilient digital future,’’ Int. J. Comput. Sci. Technol., vol. 6, no. 4, pp. 99–135, 2022.
[4] V. Stafford, Zero Trust Architecture, document NIST Special Publication 800-207, 2020.
[5] D. Li, Z. Yang, S. Yu, M. Duan, and S. Yang, ‘‘A micro-segmentation method based on VLAN-VxLAN mapping technology,’’ Future Internet, vol. 16, no. 9, p. 320, Sep. 2024.
[6] W. Alnahari and M. T. Quasim, ‘‘Privacy concerns, IoT devices and attacks in smart cities,’’ in Proc. Int. Congr. Adv. Technol. Eng. (ICOTEN), Jul. 2021, pp. 1–5.
[7] R. Saxena, D. Arora, V. Nagar, and S. Mahapatra, ‘‘Bitcoin: A digital cryptocurrency,’’ in Intelligent Systems Reference Library. Cham, Switzerland: Springer, 2021, pp. 13–28.
[8] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, ‘‘A sur vey on the adoption of blockchain in IoT: Challenges and solutions,’’ Blockchain, Res. Appl., vol. 2, no. 2, Jun. 2021, Art. no. 100006.
[9] Z. Ruan, ‘‘Blockchain technology for security issues and challenges in IoT,’’ in Proc. Int. Conf. Comput. Simul. Model., Inf. Secur. (CSMIS), Nov. 2023, pp. 572–580.
[10] M. Luecking, C. Fries, R. Lamberti, and W. Stork, ‘‘Decentralized identity and trust management framework for Internet of Things,’’ in Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), May 2020, pp. 1–9.
[11] A. Niraula, Zero Trust Architecture for Peer-to-Peer Communication Using Blockchain and Hardware-Oriented Security. Toledo, OH, USA: Univ. Toledo, 2021.
[12] T. H. Yuen, M. F. Esgin, J. K. Liu, M. H. Au, and Z. Ding, ‘‘DualRing: Generic construction of ring signatures with efficient instantiations,’’ in Proc. Annu. Int. Cryptol. Conf. Cham, Switzerland: Springer, Aug. 2021, pp. 251–281.
[13] G.Bian,R.Zhang,andB.Shao,‘‘Identity-basedprivacypreservingremote data integrity checking with a designated verifier,’’ IEEE Access, vol. 10, pp. 40556–40570, 2022.
[14] C. Bast and K.-H. Yeh, ‘‘Emerging authentication technologies for zero trust on the Internet of Things,’’ Symmetry, vol. 16, no. 8, p. 993, Aug. 2024.
[15] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, ‘‘A blockchain-inspired attribute-based zero-trust access control model for IoT,’’ Information, vol. 14, no. 2, p. 129, Feb. 2023.
[16] H. B. Mahajan and A. A. Junnarkar, ‘‘Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing,’’ Multimedia Tools Appl., vol. 82, no. 28, pp. 44335–44358, Nov. 2023.
[17] A. Jaramillo-Alcazar, J. Govea, and W. Villegas-Ch, ‘‘Advances in the optimization of vehicular traffic in smart cities: Integration of blockchain and computer vision for sustainable mobility,’’ Sustainability, vol. 15, no. 22, p. 15736, Nov. 2023.
[18] P. C. Sharma, M. R. Mahmood, H. Raja, N. S. Yadav, B. B. Gupta, and V. Arya, ‘‘Secure authentication and privacy-preserving blockchain for industrial Internet of Things,’’ Comput. Electr. Eng., vol. 108, May 2023, Art. no. 108703.
[19] Y. Liu, X. Hao, W. Ren, R. Xiong, T. Zhu, K. R. Choo, and G. Min, ‘‘A blockchain-based decentralized, fair and authenticated information sharing scheme in zero trust Internet-of-Things,’’ IEEE Trans. Comput., vol. 72, no. 2, pp. 501–512, Feb. 2023.
[20] P. Thantharate and A. Thantharate, ‘‘Zero Trust Block: Enhancing security, privacy, and interoperability of sensitive data through Zero Trust permissioned blockchain,’’ Big Data Cognit. Comput., vol. 7, no. 4, p. 165, Oct. 2023.
[21] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi, and J. Read, ‘‘Blockchain enabled intrusion detection and prevention system of APTs within zero trust architecture,’’ IEEE Access, vol. 10, pp. 89270–89288, 2022. [22] C. H. C. Han, G.-J.-K. C. Han, O. A. G.-J. Kim, A. T. O. Alfarraj, and Y. R. A. Tolba, ‘‘ZT-BDS: A secure blockchain-based zero-trust data storage scheme in 6G edge IoT,’’ J. Internet Technol., vol. 23, no. 2, pp. 289–295, Mar. 2022.
[23] D. Li, E. Zhang, M. Lei, and C. Song, ‘‘Zero trust in edge computing environment: A blockchain based practical scheme,’’ Math. Biosci. Eng., vol. 19, no. 4, pp. 4196–4216, 2022.
[24] K. Gai, Y. She, L. Zhu, K.-K.-R. Choo, and Z. Wan, ‘‘A blockchain-based access control scheme for zero trust cross-organizational data sharing,’’ ACMTrans. Internet Technol., vol. 23, no. 3, pp. 1–25, Aug. 2023. [25] U. B. Chaudhry and A. K. M. Hydros, ‘‘Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm,’’ IET Blockchain, vol. 3, no. 2, pp. 98–115, Jun. 2023. [26] P. Li, W. Ou, H. Liang, W. Han, Q. Zhang, and G. Zeng, ‘‘A zero trust and blockchain-based defense model for smart electric vehicle chargers,’’ J. Netw. Comput. Appl., vol. 213, Apr. 2023, Art. no. 103599.
[27] M. H. Mirazand M. Ali, ‘‘Integration of blockchain and IoT: An enhanced security perspective,’’ 2020, arXiv:2011.09121.
[28] O. C. Edo, D. Ang, P. Billakota, and J. C. Ho, ‘‘A zero trust architecture for health information systems,’’ Health Technol., vol. 14, no. 1, pp. 189–199, Jan. 2024.

[29] A. Padma and M. Ramaiah, "Blockchain based an efficient and secure privacy preserved framework for smart cities," IEEE Access, vol. 12, pp. 21985–22002, 2024.
[30] A. Padma and M. Ramaiah, "GLSBIoT: GWO-based enhancement for lightweight scalable blockchain for IoT with trust based consensus," Future Gener. Comput. Syst., vol. 159, pp. 64–76, Oct. 2024.
[31] P. Chinnasamy, A. Albakri, M. Khan, A. A. Raja, A. Kiran, and J. C. Babu, "Smart contract-enabled secure sharing of health data for a mobile cloud based E-health system," Appl. Sci., vol. 13, no. 6, p. 3970, Mar. 2023.
[32] P. Gangwani, A. Perez-Pons, T. Bhardwaj, H. Upadhyay, S. Joshi, and L. Lagos, "Securing environmental IoT data using masked authentication messaging protocol in a DAG-based blockchain: IOTA tangle," Future Internet, vol. 13, no. 12, p. 312, Dec. 2021.
[33] W. Zhao, I. M. Aldyaflah, P. Gangwani, S. Joshi, H. Upadhyay, and L. Lagos, "A blockchain-facilitated secure sensing data processing and logging system," IEEE Access, vol. 11, pp. 21712–21728, 2023.
[34] I. U. Din, K. H. Khan, A. Almogren, M. Zareei, and J. A. P. Díaz, "Securing the metaverse: A blockchain-enabled zero-trust architecture for virtual environments," IEEE Access, vol. 12, pp. 92337–92347, 2024. [35] A. A. Agarkar, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L. Kulkarni, "Blockchain aware decentralized identity manage ment and access control system," Meas., Sensors, vol. 31, Feb. 2024, Art. no. 101032.
[36] A. Salam, M. Abrar, F. Amin, F. Ullah, I. A. Khan, B. F. Alkhamees, and H. AlSalman, "Securing smart manufacturing by integrating anomaly detection with zero-knowledge proofs," IEEE Access, vol. 12, pp. 36346–36360, 2024.
[37] J.Duan,S.Zheng,W.Wang,L.Wang,X.Hu,andL.Gu,"ConciseRingCT protocol based on linkable threshold ring signature," IEEE Trans. Depend. Secure Comput., vol. 21, no. 5, pp. 5014–5028, Sep. 2024.
[38] W. Li, X. Deng, J. Liu, Z. Yu, and X. Lou, "Delegated proof of stake con sensus mechanism based on community discovery and credit incentive," Entropy, vol. 25, no. 9, p. 1320, Sep. 2023.
[39] A. M. Aburbeian and M. Fernández-Veiga, "Secure Internet financial transactions: A framework integrating multi-factor authentication and machine learning," AI, vol. 5, no. 1, pp. 177–194, Jan. 2024.
[40] B.Lei,J.Zhou,M.Ma,andX.Niu,"DQNbasedblockchaindatastoragein resource-constrained IoT system," in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Mar. 2023, pp. 1–6.
[41] G. Sravya, P. S. Kumar, and R. Padmavathy, "Survey of post-quantum lattice-based ciphertext-policy attribute-based encryption schemes for cloud storage: Taxonomy, open issues, and future directions," IEEE Trans. Services Comput., vol. 17, no. 6, pp. 4540–4557, Nov./Dec. 2024, doi: 10.1109/TSC.2024.3479930.
[42] Y. Zhou, Y. Ren, M. Xu, and G. Feng, "An improved NSGA-III algorithm based on deep Q-networks for cloud storage optimization of blockchain," IEEE Trans. Parallel Distrib. Syst., vol. 34, no. 5, pp. 1406–1419, May 2023.
[43] F. Tang, C. Ma, and K. Cheng, "Privacy-preserving authentication scheme based on zero trust architecture," Digit. Commun. Netw., vol. 10, no. 5, pp. 1211–1220, Oct. 2024.
[44] M. Zhang, C. Xu, and M. Huang, "Research on multiserver lightweight multi-factor authentication protocol in telemedicine environment," Inf. Netw. Secur., vol. 10, pp. 42–49, Jan. 2019.
[45] F. Zhang, W. Susilo, Y. Mu, and X. Chen, "Identity-based universal des ignated verifier signatures," In in Proc. Int. Conf. Embedded Ubiquitous Comput. Berlin, Germany: Springer, Dec. 2005, pp. 825–834.
[46] P. Rastegari, M. Berenjkoub, M. Dakhilalian, and W. Susilo, "Universal designated verifier signature scheme with non-delegatability in the stan dard model," Inf. Sci., vol. 479, pp. 321–334, Apr. 2019.
[47] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain pri vacy protection scheme based on ring signature," IEEE Access, vol. 8, pp. 76765–76772, 2020.