International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 946-974
https://doi.org/10.70917/ijcisim-2026-2609
Article

Attribute-Based Encryption and Privacy-Preserving Frameworks for Post-Quantum Cross-Chain Blockchain IoT Security: A Comprehensive Survey

Sunil Parihar[1], Jigyasu Dubey[2]

[1]Department of Computer Science & Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, Madhya Pradesh, India.
Email: sunielparihar@gmail.com
[2]Department of Computer Science & Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, Madhya Pradesh, India.
Email: jigyasudube@yahoo.co.in

Abstract: The Internet of Things (IoT) has created a huge amount of distributed data that needs to be securely stored, communicated among various stakeholders and accessed in a secure manner while preserving the privacy of the data. While blockchain offers decentralization, transparency, and immutability, current platforms still have vulnerabilities such as quantum computing attacks, cross-chain interoperability issues, and storage scalability and data management challenges. Decentralized storage can be achieved efficiently thanks to the integration of InterPlanetary File System (IPFS) and blockchain, and quantum-resistant security and fine-grained access control are possible through Post-Quantum Cryptography (PQC) and Attribute-Based Encryption (ABE). Over the past seven years, 43 studies have been published from 2019 to 2026, which is analyzed and discussed in this paper to investigate the latest advancements in secure data storage and communication in the Internet of Things (IoT) field using post-quantum blockchain networks. It highlights important research areas, security concerns, and open challenges and offers a conceptual design of a blockchain–IPFS system that satisfies the requirements for scalable, interoperable, privacy-preserving and quantum-resistant IoT ecosystems.

Keywords: Post-Quantum Cryptography; Blockchain; Internet of Things; InterPlanetary File System (IPFS); Cross-Chain Communication; Attribute-Based Encryption; Decentralized Storage; IoT Data Security; Privacy Preservation; Quantum-Resistant Blockchain.

1. Introduction

With the emerging Internet of Things (IoT) paradigm, the world now has billions of sensors, smart devices, embedded systems and cyber-physical components constantly producing huge amounts of data, which is inherently heterogeneous. The data can be used in a variety of applications such as smart agriculture, healthcare, Industrial Internet of Things (IIoT), transportation, smart grid, unmanned aerial vehicle (UAV) networks, supply chain management, smart homes, and intelligent city infrastructures [1]. With increasing deployments for IoT, secure data storage, trusted communications, privacy and fine-grained access control is becoming a big challenge. While traditional cloud-centric storage systems may experience single points of failure, lack transparency, face privacy leakage risks, data tampering, and reliance on trusted third parties, they do not possess these drawbacks. As a result, blockchain technology and InterPlanetary File System (IPFS) have proven to be potential decentralized solutions for managing IoT data securely, transparently, and tamper-proof [2].

Blockchain offers decentralization, immutability, transparency, consensus-based validation, and trusted transaction management, all of which are beneficial for securing sensitive IoT data and distributed digital services. It's

been used in agriculture, healthcare, industrial automation, smart grid, transport, electronic voting, and UAV communication to ensure the integrity of data, authentication and secure data exchange. But, it is inefficient to store large-scale IoT data on the blockchain directly, which causes high costs, storage weight and delays in transactions [3]. IPFS addresses these problems by allowing content-addressable storage, with a focus on decentralization, where large data sets are stored off-chain while blockchain records are kept to store only metadata, cryptographic hashes, and transaction records. The integration of blockchain with IPFS greatly improves the storage scalability, data availability, fault tolerance, and decentralized trust in IoT applications [4].

Yet, these benefits bring with them a major long-term danger to existing blockchain infrastructures – quantum computing. The security requirements of most existing blockchain platforms are based on common public-key cryptographic systems such as the RSA, Elliptic Curve Cryptography (ECC), and Diffie–Hellman key exchange, whose security postulates are vulnerable to attack on a quantum computer that can use Shor's algorithm [5]. In other words, future decentralized applications may be susceptible to digital signatures, authentication techniques, key exchange protocols, and transaction validation procedures. This is especially important for the IoT systems, where the information is often sensitive and demands for long-term confidentiality and integrity [6].

In response to these problems, Post-Quantum Cryptography (PQC) is emerging as a potential solution to secure blockchain-based IoT infrastructures from attacks by quantum computers. PQC is the term used to describe lattice-based cryptographic methods, code-based cryptographic methods, hash-based cryptographic methods, multivariate cryptographic methods and rank-metric cryptographic methods which are resistant to both classical and quantum attackers [7]. In particular, two methods have been studied extensively: lattice based cryptography and Ring Learning with Errors (R-LWE), which have good security properties and are compatible with the current cryptographic standardization process. Additionally, Attribute-Based Encryption (ABE) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) offer fine-grained authorization, as the access policies are based on user attributes, making them suitable for decentralized IoT environments, which include several organizations, users, and services [8].

Next-generation blockchain ecosystems also require cross-chain communication. Today, decentralized applications are increasingly deployed on several different, and often heterogeneous, blockchain environments, needing to safely share digital assets, metadata, authentication credentials, and IoT data [9]. While cross-chain solutions enhance interoperability and resource efficiency, they also pose challenges like bridge attacks, consensus disagreements, high transaction verification complexity, trust management, and increased security risks, which could be exacerbated in the post-quantum era. Hence, combining quantum resistant cryptography and secure cross-chain communication is an interesting focus for future research of blockchain-based IoT systems [10].

Preserving privacy and providing secure access control in decentralized IoT environments are still crucial. IoT devices routinely collect sensitive information related to healthcare, industrial operations, transportation, energy systems, agriculture, and smart infrastructure. Current work has investigated searchable encryption, decentralized identity management, blockchain access control, and zero-knowledge proofs to extend the level of confidentiality and trust [11]. However, many of these solutions focus on a specific application and don't integrate well with other post quantum cryptography, decentralized storage, and interoperable blockchain architectures.

While there has been substantial work done in the field of blockchain security, post-quantum cryptography, attribute-based encryption, decentralized storage, and IoT security, research is still spread across a variety of disciplines. While the majority of studies explore these technologies in isolation or in specific application areas, relatively small number of studies are devoted to possible integration of these technologies in a common architecture for secure, scalable, and quantum-resistant IoT data management [12]. In addition, issues such as computational burden, efficient cryptographic implementation, secure key management, blockchain interoperability, decentralized identity management, standardized performance assessments, and deployment in the real world are still largely unsolved.

In this review, the latest developments in post-quantum blockchain technology for secure data storage and communication for IoT applications are examined [13]. It investigates critically the advancements in blockchain interoperability, post-quantum cryptography, attribute-based encryption, decentralized storage solutions using IPFS, privacy-preserving authentication, and secure access control. Moreover, it sheds light on the future research directions and opportunities to design an interoperable, scalable and quantum resistant blockchain-based IoT ecosystems alongside with technological bottlenecks and open issues in the current research.

The major contributions of this review are summarized as follows:

1. It reviews 42 representative studies that have been published from 2019 to 2026 on topics relating to post-quantum blockchain security, cross-chain communication, attribute-based encryption, decentralized storage, and IoT data protection.
2. It categorises the literature into four key research areas: blockchain and cross-chain communication, post-quantum cryptography and attribute-based encryption, blockchain security and IoT applications, emerging quantum-resistant frameworks for cyber-physical systems and decentralised storage.
3. It has the following features: 3. It compares existing methodologies, cryptographic mechanisms, application domains, security benefits, and implementation limitations.
4. It surfaces relevant research gaps, such as the lack of a single framework that combines the concepts of post quantum cryptography, blockchain interoperability, IPFS, decentralized identity management, attribute-based access control and privacy-preserving communication.
5. It offers a conceptual architecture that identifies future research avenues for secure, scalable, interoperable, and quantum resistant blockchain-based ecosystems for next-generation IoT applications.

The rest of this paper is organised as follows. Section 2 looks at the latest advancements in blockchain interoperability, post-quantum cryptography, attribute based encryption, decentralized storage and IoT security. The identified research gaps are discussed in Section 3. Securing data storage and communication in IoT using blockchain conceptual methodology and proposed architecture is presented in Section 4. Lastly, Section 5 summarizes the paper and provides an outlook for future work.

2. Literature Review

Blockchain, post-quantum cryptography (PQC), attribute-based encryption (ABE), and Internet of Things (IoT) and InterPlanetary File System (IPFS) based decentralized storage has transformed the security landscape of the modern Internet of Things (IoT) data management. The traditional blockchain security mechanisms are facing threats from quantum computers, which makes the need for quantum-resistant cryptographic solutions for secure cross-chain communication, decentralized authentication, privacy-preserving data sharing, and reliable IoT data storage more than relevant. In recent years, research on lattice-based cryptography, blockchain interoperability, zero-knowledge proof, searchable encryption, lightweight authentication, IPFS-based storage and attribute-based access control to improve security has been conducted in the field of smart agriculture, cyber-physical systems, industrial IoT, transportation, smart grids, and UAV networks. Thus, this section surveys the current literature pertaining to three primary research directions.

2.1 Blockchain-Based Secure Cross-Chain Communication and Distributed Applications

In recent years, several studies have focused on building a bridge for secure cross-chain communication.Secure cross-chain communication mechanisms have made significant strides in recent research. Yu and Mu [1] proposed an attribute-based post-quantum cross-chain data sharing solution for smart agriculture, and applied quantum-resistant cryptographic primitives to realize secure and decentralized information sharing. Yi [3] came up with a post-quantum blockchain notary scheme that enhances the trust establishment of cross-chain transactions and lowers the complexity of the verification. Likewise, Qu et al. [5] created an efficient supply-chain based quantum blockchain transaction model to boost the integrity and scalability of transactions in industrial settings.

The security issues of cross-chain transactions have also been thoroughly studied. In particular, Tiwari and Chhetri [4] studied blockchain interoperability vulnerabilities in the quantum era and identified some attack vectors related to blockchain communication systems based on bridges. Siriweera and Naruse [8] introduced the Internet of Cross-Chains paradigm, which introduces blockchain-as-a-service platforms for smart city applications by using model-driven interoperability. In addition, Chen et al. [30] suggested an attribute-encryption-based cross-chain system for IoV applications incorporating blockchain and secure access control.

In addition to interoperability, blockchain has been successfully applied to different application areas. Luo et al. [9] summarized AIoT-related data management techniques in smart agriculture, focusing on smart traceability and intelligent decision-making by means of blockchain. Fattahzadeh et al. [10] were able to identify the significance of blockchain in agricultural supply chain management in order to preserve the transparency and authenticity of the agricultural products. Pandit et al. [21] introduced a mutual authentication protocol based on ECC for secure agricultural communication, and Zhang [25] designed a blockchain-based CP-ABE system for secure agricultural product traceability.

Blockchain applications have grown to include geospatial computing, electronic voting, smart grids, healthcare, industrial IoT, and transportation. Gu et al. [19] discussed the use of blockchain in automotive industrial value chains and Rupa et al. [20] introduced a distributed ledger system for electronic voting in order to create secure voting systems. Ghadi et al. [16] combined blockchain and AI to enhance the cybersecurity in smart grids. Srinivasarao et al. [40] also improved energy transactions with the help of blockchain technology for security. Latif et al. [39] proposed a multi-factor authentication system for e-health applications based on blockchain; and Saraya et al. [41] introduced a blockchain-based Geo-Blockchain Intelligence Risk Assessment for secure geospatial computing ecosystems. Kumar and Khari [42] conducted a thorough bibliometric study of security approaches in the Privacy-preserving Blockchain framework for Industrial Internet of Things (IIoT) environments, highlighting the growing utilization of decentralized security architectures in the emerging digital infrastructures.

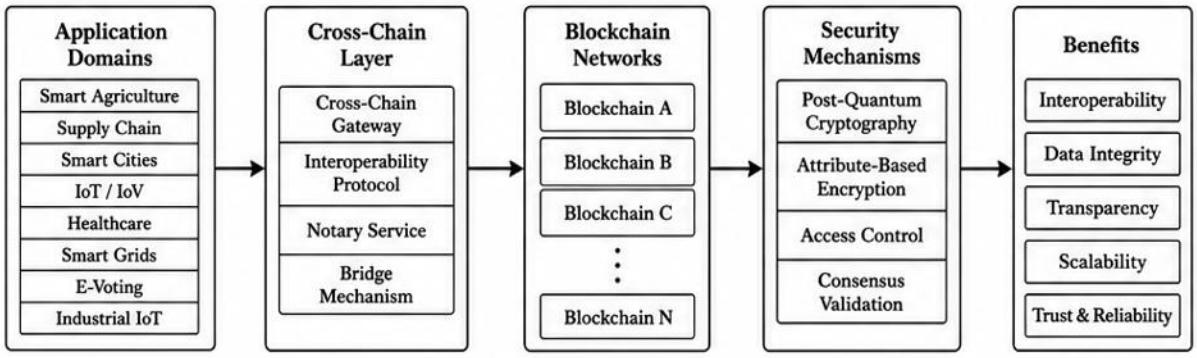

Figure 1. Framework of Secure Cross-Chain Blockchain Communication

This figure 1 represents a safe cross-chain blockchain interaction model that incorporates various blockchain networks via blockchains interoperability protocols, cross-chain gateways, and blockchain notary services. It integrates post-quantum cryptography, attribute based encryption, access control and other systems to provide secure business validation, data integrity, interoperability, transparency, scalability, and trusted communication in decentralized applications such as smart agriculture, IoT, healthcare, supply chain management, and smart city infrastructure.

2.2 Post-Quantum Cryptography and Attribute-Based Encryption for Secure Data Protection

Post-quantum cryptography is emerging as one of the most promising solutions for ensuring the security of distributed systems in the face of quantum computing attacks. Yousefipoor and Eghlidos [7] introduced a code based efficient attribute based encryption scheme with a rank metric, which provides high security guarantees and has low computation overhead in cloud computing environments. In the work of Zhao [23] provided a revocable lattice-based ABE scheme based on Ring Learning with Errors (R-LWE) problem for fine-grained access control for cloud storage. Yang [24] then followed this work by developing a practical revocable multi-authority CP-ABE scheme for scalable cloud applications.

Chen [28] introduced a CP-ABE system based on lattices and combined with blockchain to facilitate secure decentralized data sharing, and Sravya et al. [11] reviewed the latest techniques of lattice-based CP-ABE and pointed out the existing research challenges concerning scalability, revocation, computational cost, and access policy management. The transportation system's secure post-quantum searchable encryption framework is proposed in [6] that provides privacy-preserving searching of encrypted datasets. To enhance the search efficiency and authenticity of data, Perera and Fugkeaw [18] proposed a light-weight verifiable post-quantum attribute based searchable encryption scheme with provenance-aware verification for IoT-enabled healthcare system.

Recent research has broadened the use of PQC to cloud forensics, digital healthcare, cyber physical systems and distributed communication networks. Fugkeaw et al. [29] proposed an optimized post-quantum AB logging mechanism in tamper-evident cloud forensic investigation. Abugabah [31] combined multimodal transformers and post-quantum cryptography to enable the secure operation of intelligent healthcare cyber-physical systems. Hasib et al. [34] conducted a structured review of lattice based ABE techniques and summarized the existing research trends, open challenges and implementation issues. Narsimhulu et al. [35] introduced a lightweight post-quantum signature aggregation method for low-latency distributed systems while Shirisha et al. [37] examined the resource-efficient post-quantum security frameworks appropriate for resource-limited IoT devices. The integration of AI with quantum-

resistant technologies, as seen in the work of Degala and Athithan [38] on enhancing the resilience of cyber-physical systems against future quantum cyber threats, highlights how AI is becoming more deeply intertwined with quantum security solutions.The convergence of AI with quantum-resistant technologies, as exemplified in the study by Degala and Athithan [38] for enhancing the resilience of cyber-physical systems against future quantum cyber threats, underscores the integration of these two realms.

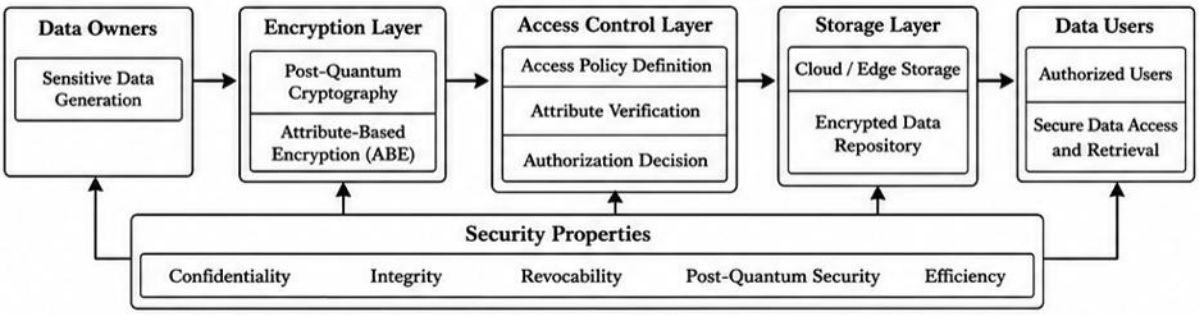

Figure 2. Post-Quantum Attribute-Based Encryption Framework for Secure Data Protection

This figure 2 shows an architecture of post-quantum attribute-based encryption (PQ-ABE) for secure data protection in the cloud and edge computing environment. The diagram illustrates how data owners, encryption modules, access control policies, encrypted storage repositories, and authorized users interact. It's focused on confidentiality, integrity, fine-grained access control, revocability, secure data retrieval, and quantum-resistant protection of distributed cloud, IoT and cyber-physical applications.

2.3 Blockchain Security, IoT Privacy, and Emerging Research Directions

With its decentralized trust, immutability, secure authentication, and privacy-preserving communication, blockchain technology has emerged as a cornerstone of security in today's Internet of Things (IoT) landscape. Recent research has been primarily focused on enhancing the blockchain infrastructure by using Post-Quantum Cryptography, secure authentication protocols, decentralized storage, and lightweight cryptographic mechanisms for resource-constrained IoT devices. Alharbi and Almazmomi [2] put forward a security mechanism for smart agriculture that utilizes blockchain technology and considers the future threat of quantum computers. Cao et al. [32] proposed a blockchain-based privacy-preserving authentication protocol for secure cross-domain UAV communication, and Tychola et al. [13] illustrated that blockchain can be used to greatly enhance trust management, decentralized identity verification, and secure communication in the context of IoD.

Additionally, blockchain has been widely used in conjunction with IoT and decentralized networking technologies to enhance data integrity and transparency, while facilitating secure and reliable information sharing. One of the first and more comprehensive overviews of distributed ledger technologies for IoT was provided by Zhu et al. [14] where the authors described blockchain as a bedrock for decentralized trust and secure data management. Wijesekara and Gunawardena [15] discussed the adoption of blockchain in the context of knowledge-defined networking and how it can enhance the transparency of the network, decentralized resource management, and secure communications. Pramanik et al. [17] introduced a decentralized data management framework using blockchain for the cellular IoT system, which facilitates trustworthy communication between the distributed edge devices. Also, Ismail et al. [36] proposed a blockchain-based IoT architecture that not only improves energy efficiency, privacy preservation, and secure communication in smart homes but also resolves issues like privacy and security in the IoT ecosystem. Verkle tree-based key exchange was also used by Simbu et al. [33] in their smart contract architecture for blockchain to improve secure device-to-device communications.

To increase blockchain's resistance and privacy protection in distributed environments, several complementary security mechanisms have been proposed. Sindiramutty et al. [22] showed the benefits of blockchain for data integrity and secure transaction handling in cybersecurity applications. Su et al. [27] presented an efficient solution to defend against double-spending attacks in consortium blockchain networks in network partitioning environment. In the context of future networks, 5G and beyond, Szczegielniak-Rekiel et al. [26] comprehensively surveyed the zero-knowledge proof (ZKP) techniques, their importance for privacy-preserving authentication, decentralized identity verification, and confidential transaction validation. In addition, secure searchable encryption, decentralized logging,

and lightweight authentication were highlighted as important elements to safeguard large-scale blockchain-based IoT infrastructures [18] [29] [39].

Overall, the literature reviewed shows that there has been significant progress in the security of blockchain networks, post-quantum cryptography, decentralized authentication, IoT privacy, and secure communication. Most of the current research, however, examines these technologies individually, or in specific application areas. The integration of post-quantum cryptography, blockchain interoperability, IPFS-based decentralized storage, attribute-based encryption, secure cross-chain communication, lightweight authentication, decentralized identity management, and privacy-preserving IoT data sharing, all in one comprehensive framework, is still limited [43]. The realization of a unified post-quantum blockchain-IPFS architecture that offers scalable, quantum-resistant, privacy-preserving and secure storage and communication for next generation IoT and cyber-physical systems is motivated by this research gap.

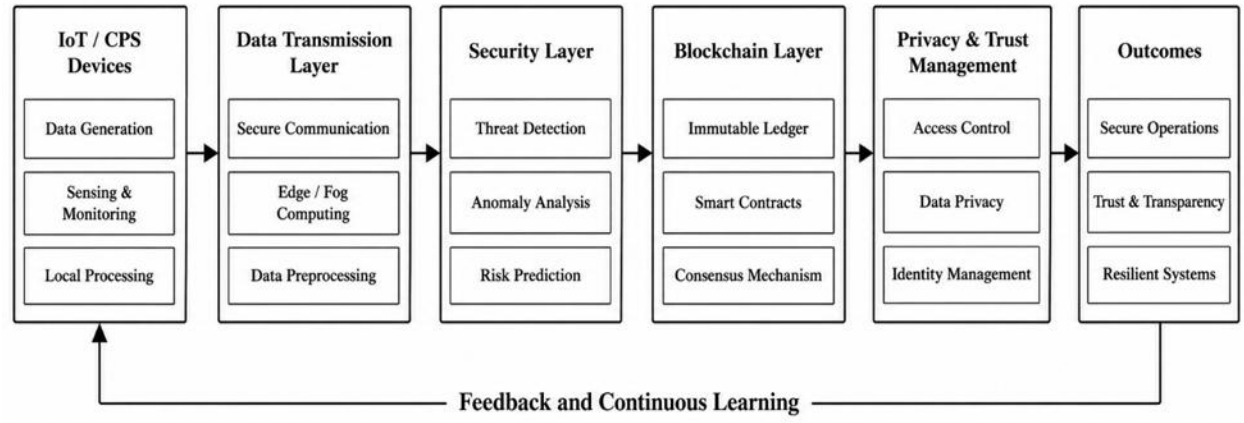

Figure 3. Conceptual Architecture of the Post-Quantum Blockchain Framework for Secure IoT Data Storage and Privacy-Preserving Communication

The proposed post-quantum blockchain architecture is depicted in Figure 3, where users' data is securely stored, communicated, and managed in a trustworthy way for Internet of Things (IoT) and Cyber-Physical Systems (CPS). Its framework starts with IoT/CPS devices which continuously generate, sense, monitor, and locally process data and then send the data via a secure communication layer that uses edge/fog computing and data processing. The processed data are then shielded in a special security layer, which conducts threat detection, anomaly analysis and risk evaluation to improve the resilience of the system. The blockchain layer is responsible for recording data in an immutable way, executing smart contracts, and verifying decentralized consensus, ensuring that the data is not tampered with and remains transparent and accurate. By ensuring access is controlled at a granular level, enforcing data privacy, and managing decentralized identities, privacy and trust management are ensured, allowing sensitive data to be shared securely among authorized entities and users. Last but not least, the framework provides secure operations, trusted transactions, increased transparency, and resilient IoT services, with a continuous feedback loop to enable further monitoring, adaptive security enhancement, and long-term operation of next generation quantum-resistant IoT ecosystems.

Table 1: Blockchain, Cross-Chain Communication & Smart Agriculture

Author	Year	Area	Method / Technology	Key Contribution	Limitation / Research Gap
Yu *et al.*	2024	Smart agriculture	Post-quantum ABE and cross-blockchain exchange	Secure data exchange across agricultural blockchains	Needs broader real-time deployment validation
Alharbi *et al.*	2025	Smart agriculture security	PQC, blockchain, GNN threat detection	Improves blockchain security using AI-based attack detection	High computational cost for large-scale farms

Yi	2023	Cross-chain exchange	Post-quantum blockchain notary	Provides quantum-resistant notary scheme for cross-chain transactions	Limited evaluation under heterogeneous blockchain networks
Tiwari *et al.*	2025	Blockchain interoperability	Quantum-era threat analysis	Identifies cross-chain vulnerabilities under quantum attacks	Mainly analytical; lacks implemented defense model
Qu *et al.*	2025	Supply chain blockchain	Quantum blockchain cross-chain transaction scheme	Enhances secure cross-chain transaction efficiency	Requires practical validation in real supply-chain systems
Siriweera *et al.*	2023	Smart cities	Cross-chain as a service	Enables model-driven cross-chain services for IoE applications	Security against quantum threats is not deeply addressed
Luo *et al.*	2025	Smart agriculture	AIoT data management review	Reviews AIoT, blockchain, and data management technologies	Requires integrated security framework
Fattahzadeh *et al.*	2024	Agriculture supply chain	Blockchain review	Highlights blockchain reliability in agricultural traceability	Limited focus on PQC-based future security
Pandit *et al.*	2024	E-agriculture	ECC-based authentication	Provides mutual authentication for agricultural systems	ECC may be vulnerable in post-quantum environments
Zhang	2022	Agricultural traceability	Blockchain and CP-ABE	Secures product traceability using blockchain and access control	Revocation and scalability issues remain

A summary of the recent blockchain interoperability, cross-chain communication, and smart agriculture applications can be seen in Table 1. The reviewed papers reveal that blockchain technology has been applied in a way that has greatly enhanced decentralized transactions in data exchange, traceability in the supply chain, and secure agricultural information management. New developments combine post-quantum cryptography (PQC), attribute-based encryption (ABE), artificial intelligence (AI), graph neural networks (GNNs), and blockchain notary mechanisms to bolster the security of cross-chain operations and boost trust among decentralized blockchain networks. The creation of smart agriculture has become one of the key application fields in which blockchain can contribute to product traceability, sharing of sensor data and transparent supply chain management. Despite the progress made, most of the current research work is concentrated on the domain-specific solutions and few focus on unified solutions that solve the challenges of cross-chain interoperability, quantum-resistant cryptography, scalability, lightweight communication, and fast deployment. Therefore, it is crucial to research and develop an integrated post-quantum blockchain architecture that can provide secure, scalable and intelligent cross-chain communication.

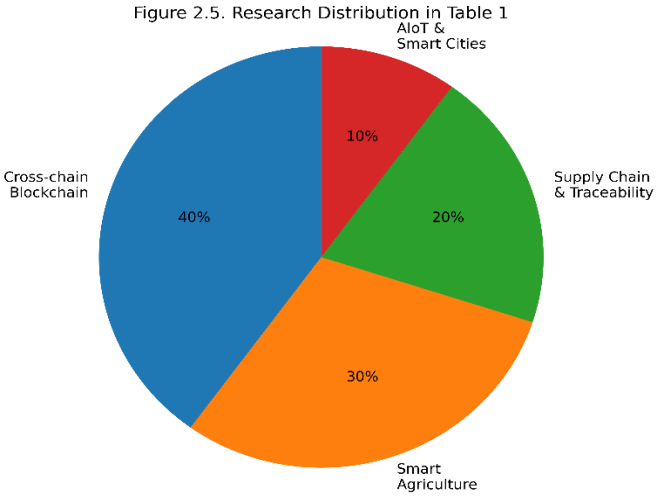

Figure 4. Research Distribution of Blockchain, Cross-Chain Communication, and Smart Agriculture Studies

The thematic distribution of the 10 research articles summarized in Table 1 is presented in Figure 4. The most popular research areas are cross-chain blockchain communication (40%), indicative of growing interest in securing blockchain interoperability and decentralized data exchange. The second largest research area is smart agriculture (30%), which focuses on the sharing of agricultural information with the help of blockchain, as well as applications of smart agriculture. Supply chain and agricultural traceability (20%) reflects the increase in blockchain's application of transparent product tracking and secure supply chain, and AIoT and smart city applications (10%) illustrate the new trend of blockchain's linking with intelligent connected infrastructures. Overall, the figure shows that the current research focuses are mostly on secure cross-chain architectures and then slowly moving towards AI-based and domain-specific blockchain applications.

Table 2: Post-Quantum Cryptography, ABE & Secure Data Sharing

Author	**Year**	**Area**	**Method / Technology**	**Key Contribution**	**Limitation / Research Gap**
Thingom	2026	Transportation systems	PQ attribute-based searchable encryption	Enables secure searchable encryption for edge transportation	Needs lightweight optimization for constrained devices
Yousefipoor et al.	2023	Cloud computing	Rank-metric post-quantum ABE	Provides efficient quantum-resistant cloud data protection	Practical cloud-scale deployment not fully explored
Sravya et al.	2024	Cloud storage	Lattice-based CP-ABE survey	Reviews taxonomy, challenges, and future scope of PQ-ABE	Requires unified implementation benchmark
Perera et al.	2026	IoT healthcare	Lightweight verifiable PQ-ABSE	Supports secure EHR search with	Healthcare interoperability

				provenance verification	remains challenging
Zhao	2022	Cloud storage	Revocable lattice ABE using R-LWE	Enables revocable access control for encrypted cloud data	Revocation overhead may increase with users
Yang	2022	Cloud computing	Multi-authority CP-ABE from RLWE	Supports practical revocable multi-authority access control	Complex authority coordination
Chen	2023	Blockchain data sharing	LWE-based CP-ABE and blockchain	Combines blockchain with lattice-based access control	Needs performance validation in large networks
Fugkeaw et al.	2026	Cloud forensics	PQ attribute-based logging	Provides tamper-evident forensic logging	Storage overhead may be high
Hasib et al.	2026	PQC review	Lattice-based ABE review	Reviews PQ-ABE methods for post-quantum security	Highlights lack of standard benchmarks
Narsimhulu et al.	2026	Distributed networks	PQ signature aggregation	Reduces latency in distributed secure authentication	Needs testing in dynamic network environments

Table 2 is a systematic review of the recent development in the area of post-quantum cryptography (PQC), attribute-based encryption (ABE), searchable encryption, and secure cloud data sharing. The surveyed literature indicates that lattice-based cryptography, Ring Learning with Errors (R-LWE), rank-metric codes, ciphertext-policy attribute-based encryption (CP-ABE), searchable encryption, and provenance-aware verification are emerging solutions to secure cloud and edge computing systems against future quantum attacks. There are a few studies that aim at enhancing the access control granularity, data confidentiality, revocation policy, and lightweight encryption for cloud computing, healthcare, transportation and forensic applications. While these methods substantially increase quantum-resistant security, most of the current solutions still suffer from high computational complexity, large key sizes, revocation overhead, and scalability limitations. In addition, there are limited studies that combine all three technologies - blockchain, AI, and quantum-resistant cryptography - into one secure data-sharing platform, suggesting significant research potential.

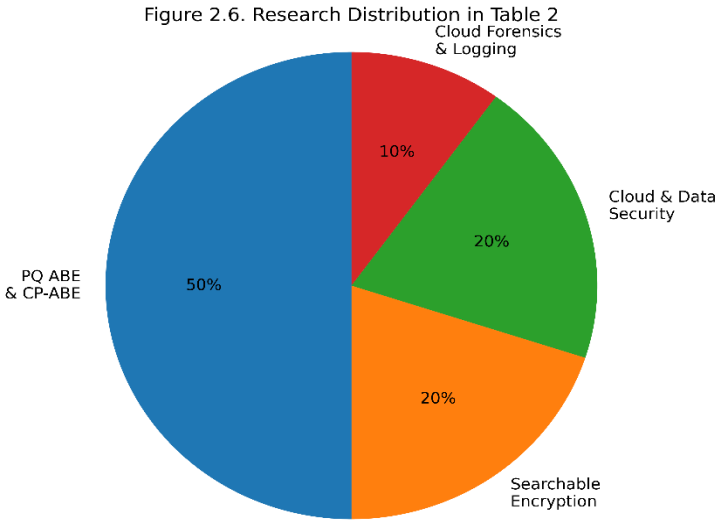

Figure 5. Research Distribution of Post-Quantum Cryptography, Attribute-Based Encryption, and Secure Data Sharing Studies

The thematic distribution of the ten research articles summarized in Table 2 is presented in Figure 5. The two greatest research interests are Post-Quantum Attribute-Based Encryption (ABE) and Ciphertext-Policy ABE (50%), reflecting the increasing significance of lattice-based cryptographic methods for fine-grained control over access rights and secure cloud computing in the quantum era. Secondly, searchable encryption (20%) is one of the main research directions which focus on secure retrieval of keywords from encrypted datasets in transportation and healthcare systems. Cloud and secure data-sharing mechanisms (20%) explore solutions to post-quantum cryptographic problems for confidentiality, access control, and scalable cloud storage, while cloud forensics and tamper-evident logging (10%) deals with maintaining data integrity and forensic accountability. Current studies tend to be focused on lightweight, scalable, and quantum-resistant encryption schemes for next-generation cloud, edge, and Internet of Things (IoT) environments.

Table 3: Blockchain Security, IoT, Industrial Applications

Author	**Year**	**Area**	**Method / Technology**	**Key Contribution**	**Limitation / Research Gap**
Alsadie	2025	UAV cybersecurity	AI-based countermeasures	Reviews AI cybersecurity challenges in UAV systems	Requires integration with PQC security
Tychola *et al.*	2024	Internet of Drones	Blockchain-enabled drone networks	Improves trust and decentralized drone communication	Energy and latency constraints remain
Zhu *et al.*	2019	IoT	Distributed ledger survey	Establishes blockchain applications for IoT security	Pre-PQC perspective
Wijesekara *et al.*	2023	Knowledge-defined networking	Blockchain review	Reviews blockchain benefits for intelligent networking	Lacks quantum-resilient architecture
Ghadi *et al.*	2025	Smart grids	Hybrid AI-blockchain framework	Enhances smart grid cybersecurity	PQC integration is limited
Pramanik *et al.*	2025	Cellular IoT	Blockchain-based decentralized management	Secures distributed IoT data management	Scalability in dense IoT networks remains open

Gu *et al.*	2025	Automotive industry	Blockchain applications	Reviews blockchain use in automotive value chains	Needs stronger privacy-preserving mechanisms
Rupa *et al.*	2022	E-voting	Distributed ledger voting system	Improves voting reliability and statistical verification	Quantum-safe voting security not addressed
Sindiramutty *et al.*	2025	Cybersecurity	Blockchain data integrity	Shows blockchain role in secure transaction management	Needs AI and PQC integration
Su *et al.*	2025	Consortium blockchain	Double-spending defense	Protects consortium blockchain under network partitioning	Limited cross-chain and PQC coverage

The research work related to blockchain security, Internet of Things (IoT), artificial intelligence, industrial application, and decentralized cybersecurity framework is reviewed in Table 3. The chosen research papers are a proof of successful solution blockchain technology has found in UAV networks, Internet of Drones, Industrial IoT, smart grid, automotive systems, electronic voting, cellular IoT and cyber security infrastructure. AI also plays a significant role in improving the blockchain's performance by providing intelligent threat detection, anomaly detection, adaptive access control, and automated decision-making. Moreover, in the future communication networks, zero-knowledge proof (ZKP) and decentralized ledger technologies enhance privacy protection and authentication. Still, most existing studies focus on a single technology, and there has been little work that proposes to integrate post quantum cryptography, blockchain interoperability, intelligent threat detection, lightweight authentication and decentralized privacy protection within a single architecture. This is a reminder of the importance of comprehensive security architecture for new distributed cyber-physical areas.

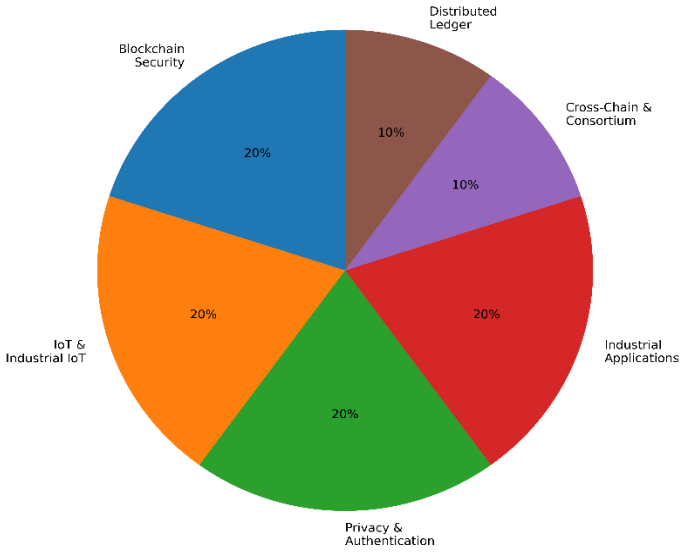

Figure 6. Keyword-Based Research Distribution of Blockchain Security, IoT, and Industrial Applications

The keyword based thematic distribution of the summarized studies shown in Table 3 is presented in figure 6. Literature found and reviewed is divided into six major categories as follows: Blockchain Security (20%), IoT and Industrial IoT (20%), Privacy and Authentication (20%), Industrial Applications (20%), Cross-Chain and Consortium Blockchain (10%), and Distributed Ledger Applications (10%). The distribution shows that the studies conducted recently are mainly on improving the security of blockchain, secure communication in the IoT, decentralized authentication and the industrial deployment of blockchain, whereas there are still fewer studies on cross-chain security related to blockchain and general enough applications of distributed ledger technologies. The results underscore the need for more efficient, integrated post-quantum blockchain solutions, IPFS-based decentralized storage, attribute-based encryption, and communication solutions that preserve privacy while enabling secure and scalable future IoT environments.

Table 4: Latest 2026 Research on PQC, Blockchain, AI & Cyber-Physical Systems

Author	Year	Area	Method / Technology	Key Contribution	Limitation / Research Gap
Abugabah	2026	Digital healthcare	PQ-secure multimodal transformer	Secures medical cyber-physical systems using AI and PQC	Requires real hospital deployment validation
Cao *et al.*	2026	UAV communication	Blockchain-based privacy authentication	Enables cross-domain UAV authentication	Scalability under large UAV swarms remains open
Simbu *et al.*	2026	D2D communication	Smart contract and Verkle tree key exchange	Secures device-to-device communication	Practical latency evaluation is needed
Ismail *et al.*	2026	Smart homes	Blockchain-based IoT framework	Improves privacy and energy efficiency	Needs stronger PQC integration
Shirisha *et al.*	2026	Resource-constrained systems	PQ security framework review	Reviews PQC trends for constrained devices	Lightweight implementation remains challenging
Degala *et al.*	2026	Cyber-physical systems	PQC and deep learning	Strengthens CPS resilience against quantum cyber threats	Needs standard dataset validation
Latif *et al.*	2026	E-health	Blockchain MFA and PQ security	Combines MFA, access control, blockchain, and PQC	Complex integration in real healthcare systems
Srinivasarao *et al.*	2026	Smart grid	Blockchain and cybersecurity	Secures energy transactions and data privacy	Real-time smart grid testing is required
Saraya *et al.*	2026	Geospatial big data	Geo-blockchain risk assessment	Reviews secure geospatial blockchain ecosystems	Needs implementation framework
Kumar *et al.*	2026	Industrial IoT	Privacy-preserving bibliometric analysis	Identifies trends in IIoT data privacy	Lacks experimental security model
Chen	2024	Internet of Vehicles	Attribute-encryption cross-chain model	Provides secure cross-chain access for urban vehicles	Needs post-quantum strengthening
Szczegielniak-Rekiel *et al.*	2025	5G and beyond	Zero-knowledge proof review	Reviews ZKP for privacy and authentication	Integration with PQC-blockchain systems remains open
Sunil Parihar and Jigyasu Dubey	2021	Post-Quantum Blockchain for Internet of Things (IoT)	Review of Blockchain, Post-Quantum Cryptography (PQC), and IoT Security	Presented one of the early reviews highlighting the integration of blockchain and post-quantum cryptography to improve security, privacy, and trust in IoT ecosystems while identifying future research directions for	Conceptual review only; lacks IPFS integration, cross-chain interoperability, attribute-based encryption, decentralized identity management, performance benchmarking, and experimental validation for large-

				quantum-resistant blockchain networks.	scale IoT environments.

The current research contributions, as shown in Table 4, are the most recent publications to the community, corresponding to the trends in post-quantum cryptography, blockchain, artificial intelligence, cyber-physical systems, healthcare, IoT, UAV communication, smart grid and geospatial computing. The reviewed studies show a strong interest in the use of deep learning, multimodal transformers, blockchain-based authentication, multi-factor authentication, Verkle tree structures, energy-efficient security mechanisms, and lightweight post-quantum cryptographic protocols, as a way to improve the security to address future threats posed by quantum computers. The focus of research has been on the design of scalable, privacy preserving and intelligent security architectures to support real-time distributed applications. Several obstacles still need to be addressed, however, such as interoperability between different blockchain systems, lightweight quantum-resistant implementations, restricted resource systems on IoT, benchmarking frameworks, and standardized frameworks. Moreover, future studies and research should focus on creating a single and AI based post-quantum blockchain security framework that provides secure, scalable, energy-efficient, and intelligent protection in future cyber-physical and distributed computing environments.

Figure 2.8. Research Distribution in Table 4

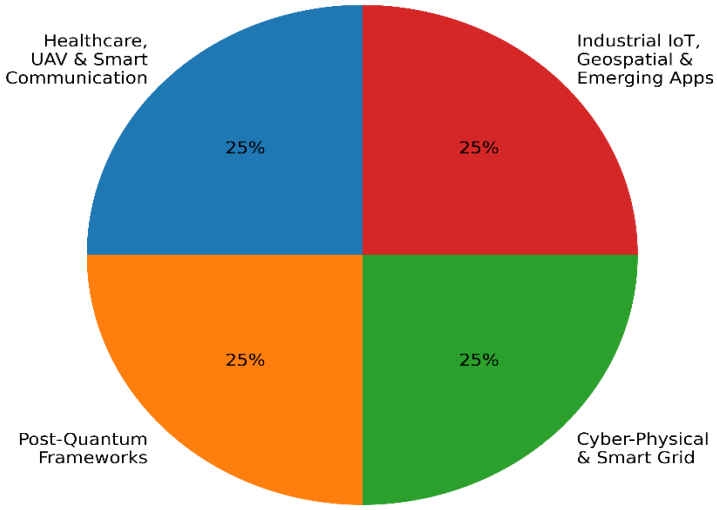

Figure 7. Research Distribution of Latest 2026 Studies on Post-Quantum Cryptography, Blockchain, Artificial Intelligence, and Cyber-Physical Systems

Figure 7 shows the thematic distribution of the last 12 articles reported in Table 4. The reviewed studies are evenly distributed into four primary research areas: Healthcare, UAV and Smart Communication (25%), Post-Quantum Security Frameworks (25%), Cyber-Physical Systems and Smart Grid Security (25%) and Industrial IoT, Geospatial and Emerging Blockchain Applications (25%). Very balanced distribution means that current research is focused on the integration of post-quantum cryptography, blockchain technology, artificial intelligence, lightweight authentication, privacy-preserving communication and intelligent cyber-physical security. The figure emphasizes the demand for scalable, quantum-resistant, and AI-driven security solutions to provide support for the next generation of distributed computing, smart healthcare, Industrial IoT, autonomous systems and sustainable digital infrastructures.

3. Research Gap

The detailed analysis of the literature selected shows that there is significant advancement in the use of blockchain technology, post-quantum cryptography (PQC), attribute-based encryption (ABE), decentralized storage, and security in the Internet of Things (IoT). The existing research efforts have been able to tackle several discrete components, such as blockchain authentication, cross-chain communication, lattice-based and searchable encryption, decentralized cloud storage, and privacy-preserving communication. Smart agriculture and healthcare, Industrial IoT, cyber-physical systems, transportation, smart grid and unmanned aerial vehicles (UAVs), and supply chain management are all fields where blockchain has been applied, and post-quantum cryptographic methods have significantly increased the resistance to attacks by quantum computers by using lattice-based encryption, revocable access control, and secure searchable encryption mechanisms.

Nevertheless, the existing literature is very fragmented, and many studies address only particular security components and do not offer the integration. The main focus of blockchain-based frameworks is on secure transaction handling, decentralized trust, or data sharing for particular app usages without the standardized post-quantum cryptographic mechanisms. On the other hand, numerous post-quantum cryptographic solutions are designed for secure data encryption and access control, but struggle to integrate with blockchain networks, decentralized data storage solutions, and cross-chain messaging. A single blockchian architecture, which can support flexible authentication, secure storage, interoperability and scalability of IoT communication, is still missing.

Secure authentication for IoT devices in post quantum blockchain systems is an important research gap. While blockchain-based authentication, decentralized identity management, and attribute-based access control have garnered a lot of attention, the current solutions are typically intended for traditional cryptographic systems and are susceptible to potential future quantum attacks. Additionally, lightweight authentication methods for resource-limited IoT devices remain scarce, especially in the context of heterogeneous and cross-chain blockchain networks.

Another major challenge is secure distributed storage of large volume of IoT data. Current blockchain solutions do not address the storage of large IoT datasets, as they simply do not have enough on-chain storage space, a high transaction fee, and latency. While blockchain–IPFS integration has grown as an interesting decentralized storage solution, there are relatively few studies that integrate IPFS with post-quantum cryptography, attribute-based encryption, secure key management and fine-grained access control in a single storage solution. Furthermore, the problem of secure metadata management, efficient content retrieval, decentralized key distribution, and long-term quantum-resistant data protection are poorly understood.

Scale-ability is another significant research problem. Many of the current blockchain IoT solutions are plagued by the issues of transaction latency, communication load, storage redundancy, consensus complexity, and limited transaction throughput. Several studies have explored cross-chain communication and blockchain bridges and interoperability protocols, but relatively little effort has been focused on scalable post-quantum blockchain architectures to seamlessly accommodate millions of heterogeneous IoT devices with low computational overhead and high transaction efficiency. Moreover, lightweight consensus mechanisms, optimized integration of blockchain–IPFS, efficient cross-chain verification, scalable quantum-resistance communication protocols are still open research questions.

In a security sense, most of the existing protocols focus on a single security aspect such as authentication, encryption, privacy protection or access control. Although the use of post-quantum authentication, attribute-based encryption, decentralized identity management, cross-chain communication, blockchain–IPFS storage, zero-knowledge proof, secure key management, and privacy-preserving access control is a necessity, the combination of these in comprehensive security architectures is still quite rare. This makes it difficult to find existing solutions that can offer end-to-end security of IoT data over its entire lifecycle, from data generation to transmission, storage, retrieval and sharing across different blockchain networks.

Another point of weakness seems to be a lack of benchmarking and practical performance assessment. Most studies validate their approach by simulation environment or theoretical security analysis and relatively few actually test it in practice, taking into account latency, scalability, computational complexity, storage overhead, communication cost, energy consumption, and interoperability between different blockchain platforms. There are no common datasets, standards and experimental frameworks in the existing post-quantum blockchain solutions, which makes it hard to compare them on an objective basis.

The recently published research papers for the year 2025–2026 reflect the increasing interest in the integration of post-quantum cryptography, blockchain interoperability, lightweight encryption, decentralized storage, and secure authentication. However, most of these contributions are application-specific and cannot solve a wide range of Quantum resistant security, secure IoT data storage, authentication and scalability. Thus, there is ample research potential to create a single post-quantum blockchain design appropriate for future decentralized IoT systems.

Based on these research gaps, this research proposes to design a single post-quantum blockchain solution for secure IoT environments. The proposed framework aims to achieve four main goals: (i) design a novel quantum-resistant authentication mechanism for IoT devices, (ii) develop a distributed storage architecture for IoT data based on blockchain–IPFS with efficient communication and storage mechanisms, (iii) enhance the scalability of post-quantum blockchain networks, and (iv) create an integrated security framework that incorporates post-quantum cryptography, attribute-based encryption, decentralized identity management, and cross-chain communication to ensure end-to-end security for IoT data throughout its lifecycle.

4. Methodological Analysis of Existing Research

With the development of blockchain technology, post-quantum cryptography, decentralized storage, and secure communication protocols, researchers are exploring various approaches to safeguarding Internet of Things (IoT) data from new threats in cyberspace. The studies in this review show that none of the methods can stand alone to meet all the requirements of secure data storage, decentralized trust, privacy protection, quantum resistance, and cross-chain interoperability. To this end, researchers have suggested a number of cryptographic, blockchain, authentication, decentralized storage, and privacy-preserving methods that can help resolve these issues. This section presents a critical review of the main methodologies used in the examined literature and their benefits, drawbacks and suitability for the next generation of blockchain-supported IoT ecosystems.

4.1 Blockchain-Based Methodologies

In today's Internet of Things (IoT) ecosystems, blockchain technology has emerged as the core approach to building decentralized trust, data immutability, secure transactions, and clear data sharing. A key distinction between traditional centralized architectures is that blockchain shares transaction records across several participating nodes, which means there are no single points of failure and so the system is more reliable and tamper-resistant than traditional systems [14]. The literature surveyed shows that blockchain methods have developed from basic use on distributed ledgers to advanced systems capable of securely sharing data, managing decentralized identities and enabling interoperability between different domains [15].

Many researchers have used blockchain techniques to protect different application areas such as smart agriculture, healthcare, transportation, industrial automation, and cyber physical systems [10]. In smart agriculture, blockchain has been applied to create trustworthy data-sharing between the farmers, suppliers, consumers and government agencies, and ensure transparency and traceability of the data in the whole agricultural value chain [1]. Likewise, blockchain-based decentralized transaction management has been applied into the trust and security area within Industrial IoT and cellular IoT area, where the information exchange and modification can be done reliably and securely, respectively, without being modified by unauthorized users [17].

Consortium blockchain and permissioned blockchain have been highlighted in recent studies due to their increased scalability, participation control, and reduced computational requirements as compared to traditional public blockchain networks [27]. The use of smart contracts, which automate transaction execution, access control and policy enforcement without intermediaries, is also a vital element of blockchain methods [33]. Besides, blockchain interoperability is becoming a key methodological direction that aims to enable the secure exchange of digital assets, metadata, authentication credentials, and transaction records between diverse blockchain platforms via the mechanisms of cross-chain communication [5].

Although these developments have been made, the current blockchain methodologies still suffer from issues such as storage overhead, transactions latency, consensus complexity, interoperability, and long-term cryptographic security [3]. The majority of blockchain implementations continue to work with traditional public-key cryptography which could be broken using quantum computers in the future, and which makes it imperative to incorporate post-quantum cryptographic mechanisms into blockchain architectures [4]. Thus, several recent studies have been dedicated to the development of blockchain technologies that can also be used for quantum-resistant communication, decentralized storage, secure authentication and cross-chain interoperability, so that they can support next generation IoT ecosystems [30].

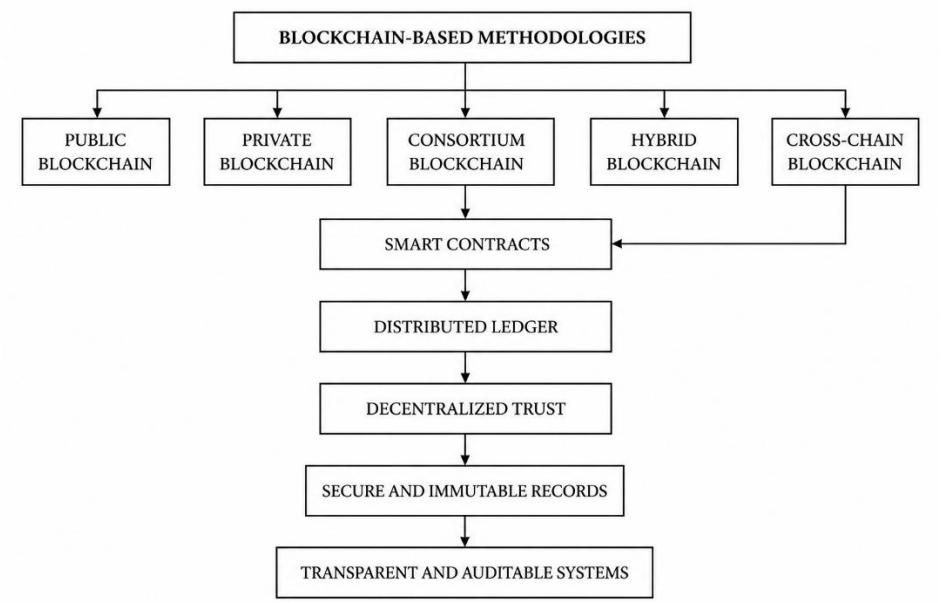

Figure 8. Classification of Blockchain-Based Methodologies for Secure and Decentralized IoT Data Management

Figure 8 shows the classification of blockchain-based methodologies that have been identified based on the reviewed literature for the development of secure, decentralized and trustworthy Internet of Things (IoT) data management systems. To serve various application needs of decentralization, scalability, governance and interoperability, five major blockchain architectures are introduced in the methodology, including Public Blockchain, Private Blockchain, Consortium Blockchain, Hybrid Blockchain and Cross-Chain Blockchain. Within this, consortium and cross-chain blockchain technologies also play a key role in designing smart contracts for their execution, facilitating automated transaction processing, policy enforcement, and secure data transmission across different blockchain networks. The transactions are then added to a distributed ledger, which guarantees that they are stored securely, verified openly, and reached to a consensus by a distributed network. This decentralized trust approach ensures that data is both authentic and reliable, while also providing a layer of security that prevents unauthorized modifications, leaving records secure and immutable throughout the blockchain lifecycle. Lastly the methodology brings transparent and auditable systems, which allow trusted transaction management, secure information sharing, decentralized governance and reliable record verification, for large-scale applications like IoT, Industrial IoT, healthcare, smart agriculture, transportation, cyber-physical systems and decentralized storage environments. Overall, the figure summarizes the evolution of blockchain methodologies towards secure, interoperable and scalable decentralized infrastructures, appropriate for next-generation post-quantum blockchain ecosystems.

4.2 Post-Quantum Cryptographic Methodologies

The advent of quantum computing marked a huge change in the landscape of new cryptographic methods that are capable of securing the blockchain-powered Internet of Things (IoT) network from potential attacks in the future [7]. Conventional public-key cryptographic algorithms, such as RSA and Elliptic Curve Cryptography (ECC), can be compromised by Shor's quantum algorithm, which is why focusing on post-quantum cryptography is a critical research area for the security of blockchain-based systems. In recent years, there has been a growing focus on using lattice-based cryptography, code-based cryptography, rank-metric cryptography, multivariate cryptography, and hash-based signature schemes as potential quantum-resistant alternatives [11].

Lattice-based cryptography is now one of the most popular cryptographic techniques, largely due to its solid mathematical basis and its ability to be compatible with the existing post-quantum standardization process [23]. Weeks widely used to build secure cryptanalysis-resistant encryption algorithms that are classical- and quantum-resistant, and have reasonable computational complexity, are Learning With Errors (LWE) and Ring Learning With Errors (R-LWE) [24]. For the purposes of secure cloud computing, rank-metric code cryptography has also been explored as a means of increasing the efficiency of encryption and its resistance to quantum computers while not adding too much computation [7].

Attribute Based Encryption (ABE) has attracted significant attention in the field of post-quantum cryptographic techniques as a means to provide more fine-grained access control on decentralized blockchain applications [11]. Different studies have combined the lattice based Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with blockchain-based systems to create secure and privacy-preserving data sharing among distributed systems [28]. These methods have been further improved by lightweight searchable encryption methods which allow efficient retrieval of encrypted data without revealing sensitive information to unauthorized parties [18].

In recent years, the research into post-quantum cryptographic techniques has been extended to various fields, such as digital signatures, secure authentication, searchable encryption, tamper-evident logging, and provenance verification for blockchain-enabled applications [29]. These methods greatly enhance confidentiality, authentication, integrity, and privacy, making blockchain networks more robust and ready for the quantum realm [35]. However, the current post-quantum cryptographic methods still have some issues of large public key size, high computation complexity, communication overhead and resource consumption in limited resource IoT devices [34]. Thus, future research will need to investigate the lightweight, scalable and standardized mechanisms of post-quantum cryptography that can be easily integrated with blockchain and decentralized storage platforms for better practical solutions in IoT applications [37].

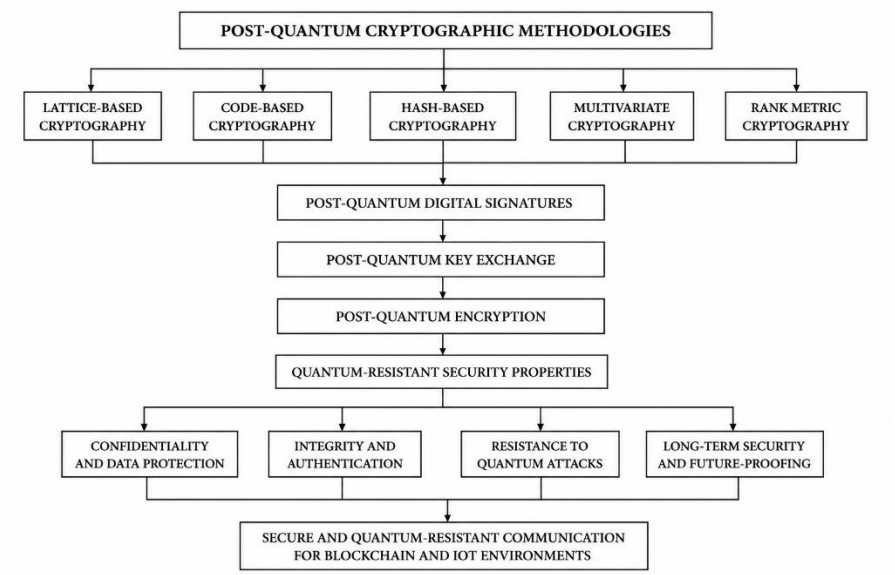

Figure 9. Taxonomy of Post-Quantum Cryptographic Methodologies for Quantum-Resistant Blockchain and IoT Security

In Figure 9, we show the taxonomy of the post-quantum cryptographic methodologies that we found from the reviewed literature for securing the blockchain-enabled Internet of Things (IoT) environment against future quantum computing threats. The methodology starts with 5 main quantum-resistant cryptographic families, including Lattice Based Cryptography, Code Based Cryptography, Hash Based Cryptography, Multivariate Cryptography and Rank Metric Cryptography, which have different families of mathematics to defend digital communications against quantum attacks. In the context of a decentralized blockchain network, these cryptographic methods all contribute to the secure and reliable authentication, confidential communication, and cryptographic protection that is necessary for maintaining the integrity and security of these systems. The integrated cryptographic mechanisms then enable quantum properties of security, such as confidentiality, data protection, integrity, authentication, resistance to quantum attack and long-term cryptographic security. The security features lay the groundwork for creating robust blockchain systems that can safeguard critical IoT information, decentralized storage solutions, and inter-chain operations against traditional and quantum threats. The figure highlights the hierarchy of the emerging post-quantum cryptographic methodologies and their synergistic contribution to enabling secure and scalable blockchain and IoT ecosystems fit for next generation decentralized applications.

4.3 Attribute-Based Encryption and Fine-Grained Access Control Methodologies

ABE is one of the most popular cryptographic techniques for achieving fine-grained access control in blockchain-based IoT networks because it enables access control decisions based on attributes of users, rather than user identities [11]. ABE is different from traditional public-key encryption schemes because it allows for the sharing of information among multiple users that requires flexible authorization policies, yet without the need for centralized access management [23]. This is especially useful for decentralized blockchain systems that involve the constant sharing of sensitive data among users, devices, organizations, and services within diverse networks [24].

From the literature surveyed, it comes to the conclusion that Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is the most widely studied ABE scheme ever since it enables to incorporate access policy into the ciphertext and enable only the legitimate users to decrypt the message successfully [28]. To gain decentralized data sharing with ensuring confidentiality and access control on the whole transaction lifecycle, several researchers have implemented CP-ABE with blockchain [25]. Multi-authority ABE schemes have also been suggested to spread trust across multiple independent authorities to achieve better scalability and eliminate the need for any central key management infrastructure [24].

The other significant methodic advance is the incorporation of revocable ABE, where the existing permissions of a user can be dynamically changed without re-encrypting all the previous data she has stored [23]. Conventional ABE is further enhanced by the introduction of Searchable Attribute-Based Encryption (ABSE) that enables searching of encrypted data without risk of unauthorized disclosure of sensitive data stored in decentralized cloud- and blockchain-based environments [6]. In a subsequent work, lightweight verifiable searchable encryption (VSE) is introduced to enhance the searching efficiency, provenance and secure access control in blockchain-based healthcare and electronic record management systems [18].

Additionally, recent research has involved the incorporation of ABE techniques into blockchain-based logging systems, tamper-evident cloud-based forensics, and decentralized auditing systems, all of which can enhance the confidentiality and accountability of distributed storage solutions [29]. While these methods offer many enhancements in terms of privacy protection and secure information exchange, they are limited in their practical application due to the computational complexity, size of the ciphertext, complexity of attribute revocation, and overhead in communication between resource-limited IoT devices [34]. New work should focus on developing lightweight post-quantum ABE schemes that enable efficient key management, scalable access control, secure searchable encryption and integration with the blockchain and decentralized storage architectures in IPFS [37].

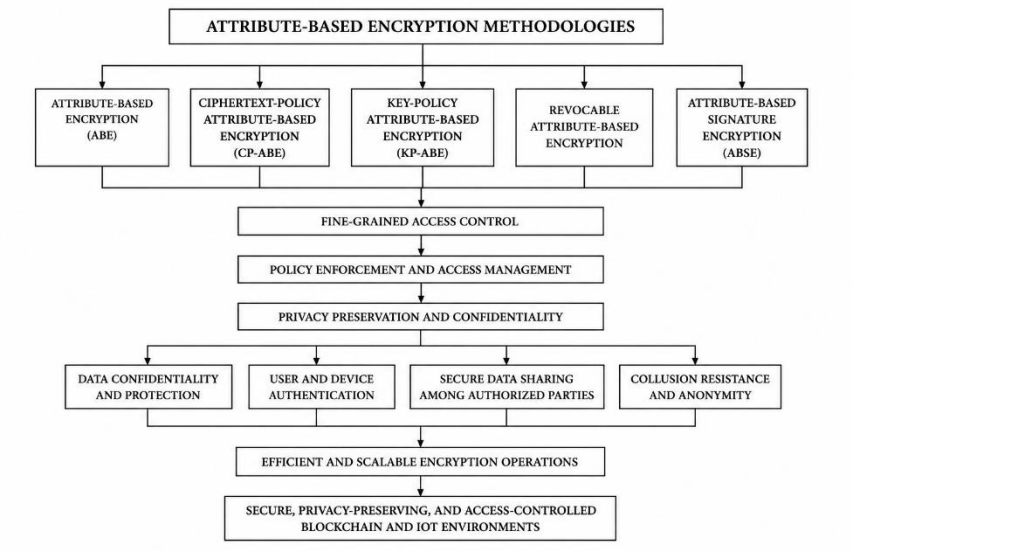

Figure 10. Taxonomy of Attribute-Based Encryption Methodologies for Fine-Grained Access Control in Blockchain and IoT Environments

The taxonomy of the Attribute-Based Encryption (ABE) methods found in the reviewed literature for fine-grained access control, security and privacy in blockchain-based IoT system is shown in figure 10. The methodology starts with the five major approaches to encryption which are Attribute Based Encryption (ABE), Ciphertext-Policy Attribute Based Encryption (CP-ABE), Key-Policy Attribute Based Encryption (KP-ABE), Revocable Attribute

Based Encryption (RABE), and Attribute Based Searchable Encryption (ABSE). These cryptographic methods offer a flexible authorization mechanism because they implement attribute-based access policies that ensure that only authorized users are able to read the protected data. The built-in encryption features then enable fine-grained access controls, while policy and access control management provide secure authentication and control over access to the resources from distributed users and devices. The framework also increases the protection of privacy and data confidentiality, ensuring that sensitive data is not shared or exposed to unauthorized parties and facilitates decentralized communication. The bottom layer of the taxonomy emphasizes the main security goals – data security and confidentiality, user identification, device identification, secure data exchange between authorized users, and collusion while maintaining user anonymity. These security properties, together, allow for efficient and scalable encryption operations, rendering it appropriate for distributed, large-scale systems like AAE. Finally, the methodology offers a safe, privacy-preserving, and access-controlled backbone for blockchain, IPFS, cloud computing, healthcare, IoT, smart farming, transportation, and other distributed computing systems that demand for quantum resistant and fine-grained protection.

4.4 Cross-Chain Communication and Blockchain Interoperability Methodologies

One of the most notable advances in methodology for enhancing interoperability between heterogeneous blockchain networks and facilitating secure exchange of digital assets, transaction records, authentication credentials, and IoT data is cross-chain communication [3]. Traditional designs of blockchain systems are built as stand-alone systems and this restricts the ability to share data and jointly work with other blockchain platforms [8]. For this reason, recent studies have centered on the creation of methodologies that allow for the trusted interaction between separate blockchains, which do not involve compromising decentralization, security, or transaction integrity [5].

Based on the reviewed studies, the methods for blockchain interoperability can be broadly divided into five categories, namely, blockchain notary schemes, cross-chain gateways, relay mechanisms, blockchain bridges, and decentralized interoperability protocols [3]. In this context, using blockchain notary mechanisms can help provide trustworthy verification of transactions before information is exchanged between the participating blockchain networks, thus lowering unauthorized transactions that may occur across chains and enhance the overall security of information communications [3]. Additionally, blockchain bridge technologies play a crucial role in improving the interoperability of blockchain networks by facilitating the secure transfer of digital assets and metadata across different blockchain platforms, ensuring consistency in transactions and decentralized verification [5].

Cross-chain approaches have been extended in several applications, such as smart agriculture, transportation systems, and Internet of Vehicles (IoV) applications, as presented by several researchers [1]. Another recent proposal is to use attribute-encryption-based cross-chain communication as a secure method of information exchange and ensure confidentiality and fine-grained access control in inter-blockchain communication [30]. Likewise, in unmanned aerial vehicle (UAV) applications that require robust communication across multiple administrative domains, blockchain-based authentication mechanisms have been proposed to enhance security and transaction validation while also enabling decentralized identity verification across domains [32].

While the current cross-chain strategies have made significant strides in improving interoperability, there are still some technical challenges that need to be addressed, such as communication latency, transaction synchronization, consensus consistency, bridge vulnerabilities, and computational complexity [4]. Moreover, the majority of the interoperability protocols currently in use still depend on the traditional public-key cryptographic algorithms which are prone to future quantum computing attacks and are not secure in the long-term future [4]. Recent studies, therefore, highlight the need for the implementation of post-quantum cryptography, attribute-based encryption, secure authentication, decentralized identity management, and blockchaining interoperability in a unified and comprehensive cross-chain communication system that can facilitate the secure, scalable, and quantum-resistant IoT ecosystem [1]. The future development of methods should emphasize creating lightweight interoperability protocols, developing standardized cross-chain transmission architecture, making IPFS-based decentralized storage integration more efficient, and establishing efficient quantum-resistant transaction verification mechanism to support distributed environments with large-scale blockchain applications [35].

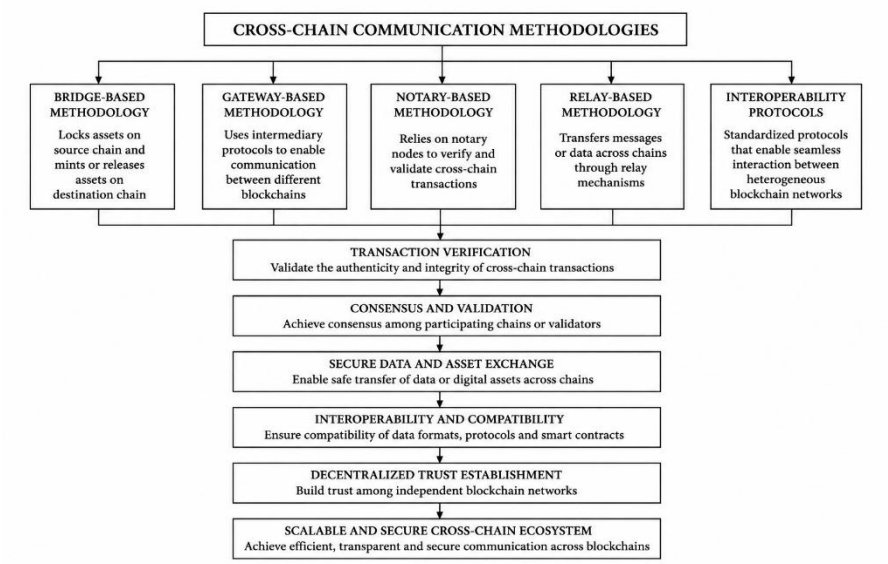

Figure 11. Taxonomy of Cross-Chain Communication Methodologies for Secure Blockchain Interoperability

The taxonomy of cross-chain communication methodologies that were identified from the literature for securing interoperability between heterogeneous blockchain networks is shown in Figure 11. The methodology starts with five major cross chain communication approaches each intended to enable trusted communication and resource exchange between independent blockchain platforms, namely Bridge-Based Methodology, Gateway-Based Methodology, Notary-Based Methodology, RelayBased Methodology and Blockchain Interoperability Protocols. While bridge-based mechanisms allow for the safe transfer of digital assets between different blockchains, gateway-based mechanisms offer communication interfaces that facilitate interoperability across heterogeneous blockchain networks. For cross-chain transactions, notaries are used to verify the transactions, and for cross-chain information, relay mechanisms can be used to transmit the information in a secure manner. Blockchain interoperability protocols also help to create standardized communication methods that facilitate compatibility between various blockchain systems. These methods ensure data integrity, authenticity, and consistency in cross-chain operations, act as transaction verification tools, contribute to consensus, and validate the transactions. Interoperability and compatibility mechanisms then allow for smooth interaction between various blockchain protocols, smart contracts, and decentralized applications, ensuring that they can all operate smoothly and work together to achieve their goals, while maintaining the decentralized trust and secure transaction processing that is central to blockchain technology. In the end, the combination of the methodologies creates a scalable and secure cross-chain blockchain ecosystem that enables transparent communication, trusted information sharing, decentralized identity management, and quantum-ready interoperability for future applications like IoT/Industrial IoT, healthcare, smart agriculture, transportation, decentralized storage, and cyber-physical systems. The whole figure reflects the development of the cross-chain communication methodology to a secure, interoperable, scalable and future-proof blockchain infrastructure.

4.5 Privacy-Preserving Security Methodologies

Given that IoT environments are characterised by the generation, transmission and storage of sensitive information by many distributed entities, privacy preservation is a fundamental requirement of the method for blockchain-based IoT environments [6]. While blockchain is intrinsically immutable, transparent and trustworthy in a decentralized manner, public transaction records can reveal private information about the users, unless privacy preserving techniques are included [14]. As such, recent research has concentrated on crafting cryptographic methods that will ensure the privacy and security of the users, integrity and security of the data, data confidentiality, and secure access, while guaranteeing blockchain transparency and decentralization [18].

The literature reviewed shows that techniques used to enhance privacy in the blockchain are searchable encryption, privacy-preserving authentication, a Zero Knowledge Proof (ZKP), decentralized identity management, and secure logging [26]. Searchable encryption is an encryption method that allows encrypted data to be queried without revealing any plaintext information, safeguarding sensitive data from the IoT, which is stored in decentralized cloud and blockchain systems, while ensuring efficient retrieval performance [6]. Likewise, the lightweight verifiable

searchable encryption is an improvement of conventional SE in which the provenance verification and secure indexing are added to guarantee integrity and confidentiality of EHRs stored in the blockchain-based storage systems [18].

Another significant approach that has gained prominence for securing communication between distributed users, Internet-of-Things (IoT) devices, and blockchain nodes is privacy-preserving authentication [32]. New authentication mechanisms that combine decentralized identity and blockchain to avoid relying on a centralized authentication authority and enhance trust and to stop unauthorized access to the system [39]. Secure logging techniques also bolster accountability by ensuring tamper-evident audit logs, helping to track transactions and build trust in digital environments, especially in decentralized ones [29]. Another area of active research is the use of zero-knowledge proof techniques to achieve privacy, authentication and decentralized identity verification in blockchain networks without revealing the information itself, thereby enhancing privacy, authentication and decentralized identity verification [26].

Although there are considerable progresses in these aspects, current privacy-preserving methods still have a few practical problems such as high computational overhead, communication overhead, key management, scalability and efficiency of implementation on resource-limited IoT devices [34]. Most of the proposed schemes are application-specific, and they lack the ability to have cross-chain blockchain platforms, decentralized storage systems, and heterogeneous blockchain architectures [36]. Moreover, the full integration of post-quantum cryptography, attribute-based encryption, decentralized storage based on IPFS, interoperability among various blockchain chains, and privacy-preserving authentication has not been fully explored in the existing blockchain ecosystems [37]. Thus, lightweight, standardized and quantum-resistant privacy-preserving methodologies that can support secure data sharing, decentralized identity management, scalable authentication and efficient access control for next-generation blockchain-based IoT applications should be developed, which is a subject of future research [42].

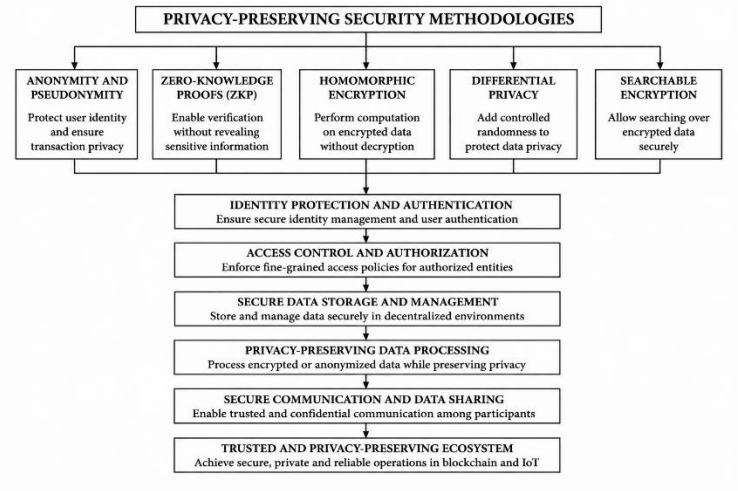

Figure 12. Taxonomy of Privacy-Preserving Security Methodologies for Secure Blockchain and IoT Environments

The taxonomy of security approaches reviewed in the literature, classified in terms of preserving user privacy, to protect sensitive information in a secure manner in the blockchain-based Internet of Things (IoT) is shown in figure 12. The methodology starts with five basic privacy-enhancing techniques namely Anonymity and Pseudonymity, Zero-Knowledge Proof (ZKP), Homomorphic Encryption, Differential Privacy and Searchable Encryption, each of which covers different aspects of privacy protection and secure information processing. All these approaches contribute to more robust identity protection and authentication, allowing users to be securely identified without providing an inordinate amount of sensitive data. Later on, the framework provides fine-grained access control and authorization, allowing for only authorized users to access the protected resources based on a pre-defined security policy. These secure data are subsequently controlled via privacy-preserving storage and processing, with the ability to store, retrieve, and process encrypted information without loss of confidentiality in decentralized blockchain and distributed storage systems. The methodology also allows for secure communication and trusted data sharing among authorized participants, ensuring that the data remains trustworthy, authentic, and private throughout the communication process. The framework combines these complementary privacy-preserving technologies into a trusted and secure blockchain-based ecosystem with application integration and support for secure authentication, decentralized identity management, confidential information exchange, and protected data storage across various

sectors such as healthcare, Industrial IoT, smart agriculture, transportation, cyber-physical systems, cloud computing, and decentralized storage. Overall, the figure exemplifies the systematic implementation of multiple privacy-preserving technologies to ensure a secure, scalable, and quantum-resistant protection for the next generation of distributed systems on the blockchain.

4.6 IoT and IPFS-Based Decentralized Storage Methodologies

Internet of Things (IoT) has been rapidly evolving and is generating massive amounts of data of diverse types which need to be securely stored, efficiently retrieved and reliably shared in a dispersed online environment [9]. When managing large amounts of data in the IoT context, centralized storage structures are becoming problematic because of privacy issues, single points of failure, failure to scale, and centralized control. Thus, the recent research has turned towards using blockchain in conjunction with other distributed storage solutions like InterPlanetary File System (IPFS) for secure data management in next generation IoT systems [17].

While blockchain offers a solution for recording transactions without the need for any central authority, IPFS has a solution for storing large files without consuming excessive bandwidth on the blockchain network. Most of the proposed methodologies do not store the full IoT data sets on the blockchain, but instead, store encrypted data in IPFS and only the cryptographic hashes, metadata and the transaction record on the blockchain to guarantee data integrity and efficient verification [30]. This hybrid storage approach greatly mitigates blockchain storage overhead, boosts scalability, and mitigates risks of failure, without compromising decentralization of data ownership, secure data sharing, and data integrity [19].

In particular, several studies have proved the capabilities of decentralized storage with blockchain technology in application areas such as the healthcare sector, smart agriculture, Industrial IoT, transportation, and cyber-physical systems [10]. Also, DBCM has been exploited to enhance secure communication between distributed IoT devices and reduce reliance on a centralized service provider and to increase system security from cyberattacks [17]. Likewise, blockchain-enabled IoT systems have been suggested to improve energy efficiency, privacy protection, and secure communication in smart homes by decentralizing data storage and handling and ensuring secure transactions [36]. In Internet of Drones (IoD), blockchain has also been leveraged to ensure secure and trusted data transfer, reliable drone coordination, and transparent management of drone operations in a decentralized setting [13].In addition, blockchain has been used in Internet of Drones (IoD) applications to facilitate trusted data exchange, drone coordination, and drone operational management in a decentralized environment [13].

While the integration of blockchain and IPFS offers numerous benefits in terms of storage scalability, data availability, and decentralized trust, there are still some technical challenges that need to be addressed [41]. While the existing methodologies face challenges with secure indexing, efficient content retrieval, decentralized key management, communication latency, storage redundancy, and synchronization between blockchain and off-chain storage repositories, these problems are not addressed in sufficient detail [42]. Moreover, only a few works have introduced post-quantum cryptography, attribute-based encryption, and cross-chain interoperability features in the blockchain–IPFS architectures to secure long-term IoT data against attacks performed in the future by quantum computers [18]. Hence, future methodological research needs to address the design of light-weight, quantum resistant, blockchain–IPFS integration framework with seamless integration of decentralized storage, fine-grained access control, secure authentication, and scalable cross-chain communication to enable secure and privacy-preserving management of the IoT data in next-generation decentralized systems [29].

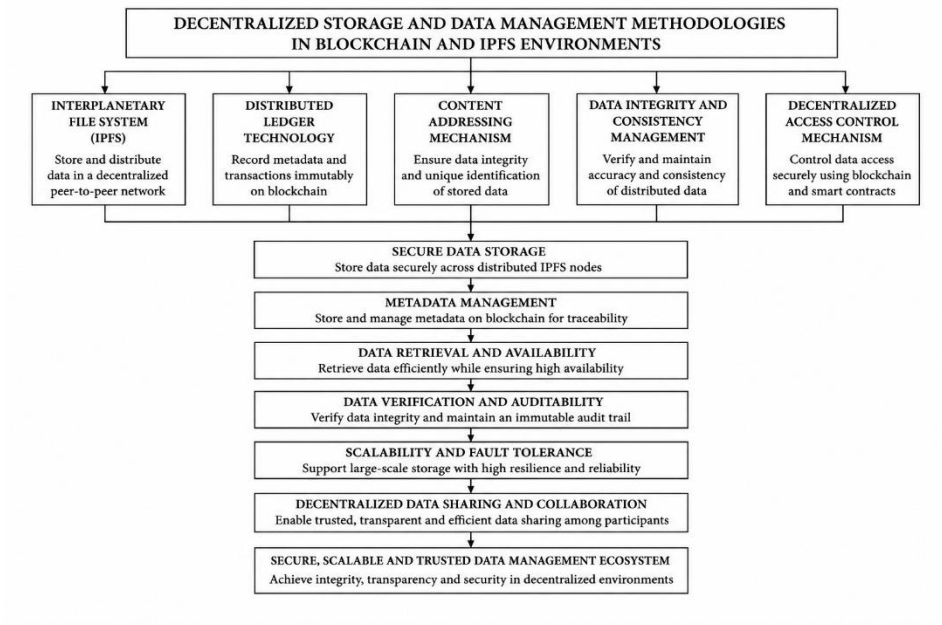

Figure 13. Methodology of Blockchain–IPFS-Based Decentralized Storage for Secure IoT Data Management

Figure 13 depicts how Blockchain can be used together with the InterPlanetary File System (IPFS) to offer secure, decentralized, and scalable data management for the Internet of Things (IoT) setting. The methodology starts with the InterPlanetary File System (IPFS) that stores and distributes the IoT data across a decentralized peer-to-peer network, and the Distributed Ledger Technology (Blockchain) that keeps a tidy record of IoT data metadata and transactions, ensuring transparency and traceability. It also includes a Content Addressing Mechanism, which uses cryptographic hashes to uniquely identify stored data, allowing for efficient retrieval and prevention of unauthorized changes. At the same time, Data Integrity and Consistency Management ensures the accuracy and integrity of the data distributed across different locations and Data Access Control Mechanism ensures secure access to data using blockchain and smart contracts for access control policies. Together, these integrated components enable the secure storage of data, management of metadata, efficient retrieval, data verification and auditability, scalability, fault tolerance and sharing of data among authorized participants. At the end of the day, the methodology creates a secure, scalable, transparent, and trustworthy blockchain–IPFS ecosystem, which is well suited for next-generation applications including smart healthcare, Industrial IoT, smart agriculture, transportation systems, cyber-physical systems, cloud computing and decentralized digital infrastructures, with enhanced data integrity, availability, confidentiality, interoperability and resilience.

4.7 Blockchain Security and Authentication Methodologies

The security and authentication approaches used in Blockchain technology are vital for securing the decentralized Internet of Things (IoT) environment against unauthorized access, data tampering, identity spoofing and cyberattacks [22]. The attributes of blockchain-based authentication systems are fundamentally different from traditional centralized systems which rely on trusted third parties, offering decentralized identity verification, non-repudiation of transactions, and consensus-based trust building among the stakeholders involved [14]. A few recent studies have thus shifted their attention to the design of secure blockchain authentication mechanisms that can be used by distributed IoT devices, cyber-physical systems, healthcare systems, transportation systems, and Industrial Internet of Things (IIoT) applications [39].

The techniques used in authentication in the literature surveyed include: blockchain-based identity management, decentralized authentication protocols, digital signatures, cryptographic key management, and secure transaction verification for the establishment of trusted communication between distributed users and devices [32]. A few researchers have suggested blockchain-based authentication methods in order to improve privacy protection and protect against impersonation attacks, unauthorized access, replay attacks and forgery of credentials in a heterogeneous communication environment [39]. Mutual authenticating protocols have also been implemented in smart agriculture and IoT systems for ensuring trusted communication between the sensing devices, the service providers and the end users, guaranteeing confidentiality and authentication integrity [21].

Along with authentication, blockchain security methods focus on ensuring the integrity of transactions and combating bad activity in a decentralized network [22]. Consensus mechanisms, tamper-resistant ledgers, and immutable transaction logs add to the accountability and the chances of unauthorized changes in decentralized blockchain structures [20]. Researchers also studied defense mechanisms against double spending attacks and the Blockchain network partitioning to enhance transaction reliability and stability in the operation of a consortium Blockchain system [27]. Additionally, blockchain-based cybersecurity systems are known for their enhanced resistance to data manipulation and fraudulent transaction processing, its ability to involve decentralized verification and secure cryptographic authentication [16].

While these approaches have significantly increased the security of the blockchain, there are still some issues that have not been addressed [40]. The current authentication methods are based on classical public-key cryptographic techniques, which could be vulnerable to attacks by quantum computers in the future [35]. Moreover, issues of decentralized identity management, secure key distribution, lightweight authentication, cross chain identity verification and scalable authentication protocols still need to be addressed in large scale IoT deployments [36]. Thus, future blockchain security methods need to combine PQC, ABE, decentralized storage with IPFS, cross-chain authentication and privacy-enhancing identity management to build scalable, quantum-resistant and trustworthy authentication systems to accommodate the next-generation D-IoT systems [37].

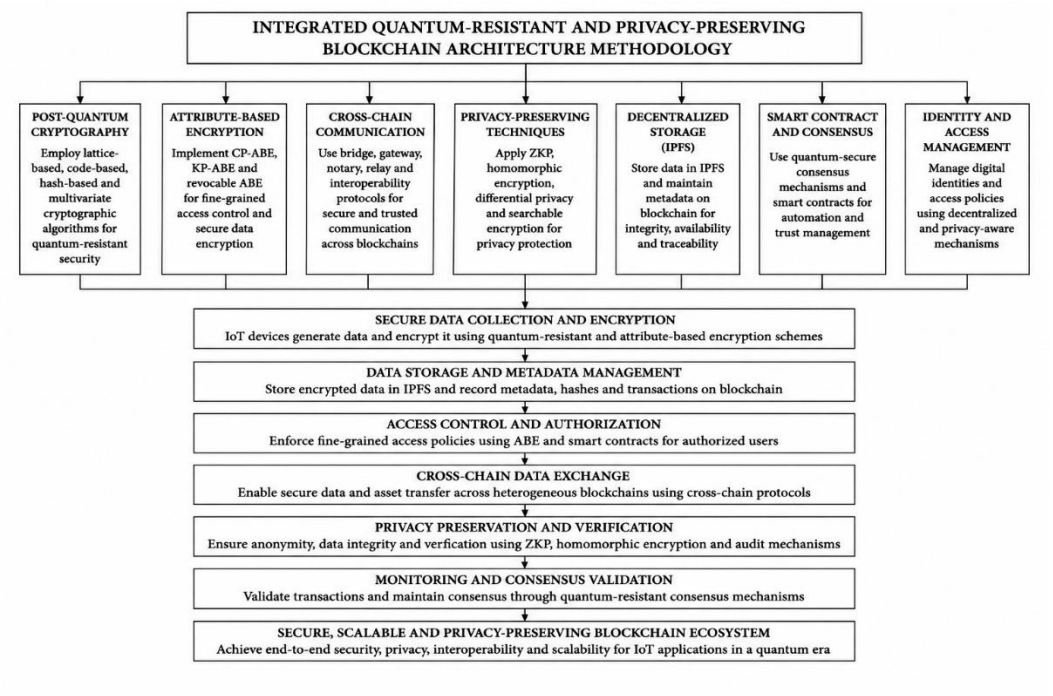

Figure 14. Methodology of Blockchain-Based Security and Authentication for Secure Decentralized IoT Ecosystems

Figure 14 shows the methodology of Blockchain Security and Authentication for Quantum Ready, Secure and Privacy-preserving decentralized Internet of Things (IoT) Ecosystem. The methodology starts from Post-Quantum Cryptography, a quantum-resistant cryptographic method that will secure encryption, digital signatures, and key management against quantum computing attacks in the future. ABE is then deployed to enable access control and confidential data sharing for authorized users and devices with fine-grained access control. Additionally, Cross-Chain Communication is included, facilitating secure cross-chained interoperability and trustworthy information sharing among diverse blockchain networks while ensuring transaction consistency and decentralized trust. The use of Privacy-Preserving Techniques, such as zero-knowledge proof, searchable encryption, and homomorphic encryption, improves the confidentiality, identity protection, and secure verification of sensitive information. Decentralized Storage (IPFS) layer is used for scalable off-chain storage of encrypted IoT data, while the blockchain securely stores immutable metadata and cryptographic hashes to ensure data integrity and traceability. Smart Contracts and Consensus Mechanisms perform authentication, authorization, transaction validation, and policy enforcement in an automated and decentralized way. The Identity and Access Management component controls decentralized identity and authorization procedures that only legitimate users can gain access to protected resources. These components all work

together to ensure secure data collection and encryption, decentralized data storage, metadata management, access control, cross-chain data transfer, privacy preservation, consensus validation, and ongoing transaction verification. The methodology creates a secure, scalable, interoperable and privacy-preserving blockchain ecosystem that can be used to support the next generation of applications such as Industrial IoT, healthcare, smart agriculture, transportation, cyber-physical systems, cloud computing and decentralized digital infrastructures, while offering long-term resilience against classical and quantum cyber threats.

4.8 Performance Evaluation Methodologies

Performance evaluation is also a crucial factor to determine the effectiveness, scalability, and applicability of blockchain-supported security solutions in the Internet of Things (IoT) context [11]. The measured efficiency of cryptographic algorithms, blockchain architectures, authentication protocols and decentralized storage systems across various operational scenarios are used by the evaluated studies and a broad spectrum of evaluation methodologies is applied [7]. The above evaluation methods involve quantitative information about the performance of computation, security of the blockchain, efficiency of communication, and feasibility of deployment in proposed blockchain-based solutions [34].

From the literature it is noted that computational performance metrics are one of the most common evaluation metrics used for post-quantum cryptographic frameworks [23]. The encryption and decryption time, key generation time, digital signature generation time, signature verification time, and overall computational complexity are usually calculated to compare the different post-quantum encryption algorithms [35]. Communication overhead and ciphertext expansion have been analyzed in several works since they are directly related to the efficiency of communications and storage space in resource limited IoT systems [18]. Typically, lightweight cryptographic schemes have shown to be more efficient in terms of computation and, at the same time, still provide a reasonable degree of quantum-resistant security [6].

The main performance metrics used for a blockchain are transaction throughput, transaction confirmation time, consensus latency, block generation time, network scalability and storage overhead [5]. Cross-chain communication frameworks have been evaluated for interoperability efficiency, transaction synchronization delay, communication latency and successful cross-chain transactions rates to evaluate their suitability for heterogeneous blockchain ecosystems [30]. Also, decentralized storage technologies assess the efficiency of storage, the speed of data retrieval, content availability, fault tolerance and storage scalability in the context of integration with off-chain storage and distributed storage systems [17].

Evaluating security also plays a crucial role in ensuring that blockchain-based systems for privacy protection are secure [22]. The reviewed studies are usually used to show the robustness of proposed security frameworks by performing security analysis with replay attacks, impersonation attacks, double-spending attacks, unauthorized access, data tampering and quantum-enabled adversaries. The accuracy of authentication, preservation ability of privacy, efficiency of access control, and the strength of cryptography are also often evaluated to ensure the robustness of blockchain authentication and encryption solutions [39].

While these existing evaluation techniques offer useful lessons about system performance, there are still issues that need to be addressed with standardised benchmarking, common evaluation measures and experimental real world validation of these evaluation techniques [42]. In most studies, a simulation environment or application-specific datasets are used; thus, it is not easy to make a direct comparison between different blockchain architectures and post-quantum cryptographic techniques [41]. Moreover, only a few studies comprehensively examine blockchain, post-quantum cryptography, decentralized storage based on IPFS, cross-chain interoperability, and attribute-based encryption in an experimental setup [29]. Moving forward, it is crucial to develop a standardized benchmarking methodology, publicly accessible datasets, consistent performance metrics, and real-world deployment scenarios to enable objective comparisons and to fast-track scalable, quantum-resistant blockchain ecosystems for secure IoT data storage and communication [37].

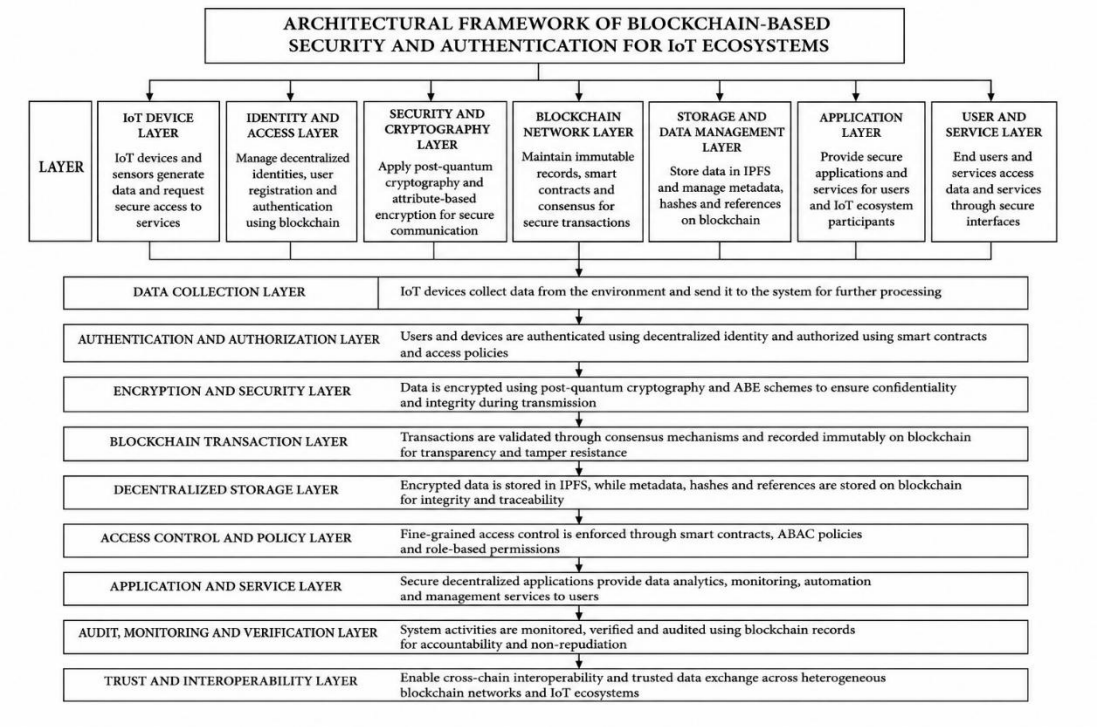

Figure 15. Performance Evaluation Methodology for Post-Quantum Blockchain-Based Secure IoT Data Management

The detailed performance evaluation framework for the security, authentication and secure decentralized data management capabilities of blockchain technology in Internet of Things (IoT) applications is shown in figure 15. Multiple architectural layers start with the IoT Device Layer, Identity and Access Layer, Security and Cryptography Layer, Blockchain Network Layer, Storage and Data Management Layer, Application Layer, and User and Service Layer, which form the backbone of a decentralized blockchain ecosystem. The methodology then takes a sequential approach to assessing the system's performance in a series of assessment layers: Data Collection, Authentication and Authorization, Encryption and Security, Blockchain Transaction Validation, Decentralized Storage, Access Control and Policy Enforcement, Application and Service Execution, Audit, Monitoring and Verification, and Trust and Interoperability. For each evaluation stage, we review the security of the system component by looking at safe data processing, distributed authentication, transaction integrity, storage reliability, and access to services. It allows for the measurement of a wide variety of critical performance parameters such as security strength, authentication efficiency, encryption / decryption time, transaction latency, throughput, storage usage, communication overhead, scalability, fault tolerance, interoperability, and overall system reliability. In addition, continuous auditing and verification provide transparency, accountability, and non-repudiation, and interoperability assessment verifies that secure communication is possible between different blockchain networks and different distributed IoT infrastructures. Overall, the methodology offers a systematic evaluation approach for intercomparing the existing state-of-the-art security solutions based on blockchain technology and validating the practical implementation of blockchain–IPFS architectures for next-generation IoT, IIoT, healthcare, transportation, smart agriculture, cloud computing and cyber-physical systems, which are characterized as being secure, scalable, preserving privacy and robust against quantum attacks.

5. Conclusion and Future Work

5.1 Conclusion

To achieve secure data storage and communications in the Internet of Things (IoT), this review summarizes the most recent progress in post-quantum blockchain solutions by analyzing 42 representative works in the published literature from 2019 to 2026. The results showed that the blockchain technology has been able to contribute a lot in the field of decentralized trust, data integrity, transparency, and secure information sharing in various IoT applications. The combination of Post-Quantum Cryptography (PQC), Attribute-Based Encryption (ABE), cross-chain

communication, and InterPlanetary File System (IPFS) has added an extra layer of security, scalability, and privacy to decentralized data management. Even though such solutions are available, they are still disjointed and grappling with issues like interoperability, lightweight quantum-resistant cryptography, decentralized identity management, secure access control, storage efficiency, and standardized performance evaluation. The proposed conceptual architecture emphasizes the importance of having a unified blockchain-IPFS solution that can facilitate interoperable, scalable, quantum-resistant and privacy-preserving IoT ecosystems. This review will be an important reference for building next-generation secure decentralised infrastructures in a post-quantum era.

5.2 Future Work

Future works are needed to explore lightweight and standardized blockchain–IPFS integration to provide secure storage, cross-chain interoperability, decentralized identity management and fine-grained access control into the IoT system. The post-quantum emphasis should focus on efficient and quantum-resistant cryptographic methods, practical testing, normalized testing, and scalable architectures for future decentralized IoT systems.

Conflict of Interest: The authors confirm that there are no conflicts of interest to declare for this publication.

Acknowledgments: The authors would like to thank the Department of Computer Science and Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya University, Indore, for providing the computational resources and research environment that supported this work.

AI Disclosure: The authors confirm that no generative AI tools were used to prepare this manuscript.

References

1. H. Yu and W. Mu, "ABE-based post-quantum cross-blockchain data exchange approach for smart agriculture," IEEE Transactions on Industrial Informatics, vol. 20, no. 10, pp. 12083-12091, 2024.
2. I. M. Alharbi and N. K. Almazmomi, "Optimized blockchain security for smart agriculture using post-quantum cryptography and graph neural network-based threat detection," Peer-to-Peer Networking and Applications, vol. 18, no. 5, p. 276, 2025.
3. H. Yi, "A post-quantum blockchain notary scheme for cross-chain exchanges," Computers & Electrical Engineering, vol. 110, Art. no. 108832, 2023.
4. A. Tiwari and Y. Chhetri, "Cross-chain vulnerabilities in the quantum era: A threat analysis of blockchain interoperability," in Proc. Int. Conf. Networks and Cryptology (NETCRYPT), 2025, pp. 1318-1323.
5. Z. Qu, Y. Li, L. Sun, Y. Yu, and G. Muhammad, "SCS-QBCT: Supply chain system-driven efficient quantum blockchain cross-chain transaction scheme," IEEE Internet of Things Journal, Early Access, 2025.
6. C. Thingom, "Secure and privacy-preserving post-quantum attribute-based searchable encryption for edge-driven transportation systems," IEEE Transactions on Consumer Electronics, vol. 72, no. 1, pp. 1865-1875, 2026, doi: 10.1109/TCE.2025.3632071.
7. V. Yousefipoor and T. Eghlidos, "An efficient post-quantum attribute-based encryption scheme based on rank metric codes for cloud computing," IEEE Access, vol. 11, pp. 99990-100000, 2023, doi: 10.1109/ACCESS.2023.3313098.
8. A. Siriweera and K. Naruse, "Internet of cross-chains: Model-driven cross-chain as a service platform for the Internet of Everything in smart cities," IEEE Consumer Electronics Magazine, vol. 12, no. 3, pp. 85-97, 2023.
9. X. Luo, S. Xiong, X. Jia, Y. Zeng, and X. Chen, "AIoT-enabled data management for smart agriculture: A comprehensive review of emerging technologies," IEEE Access, Early Access, 2025.
10. H. S. Fattahzadeh, N. Hariri, and S. Behjati, "Rigorous review of blockchain as a reliable technology in agricultural supply chains," Iran Agricultural Research, vol. 43, no. 1, 2024.
11. 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 Transactions on Services Computing, vol. 17, no. 6, pp. 4540-4557, 2024, doi: 10.1109/TSC.2024.3479930.
12. D. Alsadie, "Cybersecurity and artificial intelligence in unmanned aerial vehicles: Emerging challenges and advanced countermeasures," IET Information Security, vol. 2025, no. 1, Art. no. 2046868, 2025.
13. K. A. Tychola, K. Voulgaridis, and T. Lagkas, "Beyond flight: Enhancing the Internet of Drones with blockchain technology," Drones, vol. 8, no. 6, Art. no. 219, 2024.
14. Q. Zhu, S. W. Loke, R. Trujillo-Rasua, F. Jiang, and Y. Xiang, "Applications of distributed ledger technologies to the Internet of Things: A survey," ACM Computing Surveys, vol. 52, no. 6, pp. 1-34, 2019.
15. P. A. D. S. N. Wijesekara and S. Gunawardena, "A review of blockchain technology in knowledge-defined networking: Its applications, benefits, and challenges," Network, vol. 3, no. 3, pp. 343-421, 2023.
16. Y. Y. Ghadi, T. Mazhar, T. Shahzad, I. H. Jaghdam, S. Khan, M. A. Khan, and H. Hamam, "A hybrid AI-blockchain security framework for smart grids," Scientific Reports, vol. 15, no. 1, Art. no. 20882, 2025.

17. S. Pramanik, A. Roy, P. Rakshit, and S. Bag, "Blockchain-based decentralized management of data for the cellular Internet of Things," in Driving Socio-economic Growth with AI and Blockchain. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 249-270.
18. M. Perera and S. Fugkeaw, "LV-PQ-ABSE: A lightweight verifiable post-quantum attribute-based searchable encryption scheme with hybrid indexing and provenance-aware verification for IoT-based electronic EHRs," IEEE Internet of Things Journal, Early Access, 2026, doi: 10.1109/JIOT.2026.3695855.
19. T. Gu, S. He, H. Min, X. Chen, Z. Yan, X. Lyu, and D. Chu, "Blockchain and its applications in the automotive industrial value chain," in Proc. Int. Conf. Blockchain. Cham, Switzerland: Springer Nature, 2025, pp. 134-148.
20. C. Rupa, D. Jaya Kumari, T. R. Gadekallu, and C. Iwendi, "Distributed-ledger-based blockchain technology for reliable electronic voting systems with statistical analysis," Electronics, vol. 11, no. 20, Art. no. 3308, 2022.
21. M. K. Pandit, S. Ray, and P. Das, "MAP-ECC: Mutual authentication protocol for e-agriculture using ECC," in Proc. Int. Conf. Security and Privacy. Cham, Switzerland: Springer Nature, 2024, pp. 109-124.
22. S. R. Sindiramutty, N. Z. Jhanjhi, and S. K. Ray, "Blockchain technology enhances data integrity and transaction security in cybersecurity," in Vulnerability Assessment and Risk Management in Cyber Security. Hershey, PA, USA: IGI Global Scientific Publishing, 2025, pp. 1-40.
23. S. Zhao, "RL-ABE: A revocable lattice attribute-based encryption scheme based on the R-LWE problem in cloud storage," IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 1026-1035, 2022.
24. Y. Yang, "Practical revocable and multi-authority CP-ABE scheme from RLWE for cloud computing," Journal of Information Security and Applications, vol. 65, Art. no. 103108, 2022.
25. G. Zhang , "BCST-APTS: Blockchain and CP-ABE empowered data supervision, sharing, and privacy protection scheme for a secure and trusted agricultural product traceability system," Security and Communication Networks, vol. 2022, Art. no. 2958963, 2022.
26. A. Szczegielniak-Rekiel, K. Kanciak, and J. M. Kelner, "Zero-knowledge proof in 5G and beyond technologies: State of the arts, practical aspects, applications, security issues, open challenges, and future trends," IEEE Access, Early Access, 2025.
27. J. Su, D. Li, R. Chen, Y. Ren, and M. Jia, "Double spending defense in consortium blockchain under network partitioning," in Proc. Int. Conf. Wireless Artificial Intelligent Computing Systems and Applications. Singapore: Springer Nature, 2025, pp. 22-32.
28. T. Chen, "Lattice-inspired CP-ABE from LWE scheme for data access and sharing based on blockchain," Applied Sciences, vol. 13, no. 13, pp. 1-22, 2023.
29. S. Fugkeaw, N. Jitkhajornwanich, P. Mongkolchukaie, N. Rouengsamai, and N. Pornpinyamad, "Optimized post-quantum attribute-based logging for real-time tamper-evident cloud forensics," IEEE Transactions on Cloud Computing, vol. 14, no. 2, pp. 1098-1114, 2026, doi: 10.1109/TCC.2026.3681599.
30. M. Chen, "An attribute-encryption-based cross-chain model for urban Internet of Vehicles," Computers & Electrical Engineering, vol. 115, Art. no. 109136, 2024.
31. A. Abugabah, "Intelligent medical cyber-physical systems in digital healthcare: A post-quantum secure multimodal transformer framework," Journal of Ambient Intelligence and Humanized Computing, vol. 17, pp. 935-956, 2026, doi: 10.1007/s12652-026-05081-8.
32. L. Cao, H. Ji, Q. Wang, "Blockchain-based privacy-preserving authentication protocol for UAV cross-domain," Peer-to-Peer Networking and Applications, vol. 19, Art. no. 84, 2026, doi: 10.1007/s12083-026-02229-3.
33. A. Simbu, S. Nandakumar, and K. Saravanan, "Blockchain-driven smart contract with key exchange protocol for secure device-to-device communication using Verkle tree K-ary structures," Scientific Reports, vol. 16, Art. no. 9470, 2026, doi: 10.1038/s41598-026-38035-3.
34. S. Hasib, A. Rasool, M. Gyanchandani,, "A structured review of lattice-based attribute-based encryption methods for post-quantum security," Discover Computing, vol. 29, Art. no. 175, 2026, doi: 10.1007/s10791-026-09965-3.
35. P. Narsimhulu, P. Chithaluru, and R. Aluvalu, "Efficient post-quantum cryptographic signature aggregation for low-latency distributed networks," Journal of Information Security, vol. 2026, Art. no. 6, 2026, doi: 10.1186/s13635-026-00228-8.
36. N. A. Ismail, S. M. Abu Khadra, G. M. Attiya, "Secure and sustainable smart home networks with blockchain-based IoT framework for privacy and energy efficiency," Discover Internet of Things, vol. 6, Art. no. 58, 2026, doi: 10.1007/s43926-026-00297-8.
37. N. Shirisha, H. M. Manoj, S. J. Hussain, "Post-quantum security framework for resource-constrained systems: Emerging trends, challenges, sustainability, and future directions," Discover Computing, vol. 29, Art. no. 85, 2026, doi: 10.1007/s10791-026-09982-2.
38. D. P. Degala and S. Athithan, "Enhancing cyber-physical system security: A hybrid post-quantum cryptography and deep learning framework for resilience against quantum cyber threats," Cluster Computing, vol. 29, Art. no. 383, 2026, doi: 10.1007/s10586-026-06119-4.
39. R. Latif, B. M. Yakubu, N. S. M. Jamail, "BBAS: A blockchain-based authentication system for e-health with multi-factor authentication, access control, and post-quantum security," Scientific Reports, vol. 16, Art. no. 9163, 2026, doi: 10.1038/s41598-026-39415-5.

40. B. Srinivasarao, S. R. Khasim, M. Lavanya, "Energy efficient cybersecurity and blockchain-enhanced data privacy in smart grid infrastructure for secure energy transactions," Iranian Journal of Science and Technology, Transactions of Electrical Engineering, Early Access, 2026, doi: 10.1007/s40998-026-01061-y.
41. H. Saraya, A. Saleh, and A. Rezk, "Geo-Blockchain Intelligence Risk Assessment (GBIRA) technologies for secure and sustainable Internet of geospatial big data computing ecosystems: A survey," GeoJournal, vol. 91, Art. no. 43, 2026, doi: 10.1007/s10708-026-11569-9.
42. K. Kumar and M. Khari, "Privacy-preserving mechanisms to secure data-driven approaches in Industrial Internet of Things: A bibliometric analysis," Peer-to-Peer Networking and Applications, vol. 19, Art. no. 70, 2026, doi: 10.1007/s12083-026-02220-y.
43. Sunil Parihar, Jigyasu Dubey, “Post Quantum Blockchain for Internet of Things: A Review”, A Conference for Doctoral Students, SHODH-2021, Organized by SVVV University Indore, March-2021
44. Author Profiles
45. Sunil Parihar received the B.E. degree in Computer Science and Engineering in 2006 and the M.Tech. degree in Information Technology in 2013. He is currently pursuing the Ph.D. degree in the Department of Computer Science and Engineering at SVIIT, SVVV University, Indore, India, with a research focus on 'Design of a Post Quantum Blockchain Network to Secure and Store IoT Data.' He is currently serving as an Assistant Professor and Head of the Department of Computer Science and Engineering at Sri Aurobindo Institute of Technology, Indore, and has over 16 years of teaching, research, and academic administration experience. He is UGC-NET and GATE qualified and holds professional certifications from Microsoft and the National Programme on NPTEL. His research interests include post-quantum cryptography, blockchain security, IoT security, secure data storage, distributed systems and emerging computing technologies.
46. Dr. Jigyasu Dubey is a Professor and Head of the Department of Computer Science and Engineering at Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore. He has more than 24 years of Academic, Research and Industry experience. He is also serving as Coordinator – Center of Excellence in Simulation and Gaming, Faculty In-charge of Network Establishment & Internet Cell, and Co-coordinator of the SVVVERP system. He holds a Ph.D. in the Faculty of Computer Engineering in the field of Computer Networking and Peer-to-Peer Computing. His areas of research interest are computer networking, cyber and network security, peer-to-peer computing, software engineering, and object-oriented analysis and design. He has more than 50 publications in peer-reviewed international/national journals and conferences. He has worked as a reviewer for the IEEE Transactions on Network and Service Management and the Journal of Experimental & Theoretical Artificial Intelligence published by Taylor and Francis.