International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(7s) 2026 pp. 1073-1086
https://doi.org/10.70917/ijcisim-2026-2555
Article

A Blockchain-Driven Quantum-Safe Key Management Scheme for IoT

Kamagari Shilppaa[1,*] , Suresh Kallam[2]

[1,*]Department of Computer Science and Engineering, Vemana Institute of Technology, Bengaluru, India.
[2]School of Computer Science and Engineering, JAIN Deemed to be University, Bengaluru, India.
Email: kshilpaa.cse@gmail.com[1,*], Suresh.k@gmail.com[2]

Abstract: The existing blockchain-based security frameworks for IoT networks do not support lightweight, scalable, and quantum-resistant protection for dynamic device-to-device (D2D) environments except with cloud infrastructure or continuous blockchain interaction. Furthermore, traditional public-key cryptographic mechanisms are vulnerable to emerging quantum computing capabilities and are found to be insecure in future developments. This study proposes a decentralised quantum-resistant security framework for IoT D2D communication. In this framework, post-quantum key encapsulation (Kyber KEM) is used to generate secure shared secrets, followed by a hash-chain-based session key evolution mechanism ensuring forward secrecy with low computational overhead. This trust securing method using an event-driven blockchain secures critical transactions using a permissioned network, thus creating a light-weight, but still providing the benefits of immutability and verifiability. We also use AES-256 for encryption with an HMAC-SHA3 algorithm for authentication. The experimental results demonstrate that the proposed blockchain-assisted post-quantum IoT framework achieves lightweight computational overhead, low latency, and stable gas consumption across all security operations. Furthermore, the system ensures strong quantum-resistant security, reliable attack detection, and scalable performance suitable for dynamic device-to-device IoT environments.

Keywords: Blockchain, Device-To-Device IoT Environments, Post-Quantum Key Encapsulation, Quantum Key Distribution, Quantum-Resistant Key Management.

1. Introduction

The rapid growth of Internet of Things (IoT) ecosystems has led to the emergence of dynamic Device-to-Device (D2D) communication environments, where many different kinds of devices communicate directly without using centralised authorities [1, 2]. This kind of decentralized communication not only improves scalability and real-time responsiveness but also significantly expands the attack surface [3-5]. As many IoT devices are connected continuously to the Internet, they are highly vulnerable to identity spoofing, key compromise, replay attacks, and distributed intrusions [6]. To overcome these challenges, blockchain has appeared as an enabling technology for securing IoT D2D communications by providing a decentralised and tamper-resistant trust infrastructure [7, 8]. Blockchain was first introduced by Satoshi Nakamoto in 2008 as the basis of Bitcoin [9]. Blockchain technology allows unchangeable and confirmable transaction recording through cryptographic hash chaining mechanisms such as SHA-256 [10]. Beyond cryptocurrency applications, blockchain is widely used in cybersecurity, Software Defined Networking (SDN), and IoT systems for trust management as well as intrusion detection [11]. Smart contracts improve cooperative security mechanisms through safe storage, checking, and automatic enforcement of security policies, while off-chain methods lower insider threats by controlling decentralised identity and trust connections between IoT controllers and devices [12, 13]. Because of its decentralisation, openness and cryptographic integrity guarantees, the blockchain is a good base for making secure and trustworthy IoT D2D communications [14], as shown in Figure 1. The figure illustrates secure end-to-end communication between two users using cryptographic keys over a network, while preventing interception or attack from a malicious adversary. Recent developments in blockchain and post-quantum security have introduced various IoT network security solutions. A scalable blockchain channel security framework was proposed by using optimised blockchain channels and lightweight consensus mechanisms to enhance secure communication efficiency in IoT environments [15]. A quantum-resilient security model based on lattice-based cryptography was presented for the healthcare system of IoT, where post-quantum encryption techniques are used to achieve resistance against quantum attacks while maintaining computational feasibility for constrained devices [16]. Moreover, a federated trust management

framework based on blockchain integrated with Multi-Agent Reinforcement Learning (MARL) was created to dynamically assess trust in Industrial IoT networks [17]. However, these methods usually depend on specific structures for the domain-specific architectures, continuous blockchain interaction, and computationally intensive mechanisms. This makes them less ideal for lightweight and fully decentralised IoT D2D communication. Thus, a scalable cloud-free event-driven quantum-safe security system is still needed to support secure and efficient dynamic D2D environments in IoT.

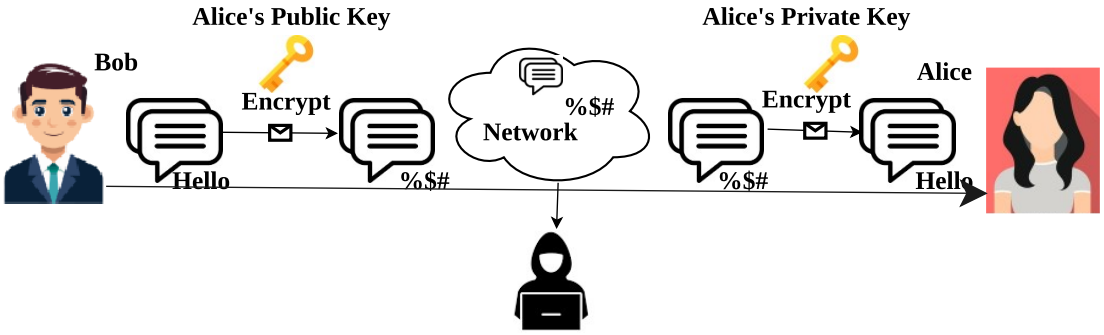

Figure 1: End-to-End Secure Communication with Key Encryption in IoT Networks

1.1. Research Contribution

The proposed work provides the following key contributions toward building a secure, scalable, and quantum-resistant IoT D2D communication framework.

- **Enhanced Security Against Classical and Quantum Attacks:** The proposed framework uses quantum-resistant mechanisms in cryptography, such as lattice-based and hash-based digital signatures. This will help to protect against both traditional attacks in cryptography and those new threats that come from quantum computing.
- **Robust Data Integrity and Authentication Mechanism:** The proposed system provides integrity for messages and events with the help of Hash-based Message Authentication Code - Secure Hash Algorithm 3 (HMAC-SHA3) plus post-quantum digital signatures. This allows strong authentication, tamper detection, spoofing attack protection, and replay attack defence.
- **Event-Driven Blockchain-Based Trust Anchoring:** The proposed framework uses an event-driven blockchain interaction model for security-critical events are hashed, digitally signed, and anchored to the blockchain. This method provides immutable, auditable, and verifiable logging with low computational and communication overhead.
- **Flexible, Scalable, and Future-Ready Design:** The proposed framework supports multiple SHA-3 hash lengths as well as quantum-safe cryptographic algorithms for adaptability. Its modular architecture allows seamless integration with heterogeneous IoT devices, enterprise infrastructures, and distributed network environments while maintaining scalability and long-term resilience

The manuscript is organised as follows. Section 2 reviews related work on blockchain and post-quantum IoT security. Section 3 presents the proposed quantum-resistant D2D framework. Section 4 provides performance evaluation and security analysis. Section 5 concludes the paper and discusses future work.

2. Literature Survey

This section analyses the existing research studies and technologies related to blockchain-assisted and post-quantum security frameworks for secure IoT D2D communication. Kale et al. [18] developed classical blockchain security mechanisms using Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Random Number Generation (QRNG) to achieve secure Decentralized Finance (DeFi) and cross-chain transactions. However, the integration of quantum communication mechanisms increased computational overhead and deployment complexity, requiring further optimization for scalable real-time blockchain environments. Abood et al. [19] designed a post-quantum resistance scheme for Internet-of-Healthcare Things (IoHTs) based on Elliptic Curve Cryptography (ECC), to guarantee the safety and storage of electronic records. This method enhanced security against phishing and the majority of attacks. However, the practical implementation of IoHTs was complex to set up as per the methodology suggested. Swetha et al. [20] presented a quantum cryptography algorithm, covering key quantum-resistant techniques such as lattice-based, hash-based, code-based, and multivariate cryptographic schemes to address vulnerabilities posed by quantum computing. The model achieved various post-quantum primitives for secure communication and encryption in future networks. However, this provided empirical performance evaluation of these techniques when integrated into real-world

systems such as blockchain or distributed ledger technologies Dhar et al. [21] designed a framework for IoT using blockchain technology with quantum cryptography to protect sensitive multimedia data. This framework enhanced data confidentiality, integrity, privacy, and anonymity by achieving QKD for secure key exchange. However, this framework did not have resilience against quantum attacks in real-world scenarios. Begimbayeva et al. [22] developed a hybrid QKD concept by integrating twin-field and measurement-device-independent protocols to support secure multi-user quantum communication. The model attained network scalability while maintaining high-security standards and reducing resource consumption. However, the system had issues with complexity and validating performance through large-scale real-world network deployments.

By analysing these existing blockchain-based and post-quantum security protocols for the IoT, we observed that ensuring lightweight, scalable, and real-time secure D2D communication remains a significant challenge. Most of the existing security solutions require computationally expensive post-quantum signatures, QKD, and hybrid encryption methods, resulting in excessive overhead, infrastructure complexity, and increased latency. Many of these attempts also require constant interaction with the blockchain, increased transaction costs and decreased scalability in large scale IoT networks. In addition, the majority of the backgrounds are difficult to employ within resource-constrained environments and have not been effectively validated within a realistic situation. Therefore, these frameworks do not adequately support efficient, decentralized, and event-driven IoT communication. To overcome these limitations, we introduce a lightweight quantum-resilient IoT security architecture that enables efficient post-quantum key agreements, hash-chain-based session key generation, symmetric encryption, and selective blockchain updates. This provides strong security while reducing computational and communication overheads.

3. Proposed Methodology

The proposed methodology introduces a quantum-resistant, event-driven IoT security framework for dynamic D2D communication. The scenario is shown in Figure 2. Each IoT device creates a post-quantum public-private key pair using Kyber Key Encapsulation Mechanism (Kyber KEM). Then it creates a hash of its own public key that is registered on a permissioned blockchain along with the device ID for the purpose of creating a decentralized trust anchor. Before communication, the sender verifies identity of the intended recipient by cross-referencing the hash of the public-key received with what is found in the blockchain. Once verification is completed, a one-time master key will be exchanged with the recipient using Kyber KEM which will then be used to generate session-specific keys by a hash chain providing for forward secrecy. All message content will be encrypted using Advanced Encryption Standard 256 (AES-256) while message authenticity is performed using HMAC-SHA3. Access to the blockchain is allowed only when one or more of the following security-related events occur: node registration, node compromise, or trust update. The proposed framework guarantees that quantum-resistant security is lightweight, easily scalable, and cloud-independent, while providing a tamper-resistant method for decentralized trust management in real-time IoT D2D communications.

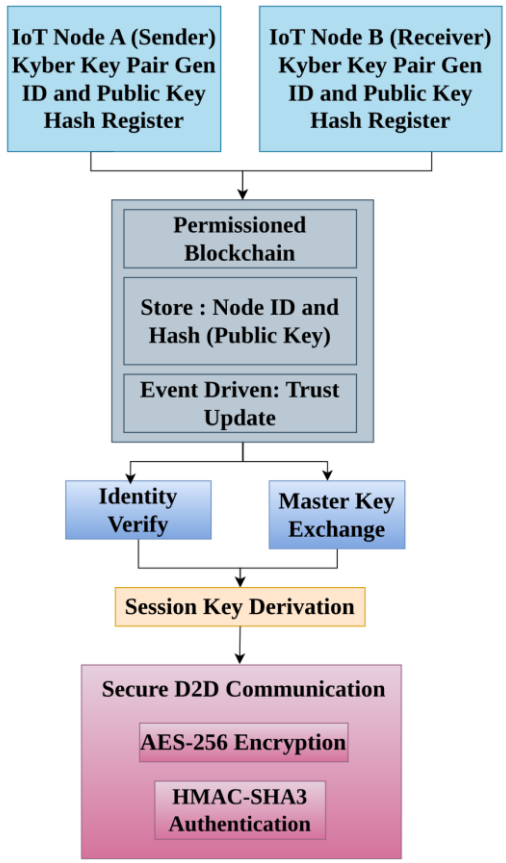

Figure 2: Secure IoT Framework with Kyber KEM and Blockchain

3.1. Node Registration and Blockchain-Based Identity Anchoring

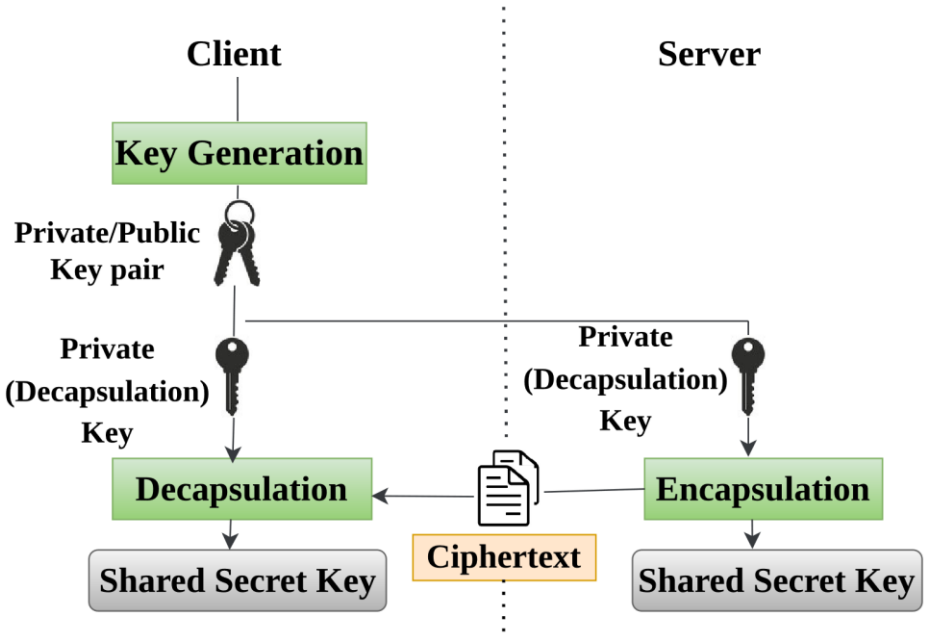

Figure 3: Kyber KEM Key Generation and Shared Secret Establishment Process

The node registration phase establishes the decentralised trust layer that is resistant to quantum threats in the proposed blockchain-assisted quantum-secure communication framework for IoT Systems [23]. Here, each IoT device independently generates its own post-quantum identity, without any centralised Certificate Authority or cloud infrastructure. The identity generation uses the Kyber KEM shown in Figure 3, based on the hardness of

the Module-Lattice Learning with Errors (MLWE) problem [24], which is considered secure against both classical and quantum adversaries.

For every node N_i, a public-private key pair is created as follows in Equation (1).

$$(pk_i, sk_i) = Kyber.KeyGen(\lambda) \quad (1)$$

where pk_i denotes the post-quantum public key and sk_i represents the equivalent private key, and λ is an imposed security parameter. This confirms that every device has a distinct quantum-resistant cryptographic identity. Since lattice-based public keys are relatively large in size, involving them directly on the blockchain would create unnecessary storage and communication overhead. To deal with this problem, a cryptographic hash of the public key pk_i is computed using SHA3-256 [25], as shown in Equation (2).

$$H_i = SHA3\text{-}256(pk_i) \quad (2)$$

where $H_i \in \{0,1\}^{256}$. The hash function gives collision resistance and pre-image resistance thus, any change in the public key will result in an entirely different hash value. Therefore, H_i serves as a compact and secure commitment to the public key of the device. Each node then creates a registration transaction using its unique identifier along with a hashed public key, and a timestamp in Equation (3).

$$RegTx_i = ID_i \parallel H_i \parallel T_i \quad (3)$$

where ID_i denotes the device identity, H_i is the hash of the public key, T_i represents the registration timestamp, and $\parallel$ indicates concatenation. To guarantee authenticity and non-repudiation, the transaction is digitally signed using the node's private key in Equation (4)

$$\sigma_i = Sign_{sk_i}(RegTx_i) \quad (4)$$

The complete registration record submitted to the permissioned blockchain is therefore given as Equation (5):

$$Record_i = \{ID_i, H_i, T_i, \sigma_i\} \quad (5)$$

After consensus validation, the record gets added into block B_k, which is cryptographically linked to the previous block as in Equation (6).

$$B_k = Hash(B_{k-1}) \parallel MerkleRoot(Record_i) \quad (6)$$

The inclusion of Hash (B_{k-1}) guarantees chain integrity, while the Merkle root ensures transaction-level immutability. Consequently, the blockchain permanently maintains an immutable mapping $ID_i \rightarrow H_i$. During future communication attempts, a node's legitimacy is verified by recomputing the hash of its presented public key and comparing it with the stored blockchain value as in Equation (7).

$$SHA3\text{-}256(pk_i^{received}) = H_i^{blockchain} \quad (7)$$

If this equation is true, then the node will be considered authenticated. Otherwise, the identity claim will be rejected. This condition also means that any efforts to replace or change a public key would be instantly noticed. With this mechanism, the node registration process combines quantum-resistant identity binding, decentralised trust anchoring, storage efficiency, and event-driven blockchain use. It creates the base trust layer for later identity verification, master key generation with Kyber KEM, and self-evolving session key derivation in the proposed secure IoT communication framework.

3.2. Identity Verification by Blockchain

In the Identity Verification by Blockchain phase, a requesting node verifies public key provided by a target node is genuine and was previously recorded in the blockchain ledger [26]. This step helps to establish decentralised trust without dependence on a centralised certificate authority. The verification method relies on the unchangeable link between device identity and the hashed public key that was recorded during the node registration phase.

Assume that the node N_s means to communicate with the node N_t. The target node sends its post-quantum public key pk_t along with its unique identity ID_t. Before initiating any key exchange or encrypted communication, the node N_s needs to verify that this public key actually belongs to N_t.

Where pk_t is received, node N_s Computes the hash of the public key using SHA3-256 as follows in Equation (8).

$$H_t^{recv} = \text{SHA3-256}(pk_t) \quad (8)$$

Here, pk_t refers to the public key received from the node N_t, H_t^{recv} represents the 256-bit hash value computed from this received public key, and SHA3-256 is a collision-resistant hash function that gives output of fixed length the node $N_s$retrieves the hash anchored in the blockchain that corresponds to the identity ID_t. This retrieval operation is expressed as Equation (9)

$$H_t^{bc} = \text{Query}(ID_t) \tag{9}$$

Where ID_t is the unique identifier of the target node N_t, and H_t^{bc} denotes the hash value that was originally registered for $N_t$and stored in the blockchain. The function Query$(\cdot)$ performs a lookup operation in the permissioned blockchain ledger and returns any stored hash associated with the given identity.

The identity of the N_t is considered valid only if the following verification condition holds as in Equation (10).

$$H_t^{recv} = H_t^{bc} \tag{10}$$

This ensures that what has been received exactly matches what was registered and anchored in the blockchain. If an adversary tries to modify or substitute the public key with a forged key pk_t'. Then, due to the pre-image and collision resistance properties of the hash function, the following variation will occur in Equation (11).

$$\text{SHA3-256}(pk_t') \neq H_t^{bc} \tag{11}$$

In this scenario, the request for communication is immediately rejected since the verification fails. The formal expression for the authentication decision function is given in Equation (12).

$$\text{Auth}(N_t) = \begin{cases} 1, & \text{if SHA3-256}(pk_t) = H_t^{bc} \\ 0, & \text{otherwise} \end{cases} \tag{12}$$

Where $\text{Auth}(N_t) = 1$ implies that identity verification was completed successfully. Conversely, $\text{Auth}(N_t) = 0$ indicates an unsuccessful authentication attempt.

This mechanism of identity verification based on blockchain ensures that only previously registered and trusted nodes may participate in secure communication. Any attempt to change the hash values stored would necessitate changing all the subsequent blocks because of immutability and the cryptographic connection between blocks in a Blockchain ledger. This is practically impossible under a permissioned consent model. Since it requires only hash computation and comparison, this process provides lightweight verification, hence applicable to resource-constrained IoT devices. Thus, Identity Verification through Blockchain provides decentralized, tamper-evident, and quantum-resilient identity authentication as the necessary trust validation step before master key establishment and secure session initiation in the proposed framework.

3.3. Master Key Generation (Kyber KEM)

In the master key generation step, a shared secret is securely established between two authenticated IoT nodes using KEM [27]. This process provides quantum-resistant key agreement without the shared secret ever being transmitted over the network.

Assume node N_s wishes to communicate with the node N_t, whose public key pk_t has been previously verified on the blockchain. The sender generates a ciphertext shared secret pair through the encapsulation function $(c, K_m) \leftarrow \text{Kyber.Encaps}(pk_t)$. Where pk_t is now the verified public key of the node N_t,c denotes the encapsulated ciphertext, and K_m denotes a master key generated by an encapsulation function. This ciphertext will be sent to the node N_t. for further processing. Upon receiving c, It derives the same master key from its private key sk_t by using the following Equation (13).

$$K_m = \textit{Kyber.Decaps}(c, sk_t) \tag{13}$$

Where sk_t represents a private key of the node N_t, and $K_m$is the recovered master key. The correctness of the Kyber KEM ensures that both parties create identical keys as shown in Equation (14).

$$K_m^{(s)} = K_m^{(t)} \tag{14}$$

The shared master key K_m shall be used as a root secret from which session-specific keys are derived afterwards, so that secure communication happens in a quantum-resistant way between IoT nodes.

3.4. Session Key Derivation (Hash Chain)

The session key derivation phase consists of generating a sequence of independent session-specific symmetric keys using a cryptographic hash chain [28]. This hash chain is constructed from an initial shared secret that is established during the master key exchange. Instead of directly using the root secret for encryption, the framework derives fresh keys for each communication session to ensure forward secrecy and key evolution. Let S_0 be the initial shared secret computed after successful key encapsulation and decapsulation between two authenticated nodes. A secure one-way hash function $h(\cdot)$, is applied iteratively to derive session keys, where $h(\cdot)$ can be SHA3-256. The first session key is derived as in Equation (15)

$$SK_1 = h(S_0) \tag{15}$$

Where S_0 is the initial shared secret, $h(\cdot)$ is a hash function that is collision-resistant and pre-image resistant, and SK_1 is the symmetric key used for the first communication session. For subsequent sessions, the key derivation process continues recursively as shown in Equation (16)

$$SK_i = h(SK_{i-1}), \text{for } i = 2,3,\dots,n \tag{16}$$

Here SK_i denotes the session key for the i-th session, SK_{i-1} is the previous session key, and n represents the total number of sessions before reinitialization. More generally, the i-th session key can be expressed as Equation (17).

$$SK_i = h^i(S_0) \tag{17}$$

where $h^i(\cdot)$ indicates that the hash function is applied iteratively i times to the initial shared secret. The security of this hash chain depends on the fact that it is easy to compute hashes but hard to invert them. Given a current session key SK_i it should be practically impossible to compute its pre-image SK_{i-1} as shown in Equation (18).

$$SK_i = h(SK_{i-1}) \tag{18}$$

Here reversing $h(\cdot)$ is intractable under standard cryptographic assumptions. Hence, the compromise of a current session key does not reveal past session keys, thereby achieving forward confidentiality. Each session key is deterministically derived but cryptographically independent, thus preventing replay and key reuse attacks. This hash-chain-based session key derivation method is computationally light, as it requires only hash evaluations. Hence, it is very appropriate for resource-constrained IoT D2D communication environments while providing strong security guarantees against both classical and quantum adversaries.

3.5. Secure Communication (AES-256 + HMAC)

In the Secure Communication phase, confidential data exchange between two authenticated IoT nodes is protected using a combination of Advanced Encryption Standard (AES-256) [29] for encryption and HMAC-SHA3 [30] for message authentication. This hybrid construction guarantees both confidentiality, integrity and authenticity of transmitted data within a quantum-secure IoT environment. Let SK_i denotes the session key corresponding to the i-th communication session, derived from the hash chain mechanism. To ensure cryptographic separation of functions, the session key is expanded using a secure Key Derivation Function (KDF) into two independent sub-keys Equation (19).

$$(K_{enc}, K_{mac}) = KDF(SK_i) \tag{19}$$

where K_{enc} is the 256-bit symmetric encryption key used for AES-256, and K_{mac} is the key used for computing the HMAC with SHA3. Given a plaintext message M, encryption is performed as in Equation (20).

$$C = AES\text{-}256_{K_{enc}}(M, IV) \tag{20}$$

where C represents the ciphertext and IV is a unique initialisation vector (nonce) generated for that message. The use of a fresh nonce for each transmission ensures semantic security and prevents ciphertext pattern leakage. To provide integrity and source authentication, a message authentication tag is computed over the ciphertext Equation (21).

$$T = HMAC_{K_{mac}}(C \parallel meta) \tag{21}$$

Where T is the authentication tag and $\parallel$ denotes concatenation. The transmitted frame consists of the tuple (IV, C, T). Upon reception, the receiving node recomputes the authentication identifier as in Equation (22).

$$T' = HMAC_{K_{mac}}(C \parallel meta) \tag{22}$$

Then, verifies the condition as in Equation (23)

$$T' = T \tag{23}$$

If the equality holds, the ciphertext is considered authentic and untampered, and decryption is performed as in Equation (24).

$$M = \text{AES-256}_{K_{\text{enc}}}^{-1}(C, IV) \tag{24}$$

If the verification fails, the message is discarded immediately. This combined AES-256 and HMAC-SHA3 construction provides strong confidentiality through symmetric encryption, high integrity and authenticity through keyed hashing, and resistance against replay or modification attacks provided that nonces and metadata are properly handled. As it is based on efficient symmetric cryptography operations and hash calculations, it makes a good acceptable for dynamic, resource-constrained IoT D2D communication environments while keeping safe from classical as well as quantum-assisted adversaries.

3.6. Blockchain Update on Security Event

In the blockchain update on security event phase, the distributed ledger is modified only when a security-critical condition ensues, such as node compromise, trust degradation, key revocation, or re-registration [31]. This event-driven update mechanism ensures that blockchain interaction with the blockchain remains lightweight while still providing an immutable and globally verifiable trust state. The security event occurs for the node N_i, ID_i denote the unique identifier of the node N_i,let E_j be the encoded representation of the j-th security event related to this particular node; and finally, T_j denote the timestamp at which this event is generated. The security update transaction will be formed as per Equation (25).

$$UpdTx_j = ID_i \parallel E_j \parallel T_j \tag{25}$$

where $\parallel$ is the concatenation operator. This structure ensures that the event is connected to a certain identity of a node and a particular time moment, thus keeping the order of events in time and allowing for checking them afterward. To make sure that the information is real and stop illegal changes to the status, the update transaction is signed digitally by the entity that reports it using its secret key. The process for generating the signature is described in Equation (26).

$$\sigma_j = Sign_{sk_{reporter}}(UpdTx_j) \tag{26}$$

where sk_{reporter} is the private key of the reporting node or an authorised validator on the blockchain, and σ_j is the digital signature that binds cryptographically binds reporter to declared event. The complete blockchain record is then formed as in Equation (27).

$$Record_j = \{ID_i, E_j, T_j, \sigma_j\} \tag{27}$$

After consensus validation in the permissioned blockchain network, the record is appended to the block B_k, which is cryptographically linked to the previous block as follows in Equation (28).

$$B_k = Hash(B_{k-1}) \parallel MerkleRoot\big(Record_j\big) \tag{28}$$

The addition of $\text{Hash}(B_{k-1})$ keep the chain integrity, while the Merkle root ensures tamper resistance at the transaction level. Once noted, the security status of the node N_i cannot be changed and can be seen by everyone. When later trying to check an identity the current trust state of the node is determined by retrieving the most recent event entry as in Equation (29).

$$\text{Status}(N_i) = f(\text{Lookup}(ID_i)) \tag{29}$$

Here $\text{Lookup}(ID_i)$ gives the latest blockchain entry associated with the node, and $f(\cdot)$ interprets the encoded event to determine whether the node is valid, revoked, compromised, or requires re-authentication. By restricting blockchain modifications strictly to security-critical events, the framework minimises computational overhead while ensuring transparent, decentralised, and tamper-resistant trust management in changing IoT networks.

4. Results and Discussion

In this section, we have provided a thorough analysis of the validation of the proposed model to evaluate its performance across various metrics. The analysis provides insights into its efficiency and effectiveness in maintaining the proposed framework's performance.

4.1. Performance Analysis of the Proposed Model

Figure 4 shows the cost efficiency of node recording for the proposed quantum-resistant IoT framework using the blockchain. Each IoT device registers through a smart contract, and the gas consumed for this transaction execution is recorded and analyzed. The distribution shows that gas consumption is very close for

several nodes, indicating similar computational requirements. There are no extreme variations to prove registration mechanism does not introduce any unpredictable financial or processing overhead. Stable gas consumption proves that the smart contract logic of smart contracts is optimized and lightweight. Hence, it can be easily scaled when onboarding large numbers of IoT devices without incurring too much cost on the blockchain. This graph finally validates the economic scalability of the proposed registration mechanism.

Figure 5 shows the confirmation time for every node registration transaction in the blockchain network. Latency values are taken for multiple registration events and analyzed for stability. The results confirm that confirmation time is kept low and nearly constant with very small variations. The absence of major spikes proves that the event-driven blockchain integration does not permit network congestion. Consistent latency ensures that device onboarding will not delay secure communication, which is critical in real-time IoT environments needing fast authentication. This graph, therefore, proves that this framework can support efficient and responsive operations on the blockchain.

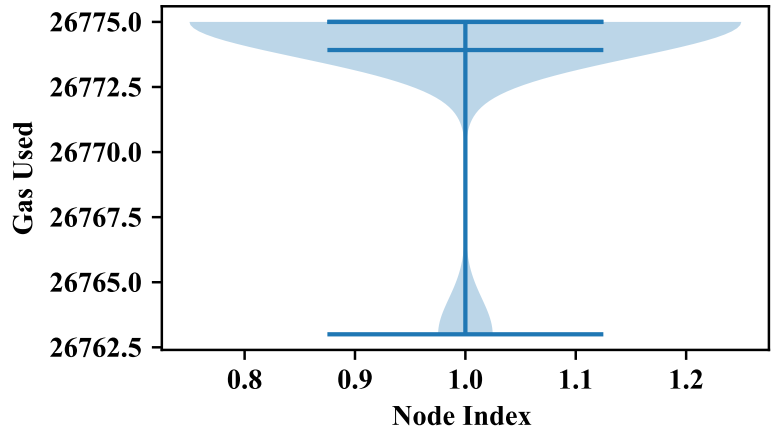

Figure 4: Gas Consumption Analysis for Smart Contract-based Node Registration

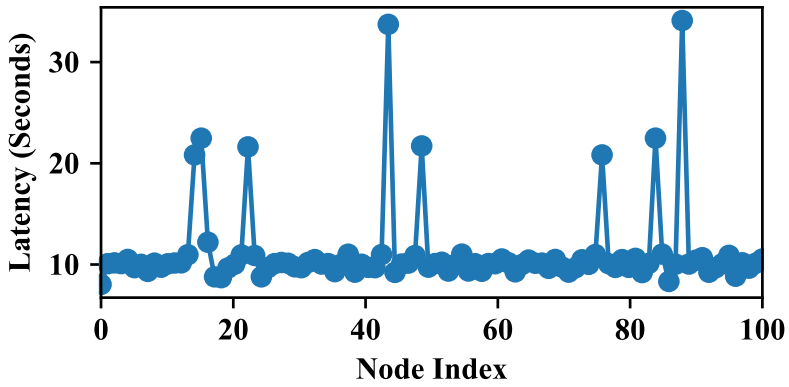

Figure 5: Blockchain Transaction Latency During IoT Node Registration

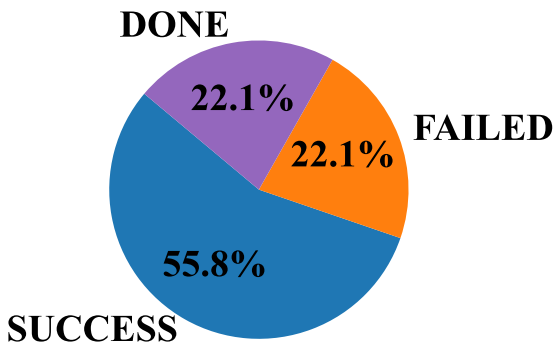

Figure 6: Execution Outcome Distribution of the Proposed IoT Security Framework

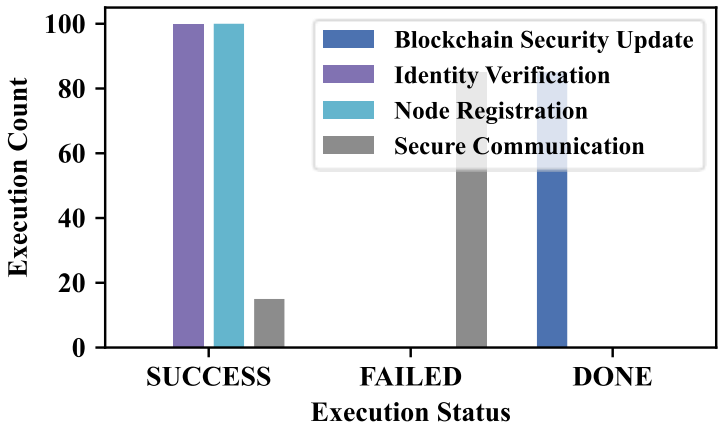

Figure 7: Workflow Step-Wise Execution Status Analysis of the Multi-Layer IoT Security Architecture

Figure 6 shows the overall execution outcomes of the IoT security system by categorizing operations into SUCCESS, FAILED, and DONE. The majority of operations are marked as SUCCESS, indicating that the security verification and authentication processes are reliable. A small proportion of FAILED outcomes reflects correctly detected anomalies or validation errors. DONE represents procedural steps completed without decision-making involvement. This distribution demonstrates that the system operates with high reliability and controlled failure detection. Limited failure rates confirm robustness against potential attacks; thus, this graph validates the operational stability of the proposed framework.

Figure 7 demonstrates the verification, node registration, secure communication, and blockchain updating. This evaluation at each step uses the SUCCESS, FAILED, or DONE counts. Security steps are critically evaluated with mostly successful outcomes, reflecting effective verification mechanisms. With minimal failure occurrences, they highlight resilience against unauthorized access. The structured comparison helps identify whether any specific stage is prone to instability. Balanced results across components confirm architectural strength. This validates the reliability of each individual security layer.

Figure 8 presents the efficiency of the session key generation mechanism employed in secure IoT communication. The time taken for the generation of a session key in the session key generation mechanism utilized in secure IoT communication. The time taken to generate session keys over different sessions has been measured and is presented in the graphical method. Most of the times for key generation fall within very low intervals, which indicates that it is computationally efficient. A narrow distribution further proves that there are no large variations; hence, consistent performance is confirmed. Since efficient key derivation allows for rapid setup of secure sessions, there would be no evidence of processing delay even under repeated executions. This provides additional proof that the hash-based key derivation process is lightweight and scalable.

Figure 9 shows the incremental improvements in the execution time of cryptographic operations such as session key derivation, AES encryption, authentication, and blockchain updates. The curve rises gradually in a smooth manner, indicating the linear nature of computational growth. The overhead added by AES encryption is minimal, confirming the efficiency of symmetric cryptography. There are no sudden spikes in the graph to indicate a bottleneck in the system. Each security component ensures an equal contribution towards controlled resource consumption. This figure validates long-term scalability as well as computational stability.

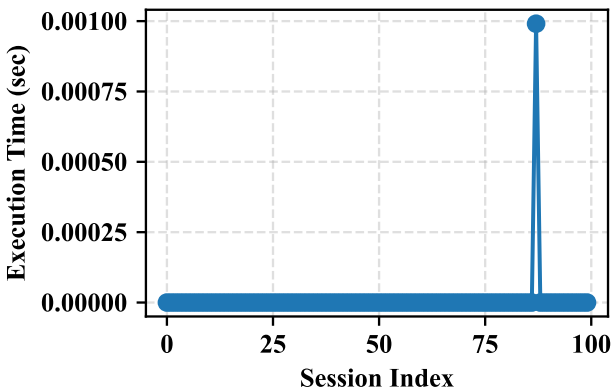

Figure 8: Session Key Generation Time Distribution and Scalability Analysis in Secure IoT Communication

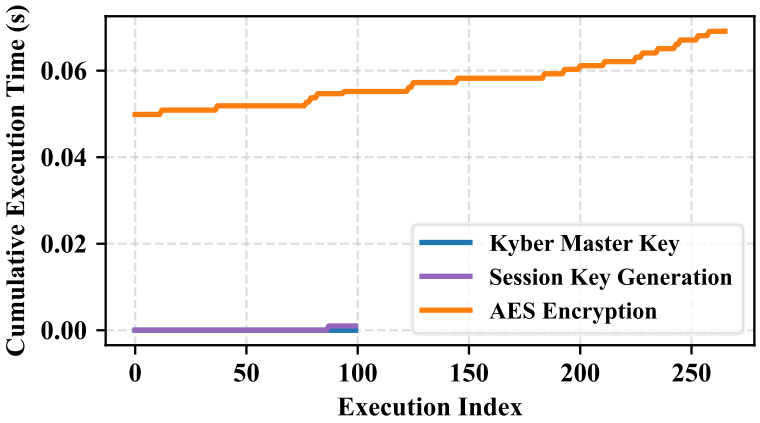

Figure 9: Cumulative Cryptographic Overhead Across Continuous Security Operations

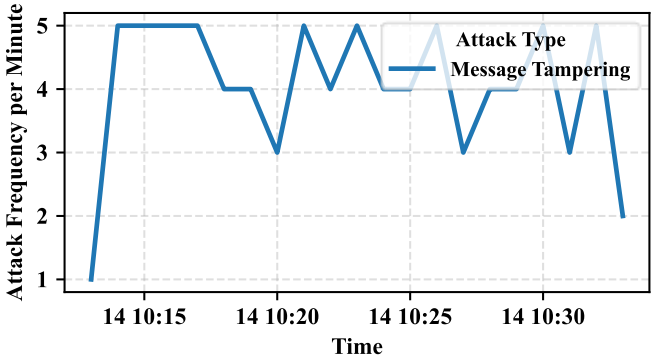

Figure 10: Temporal Analysis of Message Tampering Attack Detection Across Distributed IoT Network Nodes

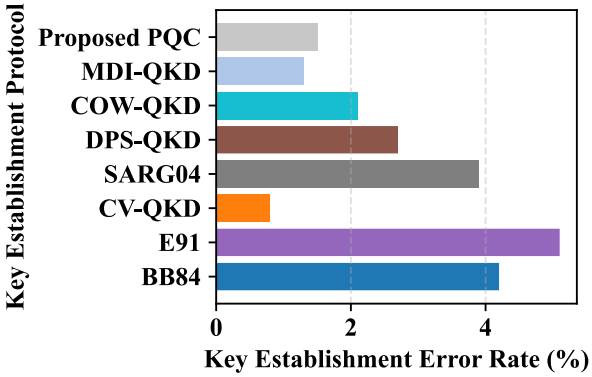

Figure 11: Key Establishment Error Rate Comparison

Table 1: Key Management and Session Tracking of IoT Nodes

13:49.0	Node-100	PublicKeyHash	475187e92b23c27126ed7cc4c4befeb6354e991c669089cf0595caafeeb24fb5
13:51.9	Node-002	MasterKey	8668e12298f0305ac57a44b578fe4e634a9abad1da191356c1fa491e0a823d96
13:51.9	Node-002	SessionCount	5
14:02.0	Node-003	MasterKey	e8645a0e35d03970a4c2161bb1235f2e03921dc867c0e3cf2e7eeab2cd60f8e1
14:02.0	Node-003	SessionCount	5

Figure 10 shows the temporal variation of detected message tampering attacks across network nodes within a specific monitoring window. The graph shows fluctuating attack frequencies, which means that the

monitoring system is actively watching network traffic and logging tampering attempts in real-time. Meanwhile, the lower values indicate relatively stable communication periods. The constant detection of attack bursts confirms that the implemented integrity verification and security mechanisms are actively identifying unauthorized modifications. This time-based analysis emphasizes the quick response and dependability of the intrusion detection system in keeping communications secure within a distributed network.

Figure 11 presents a comparison of the error rates in BB84, E91, CV-QKD, and the proposed post-quantum cryptographic approach. The proposed post-quantum cryptographic approach exhibits an error percentage lower than that of quantum-based schemes. Reduced error percentages indicate higher reliability in secure key exchange. Improved robustness ensures stable session establishment even when there is communication noise. This comparison highlights performance advantages for the proposed mechanism, as a lower error frequency will improve overall system security and further validate the superiority and effectiveness of this new key establishment approach.

Table 1 shows key management and session tracking for different IoT nodes. Each node is assigned a Public Key Hash or Master Key for secure identification and cryptographic operations. The Session Count indicates the number of active sessions for the node, helping manage secure communications. For example, Node-100 has its public key hash recorded, while Node-002 and Node-003 have master keys and currently 5 active sessions each. This ensures secure, session-aware communication across the network.

4.2. Comparative Analysis of the Proposed Model with the Existing Approaches

Table 2 presents the computational and communication complexity analysis of the proposed blockchain-assisted post-quantum IoT framework. The results show that fundamental operations such as Node Registration, Identity Verification, and Blockchain Trust Update maintain constant complexity (O (1)) for both computation and communication, ensuring lightweight and scalability as the network grows. Master Key Generation using Kyber KEM exhibits O(n) computational complexity due to lattice-based operations, while its communication complexity remains O (1). Operations like Session Key Derivation and Session-Level Sifting depend on hash iterations, resulting in O(k) computational complexity and O (1) communication overhead. Finally, Secure Communication and Attack Detection depend on message size (m), leading to O(m) complexity for both computation and communication. Overall, the analysis confirms that the framework maintains low computational and communication overheads, making it suitable for scalable, resource-constrained IoT environments.

Table 2: Performance analysis of the proposed model with the existing models

References	Method	Computational Complexity	Communication Complexity
Kale et al. [18] (2025)	Post-Quantum Cryptography (PQC)	(O (1))	(O (1))
Abood et al. [19] (2025)	Quantum Key Distribution (QKD)	(O (1))	(O (1))
Swetha et al. [20] (2024)	Quantum Random Number Generation (QRNG)	(O (n))	(O (1))
Dhar et al. [21] (2024)	Quantum-Resilient Consensus Protocols	(O (k))	(O (1))
Begimbayeva et al. [22] (2024)	Cross-Chain Security with QKD	(O (m))	(O (m))

4.3. Discussion

The proposed Blockchain-Assisted Quantum-Secure Communication Framework shows that combining post-quantum cryptography with an event-driven blockchain setup gives a suitable compromise between high security and good efficiency in IoT D2D settings. The performance analysis verifies that the gas used for registering nodes stays even when many devices are used, which means economic scalability can be predicted. No extreme change in gas proves that smart contract logic is light and optimized for large-scale IoT. Measurements of latency on the blockchain also prove that confirmation times are kept consistently low, validating the fact that the event-driven interaction model is effective in avoiding unnecessary congestion of the blockchain. The proposed system updates the blockchain only when a security-critical event takes place, such as recording a new node or an existing one being compromised. This method of selective securing considerably scores on communication overhead so far still maintains immutability and transparency of trust. The graphs of the distribution of execution results and the validation of the workflow reflect effective reliability. Most operations of the system resulted in a successful outcome related to verification and secure processing, while the failure cases corresponded with correctly detected differences. This indicates that the mechanisms concerning identity verification, Kyber-based key establishment, and hash-chain session key derivation are strong. The structured

evolution from public key verification through master key generation to session updates also validates that there is logical integration at all layers of cryptography. The session key scalability analysis proves the computational efficiency of the hash-chain mechanism since only hash operations are needed for key evolution. Session establishment remains fast and light, making it ideal for resource-constrained IoT devices. The attack detection results validate the authentication and integrity mechanisms. Attempts at tampering are detected reliably by HMAC verification, while the blockchain trust update mechanism ensures transparent recording and management of compromised nodes. A comparative error-rate evaluation also proves that post-quantum key establishment is more reliable than traditional QKD schemes. The ablation study further confirms that every security component, namely, the Blockchain Trust Layer, Kyber KEM, Hash-Chain Derivation, HMAC Authentication, and Attack Response System, is essential for the robustness of the whole system. The removal of any one component noticeably compromises the security guarantees, thus proving the architectural interdependency of this framework. In general terms, results validate that a proposed framework can achieve quantum resistance, decentralized trust management with forward secrecy as well as scalable lightweight performance without dependence on cloud infrastructure or constant blockchain interactions.

5. Conclusion

This paper presented a decentralized, blockchain-based quantum-secure communication framework for dynamic IoT D2D environments. Kyber KEM is used in the architecture for post-quantum key establishment, accompanied by a hash-chain-based session key derivation mechanism that ensures forward secrecy. AES-256 with HMAC-SHA3 provides strong confidentiality, integrity, and authentication. Unlike traditional models that require continuous interaction with the blockchain, this system operates on an event-driven permissioned blockchain where only security-critical events are recorded. This significantly reduces computational and communication overhead while still achieving decentralized trust and immutability. Performance evaluation showed stable gas usage, low latency, efficient session key generation, predictable cryptographic overhead, and reliable attack detection. Complexity analysis indicated that most operations have constant or low polynomial cost. Hence, it is suitable for scalable resource-constrained IoT systems. In general terms, it provides a lightweight cloud-independent future-proof security for quantum-resilient IoT infrastructures.

Statements and Declarations

Author contributions: All authors contributed to the conception of the problem setting and overall design of the work. K.S built the conceptualization and methodology, S.K implemented the work, Validation and writing was done by both. This version was revised and improved by both authors, who also read and approved the final manuscript.

Funding: No funding was received for conducting this study.

Conflict of interest: The authors declare that they have no conflict of interest.

Availability of data and materials: The data set is not available, only simulation with parameters is used.

Ethical approval: The research is original and the authors of this manuscript create all the figures and tables.

Consent to participate: Not applicable.

Consent for publication: All authors agree with the submission of the manuscript to this journal and possible publication afterwards.

References

1. D. Chawla, S. Kumari, R. S Rathore, P. S. Mehra, A. K. Das, N. Kumar. “Quantum blockchain for internet of things: a systematic review, proposed solutions and challenges”, *Computers and Electrical Engineering*, 126, pp.110524, 2025.
2. V. Maurya, V. Rishiwal, M. Yadav, M. Shiblee, P. Yadav, U. Agarwal, R. Chaudhry. “Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions”, *Peer-to-Peer Networking and Applications*, 18 (1), pp. 53, 2025.
3. M. M. Orabi, O. Emam, H. Fahmy. “Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review”, *Journal of Big Data*, 12 (1), pp. 55, 2025.
4. T. Mazhar, S. F. A. Shah, S. A. Inam, J. B. Awotunde, M. M. Saeed, H. Hamam. “Analysis of integration of IoMT with blockchain: issues, challenges and solutions”, *Discover Internet of Things*, 4 (1), pp. 21, 2024.
5. A. H. Allam, I. Gomaa, H. H. Zayed, M. Taha. “IoT-based eHealth using blockchain technology: a survey,” *Cluster Computing*, 27 (6), pp. 7083-7110, 2024.
6. V. Upadrista, S. Nazir, H. Tianfield. “Secure data sharing with blockchain for remote health monitoring applications: a review”, *Journal of Reliable Intelligent Environments*, 9 (3), pp. 349-368, 2023.

7. T. C. Jermin Jeaunita, T. Ramesh, C. V. S. R. Manjushsree, P. T. Shantala. “A Decentralized and Efficient Crowdfunding Framework for Secure Transactions and User Engagement”, *Radioengineering*, 34 (3), pp. 381-392, 2025.
8. H. Jebamikyous, M. Li, Y. Suhas, R. Kashef. “Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application,” *Discover Artificial Intelligence*, 3 (1), pp. 3, 2023.
9. A. Raj, S. Prakash. “Privacy preservation of the internet of medical things using blockchain,” *Health Services and Outcomes Research Methodology*, 24 (1), pp. 112-139, 2024.
10. E. I. Zafir, A. Akter, M. N. Islam, S. A. Hasib, T. Islam, S. K. Sarker, S. M. Muyeen. “Enhancing security of Internet of Robotic Things: A review of recent trends, practices, and recommendations with encryption and blockchain techniques”, *Internet of Things*, 28, pp. 101357, 2024.
11. S. Alasmari. “Optimized Blockchain-Based Deep Learning Model for Cloud Intrusion Detection”, *International Journal of Advanced Computer Science & Applications*, 15 (9), pp. 914, 2024.
12. A. Qammar, A. Karim, H. Ning, and J. Ding. “Securing federated learning with blockchain: a systematic literature review”, *Artificial intelligence review*, 56 (5), pp. 3951-3985, 2023.
13. A. S. Naik, E. Yeniaras, G. Hellstern, G. Prasad, S. K. L. P Vishwakarma. “From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance”, *Financial Innovation*, 11 (1), pp. 88, 2025.
14. M. S. Kasyapa, C. Vanmathi. “Blockchain integration in healthcare: a comprehensive investigation of use cases, performance issues, and mitigation strategies”, *Frontiers in digital health*, 6, pp. 1359858, 2024.
15. A. I. Okafor, L. A. C. Ahakonye, J. M. Lee, D. S. Kim. “Purequantum: Towards a scalable blockchain channel security in iot networks”, *Blockchain: Research and Applications*, pp. 100372, 2025.
16. Z. G. Al-Mekhlaf, M. A. Saare, J. M. H. Altmemi, M. A. Al-Shareeda, B. A. Mohammed, G. Alshammari, I. Alreshidi. “A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems”, *Journal of King Saud University Computer and Information Sciences*, 37 (6), pp. 126, 2025.
17. M. Taghavi, J. Vahidi. “Quantum-inspired multi-agent reinforcement learning for exploration–exploitation optimization in UAV-assisted 6G network deployment”, *Quantum Machine Intelligence*, 7 (2), pp. 111, 2025.
18. M. R. Kale, Y. A. B. El-Ebiary, L. Sathiya, V. K. Burugari, E. Yulduz, E. Muniyandy, R. Alanazi. “Designing Quantum-Resilient Blockchain Frameworks: Enhancing Transactional Security with Quantum Algorithms in Decentralized Ledgers”, *International Journal of Advanced Computer Science & Applications*, 16 (4), pp. 618, 2025.
19. E. W. Abood, A. A. Yassin, Z. A. Abduljabbar, V. O. Nyangaresi, A. H. Ali. “Provably lightweight and secure IoHT scheme with post-quantum cryptography and fog computing: A comprehensive scheme for healthcare system”, *MethodsX*, pp. 103631, 2025.
20. A. Swetha, S. K. Mohiddin. “Advancing Quantum Cryptography Algorithms for Secure Data Storage and Processing in Cloud Computing: Enhancing Robustness Against Emerging Cyber Threats”, *International Journal of Advanced Computer Science & Applications*, 15 (9), pp. 627-637, 2024.
21. S. Dhar, A. Khare, A. D. Dwivedi, R. Singh. “Securing IoT devices: A novel approach using blockchain and quantum cryptography”, *Internet of things*, 25, pp. 101019, 2024.
22. Y. Begimbayeva, T. Zhaxalykov, M. Makarov, O. Ussatova, S. Tynymbayev Zh. Temirbekova. “Development of a Hybrid Quantum Key Distribution Concept for Multi-User Networks”, *International Journal of Advanced Computer Science and Applications (IJACSA)*, 15 (9), pp. 409-415, 2024.
23. P. Helo, Y. Hao, and A. Gunasekaran. “Use of non-fungible tokens in operations and supply chain management”, *International Journal of Production Research*, 63 (14), pp. 5099-5121, 2024.
24. N. Nagy, S. Alnemer, L. M. Alshuhail, H. Alobiad, T. Almulla, F. A. Alrumaihi, M. Nagy. “Module-lattice-based key-encapsulation mechanism performance measurements”, *Sci*, 7 (3), pp. 91, 2025.
25. A. A. M. A. Ali, M. J. Hazar, M. Mabrouk, M. Zrigui. “Proposal of a modified hash algorithm to increase blockchain security”, *Procedia Computer Science*, 225, pp. 3265-3275, 2023.
26. L. Zhou, A. Diro, A. Saini, S. Kaisar, P. C. Hiep. “Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities”, *Journal of Information Security and Applications*, 80, pp. 103678, 2024.
27. A. A. Agarkar, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, L. Kulkarni. “Blockchain aware decentralized identity management and access control system”, *Measurement: Sensors*, 31, pp. 101032, 2024.
28. W. Zeng, Y. Wang, K. Liang, J. Li, X. Niu. “Advancing emergency supplies management: a blockchain-based traceability system for cold-chain medicine logistics”, *Advanced Theory and Simulations*, 7 (4), pp. 2300704, 2024.
29. Z. A. Hussein, O. A Naser. “Evaluation of AES-256 encryption and machine learning for securing GSM communications against sniffing attacks”, *Egyptian Informatics Journal*, 32, pp. 100832, 2025.
30. H. G. Reyes-Anastacio, J. L. Gonzalez-Compeán, V. J. Sosa-Sosa, R. Marcelín-Jiménez, M. Morales-Sandoval. “Kulla-RIV: A composing model with integrity verification for efficient and reliable data processing services”, *Software: Practice and Experience*, 54 (8), pp. 1516-1542, 2024.
31. M. T. Abdelaziz, A. Radwan, H. Mamdouh, A. S. Saad, A. S. Abuzaid, A. A. AbdElhakeem, M. S. Darweesh. “Enhancing network threat detection with random forest-based NIDS and permutation feature importance”, *Journal of Network and Systems Management*, 33 (1), pp. 2, 2025.