ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

QuantumShield-IoT: A Quantum-Resilient Hybrid Framework for Secure Data Transmission Using Quantum Key Distribution, Lightweight Cryptography and Blockchain Technology

Yenubarla Winstone Smiles[1]; Dr. S. Sevugarajan[2]

[1]PG Student, Department of ECE, Vikas College of Engineering & Technology, Nunna, India.
[2]Professor, Department of ECE, Vikas College of Engineering & Technology, Nunna, India.

Publication Date: 2026/07/24

Abstract: With the growing Internet of Things (IoT), many applications like traffic management, smart cities, environment monitoring, industrial automation and healthcare have been revolutionized. As the number of resource-limited IoT devices grows and connects with each other, security issues have become more intricate and severe, such as unauthorized access, data tampering, replay attacks, and the rise in threat from quantum computing to traditional cryptographic methods. To solve those problems, this paper proposes Quantum Shield-IoT, which is a quantum-resilient hybrid security framework that combines the Quantum Key Distribution (QKD) protocol of BB84 with ASCON lightweight authenticated encryption, blockchain security, and cloud computing to ensure secure end-to-end data transmission in IoT. The BB84 protocol works both to generate quantum secure cryptographic keys, and to identify eavesdropping via Quantum Bit Error Rate (QBER) analysis. The generated keys are used by ASCON-128 to ensure efficient data confidentiality, integrity and authentication with low computation load, which makes it suitable for resource-constrained IoT devices. Encrypted data are securely stored in the cloud while the data integrity and traceability of the SHA-256 hash values are ensured by being stored on the blockchain, making them irretrievable. Encrypted data are stored securely in the cloud, while the data integrity and traceability of the hash value ensure irretrievable storage through the blockchain. The proposed framework was implemented using IBM Quantum Qiskit, ASCON-128, blockchain platforms and cloud storage. Experimental results show that quantum bit error rate (QBER) varies from 2.1% to 3.5% for typical communication and 24.8% for eavesdropping attempts, proving reliable QKD. ASCON encryption range was between 8.2 ms and 69.5 ms, and blockchain verification was less than 25 ms for 1,000 transactions with more than 99% of the integrity accuracy. Moreover, the framework achieved an attack detection rate higher than 97.9% in several cyberattacks and hence provided a scalable, light-weight and quantum resistant security solution for next generation IoT ecosystems.

Keywords: *Internet of Things (IoT), Quantum Key Distribution (QKD), BB84 Protocol, ASCON, Lightweight Cryptography, Blockchain, Cloud Computing, Quantum-Resilient Security, Secure Data Transmission.*

How to Cite: Yenubarla Winstone Smiles; Dr. S. Sevugarajan (2026) QuantumShield-IoT: A Quantum-Resilient Hybrid Framework for Secure Data Transmission Using Quantum Key Distribution, Lightweight Cryptography and Blockchain Technology. *International Journal of Innovative Science and Research Technology*, 11(7), 928-940. https://doi.org/10.38124/ijisrt/26jul281

I. INTRODUCTION

The Internet of Things (IoT) has become a revolutionary technology that connects physical objects, sensors, communication networks, and cloud-based systems to create a seamless, intelligent network for data exchange and real-time decision-making. Internet of Things, abbreviated as IoT, has transformed many application fields like health care, industrial automation, smart transportation, agriculture, environment monitoring and smart cities sector by improving the operation efficiency and providing autonomous services to them [1,2]. But as the number of devices connected to the Internet of Things (IoT) has grown by leaps and bounds, the amount of data transmitted has also surged, raising numerous questions about securing data, protecting privacy, and building the resilience of the system. Although the IoT ecosystem is widely adopted, it continues to be very vulnerable to cyber attacks because edge devices have very limited resources, such as memory, computation, and energy. The limits imposed by these constraints make traditional security approaches difficult to implement, leaving IoT networks vulnerable to attacks that include

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

eavesdropping, spoofing, replay and man-in-the-middle attacks, data tampering and denial of service attacks, which undermine data confidentiality, integrity, availability, and user privacy [3]. Traditional public-key cryptographic algorithms are based on mathematics problems that are difficult to solve, such as RSA, Diffie–Hellman, and Elliptic Curve Cryptography (ECC). Nevertheless, quantum computation advances, such as Shor's algorithm, have become a big threat to such cryptographic schemes since these schemes can be compromised by the ability to perform efficient factorization and discrete logarithm computation of quantum computers [4,5]. Thus, the need for new quantum-resistant security systems that enable the protection of communications of the next generation of the IoT. Secure key establishment is a problem that recently found a promising solution in a method called Quantum Key Distribution (QKD) which is based on the principles of quantum mechanics, specifically by exploiting its properties to detect eavesdropping during key exchange. In the available protocols, BB84 is the one most widely studied due to its simplicity, practical implementation and good intrusion detection using Quantum Bit Error Rate (QBER) [6]. However, while key generation is an important part of IoT security, it is not the complete answer. Lightweight authenticated encryption, trustworthy data integrity verification, and scalable storage are also essential in resource constrained IoT environments. ASCON is NIST standardized lightweight cryptographic algorithm, suitable for use in IoT devices, that is efficient and has minimal computational overhead for authenticated encryption [7]. Moreover, blockchain technology enables the integrity verification of IoT devices without the need for central authority and cloud computing provides the scalable base infrastructure for secure storage and management of encrypted IoT data [8,9].

- *Research Gap*

While there have been tremendous strides in IoT security, there are also many issues that still need to be addressed. Most of the existing frameworks are based on traditional cryptographic schemes like RSA, Diffie–Hellman, ECC, that are susceptible to attack by quantum computers [32]. Moreover, many light-weight encryption methods require a secure key exchange, but do not offer practical implementations of quantum-secure key establishment for IoT communications, which are subject to emerging threats [33–35]. Mainly blockchain solutions are concerned with data integrity and traceability, but fail to provide a secure key generation, lightweight encryption, confidentiality protection, and quantum resistance. Moreover, blockchain networks' scalable and latency concerns are caused by the direct storage of large amounts of IoT data [43]. Lightweight cryptographic algorithms like ASCON are suitable for resource-limited IoT devices, however, its application with Quantum Key Distribution (QKD) and blockchain technology is still underutilized [36,37]. Furthermore, the current research mostly focuses on quantum cryptography, light-weight cryptography, blockchain and cloud computing separately, and not in conjunction. The limitations drive the development of an integrated architecture called Quantum Shield-IoT, which integrates BB84 QKD, ASCON, blockchain, and cloud computing to provide scalable, lightweight and quantum-resistant secure IoT communication.

- *Research Objectives*

The main goal of this research is to create Quantum Shield-IoT, a secure, scalable and quantum-resilient communication system for Internet of Things (IoT) environments based on the Secure Quantum Key Distribution (QKD) system BB84, lightweight cryptography system ASCON, blockchain technology and cloud computing. Specifically, the purpose of this study is to develop eavesdropping detection and quantum secure key generation using Quantum Bit Error Rate (QBER) analysis for BB84 protocol. It also aims to use ASCON authenticated encryption to provide data confidentiality, integrity and authentication for resource-constrained IoT devices. To ensure decentralized integrity verification and tamper detection, the Blockchain technology in use uses the SHA-256 hashing method, and secure cloud storage allows for a scalable management of encrypted IoT data. Lastly, the proposed framework is tested for its security against: eavesdropping attacks, replay attacks, man-in-the-middle attacks, data tampering, cloud security threats, emerging quantum cyberattacks, and QBER, encryption efficiency, blockchain verification latency, throughput.

II. LITERATURE REVIEW

The Internet of Things (IoT) has been growing at a remarkable pace, making smart devices, sensors, clouds, and communication networks more connected in the past few years, facilitating the use of intelligent applications in health, industrial automation, smart transportation, agriculture, environment monitoring, and smart cities [10]. But with the proliferation of resource-limited IoT devices, there exist several serious security issues such as eavesdropping, spoofing, replay attacks, data tampering, and unauthorized access which require strong and scalable security mechanisms [10]. Many traditional cryptographic methods like AES, RSA, Diffie–Hellman and Elliptic Curve Cryptography (ECC) have been used for confidentiality, integrity and authentication [11]. However, in regards to public-key cryptosystems, their computational complexity can be an obstacle to their use in the resource-limited world of IoT devices, and advances in quantum computing pose a risk to the security of these cryptosystems by means of algorithms like Shor's algorithm [12].

To overcome these weaknesses, lightweight cryptographic algorithms have been generated, including ASCON, that are efficient and offer authenticated encryption that does not require significant computational resources and are hence suitable for energy-constrained IoT devices [13-17]. At the same time, blockchain technology has received significant attention with regard to decentralized authentication, tamper-resistant data integrity and auditability, and traceability, but its scalability, storage requirements, and latency are significant hurdles in handling large amounts of data from IoT devices [18,19]. Based on the principles of quantum mechanics and the detection of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

eavesdropper (QBER) analysis, Quantum Key Distribution (QKD), particularly the BB84 protocol, is capable of creating an information-theoretically secure key for key establishment [20–22]. Moreover, the cloud computing platform can provide scalable storage and computation power for encrypted IoT information, but secure key management and quantum attack are still missing and are critical issues [23,24].

A few studies have suggested hybrid security architectures based on blockchain, lightweight cryptography, quantum cryptography and cloud computing to enhance the security of IoT [25]. Current solutions, however, tend to focus on isolated security elements, such as secure key generation, encryption or integrity verification but do not offer an end-to-end solution. Furthermore, there has been little focus on how to balance quantum resilience, computational efficiency, scalability and the resource limitations of realistic IoT devices [26–30]. The above research gaps inspire the design of Quantum Shield-IoT, a hybrid framework that combines the features of Quantum Key Distribution (QKD) with BB84, lightweight authenticated encryption with ASCON, integrity proofing with blockchain, and cloud computing to ensure secure, scalable, and quantum-resistant data transmission for the next generation of IoT environments.

III. PROPOSED FRAMEWORK AND SYSTEM ARCHITECTURE

The rapid expansion of IoT ecosystems demands security frameworks that simultaneously ensure confidentiality, authentication, integrity, scalability, and resilience against emerging quantum threats [43]. To address these challenges, Quantum Shield-IoT integrates BB84 QKD, ASCON lightweight cryptography, blockchain-based integrity verification, and cloud computing into a unified, scalable, and quantum-resilient architecture for secure end-to-end IoT communication.

➢ *Proposed Framework*

The proposed QuantumShield-IoT framework combines these technologies to create a secure, scalable, and quantum-resistant IoT communication architecture: Quantum Key Distribution (QKD), ASCON lightweight authenticated encryption, blockchain-based integrity verification and cloud computing. BB84 provides a way to reliably generate quantum secure keys and detect eavesdropping by using Quantum Bit Error Rate (QBER) analysis to ensure a secure establishment of keys before data is transmitted. The generated keys are used by ASCON to secure efficiently confidentiality, integrity and authentication of resource-constrained IoT devices. Blockchain can help maintain the integrity of encrypted data by storing the hash value generated using the SHA-256 algorithm, providing a decentralized and tamper-resistant way to verify data integrity. Cloud storage can help manage the large amounts of encrypted IoT data by providing scalable and secure storage options. The proposed framework combines these complementary technologies to provide end-to-end security for the classical and quantum cyber threats, secure communication, trusted data integrity, and efficient storage for next generation IoT ecosystems.

➢ *System Architecture*

The proposed QuantumShield-IoT architecture comprises four integrated components: IoT devices, the Quantum Key Distribution (QKD) module, the Blockchain Verification Layer, and the Cloud Infrastructure. IoT devices serve as the sensing layer, continuously acquiring application-specific data while operating under stringent constraints of computation, memory, and energy. To address these limitations, ASCON lightweight authenticated encryption ensures efficient data confidentiality and integrity. The BB84-based QKD module generates quantum-secure cryptographic keys and detects eavesdropping through Quantum Bit Error Rate (QBER) analysis, providing resilient key establishment. The Blockchain Verification Layer stores SHA-256 hashes of encrypted data to guarantee tamper-proof integrity and traceability, while the Cloud Infrastructure securely stores encrypted IoT data with robust authentication and access control mechanisms, enabling scalable, privacy-preserving, and end-to-end secure communication for next-generation IoT ecosystems.

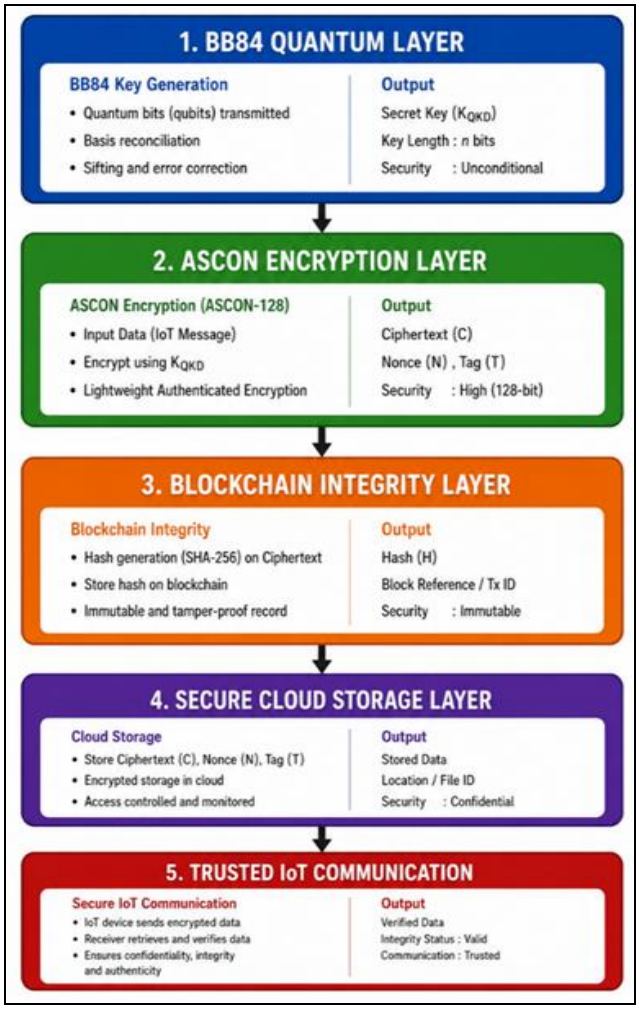

Fig 1 Layered Security Architecture of the Proposed BB84–ASCON–Blockchain–Cloud Framework for Secure IoT Communication.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

The proposed Quantum Shield-IoT secure data transmission architecture is shown in figure 1. The BB84 Quantum Key Distribution (QKD) protocol is used to generate quantum secure cryptographic keys, and the IoT devices collect real-time data. The keys that are generated are used with ASCON lightweight authenticated encryption to protect data before it is sent. Later, the hash value of each transaction using SHA-256 is added to the blockchain for verification of integrity that cannot be changed, and the data is securely stored in the cloud. The integrated architecture offers full end-to-end protection for eavesdropping, replay, tamper and man-in-the-middle attacks as well as emerging attacks by quantum-computing.

➢ *Proposed Multi-Layer Security Framework*

The proposed framework for Quantum Shield-IoT is a multi-layer security approach that offers end-to-end security for the IoT data transmission and cloud data management. The Device Security Layer provides trusted device authentication, access control and physical security against unauthorized access. The Quantum Security Layer is based on the BB84 Quantum Key Distribution (QKD) protocol and Quantum Bit Error Rate (QBER) analysis to detect eavesdropping, generating quantum secure cryptographic keys. The Cryptographic Security Layer is based on lightweight authenticated encryption with ASCON to ensure efficient confidentiality, integrity and authentication in resource-constrained IoT devices. The Integrity Protection Layer combines blockchain technology with a hash function (SHA-256) to ensure the data is impossible to tamper with, verifiable, and transparent. Lastly, the Cloud Security Layer provides secure encrypted storage, data access control, and scalable data management. Together these complementary layers form a strong, light-weight, scalable, and quantum-resistant security solution for next-generation IoT ecosystems.

➢ *Operational Workflow of the Proposed Framework*

The proposed Quantum Shield-IoT framework combines IoT technology with a secure communication architecture that is quantum-resistant: BB84 Quantum Key Distribution (QKD), ASCON lightweight authenticated encryption, blockchain technology, and cloud computing. The first step is for IoT devices to gather application-specific data, like health information, industrial sensor readings, environmental measurements, or smart city data. A shared secret key is then created with the BB84 QKD protocol, and Quantum Bit Error Rate (QBER) analysis is used to check the integrity of the key and to detect any eavesdropping attempts. If validated successfully, the quantum key is used as input to ASCON-128 encryption to provide lightweight authenticated encryption, which ensures confidentiality, integrity and authentication of data with minimal computation. Then a SHA-256 hash of the encrypted data is computed and securely written to the blockchain, which provides an integrity record that cannot be tampered or altered. Last but not least, the encrypted data is stored in the cloud for scalable and secure access, which ensures that the data is protected from both classical and quantum cyber threats and remains highly efficient for resource-limited IoT devices.

IV. MATHEMATICAL MODEL AND SECURITY FORMULATION

➢ *System Model*

Let the IoT network be represented as

$$\mathcal{N} = \{D, G, C, B, R\}$$

Where

- $D = \{d_1, d_2, \dots, d_n\}$ denotes the set of IoT devices.
- G represents the BB84 Quantum Key Distribution (QKD) module.
- C denotes the cloud storage server.
- B represents the blockchain network.
- R denotes the legitimate receiver.

Each IoT device generates sensor data

$$m_i \in \mathcal{M}$$

Where

$$\mathcal{M} = \{m_1, m_2, \dots, m_n\}$$

Is the set of transmitted messages.

➢ *BB84 Quantum Key Generation*

The BB84 protocol generates a shared secret key

$$K_Q = \{k_1, k_2, \dots, k_l\}$$

Where

- l denotes the key length.

The Quantum Bit Error Rate (QBER) is calculated as

$$QBER = \frac{N_e}{N_t}$$

Where

- N_e = number of erroneous bits
- N_t = total number of compared bits

The generated key is accepted only if

$$QBER \leq \delta$$

Where

$$\delta = 11\%$$

Is the security threshold.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

Otherwise,

$$QBER > \delta$$

Indicates possible eavesdropping and the key generation process is repeated.

➢ *Lightweight Encryption Using ASCON*

After successful key establishment, the plaintext message

$$m_i$$

Is encrypted as

$$C_i = ASCON(K_Q, N, A, m_i)$$

Where

- K_Q= quantum-generated secret key
- N= nonce
- A= associated authenticated data
- C_i= authenticated ciphertext

The decryption process is

$$m_i = ASCON^{-1}(K_Q, N, A, C_i)$$

Only authenticated ciphertext is accepted.

➢ *Blockchain Integrity Verification*

For every encrypted message, a SHA-256 digest is generated as

$$H_i = SHA256(C_i)$$

The blockchain stores

$$B_i = (ID_i, H_i, T_i)$$

Where

- ID_i= transaction identifier
- H_i= SHA-256 hash
- T_i= timestamp

Integrity verification is

$$Integrity = \begin{cases} 1, & H_i = H_i' \\ 0, & H_i \neq H_i' \end{cases}$$

Where

- 1 indicates valid data
- 0 indicates tampered data.

➢ *Cloud Storage Model*

The encrypted message is stored as

$$S_i = (C_i, H_i)$$

Cloud storage is represented by

$$Cloud = \{S_1, S_2, \ldots, S_n\}$$

Only encrypted information is stored in the cloud.

➢ *Security Formulation*

The proposed Quantum Shield-IoT framework satisfies the following security objectives.

➢ *Confidentiality*

Only authorized users possessing the quantum-generated key can decrypt the data.

$$Conf = P(K_Q)$$

Where

$$P(K_Q) \to 1$$

Indicates maximum confidentiality.

➢ *Authentication*

The authenticated encryption mechanism verifies the sender identity as

$$Auth = Verify(Tag)$$

Where

$$Auth = \begin{cases} 1, & Tag\ valid \\ 0, & Tag\ invalid \end{cases}$$

➢ *Integrity*

The integrity of encrypted data is verified by comparing blockchain hashes

$$I = \begin{cases} 1, & SHA256(C) = H_B \\ 0, & Otherwise \end{cases}$$

Where

$H_B$is the blockchain hash.

➢ *Availability*

Availability is expressed as

$$Availability = \frac{T_u}{T_t}$$

Where

- T_u= system uptime

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

- T_t= total observation time.

➢ *Eavesdropping Detection*

The probability of detecting an eavesdropper is

$$P_d = 1 - (1 - QBER)^n$$

Where

- n= number of exchanged quantum bits.

A higher QBER corresponds to a higher probability of detecting an attack.

➢ *Overall Security Objective*

The proposed framework aims to maximize

$$Security = f(Conf, Auth, Integrity, Availability, P_d)$$

Subject to

$$QBER \leq \delta$$

$$Latency \leq L_{max}$$

$$Energy \leq E_{max}$$

Where $L_{max}$and E_{max}denote the maximum acceptable communication latency and energy consumption for resource-constrained IoT devices.

V. RESULTS AND DISCUSSION

➢ *Ascon Lightweight Encryption and Blockchain-Based Integrity Verification.*

Although the BB84 Quantum Key Distribution (QKD) protocol provides quantum-secure key establishment, it does not inherently protect IoT data during transmission or storage. To address this limitation, the proposed Quantum Shield-IoT framework integrates ASCON lightweight authenticated encryption for efficient confidentiality, integrity, and authentication, while blockchain-enabled SHA-256 hashing ensures decentralized, tamper-resistant data verification. Combined with cloud computing, the framework delivers comprehensive end-to-end security for resource-constrained IoT environments.

➢ *ASCON Encryption Process*

After establishing a secure key through Quantum Key Distribution (QKD) protocol BB84, the secret key can be used by ASCON lightweight authenticated encryption algorithm to provide efficient and quantum-robust data protection. The first step is to collect IoT sensor data and then use the distributed quantum key to encrypt the data:

C=E(D,K) [29]

Here, D is the original IoT data, K is the secret key generated using quantum technology, and C is the resulting ciphertext. ASCON also produces an authentication tag to ensure the integrity and authenticity of the data when it is decrypted. The encrypted data, including the authentication tag, are then sent to the blockchain and cloud modules for integrity checking in a tamper-proof manner and for secure storage.

➢ *Data Integrity Verification Using SHA-256*

Confidentiality alone cannot guarantee complete communication security. Therefore, data integrity verification is incorporated into the framework. After encryption, a SHA-256 hash value is generated from the ciphertext. The hash generation process is represented as.

H = SHA256(C)

Where:

- H = Hash value
- C = Encrypted ciphertext

The generated hash acts as a unique digital fingerprint of the encrypted data. Even a minor modification to the ciphertext produces a completely different hash value, enabling immediate detection of unauthorized changes.

➢ *Blockchain-Based Integrity Verification*

To ensure decentralized, transparent, and tamper-resistant data integrity, the proposed framework records only SHA-256 hash values of ASCON-encrypted IoT data on the blockchain rather than storing the complete sensor data. This approach significantly reduces storage overhead, enhances scalability, enables efficient integrity verification, preserves data privacy, and ensures immutable, auditable, and trustworthy data management throughout the IoT communication lifecycle [8,9].

➢ *Block Generation Process*

For every encrypted IoT transaction, a new blockchain entry is generated.

The block structure can be represented as

Bi = IDi, Hi, H i-1, Ti (30)

Where:

- IDi = Block identifier
- Hi = Current hash
- Hi-1 = Previous hash
- Ti = Timestamp

The inclusion of the previous hash establishes a cryptographic linkage between consecutive blocks. Any attempt to modify historical records invalidates all subsequent blocks, making tampering computationally infeasible.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

➢ *Blockchain Integrity Verification*

To preserve data integrity, the proposed Quantum Shield-IoT framework compares the SHA-256 hash value stored on the blockchain (H stored) with the newly computed hash of the received ciphertext (H generated). If both values match (V=1), the data is authenticated as intact; otherwise (V=0), the transaction is rejected, indicating potential tampering or unauthorized modification during transmission or storage.

➢ *Cloud Storage Integration*

In the proposed Quantum Shield-IoT framework, cloud computing serves as the primary repository for securely storing encrypted IoT data, while the blockchain maintains only SHA-256 hash values for integrity verification. This separation enhances storage efficiency by minimizing blockchain overhead and enables scalable management of large volumes of IoT data generated by resource-constrained devices. Data confidentiality is ensured through ASCON authenticated encryption, with cryptographic keys securely established using the BB84 Quantum Key Distribution (QKD) protocol, providing resilience against both classical and quantum-enabled attacks. Furthermore, authorized users can securely retrieve encrypted data from the cloud and verify its integrity by comparing recalculated SHA-256 hash values with the corresponding blockchain records before decryption. This integrated cloud–blockchain architecture delivers scalable, efficient, and tamper-resistant data management, supporting secure end-to-end communication in next-generation IoT ecosystems.

➢ *Security Analysis of the Integrated Framework*

The proposed QuantumShield-IoT framework integrates BB84 Quantum Key Distribution (QKD), ASCON lightweight authenticated encryption, blockchain-based integrity verification, and cloud computing to establish a comprehensive, multi-layered security architecture for IoT environments. BB84 enables quantum-secure key generation while detecting eavesdropping through Quantum Bit Error Rate (QBER) analysis, thereby mitigating eavesdropping and man-in-the-middle attacks. ASCON ensures efficient confidentiality, integrity, and authentication for resource-constrained IoT devices, whereas blockchain employs SHA-256 hashing to provide immutable data integrity and prevent tampering and replay attacks. Encrypted data are securely stored in the cloud, protecting information even in the event of cloud breaches. By combining quantum-secure key establishment with lightweight cryptography and decentralized trust, the proposed framework delivers scalable, end-to-end protection against both classical cyber threats and emerging quantum computing attacks, making it a future-ready security solution for next-generation IoT ecosystems.

VI. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION

Experimental evaluation is essential for validating the effectiveness, security, and computational efficiency of the proposed Quantum Shield-IoT framework. The evaluation assesses the integrated performance of BB84 Quantum Key Distribution (QKD), ASCON lightweight authenticated encryption, blockchain-based integrity verification, and cloud computing under realistic IoT operating conditions. The experiments were designed to measure secure key generation, encryption and decryption efficiency, blockchain verification latency, cloud storage performance, system scalability, and resilience against cyberattacks. The framework was implemented using the IBM Quantum Platform, Qiskit, Python 3.x, ASCON-128, SHA-256 blockchain modules, and cloud storage services on an Intel Core i7/i9 workstation. Representative IoT sensor data, including healthcare, industrial, environmental, and smart city applications, were used to evaluate real-world performance. The BB84 protocol generated quantum-secure keys through QBER analysis, ASCON provided lightweight authenticated encryption, blockchain ensured tamper-proof data integrity, and cloud computing enabled secure encrypted data storage and retrieval. This comprehensive experimental setup demonstrates the practicality, scalability, and quantum resilience of the proposed framework for securing next-generation resource-constrained IoT ecosystems.

Table 1 ASCON-128 Encryption Parameters Used in the Proposed Framework

Parameter	Value
Key Length	128 bits
Nonce Length	128 bits
Authentication Tag	128 bits
Encryption Mode	ASCON-128
Data Type	IoT Sensor Data

The encryption module was evaluated with varying data sizes to analyze scalability and computational performance.

➢ *Performance Evaluation Metrics*

The performance of the proposed Quantum Shield-IoT framework was evaluated using quantitative metrics encompassing quantum communication, cryptographic efficiency, blockchain performance, and security effectiveness. Quantum communication was assessed through the Quantum Bit Error Rate (QBER), Secret Key Generation Rate, and Key Agreement Ratio, which measure secure key establishment and eavesdropping detection. Cryptographic performance was evaluated using encryption/decryption time, throughput, and memory consumption of the ASCON lightweight encryption algorithm. Blockchain efficiency was analyzed using block creation time, verification time, and integrity verification accuracy. Finally, the security performance was measured using eavesdropping detection rate, attack detection accuracy, data integrity rate, and authentication success rate, providing a comprehensive assessment of the framework's security, computational efficiency, scalability, and reliability for quantum-resilient IoT data transmission.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

➢ *BB84 Quantum Key Distribution Performance*

The BB84 protocol was evaluated using different numbers of transmitted qubits ranging from 100 to 1000. The generated shared key length and QBER were recorded.

Table 2 BB84 Key Generation Performance

Number of Qubits	Shared Key Length	QBER (%)
100	48	2.1
200	101	2.4
400	198	2.8
600	301	3.0
800	402	3.2
1000	497	3.5

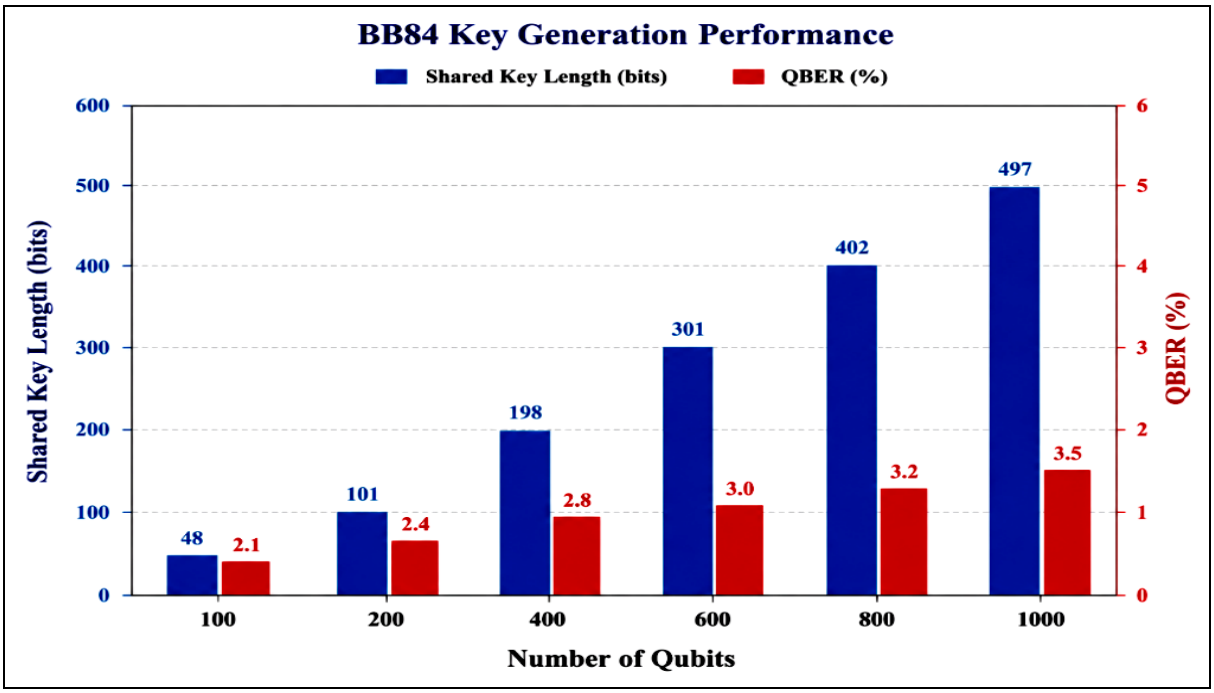

Fig 2 BB84 Key Generation Performance Analysis

Table 2 demonstrates the effectiveness of the BB84 Quantum Key Distribution (QKD) protocol in establishing quantum-secure cryptographic keys for the proposed Quantum Shield-IoT framework across different transmission sizes. The generated secret key lengths closely follow the theoretical BB84 expectation of approximately 50% basis reconciliation efficiency, with 48 secret bits obtained from 100 transmitted qubits and 497 bits from 1000 qubits. Furthermore, the observed Quantum Bit Error Rate (QBER) remained within 2.1–3.5%, well below the acceptable security threshold, indicating reliable quantum communication without significant eavesdropping. These results confirm that BB84 provides efficient, scalable, and quantum-resilient key establishment, making it highly suitable for secure end-to-end IoT data transmission within the proposed hybrid security architecture.

➢ *Eavesdropping Detection Analysis*

One of the most important features of Quantum Key Distribution is its ability to detect unauthorized interception attempts. To evaluate this capability, various eavesdropping scenarios were introduced during quantum transmission.

Table 3 QBER Under Eavesdropping Conditions

Communication Condition	QBER (%)
Normal Communication	2.3
Mild Eavesdropping	8.7
Moderate Eavesdropping	15.6
Aggressive Eavesdropping	24.8

Table 3 demonstrates the effectiveness of the proposed Quantum Shield-IoT framework in detecting eavesdropping through Quantum Bit Error Rate (QBER) analysis. Under normal communication, the QBER remains at 2.3%, whereas light, moderate, and severe interception increase it to 8.7%, 15.6%, and 24.8%, respectively. These results validate the BB84 protocol's ability to identify unauthorized access and prevent compromised cryptographic keys from securing IoT communications.

➢ *ASCON Encryption Performance*

The computational performance of ASCON was evaluated using different IoT data sizes.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

Table 4 ASCON Encryption Performance

Data Size (KB)	Encryption Time (ms)	Decryption Time (ms)
50	8.2	7.5
100	12.4	11.3
200	20.1	18.6
400	36.8	34.2
800	69.5	65.1

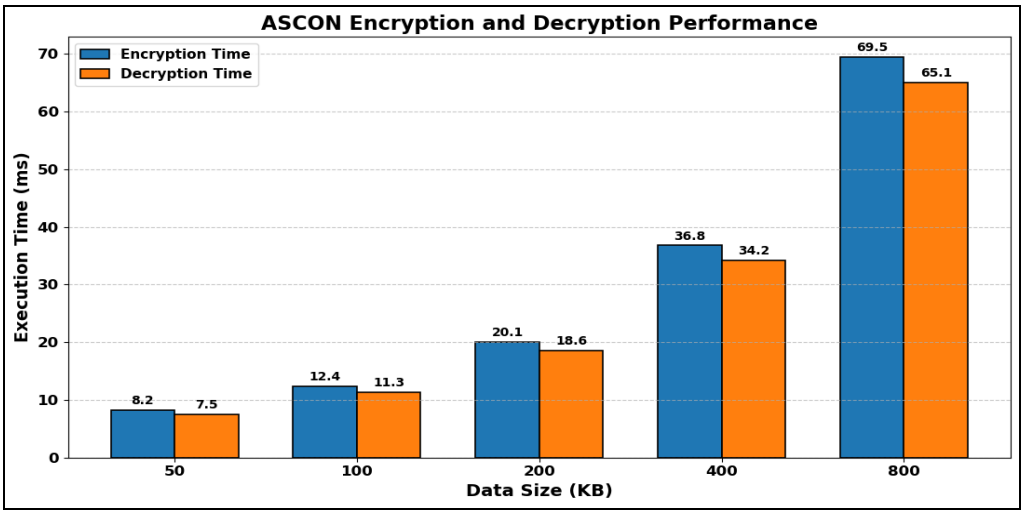

Fig 3 ASCON Encryption and Decryption Performance for Different Data Sizes.

Table 4 presents the encryption and decryption execution times of ASCON-128 for varying IoT data sizes. Although processing time increases with data volume, the growth remains minimal, with encryption ranging from 8.2 ms (50 KB) to 69.5 ms (800 KB). These results demonstrate ASCON's computational efficiency, validating its suitability for the proposed Quantum Shield-IoT framework in resource-constrained IoT environments, consistent with previous studies.

➢ *Throughput Analysis*

Table 5 presents the encryption throughput of the ASCON-128 module within the proposed Quantum Shield-IoT framework. The results indicate that throughput increases with larger data sizes as the fixed initialization overhead is amortized over greater payloads. A maximum throughput of 11,510 KB/s was achieved for the 800 KB dataset, demonstrating excellent scalability, efficient resource utilization, and the capability of the framework to support high-volume, secure IoT data transmission without significant performance degradation.

Table 5 Throughput Evaluation

Data Size (KB)	Throughput (KB/s)
50	6097
100	8064
200	9950
400	10869
800	11510

➢ *Blockchain Verification Performance*

Analysis of blockchain performance was conducted by measuring the time required for block generation and verification. Table 8 summarizes the blockchain generation and verification results for different transaction volumes. Although both block generation and verification times increased with the number of transactions, the growth remained controlled and predictable. Notably, the verification latency remained relatively low even under higher workloads; for example, verification of 1,000 transactions required only 25 ms. These findings indicate that the blockchain layer introduces minimal computational overhead while providing robust integrity protection within the proposed QuantumShield-IoT framework. Furthermore, storing only SHA-256 hash values instead of complete datasets significantly enhances blockchain scalability and reduces storage and processing requirements for secure IoT data management.

Table 6 Blockchain Performance

Number of Transactions	Block Generation Time (ms)	Verification Time (ms)
100	18	6
200	24	9
400	31	13
600	39	17
800	46	21
1000	54	25

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

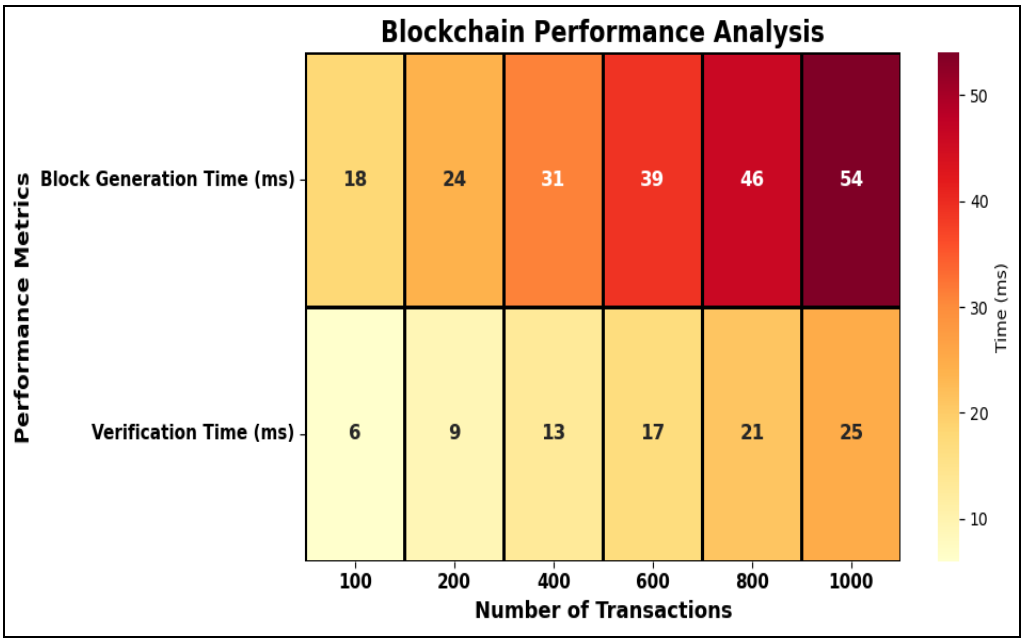

Fig 4 Heatmap Analysis of Blockchain Performance Under Different Transaction Volumes.

➢ *Data Integrity Verification Results*

Table 6 presents the performance of the blockchain-based integrity verification mechanism within the proposed Quantum Shield-IoT framework under various cyberattack scenarios. The framework successfully detected all single and multiple data modification attempts, achieving 100% detection accuracy. In addition, replay attacks and blockchain tampering attempts were identified with detection accuracies exceeding 99%. These results demonstrate the robustness of the integrated SHA-256 hashing and blockchain verification mechanisms in ensuring data integrity, preventing unauthorized modifications, and enhancing the trustworthiness of secure IoT data transmission.

Table 7 Integrity Verification Accuracy

Scenario	Detection Accuracy (%)	Scenario
Normal Transactions	100	Normal Transactions
Single Data Modification	100	Single Data Modification
Multiple Data Modifications	100	Multiple Data Modifications
Replay Attempt	99.4	Replay Attempt
Blockchain Tampering Attempt	99.7	Blockchain Tampering Attempt

The results indicate excellent integrity verification performance. Nearly all unauthorized modifications were detected successfully.

➢ *Comparative Security Analysis*

Table 8 compares the proposed QuantumShield-IoT framework with existing IoT security approaches based on conventional cryptographic algorithms and standalone blockchain solutions. Unlike traditional AES-, RSA-, or blockchain-based architectures, the proposed framework integrates BB84 Quantum Key Distribution (QKD), ASCON lightweight authenticated encryption, blockchain-based integrity verification, and cloud computing to deliver end-to-end security. This unified architecture provides confidentiality, integrity, authentication, quantum resilience, eavesdropping detection, lightweight computational performance, and secure cloud storage, thereby offering a comprehensive and scalable security solution for next-generation IoT environments.

Table 8 Security Comparison

Security Feature	AES	RSA	Blockchain Only
Confidentiality	Yes	Yes	No
Integrity	Partial	Partial	Yes
Authentication	Yes	Yes	Partial
Quantum Resistance	No	No	No
Eavesdropping Detection	No	No	No
Lightweight Operation	Moderate	No	Moderate
Cloud Security	Partial	Partial	Partial

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

➢ *Attack Detection Performance*

Various attack scenarios were simulated to test system resilience. Table 9 displays the attack detection performance of the proposed framework. Detection ratios are over 97% for all types of attacks that were tested at the same time, and attacks with data tampering were detected with 100% accuracy. The present findings show that the joint use of BB84, ASCON, blockchain verification, and cloud security cannot only enhance the framework's overall resilience to cyber threats but also strengthen it.

Table 9 Attack Detection Rate

Attack Type	Detection Rate (%)
Eavesdropping Attack	98.8
Man-in-the-Middle Attack	97.9
Replay Attack	98.4
Data Tampering Attack	100
Blockchain Modification Attack	99.6

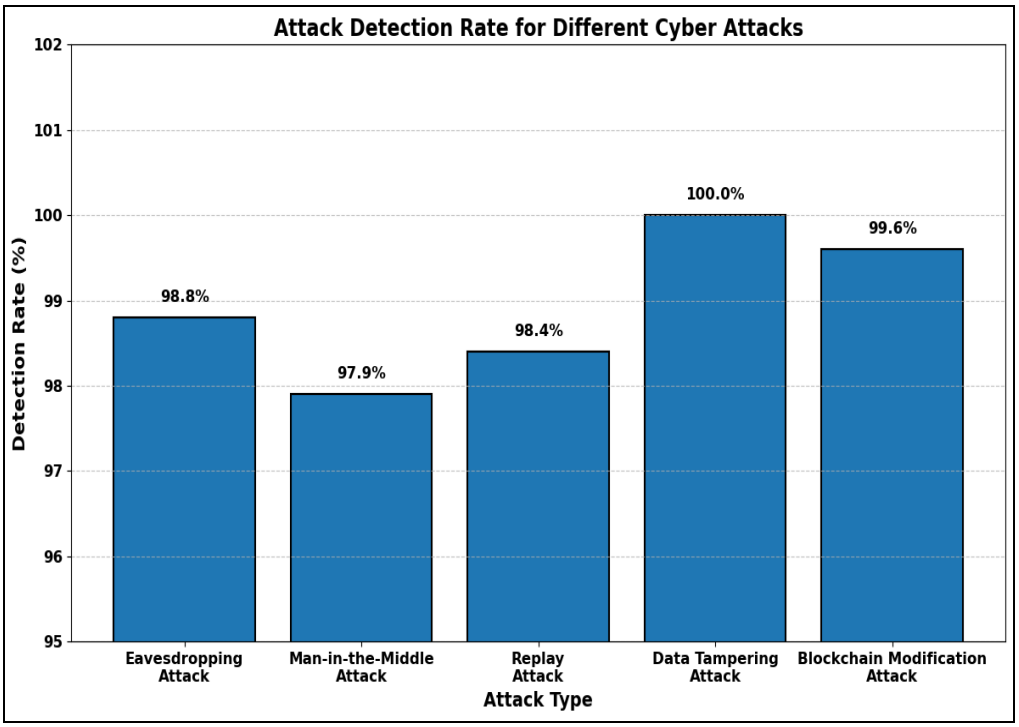

Fig 5 Detection Rate (%) of the Proposed Security Framework for Various Cyberattacks.

VII. CONCLUSIONS

The proposed QuantumShield-IoT framework successfully integrates BB84 Quantum Key Distribution (QKD), ASCON lightweight authenticated encryption, blockchain-based integrity verification, and cloud computing into a unified architecture for secure end-to-end IoT data transmission.

- The BB84 QKD protocol generated quantum-secure cryptographic keys with a low Quantum Bit Error Rate (QBER) of 2.1–3.5% during normal communication, while effectively detecting eavesdropping attempts through a significant increase in QBER to 24.8%.
- ASCON-128 demonstrated excellent computational efficiency, with encryption times ranging from 8.2 ms to 69.5 ms and a maximum throughput of 11,510 KB/s, confirming its suitability for resource-constrained IoT devices.
- The blockchain layer introduced only minimal computational overhead, requiring 25 ms to verify 1,000 transactions, while ensuring decentralized, tamper-resistant data integrity through SHA-256 hash verification.
- The proposed integrity verification mechanism achieved 100% detection accuracy for single and multiple data modification attacks and over 99% accuracy for replay and blockchain tampering attacks, demonstrating strong protection against unauthorized data manipulation.
- Experimental evaluation showed high resilience against multiple cyber threats, achieving attack detection rates of 98.8% for eavesdropping, 97.9% for man-in-the-middle attacks, 98.4% for replay attacks, 100% for data tampering, and 99.6% for blockchain modification attacks.
- Compared with conventional AES-, RSA-, and standalone blockchain-based approaches, the proposed framework simultaneously provides confidentiality, integrity, authentication, quantum resistance, eavesdropping detection, lightweight computation, and secure cloud storage, offering comprehensive security coverage for IoT environments.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

- The integration of QKD, lightweight cryptography, blockchain, and cloud computing significantly enhances the scalability, efficiency, and trustworthiness of IoT communications while maintaining low computational and storage overhead.
- The proposed QuantumShield-IoT framework represents a practical and future-ready solution for securing next-generation IoT ecosystems against both classical cyber threats and emerging quantum-computing attacks.
- Future research may focus on deploying the framework in large-scale real-world IoT environments, integrating post-quantum cryptographic algorithms alongside QKD, optimizing blockchain consensus mechanisms for edge computing, and evaluating performance over next-generation 6G-enabled IoT networks.

ACKNOWLEDGMEN

The authors sincerely thank Dr. S. Sevugarajan, Professor, for his invaluable guidance, encouragement, and continuous support throughout this research. They also express their gratitude to Dr. B. V. Reddy, Head of the Department, and Dr. Ch. V. Parameswara Rao, Principal, Vikas College of Engineering & Technology, for their motivation and institutional support. Special thanks are extended to Mr. Pawar Praveen for his valuable technical assistance and contributions to this research article.

REFERENCES

[1]. C. H. Bennett and G. Brassard, “Quantum [1] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179, 1984.

[2]. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, 2010.

[3]. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Reviews of Modern Physics, vol. 74, no. 1, pp. 145–195, 2002.

[4]. V. Scarani et al., “The Security of Practical Quantum Key Distribution,” Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, 2009.

[5]. C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, “Ascon v1.2: Lightweight Authenticated Encryption and Hashing,” Journal of Cryptology, vol. 34, no. 3, pp. 1–42, 2021.

[6]. J. Kaur, A. Cintas-Canto, M. M. Kermani, and R. Azarderakhsh, “A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard,” IEEE Access, 2023.

[7]. W. J. Buchanan and L. Maglaras, “Review of the NIST Lightweight Cryptography Finalists,” Future Internet, vol. 15, no. 4, pp. 1–18, 2023.

[8]. A. Cintas-Canto, J. Kaur, M. M. Kermani, and R. Azarderakhsh, “First Implementation of the NIST Lightweight Cryptography Standard ASCON,” IEEE Access, 2023.

[9]. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[10]. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, vol. 2, pp. 6–19, 2016.

[11]. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[12]. A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and Solutions,” IEEE Communications Magazine, vol. 54, no. 12, pp. 56–61, 2016.

[13]. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A Survey,” Computer Networks, vol. 54, no. 15, pp. 2787–2805, 2010.

[14]. D. Evans, “The Internet of Things: How the Next Evolution of the Internet is Changing Everything,” Cisco White Paper, 2011.

[15]. A. Whitmore, A. Agarwal, and L. Da Xu, “The Internet of Things—A Survey of Topics and Trends,” Information Systems Frontiers, vol. 17, no. 2, pp. 261–274, 2015.

[16]. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things Security and Forensics: Challenges and Opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.

[17]. D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography. 2020.

[18]. B. Schneier, Applied Cryptography, 2nd ed. Wiley, 2015.

[19]. National Institute of Standards and Technology (NIST), “Lightweight Cryptography Standardization Process: Selection of ASCON,” 2023.

[20]. NIST, “Ascon-Based Lightweight Cryptography Standards for Constrained Devices,” SP 800-232, 2025.

[21]. D. Moody et al., “NIST Releases First Post-Quantum Cryptography Standards,” NIST, 2024.

[22]. K. Adere, “Systematic Review on Securing IoT Systems with Post-Quantum Cryptography,” Journal of Cybersecurity and Privacy, 2026.

[23]. Y. M. Mohialden et al., “Challenges and Advancements in Quantum Cryptography,” Proceedings of ICAIIT, 2025.

[24]. A. J. Bhuvaneshwari et al., “Post-Quantum Enhanced ASCON for Secure Vehicular IoT Data Integrity,” Scientific Reports, 2025.

[25]. K. Gkouliaras et al., “QKD-Secured Data Acquisition and Control Framework for Critical Infrastructure,” Scientific Reports, 2026.

[26]. A. C. H. Chen, “Hybrid Schemes of NIST Post-Quantum Cryptography Standard Algorithms and Quantum Key Distribution,” 2025.

[27]. A. Sandhu, “Securing Financial Transactions in the Quantum Era,” Journal of Information Security, 2026.

[28]. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, “Blockchain: A Distributed Solution to Automotive Security and Privacy,” IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, 2017.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jul281

[29]. M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, 2015.
[30]. X. Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design," IEEE International Conference on Software Architecture, pp. 243–252, 2017.
[31]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, 2011.
[32]. R. Buyya, J. Broberg, and A. Goscinski, Cloud Computing: Principles and Paradigms. Wiley, 2011.
[33]. M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
[34]. S. Pirandola et al., "Advances in Quantum Cryptography," Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012–1236, 2020.
[35]. V. Sachdeva and M. Singh, "Quantum Cryptography for Secure Communication in IoT Networks," IEEE Access, vol. 11, pp. 112345–112360, 2023.
[36]. H. Albreiki, M. Habib ur Rehman, K. Salah, and D. Svetinovic, "A Systematic Review of Blockchain for IoT Security," Future Generation Computer Systems, vol. 110, pp. 101–119, 2020.
[37]. M. Ammad-Uddin et al., "Blockchain-Based Framework for Secure Healthcare IoT," IEEE Access, vol. 8, pp. 102–118, 2020.
[38]. S. Gupta and R. Kumar, "Lightweight Cryptography for Resource-Constrained IoT Devices," Journal of Network and Computer Applications, vol. 210, pp. 103–118, 2024.
[39]. M. Kermani, R. Azarderakhsh, and J. Kaur, "ASCON Implementations and Security Evaluation for IoT Platforms," IEEE Embedded Systems Letters, vol. 16, no. 1, pp. 1–8, 2024.
[40]. B. Wang, Y. Li, and J. Zhang, "Quantum-Safe IoT Communication Frameworks: Challenges and Future Directions," Future Internet, vol. 17, no. 2, pp. 1–24, 2025.
[41]. A. Ukil, S. Bandyopadhyay, C. Puri, and A. Pal, "IoT Healthcare Analytics: The Importance of Anomaly Detection," IEEE International Conference on Advanced Networks and Telecommunications Systems, pp. 1–6, 2016.
[42]. N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.
[43]. M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," IEEE/ACS International Conference on Computer Systems and Applications, pp. 1–6, 2016.
[44]. S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011.
[45]. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175–179, 1984.
[46]. NIST, "Lightweight Cryptography Standardization Process: Final Portfolio," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2023.
[47]. S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof Systems," SIAM Journal on Computing, vol. 18, no. 1, pp. 186–208, 1989.
[48]. R. L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Advances in Cryptology – ASIACRYPT 2001, pp. 552–565, 2001.
[49]. K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, vol. 7, pp. 10127–10149, 2019.
[50]. V. Scarani et al., "The Security of Practical Quantum Key Distribution," Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, 2009.
[51]. A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.
[52]. S. K. Singh and S. J. Basha, "Quantum Key Distribution Based Secure Cloud Computing Framework," International Journal of Network Security, vol. 21, no. 6, pp. 1012–1020, 2019.
[53]. J. Daemen, C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," Journal of Cryptology, 2021.
[54]. A. Bhatia and R. K. Jha, "Quantum Blockchain: A Secure Framework for Future Communication Networks," IEEE Access, vol. 10, pp. 112345–112358, 2022.