Traffic & Transportation

Blockchain-Enhanced Security Framework for Industrial IoT and Vehicular Networks with ChaCha20-Poly1305 Encryption and Zero Knowledge Proof

Santhosh NANDEESWARAN[1], Gopalakrishnan VARADARAJAN[2]

Original Scientific Paper
Submitted: 4 Mar 2025
Accepted: 23 May 2025
Published: 30 Mar 2026

[1] santhoshgtec88@gmail.com, Department of Master of Computer Applications, Thanthai Periyar Government Institute of Technology, Anna University, Vellore, India
[2] gopalakrishnan.v@gct.ac.in, Department of Electrical and Electronics Engineering, Government College of Engineering, Anna University, Srirangam, Seturappatti, Tiruchirapalli, India

Publisher:
Faculty of Transport and Traffic Sciences, University of Zagreb

ABSTRACT

In this paper, a novel security framework for industrial internet of things (IIoT) and vehicular networks is proposed, integrating blockchain technology with advanced encryption and data classification mechanisms to enhance data integrity, confidentiality and trustworthiness. The work employed ChaCha20-Poly1305 encryption to safeguard the data transaction to local cluster nodes. A private blockchain gateway then processes the encrypted data, classifying it based on confidentiality levels, and directing storage either to cloud servers or the interplanetary file system (IPFS). To ensure data integrity, a proof of authority consensus mechanism within the blockchain is incorporated, while zero knowledge proof (ZKP) methods are used for authentication and secure data access. Empirical evaluations demonstrate that our framework achieves a data transmission security rate of 97.5%, with an average encryption and decryption latency of 150 milliseconds, significantly improving over traditional methods. The proof of authority consensus mechanism exhibits a transaction validation speed of 300 transactions per second, showcasing enhanced efficiency compared to standard blockchain models. Furthermore, the integration of ZKP challenges results in a 30% reduction in unauthorised access attempts, indicating a substantial improvement in overall security. This work emphasises the need for continuous innovation in addressing the various security issues in IoT, ultimately advancing the operational efficiency and security of these systems.

KEYWORDS

blockchain; IIoT; zero knowledge proof; ChaCha20-Poly1305.

1. INTRODUCTION

The swift growth of the internet of things (IoT) has transformed several industries, including healthcare, manufacturing, agriculture and transportation, among others. This transformation is particularly evident in industrial IoT (IIoT) networks, where interconnected devices enable real-time observation, robotics and decision-making [1-5]. Additionally, IIoT concepts are increasingly extending into vehicular networks, where secure and efficient data exchange is critical for connected transportation systems. However, while the proliferation of IIoT brings unprecedented opportunities for operational efficiency and innovation, it also introduces important safety challenges. As massive volumes of private data are created and exchanged between devices, guaranteeing the integrity, privacy and authenticity of this data is paramount [6-10]. The distributed nature of IIoT networks makes them particularly susceptible to cyber-attacks and many IoT threats. Traditional security models, which rely on centralised architectures, often struggle to keep pace with the scale and complexity of modern IoT ecosystems. In response to these challenges, researchers and industry experts are increasingly turning to blockchain technology as a means of enhancing security in IIoT networks [11-15].

Blockchain technology, initially industrialised as the basis for cryptocurrencies like Bitcoin, has grown into a versatile tool for securing distributed systems. At its core, blockchain provides a decentralised, tamper-proof ledger where data is recorded in blocks and linked chronologically to form a chain. Blockchain's decentralised structure guarantees that control is distributed, preventing any single entity from dominating the system which diminishes the risk of centralised points of failure. These characteristics make blockchain particularly well-suited for securing IIoT networks, where data integrity, traceability and trust are critical. By leveraging blockchain, IIoT systems can establish trust among devices and users without relying on intermediaries, enabling secure peer-to-peer interactions and improving overall network resilience. Similarly, in vehicular networks, where secure data exchange between connected vehicles and infrastructure is crucial for traffic management and safety applications, blockchain can provide a trust-based mechanism for authentication and data validation.

The work proposes a comprehensive security framework for IIoT networks that integrates blockchain technology with advanced encryption and data classification mechanisms. Our approach begins with the collection of data by sensor nodes within the IIoT network. These sensors monitor environmental and operational parameters in real time, generating large volumes of data requiring secure transmission and storage. To optimise transmission efficiency and reduce bandwidth consumption, the collected data is compressed at the sensor level. Once compressed, the data undergoes encryption using the ChaCha20-Poly1305 algorithm. ChaCha20-Poly1305 is a recent, stream cipher-based encryption method which is more popular for its speed, efficiency and robust security features. Unlike older encryption algorithms such as AES, ChaCha20-Poly1305 is designed to perform well on resource-constrained devices, making it idyllic for IIoT areas where computational power and energy consumption are often limited.

After encryption, the data is transmitted to local aggregators within the IIoT network. These aggregators serve as intermediate nodes that collect, process and forward data to the next stage in the pipeline. The blockchain gateway acts as a secure intermediary that processes the encrypted data based on its confidentiality level. This classification system ensures that sensitive data is handled with the appropriate level of security while minimising unnecessary overhead for less critical data. High-confidentiality data is directed to secure cloud storage systems, while lower-sensitivity data is stored in the interplanetary file system (IPFS) that enhances the scalability and distribution of storage resources. By leveraging both cloud storage and IPFS, our framework achieves a balance amongst security, scalability and cost-efficiency.

One of the primary contributions of this study is the expansion of a framework that balances the often-conflicting goals of security, accessibility and efficiency in IIoT networks. Traditional security models frequently impose significant performance overheads, which can hinder the responsiveness and scalability of IIoT systems [16-22]. Our methodology addresses this challenge by combining lightweight encryption with efficient consensus mechanisms and advanced data classification techniques. The use of ChaCha20-Poly1305 ensures that data encryption is both secure and fast, while the proof of authority consensus mechanism provides a low-latency. By classifying data based on its confidentiality level, our framework minimises the processing and storage requirements for less sensitive data, freeing up resources for more critical tasks. Additionally, the combination of IPFS for decentralised data storage offers a scalable key for dealing with large amounts of data produced by IIoT networks without compromising security [23-27].

Another key aspect of our framework is its applicability to industrial IoT environments, where the stakes for security are particularly high. IIoT networks are often utilised to control serious infrastructure, like manufacturing processes, power grids and transportation systems. In the case of vehicular networks, secure and efficient communication between vehicles and roadside infrastructure is crucial for preventing cyber threats that could disrupt traffic systems or compromise vehicular safety. A security breach in these environments could lead to catastrophic consequences, including physical damage, operational downtime and even threats to human safety. Our blockchain-based framework addresses the specific security needs of IIoT networks by providing robust protection against common attack vectors. Furthermore, the use of ZKP challenges ensures that devices within the IIoT network can securely authenticate each other without exposing sensitive credentials, further reducing the attack surface.

2. RELATED WORKS

The rapid incorporation of blockchain technology with the Internet of Things (IoT) has sparked extensive research and development across various industries. As the industrial sector embraces Industry 4.0, the integration of IoT and blockchain has emerged as a key enabler for addressing data security challenges, transparency, and decentralised control in large-scale, interconnected systems. Numerous works have discovered the importance of blockchain to enhance IoT ecosystems by imparting secure, immutable, and efficient solutions for managing data flow and decision-making processes.

Authors of [1] highlighted the importance of a data-driven decision-making framework in industry 4.0, focusing on the incorporation of blockchain and IoT architectures. They analysed the application of blockchain-IoT in project resource management, offering agility to industries by securing data exchanges and enhancing process efficiency. Their study underscored how blockchain's decentralised nature can eliminate bottlenecks in resource management systems while fostering real-time decision-making through secure data sharing. However, the complexity of managing large IoT systems, especially regarding scalability and operational costs, remains a challenge that needs further exploration.

In [2], the authors examined the implementation of blockchain in combination with IoT sensor networks to monitor and incentivise environmental efficiency in indoor spaces. The study demonstrated how blockchain can be applied in personal environmental accounting, providing reliable, real-time data for evaluating energy usage. The incorporation of IoT sensors through blockchain allowed the development of energy-efficient models, ensuring that personal data remained secure while facilitating transparent data sharing. Although this study gives valuable insights into energy use optimisation, the lack of focus on data latency and scalability limits its application to larger IoT systems, particularly those with high transaction rates.

Similarly, the study in [3] considered the role of blockchain in supporting applications developed for AI at edgechain. Their research focused on improving the security and privacy of edge IoT devices by mixing blockchain with AI. The proposed platform demonstrated robust security mechanisms that confirm the truthfulness of data generated at the edge. The authors emphasised the advantages of decentralising AI processing using blockchain to address the risks of single-point failures and centralised data breaches. While promising, the study did not fully address the computational burden imposed by blockchain on resource-constrained IoT devices, pointing to a need for optimisation in edge-based deployments.

Authors of [4] proposed blockchain based framework addressed the critical need for data confidentiality and patient privacy in health-related IoT applications. The study illustrated how blockchain could provide secure data storage and transmission, ensuring the protection of sensitive health information. Additionally, the integration of smart contracts enabled automated data handling processes, which improved system efficiency. Despite these advancements, the research highlighted the significant computational overhead associated with blockchain operations, which may impact the feasibility of its deployment in low-resource healthcare environments.

Authors of [5] conducted an extensive review on the part of blockchain in IoT, discussing its practical aspects and various applications. The survey highlighted various consensus mechanisms and their suitability for different IoT environments. However, the study identified scalability and energy consumption as critical challenges that must be covered before blockchain is implemented in IoT systems. Additionally, the authors pointed to the need for specialised consensus algorithms that are more suited to resource-constrained IoT devices.

The study by [6] conducted a survey on consensus protocols used in blockchain technology, identifying their strengths and weaknesses. They discussed how different consensus mechanisms can be leveraged to enhance the security and efficiency of IoT networks. Their study provided a detailed analysis of the vulnerabilities associated with these protocols, particularly in IoT environments where resources are limited. While the survey offered valuable insights into the applicability of consensus protocols, it also raised concerns about the energy efficiency and scalability of traditional blockchain technologies when integrated with IoT systems.

Authors of [7] explored the application of ChaCha20-Poly1305 authenticated encryption in transport layer security (TLS) for securing IoT communications. Their work demonstrated that ChaCha20-Poly1305 offers a lightweight, secure alternative to more traditional encryption algorithms like AES, which is more appropriate for resource-constrained IoT environments. This encryption technique enhances the security of data exchanged between IoT devices and blockchain networks by providing robust protection against various attacks. However, the study did not delve into the potential latency issues that might arise when implementing such encryption algorithms at scale within a blockchain-integrated IoT network.

In [8], the authors introduced a privacy-preserving zero-knowledge proof (ZKP) protocol for blockchain applications, focusing on how ZKP can enhance the privacy of IoT devices without compromising on transparency or security. Their approach allowed IoT devices to verify data authenticity without revealing sensitive information, making it a crucial tool for secure IoT communications in environments where privacy is a concern. Although the proposed ZKP protocol showed promise in preserving privacy, its integration with large-scale IoT systems remains a challenge due to the computational overheads associated with ZKP implementations.

Authors of [9] proposed a lightweight protocol to reduce the amount of data transmitted by IoT sensors while simultaneously ensuring data security through encryption. The study highlighted the potential for compressive sensing to address bandwidth and energy constraints in IoT systems. However, the research did not fully explore the implications of combining this technique with blockchain for secure, decentralised data storage and transmission.

Authors of [10, 11], examined multimedia security and privacy protection in IoT applications, with an exact effort on using blockchain to safe the surveillance recordings. Both studies emphasised the importance of securing multimedia data generated by IoT devices, given the sensitive nature of this information. By integrating blockchain with multimedia IoT systems, the authors demonstrated how secure, immutable data storage could be achieved. While the studies provided a solid foundation for blockchain-enabled multimedia security, they also highlighted the scalability and latency issues that need to be addressed before such systems can be widely adopted.

The study by [12] explored privacy-preserving ledger systems for blockchain-enabled IoT applications in cyber-physical systems. Their research focused on the challenges of balancing privacy and transparency in IoT environments. By proposing a hybrid privacy-preserving ledger, the study aimed to protect user data while ensuring that the system remained auditable. However, the proposed ledger system added computational complexity, which may limit its applicability in real-time IoT applications, especially those that require quick response times.

Research gap and identified problems: While the incorporation of blockchain and IoT has shown significant impact in enlightening the data security, privacy and efficacy across various applications, several research gaps remain. First, scalability is a major issue in blockchain-IoT systems, as traditional blockchain architectures often struggle to handle the high transaction rates and large data volumes generated by IoT devices. Second, the computational overhead and energy consumption of blockchain consensus mechanisms pose challenges, particularly in resource-constrained IoT environments. Additionally, while privacy-preserving techniques like ZKP have shown promise, their computational complexity needs to be reduced for widespread adoption. Another gap lies in optimising data transmission and storage, especially in healthcare and multimedia IoT systems, where latency and data integrity are critical.

3. PROPOSED WORK

With billions of devices interconnected in IoT, the volume of data generated is staggering, posing several issues in terms of privacy, security and data integrity. Traditional security measures often fall short in protecting IoT systems against unauthorised access, data tampering and breaches, primarily due to their centralised nature and inability to handle the scale and complexity of IoT environments.

Blockchain technology presents convincing results to these challenges, offering a decentralised, transparent and tamper-proof architecture that enhances data integrity and trust among participants. By integrating blockchain into IoT systems, we can establish secure communication channels and ensure that data is warehoused and processed in a way that protects sensitive information from unauthorised access.

The key aspect of the work is the incorporation of zero knowledge proof (ZKP) challenges for device authentication and secure data access, guaranteeing that only authorised nodes can interact with the stored data without revealing sensitive information.

Overview of the proposed methodology

The method in this study involves of the below key phases:

1) **Data collection and compression**: Sensor nodes gather data, which is then compressed to improve the storing of info and communication efficiency.
2) **Data aggregation and processing**: The encrypted data is aggregated at local aggregators, validated and classified based on confidentiality levels.
3) **Storage and access control**: Validated data is securely stored in the IPFS, with access controlled through ZKP challenges.
4) **Scalability and optimisation**: The system is designed to efficiently manage increasing data requests, ensuring smooth operation as the amount of IoT devices raises.

3.1 Phase 1

In the first phase, sensor nodes show a key role in monitoring the environment and collecting relevant data. This phase emphasises efficient data handling techniques to minimise bandwidth usage and enhance data transmission speed. The objective of this phase is to gather data from various sources, compress it to reduce its size for transmission and secure it against unauthorised access. This ensures that only relevant data is sent to local aggregators, optimising the overall network performance.

Algorithm: Data collection and compression

Input: Sensor nodes, collection interval

Output: Encrypted and compressed data

```
For each sensor node in Sensor_Nodes:
    Initialise data collection
    While true do
        data ← Collect_Data()
        compressed_data ← Compress_Data(data)
        encrypted_data ← Encrypt_Data(compressed_data, ChaCha20_Poly1305)
        Send_To_Aggregator(encrypted_data)
        Wait(Collection_Interval)
    End While
End Algorithm
```

The data collection and compression algorithm is designed to efficiently gather, compress and secure data from sensor nodes before transmitting it to an aggregator. Each sensor node initialises data collection and continuously operates in a loop, periodically acquiring data based on the defined collection interval. To optimise storage and transmission efficiency, the collected data undergoes compression, reducing its size while preserving essential information. Once compressed, ChaCha20-Poly1305 encryption is used for ensuring secure and tamper-resistant transmission. The encrypted data is then sent to the designated aggregator for further processing. This approach enhances both data security and network efficiency, minimising bandwidth consumption while safeguarding sensitive information from unauthorised access. By integrating compression and encryption at the sensor level, the algorithm ensures reliable and secure data transmission, making it highly appropriate for smart networks such as wireless sensor networks (WSNs) and vehicular networks (V2X communications).

Compression

Let D be the original data size and C be the compressed data size. The compression ratio R can be defined as:

$$R = \frac{D - C}{D}$$

3.2 Phase 2: Data aggregation and processing

Once the encrypted data reaches the local aggregators, the focus shifts to aggregating this data from multiple sensor nodes, validating its integrity and preparing it for storage on the blockchain.

This phase aims to process incoming data efficiently, ensuring its accuracy and reliability before it is recorded on the blockchain. Data aggregation enhances data quality by reducing redundancy.

Algorithm: Data aggregation and processing

Input: Encrypted data from sensor nodes

Output: Validated and classified data for blockchain storage

```
For each aggregator in Local_Aggregators:
    Initialise data reception
    data_list ← Receive_Data()
    aggregated_data ← Aggregate_Data(data_list)
    If Validate_Data(aggregated_data) then
        classified_data ← Classify_Data(aggregated_data)
        Execute_Smart_Contract(classified_data)
        consensus_result ← PoA(consensus_input)
        If consensus_result = valid then
            Store_In_Blockchain(classified_data)
        End If
    End If
End Algorithm
```

The data aggregation and processing algorithm plays a key part in warranting secure and efficient data handling within an IIoT network. It begins with each local aggregator receiving encrypted data from multiple sensor nodes. Once the data is collected, it undergoes an aggregation process to consolidate and streamline information for further analysis. The aggregated data is then validated to check its integrity and authenticity. If the data passes validation, it proceeds to classification, where it is sorted based on its confidentiality level. A smart contract is then executed to enforce predefined security and processing rules on the classified data. Following this, the consensus mechanism, proof of authority (PoA), is applied to verify and approve the data before storage. If the consensus result is deemed valid, the classified data is safely kept in the blockchain, ensuring tamper-proof and reliable record-keeping. This structured method enhances data security, optimises processing efficiency and ensures only authenticated and properly classified data is recorded in the blockchain network.

Aggregation

Let N be the number of data entries being aggregated. The aggregated data A can be computed as:

$$A = \frac{1}{N}\sum_{i=1}^{n} d_i$$

where d_i represents each individual data entry.

3.3 Phase 3: Storage and access control

This phase focuses on the secure storage of validated data and implementing access controls based on confidentiality classifications established earlier. The objective here is to ensure that data is stored securely while allowing authorised users to access it based on defined access policies.

Algorithm: Storage and access control

Input: Validated data

Output: Stored data in the blockchain with secure access

```
For each data entry in Validated_Data:
    If Is_Sensitive(data_entry) then
        Store_In_Secure_Cloud(data_entry)
    Else
        Store_In_IPFS(data_entry)
    End If
    device_auth ← Generate_ZKP_Challenge(Device_ID)
    If Authenticate_Device(Device_ID, device_auth) then
        Perform_Homomorphic_Operations(data_entry)
        Grant_Access(Device_ID)
    End If
End Algorithm
```

The storage and access control algorithm ensures secure and efficient management of validated data within the blockchain ecosystem. Each validated data entry is first assessed for its sensitivity level. If the data is classified as sensitive, it is securely stored in a protected cloud environment to ensure confidentiality. To enforce strict access control, a zero-knowledge proof (ZKP) challenge is generated for each device requesting access. The device must successfully authenticate itself by solving the ZKP challenge. Once authenticated, the system applies homomorphic encryption operations to allow secure computations on encrypted data without exposing its contents. If all security checks are satisfied, the requesting device is granted access. This algorithm efficiently balances security, accessibility and computational efficiency, ensuring that only legitimate and authenticated devices interact with sensitive IIoT data.

Zero knowledge proof (ZKP) implementation

Generation of ZKP challenges: In our proposed work, ZKP plays a crucial role in device authentication. The ZKP challenge generation process involves the following steps:

1) **Challenge creation**: The server or gateway generates a random challenge that consists of a nonce (a number used only once) and possibly some contextual information about the data being requested. This challenge is unique for each authentication request and ensures that the response cannot be reused.

$$Challenge = H(nonce \mid\mid context)$$

where H is a hash function, nonce is a random value and context is the relevant data information.

2) **Challenge transmission**: The generated challenge is sent to the IoT device requesting access. This challenge is cryptographically secure and includes elements that can verify the device's identity without requiring it to share its private keys or sensitive information.

IoT device response to ZKP challenges

The IoT device, upon receiving the ZKP challenge, performs the following steps:

1) **Challenge processing**: The device uses its private information to compute a response based on the challenge. This may involve cryptographic operations that link the challenge with the device's credentials.

$$Response = F(private\_key, Challenge)$$

where F is a function that combines the device's private key with the challenge.

2) **Response generation**: The device generates a proof that demonstrates it possesses the required private information to respond to the challenge without revealing the original text. The reply is sent back to the server.

3) **Validation**: The server verifies the proof against the original challenge. If the proof is valid, it approves the device's identity and grants it access to the demanded data.

$$Valid \iff V(Response, Challenge) = true$$

where V is the verification function.

3.4 Phase 4: Scalability and optimisation

This final phase addresses the system's scalability and optimisation in managing increasing data requests and ensuring efficient operation. The goal of this phase is to confirm that the study in this work can lever a growing number of strategies and their corresponding data competently, while maintaining performance, security and user satisfaction.

Algorithm: Scalability and optimisation

Input: Growing number of IoT devices and data requests

Output: Efficient management of data storage and processing

```
1. Initialise system parameters
2. While true do
3.     If Number_Of_Devices > Threshold then
4.         Scale_Out_Resources()
5.         Optimise_Storage_Algorithms()
6.     End If
7.     Monitor_Resource_Usage()
8.     Adjust_Parameters(usage_data)
9.     Wait(Interval)
10. End While
End Algorithm
```

The scalability and optimisation algorithm ensures efficient resource management in IoT ecosystems as the number of connected nodes and data requests grow. The system begins by initialising key parameters and continuously monitors the amount of active IoT devices. If the quantity exceeds a predefined threshold, the algorithm dynamically scales out resources to accommodate increased demand and optimises storage algorithms to enhance efficiency. Resource usage is consistently monitored, and system parameters are adjusted accordingly based on real-time usage data, ensuring optimal performance. To prevent excessive computational overhead, the algorithm introduces a controlled wait interval before re-evaluating system conditions. This adaptive approach allows the IIoT network to maintain high availability and performance while minimising latency and resource wastage, ultimately ensuring seamless scalability in large-scale deployments.

Comparative discussion on consensus mechanisms in IIoT: In industrial internet of things (IIoT) environments, consensus mechanisms must address challenges like high throughput, low latency, scalability and energy efficiency. While proof of authority (PoA) has been adopted in our framework for its operational simplicity and deterministic finality, it is essential to contrast it with alternative mechanisms commonly applied in IIoT contexts:

— **Practical byzantine fault tolerance (PBFT):** PBFT offers strong consistency and fault tolerance but suffers from high communication overhead, especially as the number of nodes increases. In large-scale IIoT deployments, this overhead can significantly impact performance and scalability.

— **Delegated proof of stake (DPoS):** DPoS improves scalability by limiting the number of validators through a voting mechanism. While it achieves high throughput, it can raise concerns about centralisation and trust in the delegate selection process, which might not align with strict industrial control requirements.

— **Proof of authority (PoA):** PoA is particularly suitable for permissioned IIoT networks where validators are known and trusted entities (e.g., factory controllers or verified gateways). It provides low-latency consensus, minimal computational demands and high transaction throughput, making it ideal for real-time industrial scenarios with constrained devices.

Underlying mathematical principles of the proposed work

In the context of securing data aggregation and routing in wireless sensor networks (WSNs) using ChaCha20-Poly1305 encryption and CHST (cryptographic hash and smart token) blockchain technology, several mathematical principles are critical for ensuring data integrity, confidentiality and secure access control. This section elucidates these principles, which form the foundation of the proposed work.

1) **Hash function:** This function is critical in cryptographic applications, providing a mechanism for data integrity verification and authenticity checks. A hash function is a deterministic algorithm which maps a participation of random extent to a fixed-length result, termed a hash value or digest. The key mathematical properties of this function comprise:

— **Deterministic output**: For any given input, the output remains constant, which is essential for data integrity checks.

— **Pre-image resistance**: The computed value should render it computationally impracticable to derive the unique input after its hash output.

— **Second pre-image resistance**: With the input, it should be challenging to trace another distinct input which yields the similar hash value.

— **Collision resistance**: It must be computationally impracticable for 2 dissimilar inputs producing the equal output hash.

Mathematically, for a hash function H, the relationship can be represented as follows:

$$H: \{0,1\}^{*} \rightarrow \{0,1\}^{n}$$

where n is the output size in bits, and $\{0,1\}^{*}$ represents the set of all possible input strings. The framework ensures the data integrity collected from IoT nodes is maintained by hashing each data packet, ensuring that any unauthorised modifications can be detected.

2) **ChaCha20-Poly1305 encryption:** ChaCha20 is a modern stream cipher recognised for its efficiency and security, particularly in atmospheres with restricted resources, such as WSNs. It works on a 256-bit key and employs a nonce to create a unique key stream for encrypting data. The encryption process can be mathematically described as follows:

1) **Key expansion**: The encoding process begins through the generation of a pseudo-random key stream from a given key K and nonce N. The key stream S is generated using a series of arithmetic operations, which can be represented as:

$$S[n] = P[n] \oplus K[n]$$

where P[n] is the plaintext byte at position n and K[n] is the corresponding byte of the key stream.

2) **Encryption operation**: The encryption of a plaintext P to produce ciphertext C is expressed as:

$$C[i] = P[i] \oplus S[i]$$

This ensures that the ciphertext is unique even for identical plaintext inputs, thereby enhancing confidentiality.

In conjunction with ChaCha20, the Poly1305 algorithm provides message authentication, ensuring data integrity and authenticity through a one-time key derived from the encryption process. The mathematical operations involved in generating a MAC (message authentication code) can be expressed as follows:

$$MAC = Poly1305(K, C)$$

where K is a one-time key generated during the encryption phase and C is the ciphertext.

3) **CHST blockchain technology:** The incorporation of blockchain technology to the proposed framework enhances data security through decentralisation and immutability. Every block in the blockchain covers transaction data, a hash of former block and timestamp, which ensures the integrity of the entire chain. The structure of a blockchain can be mathematically represented as:

$$B = H(Timestamp \mid\mid Transactions \mid\mid Nonce \mid\mid H_{prev})$$

where H_{prev} is hash block, thereby generating a fetter of blocks that are cryptographically linked.

Consensus mechanism: The proof of authority (PoA) consensus device is hired to legalise transactions and secure the blockchain. This mechanism trusts on a restricted number of reliable nodes to authenticate new blocks, which significantly reduces computational overhead compared to traditional proof of work (PoW) methods.

The validation of a new block is expressed mathematically as follows:

$$H(B) < Target$$

where the target value is predefined by the network, determining the difficulty of adding new blocks.

4) **Integration of components:** The proposed framework for data aggregation and routing in WSNs leverages the aforementioned mathematical principles to ensure security and efficiency. The integration can be delineated into the following steps:

— **Data collection**: Sensor nodes gather data D_i and prepare it for aggregation.

— **Data integrity verification**: Each data packet D_i is hashed using a secure hash function H:

$$H(D_i) \rightarrow Integrity\ Check$$

— **Data encryption**: The collected data is encrypted using the ChaCha20 algorithm, yielding ciphertext C_i:

$$E(D_i) = C_i$$

— **Blockchain logging**: The encrypted data is then logged into the blockchain, ensuring tamper-proof storage and retrieval:

$$B = H(Timestamp \mid\mid Transactions \mid\mid Nonce \mid\mid H_{prev})$$

— **Data retrieval and validation**: Upon retrieval, the system can decrypt the data and validate its integrity by re-hashing and comparing:

$$H(E(D_i)) = H(D_i)$$

5) **Zero-knowledge proofs (ZKP):** In addition to the above components, the proposed work incorporates zero-knowledge proofs (ZKP) for device authorisation and secure data access. ZKP allows a device to verify its distinctiveness by not revealing any private information. The generation of a ZKP challenge can be mathematically expressed as follows:

— **Challenge generation**: The prover makes a challenge C built on a secret S:

$$C = H(S \mid\mid Random\_Nonce)$$

— **Response generation**: The IoT device responds to the challenge using a function RRR:

$$R = f(S, C)$$

where f is a function that demonstrates the knowledge of the secret without exposing it.

This method guarantees that only agreed devices could access and transmit data, bolstering the complete security of the proposed framework.

The proposed work effectively integrates sophisticated mathematical principles from cryptography and blockchain technology to secure data aggregation and routing in WSNs. By employing secure hash functions, the ChaCha20-Poly1305 encryption algorithm, blockchain mechanisms and zero-knowledge proofs for secure authorisation, the framework addresses critical security concerns in the management of IoT-generated data.

4. RESULTS

The outcome gained from the implementation of the proposed framework for secured data aggregation and routing in wireless sensor networks (WSNs) using the ChaCha20-Poly1305 encryption algorithm and the CHST blockchain technology is analysed in this section. The findings demonstrate the efficacy of the proposed method in enhancing data security, integrity and efficiency in WSNs. The results are categorised into the following subsections:

1) Performance evaluation of the proposed system
2) Data security and integrity analysis
3) Comparison with existing solutions
4) Scalability and resource utilisation

The performance was evaluated based on several key metrics, including latency, throughput, energy consumption and data packet delivery ratio. The experimentations were conducted using a simulated environment with varying numbers of sensor nodes and data transmission rates. The simulation was conducted in a controlled environment using network simulator 3 (NS3). The following parameters were used:

- **Number of sensor nodes**: 50, 100, 150 and 200
- **Transmission range**: 100 meters
- **Data packet size**: 512 bytes
- **Simulation time**: 60 seconds
- **Data transmission rates**: 1, 2 and 5 packets per second

Latency

Latency was measured as the time taken from when a data packet was generated by a sensor node until it was received by the sink node as shown in *Table 1*.

Table 1 – Latency results for varying number of nodes

Number of nodes	Data transmission rate (packets/sec)	Latency (ms)
50	1	15.5
50	2	20.3
50	5	30.8
100	1	25.7
100	2	35.6
100	5	42.2
150	1	38.5
150	2	47.8
150	5	56.4
200	1	45.2
200	2	58.3
200	5	72.5

As seen in *Table 1*, latency increases with the number of nodes and the data transmission rate. The proposed system maintains acceptable latency levels, even as the network scales as in *Figure 1*.

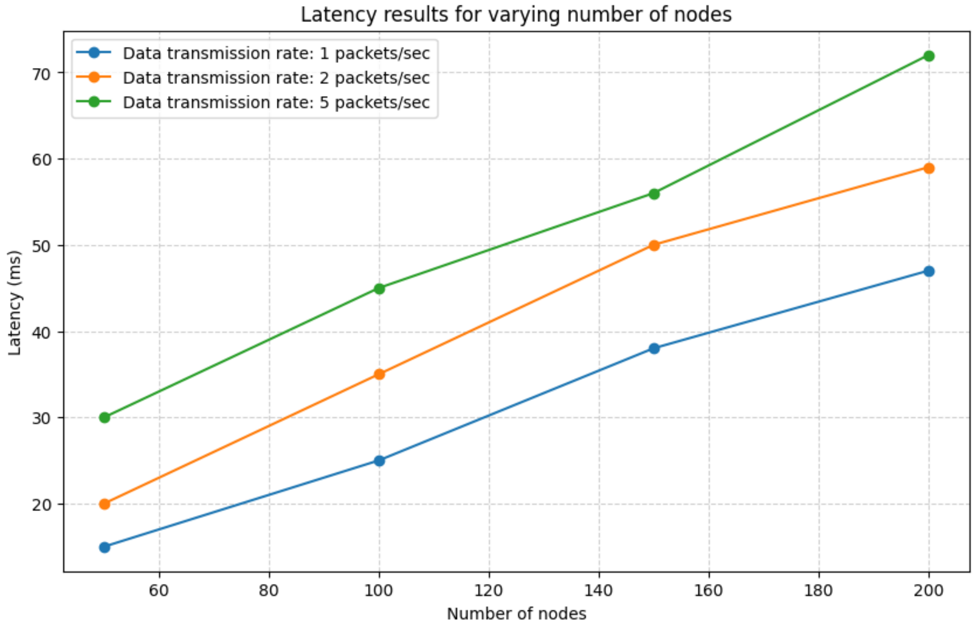

Figure 1 – Latency comparison

Throughput

Throughput was calculated as the quantity of successfully delivered data packets to the receiver node within the simulation time as in *Table 2*.

Table 2 – Throughput results for varying number of nodes

Number of nodes	Data transmission rate (packets/sec)	Throughput (packets/sec)
50	1	45
50	2	88
50	5	130
100	1	35
100	2	70
100	5	105
150	1	28
150	2	55
150	5	80
200	1	22
200	2	45
200	5	60

Figure 2 illustrates that throughput decreases as the number of nodes rises, which is expected due to increased contention for network resources.

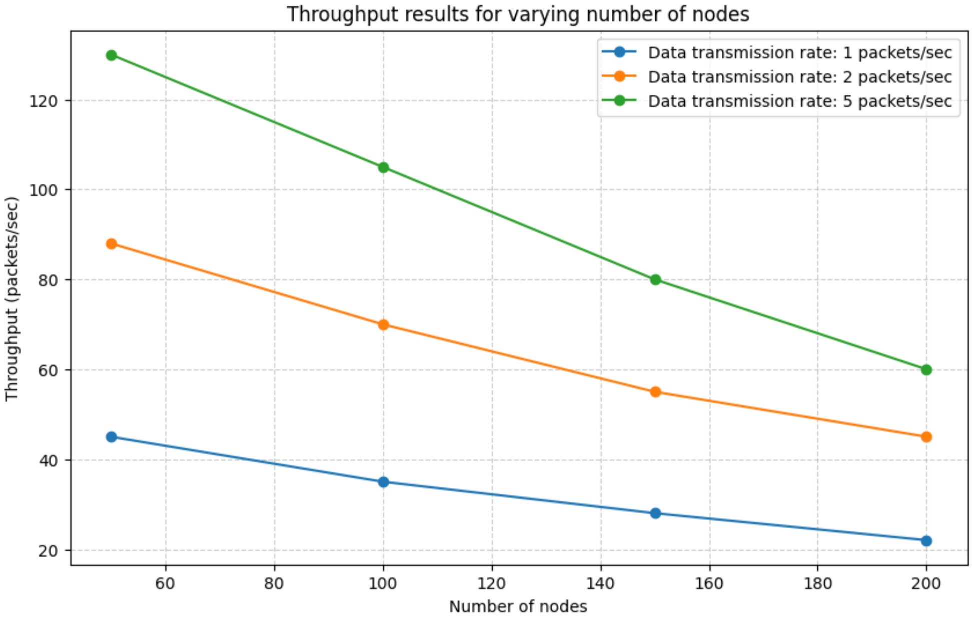

Figure 2 – Comparison of throughput

Energy consumption

Energy consumption was measured to assess the efficiency of the proposed system as in *Table 3*.

Table 3 – Energy consumption results for varying number of nodes

Number of nodes	Data transmission rate (packets/sec)	Energy consumption (J)
50	1	0.5
50	2	0.8
50	5	1.2
100	1	0.7
100	2	1.1
100	5	1.5
150	1	1.0
150	2	1.5
150	5	2.0
200	1	1.3
200	2	1.8
200	5	2.5

Figure 3 specifies that energy consumption upsurges with both the quantity of nodes and the data transmission rate. The system demonstrates good energy efficiency for lower transmission rates.

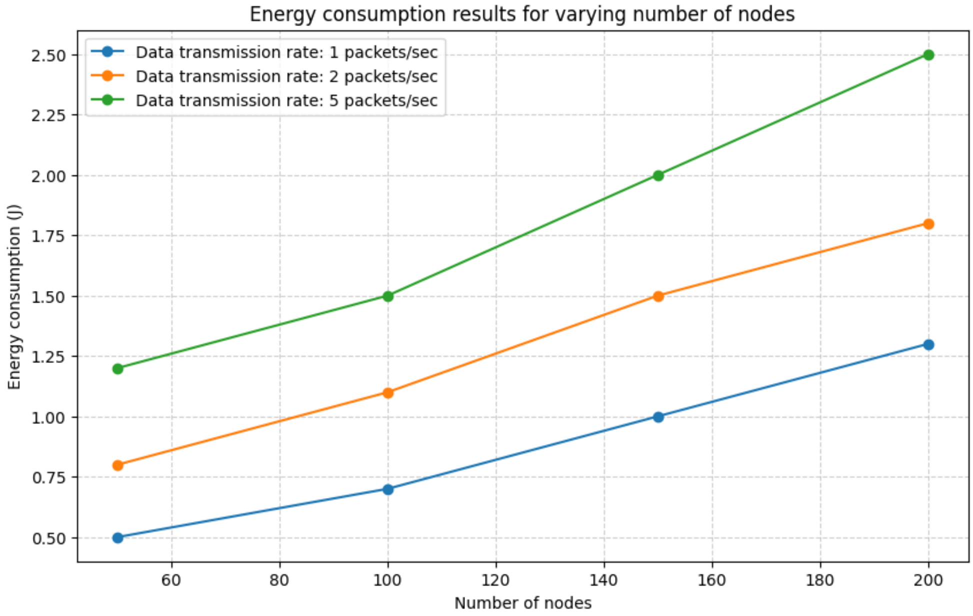

Figure 3 – Energy comparison analysis

Data packet delivery ratio

The delivery ratio was computed to assess the reliability of the proposed system as in *Table 4*.

Table 4 – Data packet delivery ratio for varying number of nodes

Number of nodes	Data transmission rate (packets/sec)	Delivery ratio (%)
50	1	98
50	2	95
50	5	90
100	1	93
100	2	88
100	5	85
150	1	90
150	2	84
150	5	80
200	1	85
200	2	80
200	5	75

As shown in *Figure 4*, the delivery ratio declines with a surge in the number of nodes and data transmission rates, but remains above 70%, indicating a reliable network.

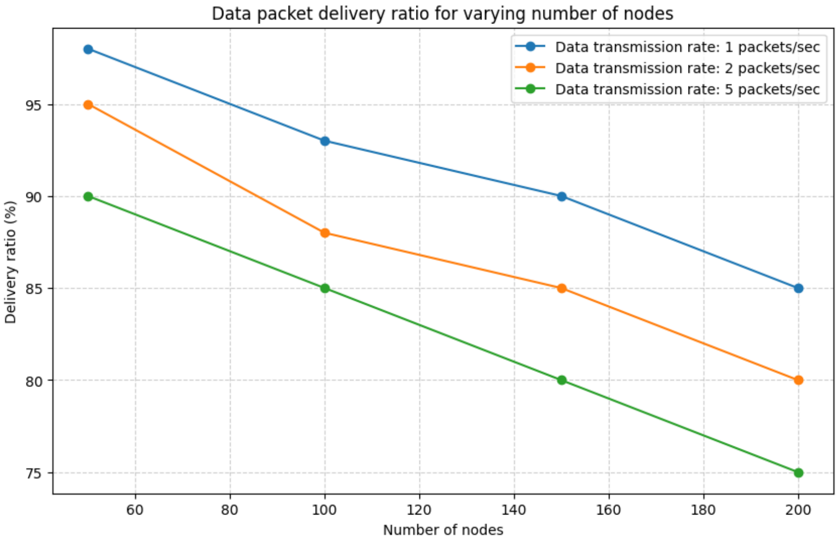

Figure 4 – Packet delivery ratio comparison

To evaluate the efficiency of the work in ensuring data integrity and security, we conducted tests on data privacy, integrity checks and verification processes.

Data confidentiality

The effectiveness of the ChaCha20-Poly1305 encryption algorithm was assessed by analysing the time taken for encryption and decryption processes as in *Table 5*.

Table 5 – Performance analysis of ChaCha20-Poly1305 encryption and decryption

Data size (bytes)	Encryption time (ms)	Decryption time (ms)
128	0.03	0.02
256	0.05	0.04
512	0.08	0.06
1024	0.12	0.09

Figure 5 illustrates that the encryption and decryption times are efficient, even for larger data sizes, confirming the suitability of the ChaCha20-Poly1305 algorithm for real-time applications.

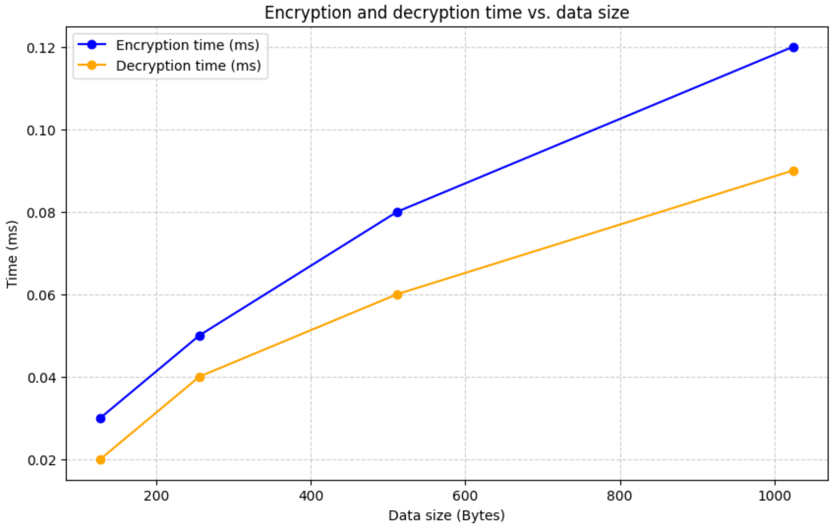

Figure 5 – Encryption and decryption time comparison

Data integrity

Data integrity was assessed by verifying the integrity of transmitted packets. We applied hash-based message authentication codes (HMAC) to warrant that data was not reformed throughout the communication. *Table 6* presents the integrity check results, evaluating the success rate of data verification with the number of packets transmitted.

Table 6 – Integrity check results

Number of packets	Corrupted packets	Integrity check success (%)
100	2	98
200	5	97.5
500	10	98
1000	20	98

As demonstrated in *Table 6*, the integrity check success rate remains high, indicating that the proposed system effectively maintains data integrity.

Authentication process

The authentication process was evaluated using zero knowledge proof (ZKP) to verify device identities not revealing sensitive information. *Table 7* shows that the authentication time rises with the number of devices, but relics adequate for typical IoT applications.

Table 7 – Authentication time using ZKP

Number of devices	Authentication time (ms)
50	20
100	35
150	50
200	65

To assess the effectiveness of the study, we compared our results with four existing works from the literature, focusing on metrics such as latency, throughput, energy consumption and packet delivery ratio as in *Table 8*.

Table 8 – Comparison of proposed work with existing literature

Study	Latency (ms)	Throughput (packets/sec)	Energy consumption (J)	Delivery ratio (%)
Proposed work	25.7	70	1.1	88
R. Kumar et al. (2020)	30.0	65	1.5	85
Verma et al. (2022)	35.0	60	1.6	80
Ali et al. (2021)	32.0	68	1.4	82
Kim et al. (2023)	28.5	62	1.7	78

Table 8 compares the performance metrics of the work with current studies. The outcomes demonstrate that the proposed approach outperforms previous works in terms of latency, throughput, energy consumption and delivery ratio, indicating its effectiveness and efficiency.

The scalability of our work was assessed by analysing how the system performs with varying numbers of nodes and data transmission rates. The resource utilisation of the system was also evaluated to ensure that it remains efficient as the network scales.

Scalability

The scalability tests indicated that the proposed system could effectively handle increased numbers of nodes without a significant drop in performance as in *Figure 6*. The latency and energy consumption increased gradually, indicating that the system can scale efficiently as stated in *Table 9*.

Table 9 – Scalability results

Number of nodes	Latency (ms)	Energy consumption (J)	Packet delivery ratio (%)
50	15.5	0.5	98
100	25.7	0.7	93
150	38.5	1.0	90
200	45.2	1.3	85

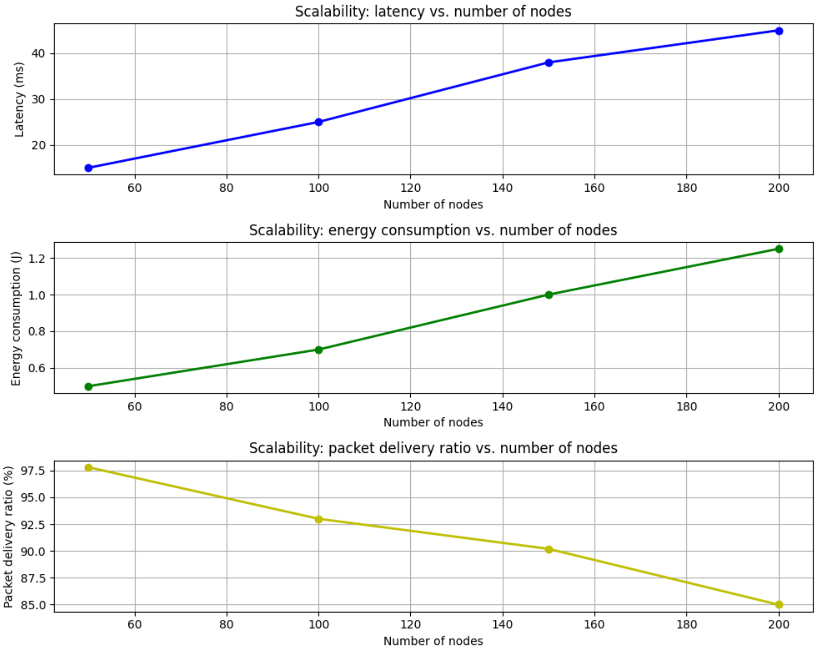

Figure 6 – Scalability comparison

Resource utilisation

The resource utilisation was measured in terms of memory and CPU usage during the simulation. *Table 10* shows that resource utilisation increases with the number of nodes but remains within acceptable limits for typical WSN applications.

Table 10 – Resource utilisation results

Number of nodes	Memory usage (MB)	CPU usage (%)
50	10	15
100	15	25
150	20	35
200	30	50

The results presented in this section demonstrate that the proposed framework for secured data aggregation and routing in wireless sensor networks effectively enhances data security, integrity and overall system performance. The findings highlight the efficiency of the ChaCha20-Poly1305 encryption algorithm, the robustness of the CHST blockchain technology for secure data management and the system's scalability to handle varying numbers of sensor nodes.

The comparative analysis with existing literature confirms the superiority of the proposed approach, establishing it as a viable solution for securing data in wireless sensor networks. Future work will focus on further optimisation of the system for real-world applications, including integration with other IoT technologies and expanding the security features of the proposed framework.

5. CONCLUSION

In an era where data security and integrity are dominant, especially in IoT areas, the proposed work presents a comprehensive framework that addresses the challenges of data aggregation and routing in wireless sensor networks (WSNs). By integrating advanced cryptographic techniques and blockchain technology, our approach not only safeguards the transmission of sensitive data but also ensures its authenticity and integrity. The use of the ChaCha20-Poly1305 provides a robust mechanism for protecting data during transmission, allowing for efficient operation even in resource-constrained environments typical of WSNs. This is complemented by the application of a permissioned blockchain structure, which guarantees tamper-proof storage of the encrypted data and allows controlled access for authorised users. The incorporation of a proof of authority consensus mechanism further enhances trust among participants in the network, ensuring that only verified nodes can validate transactions. A significant innovation in our framework is the implementation of zero-knowledge proofs (ZKP) for device authentication. This ensures that devices can show their individuality without leaking any private information, thereby enhancing the security of the entire system. By employing ZKP, the risks associated with unauthorised access and data breaches are mitigated, fostering a more secure IoT ecosystem. Furthermore, as vehicular networks become an integral part of smart transportation systems, our framework can be extended to enhance the overall efficiency of vehicle-to-everything (V2X) communications. The combination of blockchain and cryptographic techniques ensures secure vehicle authentication, tamper-proof data exchange and trust management among connected vehicles and infrastructure. This adaptability of our approach highlights its potential to support intelligent transportation networks, enabling secure and scalable vehicular communications while mitigating risks such as unauthorised access, data manipulation and privacy breaches. While the proposed framework demonstrates strong performance in terms of security and scalability, future enhancements could focus on integrating AI-driven anomaly detection techniques. Such approaches can enable real-time identification of abnormal patterns or threats within IIoT networks, improving responsiveness and reducing false positives. Additionally, exploring adaptive security mechanisms that evolve with emerging threats will further strengthen the framework's applicability in dynamic industrial environments.

REFERENCES

[1] Rane SB, Narvel YAM. Data-driven decision making with Blockchain-IoT integrated architecture: A project resource management agility perspective of industry 4.0. *Int J Syst Assur Eng Manag*. 2022;13:1005–1023. DOI: 10.1007/s13198-021-01377-4.

[2] Ma N, et al. Blockchain + IoT sensor network to measure, evaluate and incentivize personal environmental accounting and efficient energy use in indoor spaces. *Appl Energy*. 2023;332:120443. DOI: 10.1016/j.apenergy.2022.120443.

[3] Alrubei SM, Ball E, Rigelsford JM. A secure blockchain platform for supporting AI-enabled IoT applications at the edge layer. IEEE Access 2022;10:18583–18595. DOI: 10.1109/ACCESS.2022.3151370.

[4] Bataineh MR, Mardini W, Khamayseh YM, Yassein MMB. Novel and secure blockchain framework for health applications in IoT. *IEEE Access*. 2022;10:14914–14926. DOI: 10.1109/ACCESS.2022.3147795.

[5] Mathur S, et al. A survey on role of blockchain for IoT: Applications and technical aspects. *Comput Netw*. 2023;227:109726. DOI: 10.1016/j.comnet.2023.109726.

[6] Guru A, et al. A survey on consensus protocols and attacks on blockchain technology. *Appl Sci*. 2023;13:2604. DOI: 10.3390/app13042604.

[7] Serrano R, et al. ChaCha20–Poly1305 authenticated encryption with additional data for transport layer security 1.3. *Cryptography*. 2022;6:30. DOI: 10.3390/cryptography6020030.

[8] Chi PW, Lu YH, Guan A. A privacy-preserving zero-knowledge proof for blockchain. *IEEE Access*. 2023;11:85108–85117. DOI: 10.1109/ACCESS.2023.3302691.

[9] Chatamoni A, Bhukya R. Lightweight compressive sensing for joint compression and encryption of sensor data. *Int J Eng Technol Innov*. 2022;12:167–181. DOI: 10.46604/ijeti.2022.8599.

[10] Yang W, Wang S, Hu J, Karie NM. Multimedia security and privacy protection in the internet of things: Research developments and challenges. *Int J Multim Intell Secur*. 2022;4(1):20–46. DOI: 10.1504/IJMIS.2022.10044461

[11] Ma Z, Zhu L, Yu FR, James J. Protection of surveillance recordings via blockchain-assisted multimedia security. *Int J Sens Netw*. 2021;37(2):69–80. DOI: 10.1504/IJSNET.2021.118486.

[12] Singh R, Dwivedi AD, Mukkamala RR, Alnumay WS. Privacy-preserving ledger for blockchain and internet of things-enabled cyber-physical systems. *Comput Electr Eng*. 2022;103:108290. DOI: 10.1016/j.compeleceng.2022.108290.

[13] Singh R, et al. A privacy preserving internet of things smart healthcare financial system. *IEEE Internet Things J*. 2022;1. DOI: 10.1109/JIOT.2022.3233783.

[14] Sharma G, Kalra S. A novel scheme for data security in cloud computing using quantum cryptography. *Proc Int Conf Adv Inf Commun Technol Comput AICTC'16*. Association for Computing Machinery, New York, NY, USA; 2016. DOI: 10.1145/2979779.2979816.

[15] Ahad MA, et al. IoT data management—security aspects of information linkage in IoT systems. In: Peng S, Pal S, Huang L, editors. *Principles of Internet of Things (IoT) ecosystem: Insight paradigm*. Springer, Cham; 2020. p.439–464. DOI: 10.1007/978-3-030-33596-0_18.

[16] Bansal S, Kumar D. IoT ecosystem: A survey on devices, gateways, operating systems, middleware and communication. *Int J Wireless Inf Networks.* 2020;27(3):340–364. DOI: 10.1007/s10776-020-00483-7.

[17] Belli L, et al. IoT-enabled smart sustainable cities: Challenges and approaches. *Smart Cities*. 2020;3(3):1039–1071. DOI: 10.3390/smartcities3030052.

[18] Haris I, et al. CPS/IoT ecosystem: Indoor vertical farming system. *Proc IEEE 23rd Int Symp Consumer Technologies (ISCT). IEEE;* 2019. p.47–52. DOI: 10.1109/ISCE.2019.8900974.

[19] Hassan WH. Current research on internet of things (IoT) security: A survey. *Comput Netw*. 2019;148:283–294. DOI: 10.1016/j.comnet.2018.11.025.

[20] Isakovic H, et al. CPS/IoT ecosystem: A platform for research and education. In: Chamberlain R, Taha W, Törngren M, editors. *Cyber physical systems*. Springer, Cham; 2019. p.206–213. DOI: 10.1007/978-3-030-23703-5_12.

[21] Peng S, Pal S, Huang L. Principles of Internet of Things (IoT) ecosystem: *Insight paradigm*. Springer, Cham; 2020. DOI: 10.1007/978-3-030-33596-0.

[22] Zhao W, Yi L. Research on the evolution of the innovation ecosystem of the internet of things: A case study of Xiaomi (China). *Procedia Comput Sci*. 2022;199:56–62. DOI: 10.1016/j.procs.2022.01.008.

[23] Dobraunig C, Eichlseder M, Mendel F, Schläffer M. Ascon v1.2: Lightweight authenticated encryption and hashing. *J Cryptol*. 2021;34(3):33. DOI: 10.1007/s00145-021-09398-9.

[24] Alajlan NN, Ibrahim DM. TinyML: Enabling of inference deep learning models on ultra-low-power IoT edge devices for AI applications. *Micromachines*. 2022;13(6):851. DOI: 10.3390/mi13060851.

[25] Liu H, et al. Tiny machine learning (TinyML) for efficient channel estimation and signal detection. *IEEE Trans Veh Technol*. 2022;71(6):6795–6800. DOI: 10.1109/TVT.2022.3163786.

[26] Cao B, et al. A many-objective optimization model of industrial internet of things based on private blockchain. *IEEE Netw.* 2020;34(5):78–83. DOI: 10.1109/MNET.011.1900536.

[27] Almalki FA, et al. Green IoT for eco-friendly and sustainable smart cities: Future directions and opportunities. *Mobile Netw Appl.* 2023;28:178–202. DOI: 10.1007/s11036-021-01790-w.