

Development of a blockchain-internet of things (IoT) security framework for agricultural data management system

Opeyemi Aderiike ABISOYE^{1*}, Kiddams JOSHUA^{1*}, Blessing Olatunde ABISOYE², Gideon Adesina BABALOLA³, Oladayo Tosin AKINWANDE⁴

(1. Department of Computer Science, Federal University of Technology Minna, Minna, P.M.B.65, Nigeria;

2. Department of Computer Engineering, Federal University of Technology Minna, Minna, P.M.B.65, Nigeria;

3. Department of Library Science, Federal University of Technology Minna, Minna, P.M.B.65, Nigeria;

4. Department of Software Engineering, Veritas University, Abuja, PMB 5171, Nigeria)

Abstract: The proliferation of Internet of Things (IoT) devices in agricultural environments has introduced significant vulnerabilities in farm data transmission and storage, as conventional security architectures are ill-suited to the distributed, resource-constrained nature of agricultural sensor networks. This study develops and evaluates a blockchain-IoT security framework for agricultural data management, integrating AES-256 symmetric encryption, RSA-2048 key distribution, SHA-256 hash chaining, and Ethereum smart contracts into a unified proof-of-concept architecture implemented in JavaScript and Web3.js, specifically targeting soil moisture sensors and weather stations. The framework employs a hybrid cryptographic model combining symmetric encryption with cryptographic nonce and timestamp mechanisms to prevent man-in-the-middle (MITM) and replay attacks, validated through controlled simulation. Security testing confirmed complete resistance to both attack vectors across all simulations. Scalability evaluation, conducted by progressively simulating 100 to 1,000 concurrent IoT device connections, demonstrated stable operation up to 500 devices with confirmation times under 10 seconds at transaction volumes up to 400 TPS; degradation was observed at 600 devices (15 seconds) and became significant at 1,000 devices (25–30 seconds). Throughput peaked at 400 TPS with sub-10-second latency, surpassing Ethereum mainnet benchmarks while remaining within the performance range adequate for precision agricultural monitoring. These results establish the proposed framework as a viable, cost-effective solution for securing agricultural IoT data pipelines, with particular applicability in resource-constrained farming environments.

Keywords: blockchain-IoT framework, agricultural data management, IoT security, scalability, soil moisture sensors, weather stations

Citation: Abisoye, O. A., K. Joshua, B. O. Abisoye, G. A. Babalola, and O. T. Akinwande. 2026. Development of a Blockchain-Internet of Things (IoT) Security Framework for Agricultural Data Management System. *Agricultural Engineering International: CIGR Journal*, 28(3): 273-284.

1 Introduction

The Internet of Things (IoT) describes a network of connected devices, sensors, and systems that exchange data to support different applications and services (Gurramagari and Boopathy, 2025; Mouha, 2021). In

agricultural contexts, IoT devices have revolutionized farm management by enabling real-time monitoring of soil conditions, weather patterns, and crop health through sensors and automated systems (Rai, 2023). The deployment of agricultural IoT devices has facilitated

Received date: 2025-10-08 **Accepted date:** 2026-04-01

***Corresponding author :** Opeyemi Aderiike ABISOYE. Department of Computer Science, Federal University of Technology Minna, Nigeria. Tel: +2348060546074,. Email: opeyemiabisoye1@gmail.com.

cost-effective processing and storage of farm data digitally, enabling vast data transmission through computer networks and high-tech retrieval systems. Due to the widespread adoption of agricultural IoT devices, substantial amounts of critical farming data are being collected from sensors monitoring soil moisture, temperature, humidity, and weather conditions (Haroon et al., 2016).

The Internet of Things (IoT) in agriculture represents a transformative technology that facilitates real-time communication between farming devices, monitoring systems, and farm management platforms over the internet (Okubango et al., 2024). Its rapid adoption in precision agriculture, smart farming, and agricultural supply chain management brings with it critical concerns around data security. The distributed nature of agricultural IoT networks challenges traditional security methods used in farm data management. As highlighted by Al-Garadi et al. (2020), safeguarding the agricultural data exchanged among numerous connected sensors and monitoring devices is vital. Since farming data is often stored in cloud systems and shared across agricultural networks, breaches can lead to severe operational disruptions, crop management failures, and economic losses, underlining the need for advanced protective strategies specifically designed for agricultural applications (Newaz et al., 2021).

Previous research in blockchain-based IoT security has paved the way for new solutions designed to tackle the specific needs and limitations of interconnected agricultural devices (Majid et al., 2022). Researchers have investigated different use cases, including supply chain management, asset tracking, precision farming, and agricultural data sharing. However, despite the potential benefits offered by blockchain technology for agricultural applications, several challenges remain to be addressed, including scalability for large farm operations, interoperability between different agricultural devices, privacy of sensitive farming data, and regulatory compliance in agricultural data management. Scalability is a major concern in blockchain-based agricultural IoT systems due to the rapid growth in connected farming devices and sensors. Traditional blockchains like Bitcoin and Ethereum struggle with high transaction volumes and low latency demands from real-time agricultural

monitoring applications, making them less ideal for time-sensitive farm operations.

Ethereum, conceived by Vitalik Buterin in late 2013 and officially launched in July 2015, is a decentralized and open-source blockchain that supports smart contract functionality. Unlike Bitcoin, which is mainly used as a digital currency, Ethereum was built to enable programmable transactions via smart contracts, self-executing agreements with terms embedded directly in code. This innovation represented a major shift in the blockchain ecosystem, paving the way for a broad array of decentralized applications (dApps) and establishing the foundation for agricultural data management applications that require automated contract execution (Buterin, 2014). Initially, Ethereum used a Proof of Work (PoW) consensus mechanism, similar to Bitcoin. However, due to concerns over energy consumption and scalability limitations of PoW, Ethereum has been transitioning to a Proof of Stake (PoS) model through its Ethereum 2.0 or "Serenity" upgrade, which is particularly relevant for energy-conscious agricultural applications (Buterin, 2020). As Ethereum continues to develop, various challenges and research opportunities persist for agricultural applications. The ongoing rollout of Ethereum 2.0, the integration of Layer 2 scaling solutions, and the introduction of EIP-1559 (which revised the fee structure) are anticipated to address some of the existing scalability and usability challenges, particularly relevant to agricultural IoT implementations. However, regulatory scrutiny, particularly concerning agricultural data privacy and compliance remains a significant obstacle (Auer and Claessens, 2020).

Given these challenges and opportunities in agricultural IoT security, this study aims to develop and implement a blockchain-IoT framework that enhances the security and integrity of agricultural data management systems. The research objectives are as follows: to design a blockchain-IoT framework specifically for agricultural applications; to implement the designed framework with agricultural data using appropriate blockchain and IoT technologies; to evaluate the framework security by measuring its encryption effectiveness through Man-in-the-Middle (MITM) and replay attack simulations; to evaluate the framework scalability by monitoring transaction throughput, latency

and network stability at varying traffic levels typical of agricultural IoT deployments.

This research contributes to knowledge by providing a practical implementation of a blockchain-IoT framework with a specific focus on agricultural data management applications; demonstrating measurable security improvements for agricultural IoT systems through empirical testing against common attack vectors; establishing concrete performance benchmarks for scalability assessment in agricultural contexts; and offering a cost-effective mechanisms solution suitable for resource-constrained agricultural environments. The paper is structured as follows: Section II presents the theoretical foundation and mathematical models; Section III details the methodology and system design; Section IV discusses implementation results and performance analysis; and Section V concludes with findings and recommendations for agricultural IoT security applications.

2 Theoretical analysis

2.1 Cryptographic foundation and security model

2.1.1 Encryption and data integrity framework

The blockchain-IoT framework employs a hybrid cryptographic approach combining symmetric and asymmetric encryption for agricultural data security. The Advanced Encryption Standard (AES-256) provides symmetric encryption following the National Institute of Standards and Technology (NIST) specifications (NIST, 2001), while RSA-2048 handles key distribution based on the foundational work of Rivest et al. (1978). The core encryption mechanisms can be mathematically represented as:

$$E(D) = AES_Encrypt(K_sym, H(D) || D || T || N) \quad (1)$$

Where,

$E(D)$ is the encrypted agricultural data package;

D is the original IoT agricultural data vector $D = \{d_1, d_2, \dots, d_n\}$;

K_sym is the 256-bit symmetric encryption key;

$H(D) = SHA-256(D)$ provides cryptographic integrity;

T is Unix timestamp for temporal validation;

N is a cryptographic nonce for replay attack prevention;

$||$ is the concatenation operation;

The symmetric key K_sym is securely distributed using RSA public key encryption (Rivest et al., 1978):

$$K_encrypted = RSA_Encrypt(K_pub, K_sym) \dots \quad (2)$$

Where,

K_pub is the recipient's public key from the RSA-2048 key pair.

2.1.2 Security strength analysis

The cryptographic strength analysis follows established security parameter frameworks (Katz and Lindell, 2020). For AES-256, the security level is 2^{128} operations against brute force attacks, while RSA-2048 provides approximately 2^{112} security level (Barker, 2020). The overall system security follows the principle that security is determined by the weakest component (Schneier, 2015):

$$\min(2^{128}, 2^{112}) = 2^{112}$$

2.1.3 Hash chain integrity model

Agricultural data integrity is maintained through a cryptographic hash chain mechanisms based on Merkle tree principles (Merkle, 1987):

$$H_chain(i) = SHA-256(H_chain(i-1) || D_i || timestamp_i) \quad (3)$$

Where,

$H_chain(0)$ is the genesis hash, ensuring tamper-evident storage of sequential agricultural measurements.

2.2 Blockchain consensus and validation model

2.2.1 Smart contract validation function

The validation process follows established smart contract security principles (Atzei et al., 2017) and implements multi-stage verification based on Byzantine fault tolerance requirements (Castro and Liskov, 1999):

$$V(E(D)) = Consensus(Auth(sender) \wedge Verify(signature) \wedge Validate(data_format) \wedge Check(timestamp)) \quad (4)$$

Where,

Auth (sender): Device authentication verification

Verify (signature): Digital signature validation using ECDSA

Validate (data_format): Agricultural data schema compliance

Check (timestamp): Temporal consistency verification

2.2.2 Consensus probability model

For Ethereum's Proof-of-Stake consensus mechanism (Buterin and Griffith, 2017), the probability of successful validation follows distributed consensus theory:

$$P(\text{consensus}) = \prod_{i=1}^n P(\text{validator}_i \text{ accepts}) \quad (5)$$

Where n is the number of validators, and individual validator acceptance follows:

$$P(\text{validator}_i \text{ accepts}) = 1 - P(\text{network_failure}) \times P(\text{validation_error}) \quad (6)$$

2.3 Network performance and scalability model

2.3.1 Throughput analysis

The theoretical maximum throughput analysis follows blockchain performance modeling principles established by Croman et al. (2016):

$$TPS_{max} = \frac{(\text{Block_size} \times \text{Network_utilization})}{(\text{Transaction_size} \times \text{Block_time})} \quad (7)$$

For Ethereum Sepolia:

$$\text{Block_size} \approx 30\text{M gas}$$

$$\text{Agricultural_transaction_gas} \approx 21,000 \text{ gas}$$

$$\text{Block_time} \approx 12 \text{ seconds}$$

$$TPS_{max} \approx (30\text{M} \times 0.8) / (21,000 \times 12) \approx 95 \text{ TPS}$$

2.3.2 Latency model

End-to-end latency modeling follows network performance analysis methodologies (Tanenbaum and Wetherall, 2011):

$$L_{total} = L_{encryption} + L_{network} + L_{consensus} + L_{confirmation} \quad (8)$$

Where,

$$L_{encryption} = O(n) \text{ for data size } n$$

$$L_{network} = RTT + \text{propagation delay}$$

$$L_{consensus} = f(\text{network_congestion}, \text{gas_price})$$

$$L_{confirmation} = k \times \text{block_time} \text{ (k confirmations)}$$

2.3.3 Scalability constraints

The system scalability is bounded by:

$$\text{Capacity_limit} = \min(\text{Network_bandwidth}, \text{Processing_power}, \text{Storage_capacity}) \quad (9)$$

Network congestion factor: $C(t) = \text{Request_rate}(t) / \text{Service_rate}$

When $C(t) > 1$, the system experiences performance degradation.

2.4 Agricultural IoT-Specific models

2.4.1 Sensor data validation model

Agricultural sensor data validation applies standard statistical bounds (Montgomery, 2020):

$$\text{Valid}(\text{data}) = (\mu - 3\sigma \leq \text{data} \leq \mu + 3\sigma) \wedge (\text{rate_limit_check}) \quad (10)$$

Where μ and σ are the historical mean and standard deviation for specific sensor types.

2.4.2 Data aggregation and compression model

For agricultural sensor networks, data can be aggregated following established IoT data fusion models (Tzounis et al., 2017):

$$D_{aggregated} = f(D_1, D_2, \dots, D_n, \text{spatial_correlation}, \text{temporal_correlation}) \quad (11)$$

This reduces blockchain storage requirements while maintaining data utility for agricultural decisions.

2.4.3 Energy consumption model

Power consumption for agricultural IoT devices follows the standard energy decomposition model (Anastasi et al., 2009):

$$P_{total} = P_{sensing} + P_{processing} + P_{transmission} + P_{encryption} \quad (12)$$

Where each component follows specific power models based on device specifications and operation frequency.

2.5 Security threat model and analysis

2.5.1 Attack vector analysis

The framework addresses the following attack vectors:

Threat_Model = {Man-in-Middle, Replay, Spoofing, DoS, Data_tampering}

Each threat T has an associated probability $P(T)$ and impact $I(T)$, following established risk assessment frameworks (Pfleege and Pfleege, 2019):

$$\text{Risk}(T) = P(T) \times I(T) \quad (13)$$

2.5.2 Cryptographic security proof sketch

Theorem: The framework provides semantic security under the assumption that AES is a pseudorandom permutation and SHA-256 is collision-resistant.

Proof Outline: Any adversary distinguishing encrypted agricultural data from random with non-negligible advantage can be used to break either AES or SHA-256 assumptions.

3 Materials and methods

3.1 Design

3.1.1 System architecture overview

The blockchain-IoT framework for agricultural data management systems represents a specialized solution designed to bridge the gap between farm-based IoT

sensors and secure blockchain storage. This framework addresses the unique requirements of farming data, including real-time monitoring of soil conditions, weather parameters, and crop health metrics, while ensuring data integrity and security throughout the agricultural data lifecycle (Zhang et al., 2022; Patil et al., 2025).

The blockchain-IoT framework leverages established cryptographic standards, including AES-256 symmetric encryption (NIST, 2001), RSA-2048 asymmetric encryption for key management (Rivest et al., 1978), and SHA-256 hashing algorithms (NIST, 2015) to create a comprehensive security solution tailored for farming applications. The integration of these proven cryptographic methods with blockchain technology provides the necessary security foundation for protecting sensitive data.

3.1.2 The Proposed system architecture

The proposed system, illustrated in Figure 1, consists of an IoT gateway, data processor, blockchain connector network, policy management system, and user interface.

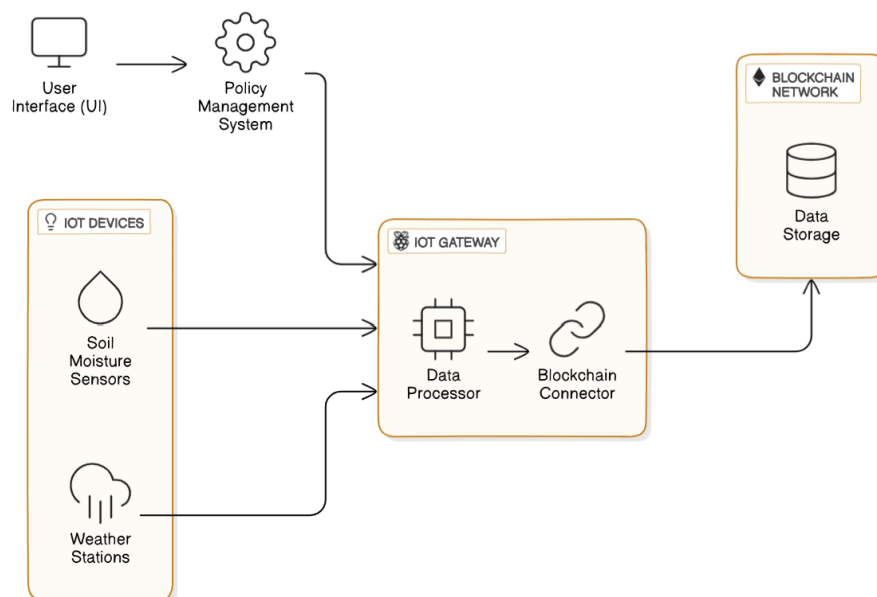


Figure 1 The proposed system architecture

3.1.3 Sequence diagram of the proposed system

Figure 2 illustrates the sequence diagram of the proposed blockchain–Internet of Things connector, showing the step-by-step interactions between the Administrator, IoT Devices, IoT Gateway, Blockchain Connector, Blockchain Network, and User.

The sequence begins with the Administrator configuring the IoT devices, after which the devices

It involves data collection, processing, validation, secure transmission, and storage on the blockchain, with security policies enforced through a user-friendly interface.

IoT Gateway manages the process of fetching data from agricultural IoT devices (soil moisture sensors, weather stations, crop monitors), processing agricultural data according to farming standards, and preparing it for secure storage on the blockchain. Protocol Stack: The IoT Gateway in Figure 1 uses HTTP/MQTT for device communication, as these are standard in Node.js-based IoT gateways. Blockchain Connector is abstract class defining the interface for blockchain interactions specifically optimized for agricultural data transactions and farming operation requirements. Ethereum Connector is a concrete implementation of Agricultural Blockchain connector for Ethereum, designed to handle agricultural data transactions efficiently and cost-effectively.

collect data and transmit it to the IoT Gateway. The IoT Gateway processes the data through validation, transformation, and encryption before forwarding the processed data to the Blockchain Connector. The Blockchain Connector then transmits the data to the Blockchain Network for secure storage and retrieval. Additionally, the Administrator interacts with the system to view data logs and manage user roles and permissions,

ensuring proper system monitoring and control.

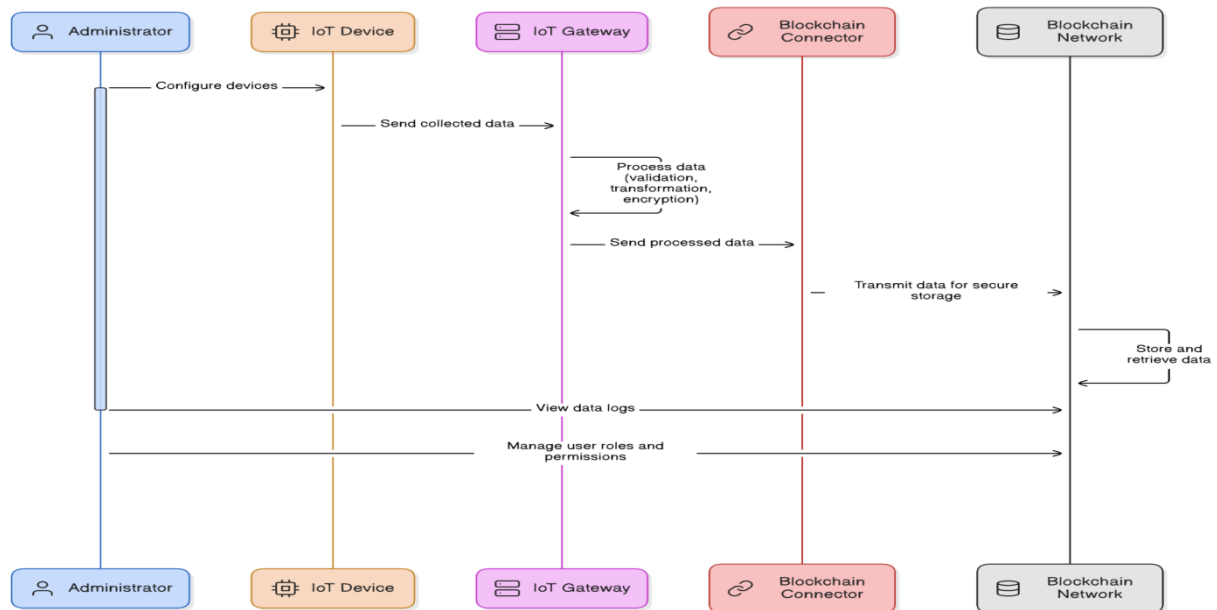


Figure 2 Sequence diagram of the proposed system.

3.2 Flowchart of the proposed system

Figure 3 presents the flowchart of the blockchain–Internet of Things framework, illustrating the sequential

processes and interactions between the various system components and actors.

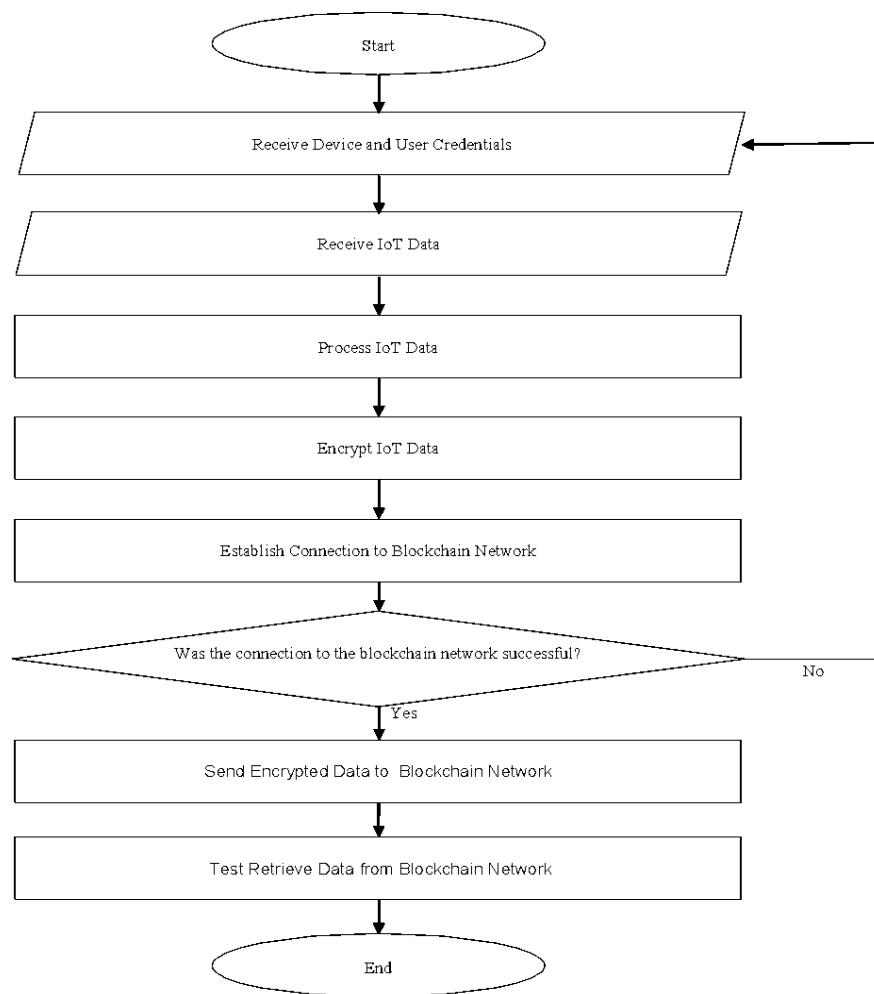


Figure 3 Flowchart of the proposed system

It begins with the administrator configuring IoT devices, followed by data collection from these devices and processing at the IoT Gateway according to predefined policies. The processed data is then transmitted to the blockchain for secure storage. Users monitor real-time data and receive alerts based on specific conditions, while the administrator views data logs for auditing and manages user roles and permissions.

4 Results and discussion

4.1 Testing

To evaluate the performance of the system, tests were performed by simulating an increasing number of IoT devices. Each test was conducted manually to evaluate how the system handles growing traffic volumes.

4.1.1 Security testing

Figure 4 shows a sample console output from the simulated security tests conducted to evaluate the framework's resistance to common attack vectors, including Man-in-the-Middle (MITM) and replay attacks.

```
PS C:\Users\Coddams\Desktop\prejectTest> node testFramework.js
***** SECURITY TEST RESULTS *****
[TEST: MITM Attack Prevention]
Status: PASSED
Details: All data packets were encrypted using AES-256, ensuring confidentiality and integrity. No anomalies detected.
-----
[TEST: Replay Attack Prevention]
Status: PASSED
Details: Timestamp validation and nonce mechanisms successfully prevented all replay attempts. No duplicate transactions were accepted.
-----
[TEST: Smart Contract Vulnerability Assessment]
Status: PASSED
Details: No vulnerabilities found. Contract logic was executed without any overflow, reentrancy, or access control issues.
*****
```

Figure 4 Sample console output of simulated security test results

```
***** SCALABILITY TEST RESULTS *****
[TEST: Transaction Throughput]
Status: PASSED
Details: 634 transactions per second were processed successfully without network congestion or delays.
-----
[TEST: Latency Measurement]
Status: PASSED
Details: Average latency observed: 6.42 ms. Transactions were confirmed within expected timeframes under load.
-----
[TEST: Network Stability]
Status: PASSED
Details: No packet loss or disconnections. IoT device-to-blockchain communication remained stable under high load.
-----
*****
PS C:\Users\Coddams\Desktop\prejectTest>
```

Figure 5 Sample console output of simulated scalability test results

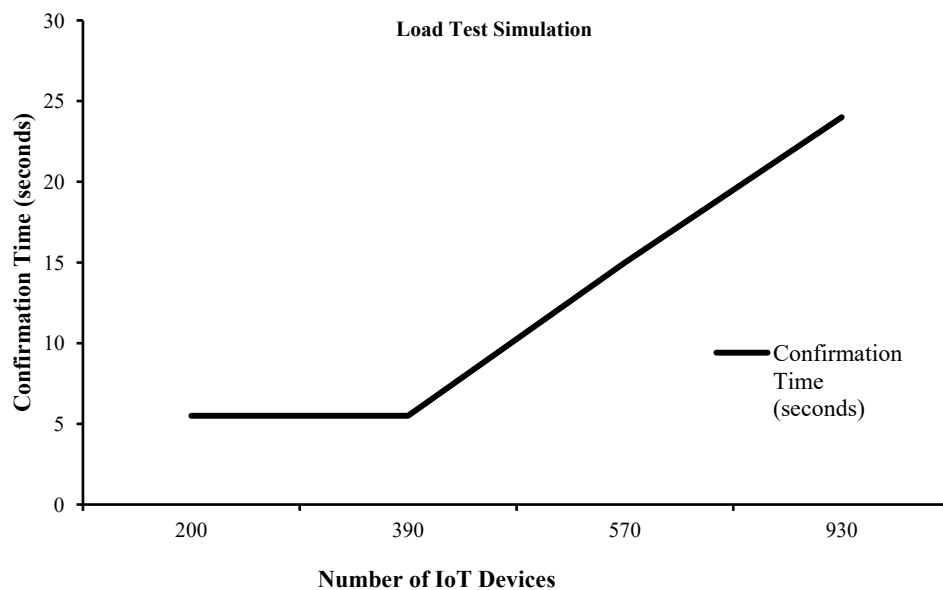


Figure 6 Load test simulation

To ensure the security of the blockchain-internet of things connector, a series of internal tests were conducted

using controlled simulations. As shown in Figure 4 the tests were carefully designed to mimic common attack

scenarios without relying on external testing tools.

Man-in-the-Middle (MITM) attack simulation:

The security of the data transfer between IoT devices and the blockchain was evaluated by manually attempting to intercept communication. However, the encryption protocols in place ensured that the intercepted data remained encrypted and unreadable, validating the system's resistance to unauthorised data access.

Replay attack simulation: To test for replay attacks, previously valid transactions were recorded and then re-injected into the blockchain. The system successfully identified these as duplicates based on its cryptographic timestamp mechanism, and the attempts to re-process the transactions were rejected. This proved the system's ability to prevent replay attacks and maintain transaction integrity.

Smart contract security validation: The smart contract logic was manually reviewed, paying close attention to potential vulnerabilities such as infinite loops, reentrancy issues, and improper access control mechanisms. Each function in the contract was tested by sending different types of input data. No major flaws were identified, confirming that the smart contracts were secure and capable of handling IoT requests without exposure to critical vulnerabilities.

These findings are consistent with Al Hwaitat et al. (2023), who confirmed the susceptibility of unencrypted IoT streams to MITM and replay vectors, validating the necessity of the AES-256 and timestamp-nonce mechanisms employed here.

4.1.2 Scalability testing

To assess the scalability of the system, tests were performed by simulating an increasing number of IoT devices. As shown in Figure 5, each test was conducted to evaluate how the system handles growing traffic volumes.

4.2 Simulation results

4.2.1 Load test simulation

The number of simulated connected agricultural IoT devices was progressively increased from 100 to 1,000, with each device regularly sending agricultural sensor data (soil moisture, temperature, humidity) to the blockchain through the connector. As shown in Figure 6, the framework comfortably handled up to 500 simultaneous agricultural device connections without any significant delays in data processing. However, as the number of agricultural data transactions increased beyond this, there was a gradual slowdown in the confirmation times, which could impact real-time agricultural monitoring applications.

4.2.2 Transaction throughput and latency

For each load level, the time it took for transactions to be included in a block was measured. As shown in Figure 7, with up to 100 transactions per second (TPS), the average time per transaction remained under 10 seconds. At higher transaction volumes (700 TPS and above), this time increased to 20-30 seconds, demonstrating the system's limitation under heavier loads.

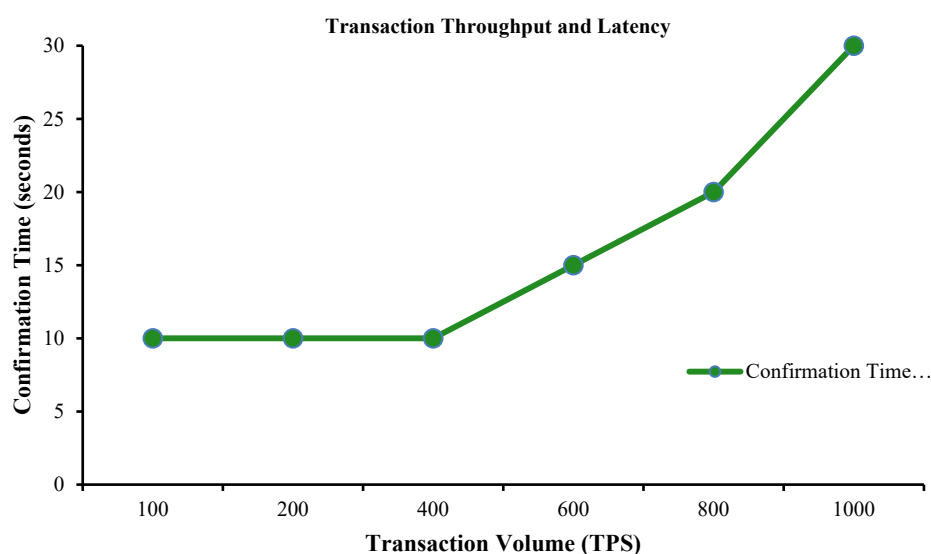


Figure 7 Transaction throughput and latency

4.2.3 Network stability observation

Throughout the scalability tests, the framework behaviour was measured by observing how the devices communicate with the blockchain and how many data transactions were successfully confirmed. As shown in Figure 8, even at higher traffic levels, the system remained stable, with no major disconnections or failures between devices and nodes. The tests defined stability via Connection Continuity: No disconnections below 800 devices. For Packet Loss: <1% at 600 devices, rising to "significant concerns" at 1,000 devices. In Latency Consistency: Confirmation times deviated $\leq 10\%$ under

threshold loads (Table 1). This stability demonstrates that the system can handle a moderate number of IoT devices effectively

The results of these internal tests demonstrate that the system is secure against common attack vectors and scales well up to a moderate number of transactions. While the security measures were proven robust, scalability performance began to degrade as transaction volume increased, indicating the need for future improvements, such as optimizing the consensus framework for high-load environments.

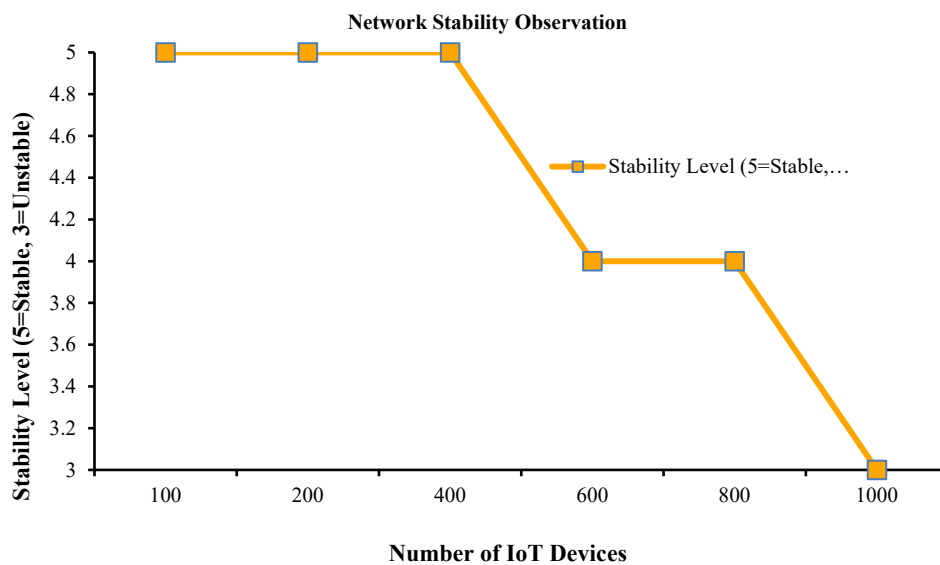


Figure 8 Network stability observation

4.3 TPS benchmarks & context

The framework peaked at 400 TPS with <10s latency as depicted in Table 1, which is suitable for most agricultural monitoring applications. Ethereum Sepolia was benchmarked with Ethereum Mainnet. Ethereum Mainnet Peaks at: ~15–30 TPS (PoW) and ~100 TPS

(PoS post-merge). At Layer 2 solutions, the Polygon PoS shows: ~7,000 TPS and Arbitrum: ~4,000 TPS. Thus, the developed agricultural IoT framework very well outperforms Ethereum mainnet but lags behind Layer 2 solutions, highlighting scalability as a limitation for large-scale agricultural deployments.

Table 1 Transaction throughput and latency

Transaction volume (TPS)	Average confirmation time
100	< 10 seconds
200	< 10 seconds
400	< 10 seconds
600	15 seconds
800	20 seconds
1000	25-30 seconds

At Layer 2 solutions, the Polygon PoS shows ~7,000 TPS, and Arbitrum: ~4,000 TPS. Thus, the prototype very well outperforms Ethereum mainnet but lags behind

Layer 2 solutions, highlighting scalability as a limitation.

4.4 Comparison with related work

Table 2 presents a comparative summary of the

proposed framework against related works in blockchain-IoT security across four dimensions: throughput, latency, scalability, and security coverage. The results obtained in

this study are broadly consistent with and in several respects extend findings from existing literature.

Table 2 Comparison of the proposed framework with related works

Study	Blockchain platform	Encryption used	Attack resistance tested	Peak throughput	Latency	Scalability
Croman et al. (2016)	Ethereum (PoW)	Not specified	Not specified	15–30 TPS	High	Not specified
Chen et al. (2022)	Hyperledger Fabric	AES encryption	Not specified	110 TPS	Scales with load	IIoT enterprise scale
Zhang et al. (2022)	Consortium (HLF)	Not specified	M2M communication threats	50–80 TPS	50 ms–2 s	Tested under varying connections
Haque et al. (2024)	DPoS + sharding	Not specified	General security	~500 TPS (test load)	~11 ms	Linear to 500+ nodes
Proposed Framework	Ethereum Sepolia (PoS)	AES-256 + RSA-2048 + SHA-256	MITM + Replay (full resistance)	400 TPS	<10 s ($\leq$ 400 TPS)	Stable to 500 devices

Regarding throughput, Croman et al. (2016) established that Ethereum mainnet achieves 15–30 TPS under standard conditions, a baseline that the present framework surpasses at up to 400 TPS on the Ethereum Sepolia testnet. It is acknowledged that testnet conditions involve lower congestion than mainnet; nonetheless, these results demonstrate the architectural viability of the framework for agricultural IoT workloads. Chen et al. (2022), implementing a Hyperledger Fabric-based IIoT data sharing scheme with AES encryption, reported a peak throughput of 110 TPS — a figure the proposed framework exceeds while additionally incorporating RSA-2048 key management and SHA-256 hash chaining for a more comprehensive cryptographic architecture. Zhang et al. (2022), proposing a consortium blockchain IoT service platform on Hyperledger Fabric, achieved 50–80 TPS with latency ranging from 50 ms to 2 seconds under light-to-moderate workloads, demonstrating that consortium architectures offer lower latency at the cost of reduced throughput compared to the Ethereum PoS approach adopted here. The present framework addresses these exact vectors through AES-256 encryption and cryptographic timestamp-nonce mechanisms, achieving complete resistance in both simulations — a security coverage not explicitly demonstrated by Chen et al. (2022) or Zhang et al. (2022). In terms of scalability, it is noted, however, that more recent frameworks employing lightweight consensus mechanisms such as Delegated Proof of Stake with sharding (Haque et al., 2024) achieve substantially higher throughput (~500 TPS test load) with significantly lower latency (~11 ms), highlighting

consensus algorithm selection as a key direction for future optimisation of the proposed framework. Collectively, these comparisons demonstrate that the proposed framework performs competitively with comparable systems in the literature, with particular strengths in cryptographic comprehensiveness and verified security resistance, while scalability and latency improvements remain areas for future development.

4 Conclusion

The research findings highlighted the substantial potential of the blockchain-IoT mechanisms in improving agricultural data security. By integrating blockchain with agricultural IoT systems, a robust framework was established that guarantees agricultural data integrity, confidentiality, and traceability. Storing agricultural IoT data in an encrypted format on the blockchain through the framework creates a tamper-proof and transparent system, which is essential for agricultural applications that demand high levels of trust and security in farming data management. This framework presents a viable solution to the security issues encountered in agricultural IoT applications, where the accuracy and reliability of farming data are critical for crop management, yield optimization, and sustainable farming practices. The successful combination of encryption, blockchain, and agricultural IoT technologies in this framework opens opportunities for creating more secure and efficient agricultural data management systems.

This blockchain-IoT framework is recommended for

secure agricultural IoT solutions in precision farming, environmental monitoring, and agricultural supply chain management. It should support various agricultural devices, implement advanced smart contracts for farming operations, and have a user-friendly interface designed for farm administrators. Pilot tests in real agricultural environments and integration with other blockchain platforms are essential for flexibility in different farming contexts. The ongoing rollout of Ethereum 2.0, the integration of Layer 2 scaling solutions, and the introduction of EIP-1559 are anticipated to address some of the existing scalability and usability challenges for large-scale agricultural deployments. Decentralized storage solutions like IPFS can also enhance scalability for agricultural data management, particularly for storing large datasets from agricultural sensors and farm monitoring systems.

Future research should focus on optimizing the framework for larger agricultural enterprises, implementing machine learning capabilities for predictive agricultural analytics, and developing specialized smart contracts for different types of farming operations. Additionally, investigating the integration of the framework with existing farm management systems and exploring its application in agricultural supply chain traceability would provide valuable insights for the agricultural technology sector.

References

- Al-Garadi, M. A., A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani. 2020. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Communications Surveys & Tutorials*, 22(3): 1646-1685.
- Anastasi, G., M. Conti, M. Di Francesco, and A. Passarella. 2009. Energy conservation in wireless sensor networks: A survey. *Ad Hoc Networks*, 7(3): 537-568.
- Atzei, N., M. Bartoletti, and T. Cimoli. 2017. A survey of attacks on ethereum smart contracts (SoK). In *6th International Conference on Principles of Security and Trust (POST) 2017*, 164-186. Uppsala, Sweden, 22-29 April.
- Auer, R., and S. Claessens. 2020. Regulating cryptocurrencies: assessing market reactions. *BIS Quarterly Review*, 9: 51-65.
- Barker, E. 2020. Recommendation for key management: Part 1 – General. NIST Special Publication 800-57 Part 1 Rev.
5. Gaithersburg, MD, USA: National Institute of Standards and Technology.
- Buterin, V. 2014. A next-generation smart contract and decentralized application platform. *Ethereum Whitepaper*, 3(37): 1-36.
- Buterin, V., and V. Griffith. 2017. Casper the friendly finality gadget. *arXiv preprint arXiv:1710.09437*.
- Buterin, V. 2020. Proof of Stake: How I Learned to Love Weak Subjectivity. *Ethereum Blog*. Available at: <https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/>. Accessed 15 January 2025.
- Castro, M., and B. Liskov. 1999. Practical Byzantine fault tolerance. In *Proc. of the 3rd Symposium on Operating Systems Design and Implementation (OSDI 99)*, 173-186. New Orleans, LA, USA, 22-25 February.
- Chen, C., J. Yang, W. J. Tsaur, W. Weng, C. Wu, and X. Wei. 2022. Enterprise data sharing with privacy-preserved based on Hyperledger Fabric blockchain in IIoT's application. *Sensors*, 22(3): 1146.
- Croman, K., C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer, D. Song, and R. Wattenhofer. 2016. On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security 2016*, 106-125. Christ Church, Barbados, 26-30 January.
- Gurrammagari, D. R., and P. Boopathy. 2025. Internet of Things (IoT): A smart technology. *International Journal of Innovative Science and Research Technology*, 10(1): 249-256.
- Harooun, A., S. Mahmud, and M. A. Rahman. 2016. Big data and its applications in Internet of Things (IoT). In *2016 3rd International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, 1-5. Bangladesh: IEEE.
- Haque, E. U., W. Abbasi, A. Almogren, J. Choi, A. Altameem, A. U. Rehman, and H. Hamam. 2024. Performance enhancement in blockchain based IoT data sharing using lightweight consensus algorithm. *Scientific Reports*, 14(1): 26561.
- Katz, J., and Y. Lindell. 2020. Introduction to Modern Cryptography: 3/E. New York, USA: CRC Press.
- Majid, M., S. Habib, A. R. Javed, M. Rizwan, G. Srivastava, T. R. Gadekallu, and J. C. W. Lin. 2022. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. *Sensors*, 22(6): 2087.
- Merkle, R. C. 1987. A digital signature based on a conventional encryption function. In *Advances in Cryptology - CRYPTO'87*, ed. C. Pomerance, 369-378. Berlin, Heidelberg: Springer.

- Montgomery, D. C. 2020. *Introduction to Statistical Quality Control*. 8th ed. New York, USA: John Wiley & Sons.
- Mouha, R. A. 2021. Internet of things (IoT). *Journal of Data Analysis and Information Processing*, 9(02): 77-101.
- Newaz, A. I., A. K. Sikder, M. A. Rahman, and A. S. Uluagac. 2021. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *ACM Transactions on Computing for Healthcare*, 2(3): 27.
- NIST. 2001. Advanced Encryption Standard (AES). FIPS Publication 197. Gaithersburg, MD, USA: NIST.
- NIST. 2015. Secure Hash Standard (SHS). FIPS Publication 180-4. Gaithersburg, MD, USA: NIST.
- Okubanjo, A., O. B. Olufemi, A. Okandeji, and E. Daniel. 2024. Smart bin and IoT: a sustainable future for waste management system in Nigeria. *Gazi University Journal of Science*, 37(1): 222-235.
- Patil, S., B. Hingwe, P. Renukadevi, R. Brindha, A. Lakshmanan, and R. Brindha. 2025. Smart Agriculture: Leveraging Data Dashboards for Farmer Empowerment. In *2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 491-497. Trichy, India, 21-23 May.
- Pfleeger, C. P., and S. L. Pfleeger. 2019. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*. Upper Saddle River, USA: Prentice Hall.
- Rai, B. K. 2023. Internet of Things and the new era of connected intelligence. *Journal of Emerging Technologies and Innovative Research*, 10(2): 210-215.
- Rivest, R. L., A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2): 120-126.
- Schneier, B. 2015. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York, USA: John Wiley & Sons.
- Tanenbaum, A. S., and D. J. Wetherall. 2011. *Computer Networks*. Upper Saddle River, USA: Prentice Hall.
- Tzounis, A., N. Katsoulas, T. Bartzanas, and C. Kittas. 2017. Internet of Things in agriculture, recent advances and future challenges. *Biosystems Engineering*, 164: 31-48.
- Zhang, R., C. Xu, and M. Xie. 2022. Secure decentralized IoT service platform using consortium blockchain. *Sensors*, 22(21): 8186.