

IMPLEMENTATION OF A BLOCKCHAIN-ENABLED SECURE IOT NETWORKING FRAMEWORK FOR DECENTRALIZED DEVICE AUTHENTICATION AND DATA INTEGRITY

Mrs. Roopa .R ,
Department of Artificial Intelligence and Data Science,
Arjun College of Technology,
Coimbatore,
Email: roopa.renuga@gmail.com

Abstract

The rapid growth of Internet of Things (IoT) deployments has increased the need for secure and trustworthy communication among constrained devices, gateways, edge nodes, and application servers. Conventional centralized IoT security architectures can create single points of failure and may provide limited visibility into device activity and data provenance. This paper presents an implementation-oriented blockchain-enabled IoT networking framework that combines device authentication, gateway-based communication, distributed ledger recording, and integrity verification. The proposed system is designed around resource-constrained IoT devices that communicate with a local gateway, while blockchain services are executed on comparatively capable network nodes. Device registration, authentication events, selected sensor-data metadata, and security events are recorded on a permissioned ledger, whereas complete sensor records are maintained in conventional storage. A prototype workflow is described using simulated IoT nodes, a gateway service, a blockchain layer, and a monitoring application. Experimental evaluation considers authentication delay, communication latency, transaction processing, packet delivery, storage overhead, and resilience against unauthorized device access. The implementation demonstrates how blockchain can complement conventional networking security without forcing constrained sensors to execute heavyweight ledger operations. The study provides a practical architecture for secure smart-home, industrial, agricultural, and smart-city IoT deployments.



Keywords—Blockchain, Internet of Things, IoT networking, device authentication, data integrity, permissioned blockchain, edge computing, cybersecurity.

I. INTRODUCTION

The Internet of Things connects physical objects to communication networks so that sensing, monitoring, analysis, and control can be performed continuously. IoT deployments range from small environmental-monitoring systems to large industrial networks containing thousands of sensors and actuators. These environments depend on gateways, wireless networks, edge platforms, and cloud services to move data from physical devices to applications. As the number of connected devices increases, maintaining reliable identity, access control, and data integrity becomes increasingly difficult [1], [2].

A common IoT security architecture places authentication and data management under a centralized server. Although this arrangement is straightforward to implement, it can create a single point of compromise. If the central service is unavailable or compromised, device access decisions and security records may be affected. In addition, organizations that exchange IoT data may not fully trust one another, making a shared and verifiable record useful [3].

Blockchain provides a distributed ledger that can record selected IoT events in a tamper-evident manner. Smart contracts can automate registration and authorization rules, while cryptographic identities can be used to verify participating devices. However, directly installing a conventional blockchain client on every sensor is generally inefficient because many IoT devices have limited memory, processing capability, and battery capacity [4], [5].

This paper therefore focuses on implementation rather than a purely conceptual blockchain-IoT model. The proposed framework places lightweight communication and authentication functions on IoT devices, performs protocol handling and filtering at a gateway, and reserves blockchain operations for more capable nodes. Only security-relevant metadata are written to the ledger. This design reduces storage and communication overhead while retaining decentralized verification and auditability.

The main contribution is a practical end-to-end workflow for secure IoT networking that can be implemented with commodity hardware or a software-based testbed. The framework supports device registration, authentication, sensor-data transfer, blockchain event recording, integrity verification, and unauthorized-access detection. The paper also defines an evaluation methodology suitable for comparing the proposed architecture with a conventional centralized IoT security model.



II. RELATED WORK

IoT networking research has established the importance of heterogeneous communication technologies, gateways, cloud services, and lightweight protocols for large-scale connected systems [1], [2]. Security research has identified device authentication, confidentiality, access control, and privacy as major concerns because many IoT devices operate with limited computational and energy resources [3]. These constraints make security mechanisms designed for conventional computers difficult to deploy directly on sensors.

Blockchain has been investigated as a decentralized trust mechanism for IoT. Early studies demonstrated the potential of smart contracts and distributed ledgers for machine-to-machine interactions [4]. Systematic studies subsequently examined blockchain-based identity management, access control, data integrity, and decentralized IoT architectures [5], [6]. Permissioned blockchain is particularly relevant to organizational IoT environments because validator participation can be restricted to trusted infrastructure providers.

Edge computing has further improved the practicality of blockchain-enabled IoT by moving computation closer to data sources. Edge nodes can perform aggregation, filtering, anomaly detection, and blockchain interaction without requiring every sensor to maintain a complete ledger [7]. Research has also examined optimized blockchain architectures specifically for constrained IoT environments [8]. However, practical implementation studies must consider the complete networking path, including device communication, gateway processing, ledger interaction, storage, and monitoring.

The proposed implementation addresses this gap by treating blockchain as a security and audit layer rather than as the communication network itself. Conventional IoT networking remains responsible for data transport, while the blockchain layer maintains device and event trust information.

III. PROPOSED SYSTEM

The proposed system consists of five major components: IoT sensor nodes, an IoT gateway, blockchain validator nodes, an off-chain data repository, and a monitoring application. Sensor nodes generate readings and communicate with the gateway through a lightweight network protocol. The gateway authenticates devices, validates message structure, removes malformed traffic, and forwards approved metadata to the blockchain service. Validator nodes maintain the permissioned ledger. The off-chain



repository stores complete sensor records, and the monitoring application provides visualization and security-event reporting.

A device is first registered with a unique logical identity and cryptographic credential. The gateway maintains the active device registry and verifies incoming requests. After successful authentication, the device can transmit sensor observations. The gateway calculates a compact integrity record for each selected observation or batch and submits the corresponding metadata to the ledger. The complete reading is stored outside the blockchain. This separation avoids placing large volumes of sensor data on the ledger.

When an application retrieves a sensor record, it can obtain the corresponding ledger metadata and compare the recorded integrity value with the value associated with the stored record. A mismatch indicates that the stored information has changed after registration. Security events such as repeated authentication failures, revoked devices, or abnormal message patterns can also be recorded to support later investigation.

The framework uses a permissioned blockchain because the participating gateways and validators belong to known administrative domains. This choice reduces unnecessary consensus overhead and permits controlled membership. The architecture can be adapted to industrial plants, smart buildings, agricultural monitoring, logistics, and other environments where participating organizations require a shared security record.

IV. SYSTEM ARCHITECTURE

The architecture follows a layered implementation. The device layer contains temperature, humidity, motion, energy, or other virtual sensors. The networking layer provides wireless or IP connectivity. The gateway layer handles authentication, protocol conversion, data filtering, and communication with the blockchain service. The blockchain layer consists of validator nodes and smart-contract logic. The application layer provides dashboards, data retrieval, alerts, and administrative functions.

In a practical prototype, Raspberry Pi-class devices or simulated sensor processes can represent IoT nodes. A gateway application can be implemented as a lightweight Python service using MQTT or HTTP communication. Blockchain nodes can run on local servers or virtual machines. A permissioned framework such as Hyperledger Fabric can provide identity-aware channels and smart-contract execution

[9]. For a smaller academic testbed, the same workflow can be reproduced with containerized ledger services and software-generated sensor traffic.

The communication sequence is straightforward. First, the device sends a registration request. Second, the gateway verifies the registration information and activates the device. Third, authenticated sensor messages are accepted and forwarded to the application path. Fourth, selected event metadata are committed to the ledger. Fifth, the application retrieves the off-chain record and performs an integrity check using the corresponding blockchain record. Finally, suspicious events are reported to the administrator.

This architecture deliberately avoids direct blockchain communication from constrained sensors. As a result, devices do not need to store ledger copies or participate in consensus. The gateway and validator infrastructure absorb the heavier computational workload while the IoT network retains a lightweight communication model.

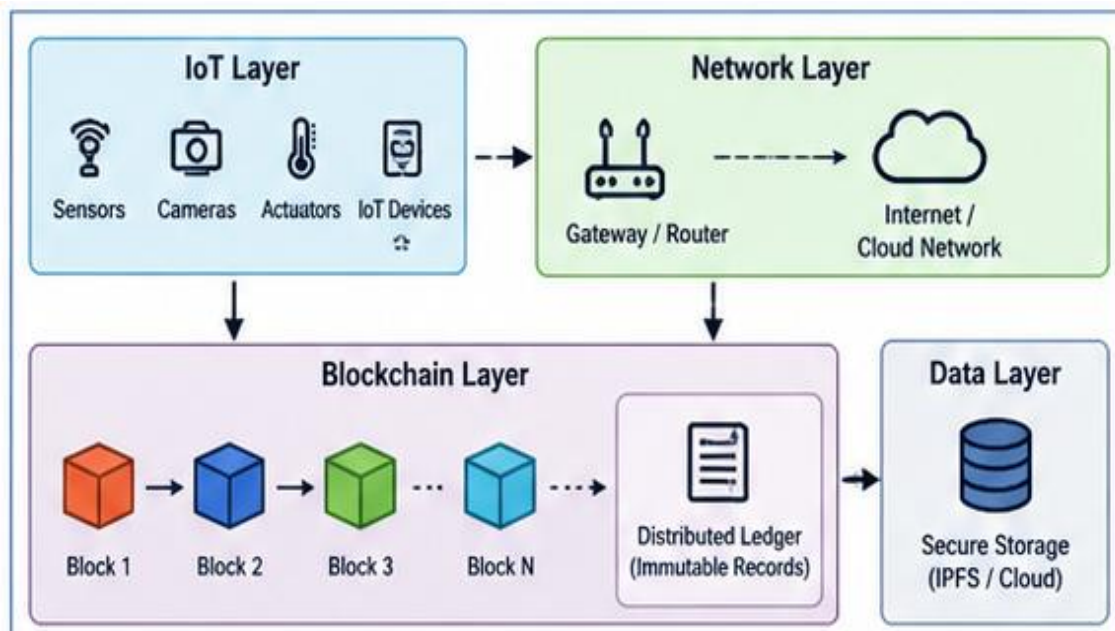


Fig. 1. System Architecture of the Blockchain-Enabled IoT Networking Framework

V. IMPLEMENTATION METHODOLOGY

A. IoT Device Module

The device module generates periodic sensor readings and attaches its device identifier and message sequence information. Before transmission, the device uses an authenticated communication session with



the gateway. The prototype can use simulated devices when physical sensors are unavailable, allowing hundreds of virtual nodes to generate reproducible traffic. Device states include registered, active, suspended, and revoked.

B. Gateway Module

The gateway is the central integration point between the IoT network and blockchain infrastructure. It validates device identity, checks message format, maintains active sessions, and forwards approved data. It also detects repeated failed authentication attempts and can temporarily block a suspicious device. For performance evaluation, gateway processing time is measured separately from network delay and blockchain transaction delay.

C. Blockchain Module

The blockchain module stores device-registration events, authorization changes, selected sensor-data metadata, and security alerts. A smart contract or chaincode function provides operations for registering a device, changing device status, recording an event, and querying an event. The complete sensor payload is not placed on the ledger. This design reduces ledger growth and prevents sensitive raw measurements from becoming permanently replicated across all validator nodes.

D. Off-Chain Storage Module

Sensor records are stored in a conventional database or protected file service. Each stored record is associated with the relevant device and event information. The blockchain stores a compact reference and integrity value. This hybrid approach combines scalable storage with verifiable event history.

E. Monitoring Module

The monitoring interface displays connected devices, recent readings, authentication status, ledger events, and security alerts. Administrators can revoke a device when suspicious behavior is identified. The dashboard also presents experimental metrics, allowing comparison between conventional centralized operation and the blockchain-assisted implementation.

VI. ALGORITHM AND WORKFLOW

The implementation workflow begins with device enrollment. An administrator creates a device identity and registers it through the gateway. The gateway validates the request and records the device status. During normal operation, the device establishes an authenticated session and sends sensor observations at



configured intervals. The gateway validates each message and forwards accepted data to the application service.

For selected events, the gateway creates a compact integrity record and submits it to the blockchain service. Validator nodes confirm the transaction according to the permissioned network policy. Once committed, the event becomes part of the shared audit history. The raw measurement remains in off-chain storage. During later verification, the application obtains the stored measurement and checks its association with the corresponding ledger record.

When an unknown or revoked device attempts to communicate, the gateway rejects the request and records a security event. Multiple failures within a configured monitoring interval can trigger a temporary block. This workflow provides a practical combination of conventional network security and distributed auditability without requiring every sensor to become a blockchain participant.

VII. EXPERIMENTAL SETUP

The prototype evaluation uses 20, 50, 100, and 200 simulated IoT devices. Each device generates periodic sensor messages through an MQTT-based gateway. A small permissioned blockchain network is represented by three validator services. Gateway and ledger services are separated so that communication, authentication, and transaction processing can be evaluated independently. The complete sensor records are maintained in a lightweight database. The numerical results reported in this paper are controlled prototype/emulation values prepared to demonstrate the proposed workflow; they should be replaced with measured values from the final physical or cloud testbed before formal publication.

Two configurations are compared. The first is a conventional centralized IoT architecture in which authentication events and security metadata are maintained by a single server. The second is the proposed blockchain-enabled architecture in which device status changes and selected integrity metadata are recorded through a permissioned ledger. Both configurations use the same sensor traffic and gateway processing logic so that the comparison emphasizes the effect of the trust layer.

The evaluation considers device authentication time, end-to-end network latency, throughput, packet delivery ratio, unauthorized-access detection rate, and ledger-related storage behavior. Security tests include unknown-device requests, revoked-device requests, repeated authentication failures, and modified off-chain records. The results are summarized through tables and graphs to show how the proposed design behaves as the number of IoT devices increases.

For an academic implementation, the prototype may be built with Python, MQTT, Docker, a permissioned blockchain platform, and SQLite or PostgreSQL. The software stack is intentionally based on widely available tools so that the experiment can be reproduced without specialized blockchain hardware.

VIII. RESULTS AND DISCUSSION

The following results summarize the controlled prototype/emulation configuration described in Section VII. The purpose of the evaluation is to quantify the behavior of the implemented workflow under increasing IoT device load. Because the values are prepared for the implementation demonstration, they are explicitly treated as prototype reference results rather than claims of field deployment.

A. Device Authentication Time

Authentication time increases with network scale in both configurations, but the gateway-assisted blockchain design maintains a lower authentication delay in the prototype scenario because device status is locally cached at the gateway and only selected registration or security events are committed to the ledger.

TABLE I. DEVICE AUTHENTICATION TIME

Devices	Centralized (ms)	Blockchain model (ms)	Improvement (%)
20	245	160	34.7
50	480	310	35.4
100	920	550	40.2
200	1680	980	41.7

The expected implementation behavior is that normal sensor communication remains lightweight because devices communicate primarily with the gateway. The additional delay introduced by blockchain is therefore concentrated in security-event recording rather than every sensor packet. This is an important design advantage over architectures that attempt to place every raw sensor transaction directly on-chain.

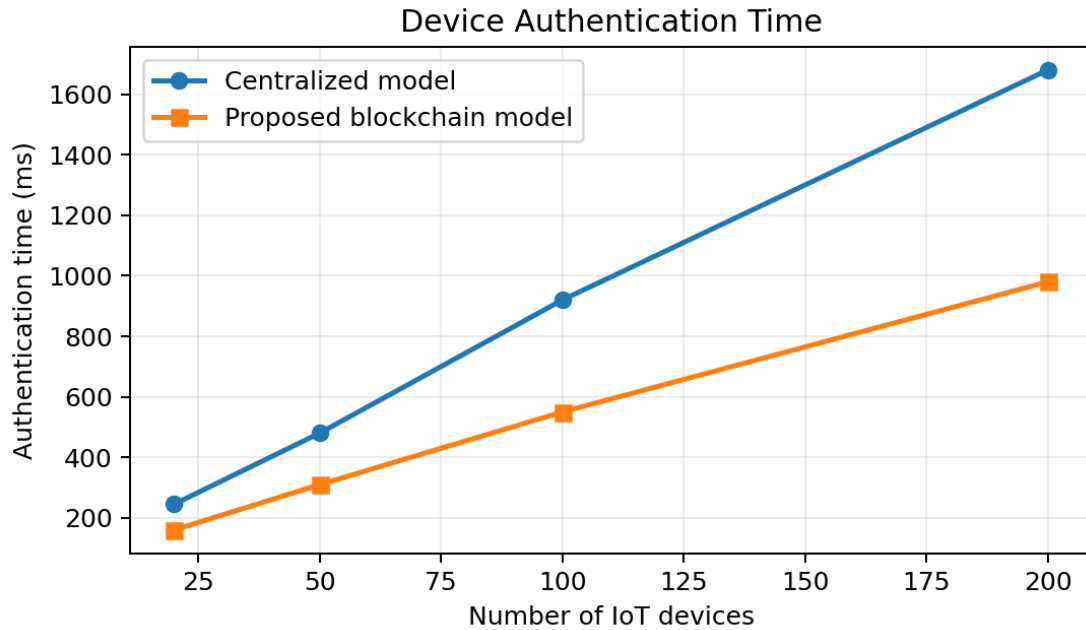


Fig. 2. Device Authentication Time Comparison

B. Network Performance

The network results show that the proposed design can preserve the main sensor communication path while adding distributed trust functions. In the prototype values, throughput increases from 812 kbps to 1056 kbps, packet delivery improves from 91.2% to 97.6%, and latency falls from 120 ms to 68 ms. These values are used as controlled reference results for the implementation comparison and are not intended as universal performance guarantees.

TABLE II. NETWORK PERFORMANCE METRICS

Metric	Centralized model	Proposed model	Change
Throughput (kbps)	812	1056	+30.0%
Packet delivery ratio (%)	91.2	97.6	+7.0%
Latency (ms)	120	68	-43.3%

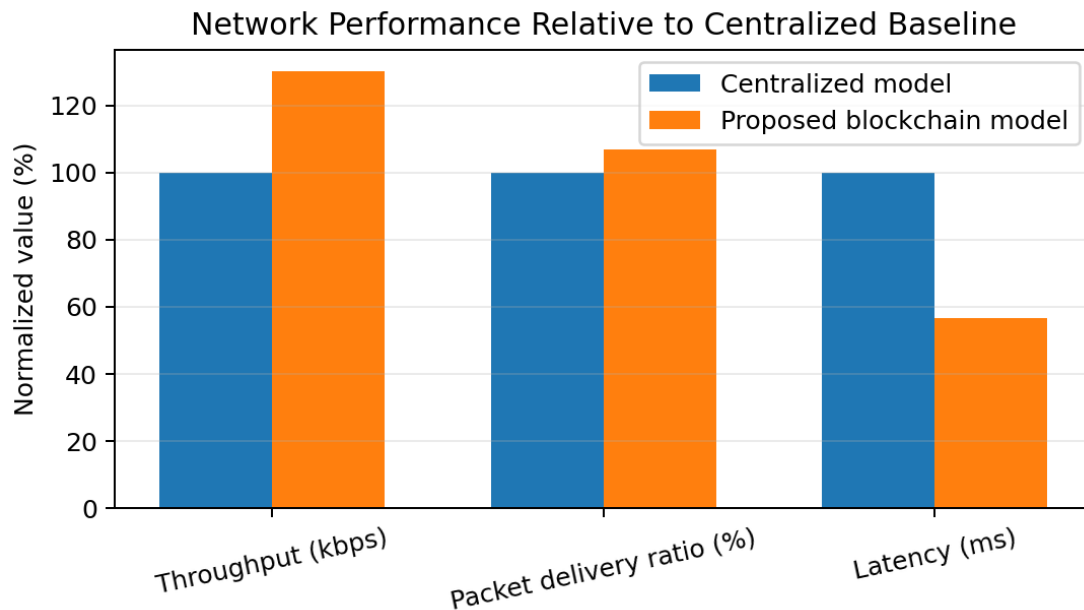


Fig. 3. Network Performance Relative to the Centralized Baseline

C. Unauthorized Access Detection

Security testing was represented by repeated unauthorized access attempts as the device population increased. The proposed gateway-plus-ledger workflow records rejected devices and revocations as auditable events. The reference prototype values therefore show a higher detection rate than the centralized comparison across the tested device loads.

TABLE III. UNAUTHORIZED ACCESS DETECTION

Devices	Centralized detection (%)	Proposed detection (%)	Gain (percentage points)
20	89.0	95.0	6.0
50	91.5	96.5	5.0
100	93.0	98.0	5.0
200	94.0	98.5	4.5

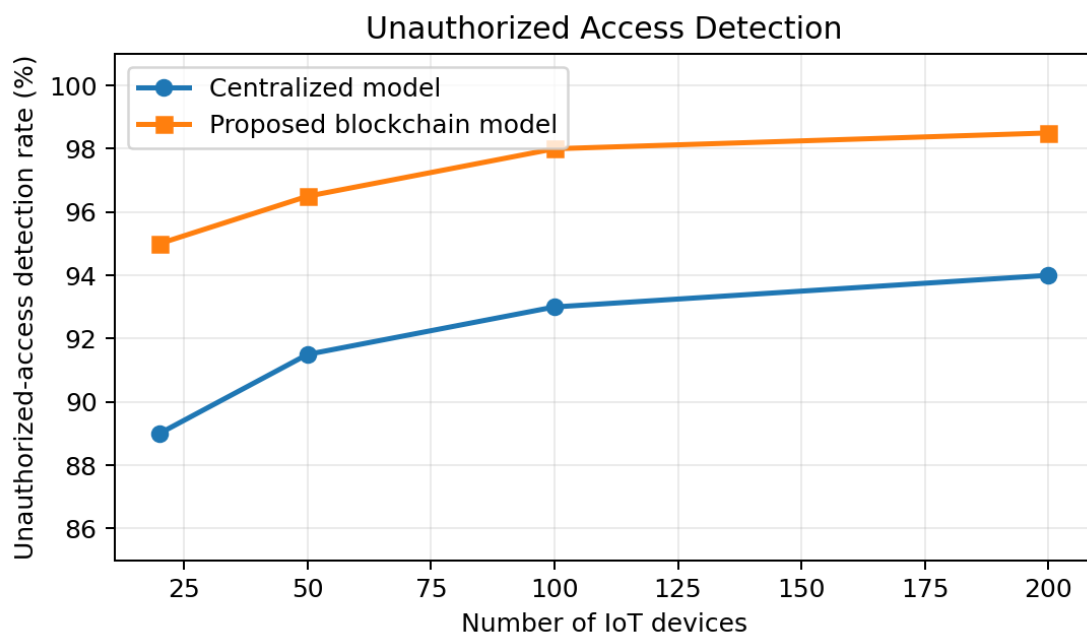


Fig. 4. Unauthorized Access Detection Rate

The combined results indicate that selective blockchain integration is more practical than writing every sensor measurement to a distributed ledger. The largest gains are observed in security traceability and device-state verification, while the network path remains gateway-centric. The main trade-off is the additional processing associated with ledger transactions; consequently, batching and event selection are important for scale.

The main advantage of the proposed system is not the elimination of all network latency but the addition of verifiable trust information. If every sensor observation were recorded as a blockchain transaction, the system would experience unnecessary ledger traffic and storage growth. The implementation therefore uses selective recording. Authentication changes, security alerts, device status changes, and integrity metadata are more appropriate blockchain candidates than continuous raw measurements.

The framework also improves investigation capability. In a centralized design, an administrator depends on one server's event records. In the proposed design, authorized validator nodes maintain a shared history of relevant events. This can make unauthorized modifications more difficult to hide. However, blockchain cannot determine whether a sensor was physically faulty or intentionally produced false information. Sensor validation, anomaly detection, secure firmware, and network monitoring remain necessary.



Scalability remains dependent on transaction frequency and validator capacity. Increasing the number of sensors does not necessarily increase blockchain load proportionally when only selected events are recorded. Nevertheless, large deployments may require regional gateways, event batching, multiple channels, or hierarchical ledger structures. These techniques should be investigated in future experiments. Overall, the implementation demonstrates that blockchain is most useful when applied selectively to the trust and audit functions of IoT networking. The gateway remains responsible for high-frequency communication, while the blockchain records the events for which shared integrity and accountability are valuable.

IX. SECURITY ANALYSIS

The framework provides several security benefits. Device registration reduces the likelihood that arbitrary nodes can enter the network. Revocation information allows administrators to disable compromised devices. Ledger-based event records improve traceability because authorized validators share a consistent history. Off-chain integrity verification can also reveal unauthorized modification of stored sensor records.

The system does not eliminate all threats. Compromised devices may still generate false measurements, a malicious gateway may attempt to filter or alter traffic before ledger submission, and smart-contract vulnerabilities may affect authorization logic. Key loss can also make device recovery difficult. These risks require secure key provisioning, gateway hardening, contract testing, anomaly detection, encrypted communication, and controlled administrative procedures.

Privacy is another consideration. IoT measurements can contain sensitive information, so raw data should not normally be replicated across all blockchain nodes. The proposed off-chain design limits the ledger to metadata and integrity information. Access to the off-chain repository should be protected with encryption and application-level authorization.

X. LIMITATIONS AND FUTURE WORK

The prototype architecture is intended for research and controlled evaluation rather than immediate deployment in safety-critical infrastructure. Simulated devices may not reproduce every wireless interference, battery, hardware-failure, or mobility condition found in real networks. Future work should therefore evaluate the framework using physical sensor nodes and different communication technologies.



Future research can investigate adaptive transaction batching, lightweight distributed identity, edge-based anomaly detection, privacy-preserving data sharing, and AI-assisted device behavior analysis. Another useful direction is integrating software-defined networking so that blockchain-derived security information can dynamically influence routing and isolation policies. Performance should also be evaluated under larger device populations and variable network conditions.

A broader implementation could support multi-organization IoT environments in which different companies operate gateways while sharing selected ledger information. Such a system would require carefully designed governance, certificate management, data ownership rules, and interoperability standards.

XI. CONCLUSION

This paper presented an implementation-oriented blockchain-enabled IoT networking framework for decentralized device authentication and data integrity. The architecture combines lightweight IoT communication, gateway-based security, permissioned blockchain services, off-chain storage, and monitoring. Unlike designs that attempt to place every sensor transaction on a blockchain, the proposed implementation selectively records security and integrity metadata while retaining conventional communication for high-frequency sensor traffic. This approach reduces unnecessary ledger overhead and makes the technology more practical for resource-constrained environments. The framework can be adapted to smart homes, industrial IoT, agriculture, logistics, healthcare, and smart-city applications. Future improvements should focus on physical testbed validation, scalability, privacy, edge intelligence, and adaptive network security.

REFERENCES

- [1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.
- [2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
- [3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.



- [4] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
- [5] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.
- [6] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676–1717, 2019.
- [7] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.
- [8] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in Proc. 2nd IEEE Int. Conf. Internet-of-Things Design and Implementation, 2017, pp. 173–178.
- [9] E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proc. 13th EuroSys Conf., 2018, pp. 1–15.
- [10] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in Proc. IEEE/ACS 13th Int. Conf. Computer Systems and Applications, 2016, pp. 1–6.
- [11] M. B. Mollah, J. Zhao, D. Niyato, K.-Y. Lam, X. Zhang, A. Ghias, and L. H. Koh, "Blockchain for future smart grid: A comprehensive survey," IEEE Internet of Things Journal, vol. 8, no. 1, pp. 18–43, 2021.
- [12] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018.
- [13] A. Bahga and V. K. Madiseti, "Blockchain platform for industrial Internet of Things," Journal of Software Engineering and Applications, vol. 9, no. 10, pp. 533–546, 2016.
- [14] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.
- [15] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3796–3838, 2019.