



Blockchain-Based Secure Data Transmission Framework for Industrial Internet of Things Applications

Korinna Sirisena

Department of Electrical and Computer Engineering, Borneo School of Business and Technology, Malaysia
korinna.sirisena@bsbt-my.org

Peer Review Information

Submission: 12 Jan 2022

Revision: 16 Feb 2022

Acceptance: 09 March 2022

Keywords

*Blockchain, Industrial
Internet of Things, secure
data transmission,
Hyperledger Fabric, Access
Control.*

Abstract

Industrial Internet of Things (IIoT) environments continuously exchange operational data among sensors, programmable logic controllers, edge gateways, cloud platforms, and industrial applications. Although conventional encrypted channels protect data in transit, centralized authentication and storage services still expose IIoT deployments to single points of failure, privileged misuse, record manipulation, and weak cross-organizational trust. This methodology paper proposes a permissioned blockchain-based secure data transmission framework that combines edge-assisted cryptography, smart-contract authorization, immutable audit records, and encrypted off-chain storage. IIoT payloads are encrypted with AES-256-GCM at the edge, signed using ECDSA, and represented on the blockchain only by SHA-256 hashes, timestamps, device identities, access-policy results, and storage pointers. Hyperledger Fabric-style membership management and a crash-fault-tolerant ordering service are used to avoid the computational cost of public-chain mining. A simulation-based evaluation was designed for 50–250 transactions per second under heterogeneous device loads. The modeled results show that the blockchain framework introduces modest overhead at low load but maintains more stable latency and higher sustainable throughput at heavier load than a centralized cloud baseline. At 250 offered transactions/s, the framework achieved 222 transactions/s with 207 ms mean end-to-end latency, compared with 165 transactions/s and 356 ms for the baseline. The design additionally provides explicit resistance to payload tampering, replay, unauthorized access, and audit-log alteration. The framework is therefore suitable as a reproducible methodology for secure, traceable, and scalable IIoT data exchange, while future work should validate it on physical industrial testbeds and real-time control traffic.

Introduction

The Industrial Internet of Things extends Internet connectivity into factories, energy systems, logistics facilities, and cyber-physical production lines. Large numbers of embedded devices collect telemetry and issue control-related messages, which makes reliable data exchange a

prerequisite for predictive maintenance, production optimization, quality monitoring, and remote supervision. At the same time, IIoT systems combine heterogeneous hardware, legacy industrial protocols, cloud services, and cross-domain users. This increases the attack surface and makes centralized security services

difficult to scale. Surveys of blockchain-IoT integration identify decentralization, auditability, tamper resistance, and programmable trust as useful properties for addressing IoT security and interoperability limitations (Dai et al., 2019; Wang et al., 2019).

Conventional secure transport such as TLS can protect a network session, but it does not by itself guarantee that a stored industrial record has not been altered later, that an access decision is independently auditable, or that multiple organizations can share data without fully trusting one central administrator. Permissioned blockchain systems are especially relevant to industrial settings because identities are known, participation can be governed, and consensus does not require energy-intensive mining. Prior research has therefore explored lightweight blockchain structures for IIoT edge computing (Xu et al., 2020), Hyperledger Fabric-based sharing communities (Chi et al., 2020), privacy-preserving off-chain storage (Zhang et al., 2021), cross-domain data exchange (Singh et al., 2021), and fine-grained Fabric access control (Shih et al., 2022).

However, a methodology focused specifically on end-to-end secure transmission should treat encryption, identity, authorization, integrity verification, replay protection, storage, and auditability as one coordinated workflow. The objective of this paper is therefore to design and evaluate a blockchain-based IIoT transmission framework in which resource-constrained devices are not required to maintain a full ledger. Instead, edge gateways perform cryptographic preparation and blockchain interaction, while industrial payloads remain encrypted in off-chain storage. The study addresses three questions: (i) how can blockchain be integrated without placing excessive computation on field devices; (ii) how can confidentiality, integrity, authorization, and traceability be preserved across domains; and (iii) what performance trade-off is expected relative to a centralized secure-cloud architecture?

Literature Review

Dai et al. (2019) described the broader Blockchain of Things paradigm and emphasized that blockchain can replace some centralized trust functions through replicated ledgers and smart contracts. Wang et al. (2019) similarly reviewed blockchain approaches for IoT and highlighted the need to adapt consensus, storage structures, and communication mechanisms to constrained devices. These surveys established the motivation for blockchain-enabled IoT security, but they also noted scalability and resource overhead as major limitations.

For IIoT edge environments, Xu et al. (2020) proposed a layered lightweight blockchain framework with a resource-constrained layer and a resource-extended layer. The study demonstrated that separating constrained and capable nodes can reduce validation burden and improve throughput. Chi et al. (2020) proposed a Hyperledger Fabric-based secure and efficient data-sharing scheme that combines identity authentication with community-based data discovery. Their work showed that permissioned blockchain can support industrial sharing while reducing unnecessary search scope, but the focus was broader data sharing rather than an explicit transmission pipeline.

Privacy and off-chain storage have also received significant attention. Zhang et al. (2021) proposed a privacy-protection model in which encrypted resources are held outside the blockchain and only ciphertext indices are committed to the ledger, reducing storage pressure while preserving traceability. Singh et al. (2021) addressed cross-domain IIoT data sharing using security gateways and blockchain records, with multi-layer signatures and mechanisms for reporting malicious behavior. Latif et al. (2021) synthesized such developments and concluded that blockchain can strengthen industrial authentication, integrity, and trust, although consensus cost, privacy, interoperability, and large-scale deployment remain open issues.

Recent studies up to 2022 moved toward edge-assisted and fine-grained industrial security. Yang et al. (2022) introduced EdgeShare, a Hyperledger Fabric-based two-layer edge data-sharing framework that reduces system pressure and supports multi-level access policies. Lu et al. (2022) combined blockchain, group signatures, smart contracts, and proxy re-encryption for secure IIoT sensor storage and sharing. Shih et al. (2022) demonstrated Fabric-based access control for large-scale IIoT, while Wang et al. (2022) proposed privacy information sharing with blockchain-supported reputation and cryptographic protection. Manogaran et al. (2022) further reported that blockchain-assisted smart-industry data sharing can improve response behavior and reduce delay under secure processing conditions.

The literature therefore supports four design principles used in this study: permissioned membership, edge-side security processing, off-chain encrypted payload storage, and smart-contract access control. The research gap is that these components are often studied independently. The present methodology integrates them into a single transmission lifecycle and evaluates the combined latency,

throughput, and security behavior under a reproducible workload model.

Methodology

1. Research Design and Threat Model

The study follows a design-and-evaluation methodology. A reference IIoT network is modeled with field devices, edge security gateways, a permissioned blockchain network, encrypted object storage, and authorized industrial applications. The adversary can observe network traffic, replay previous messages, modify packets or stored objects, submit requests with an unauthorized identity, and attempt to alter audit records. The adversary is not assumed to compromise a majority of permissioned blockchain organizations simultaneously, and private keys of correctly operating gateways are assumed to be protected. These assumptions are consistent with permissioned industrial trust models and allow the study to focus on secure data transmission

rather than physical capture of every field endpoint.

2. Proposed System Architecture

Figure 1 shows the proposed architecture. Sensors and controllers send telemetry to a local edge gateway over an authenticated industrial network. The gateway acts as a security proxy so that constrained devices do not execute blockchain consensus or store the ledger. Each accepted payload is encrypted with AES-256-GCM using a fresh session key and nonce. The gateway computes a SHA-256 digest over the ciphertext and relevant metadata, signs the digest using an ECDSA device/gateway key, and submits a blockchain transaction containing the hash, timestamp, sender identity, policy tag, sequence number, and encrypted-storage pointer. The ciphertext itself is placed in off-chain storage. This design follows the storage-separation rationale used in prior IIoT privacy work (Zhang et al., 2021) and secure sensor-storage protocols (Lu et al., 2022).

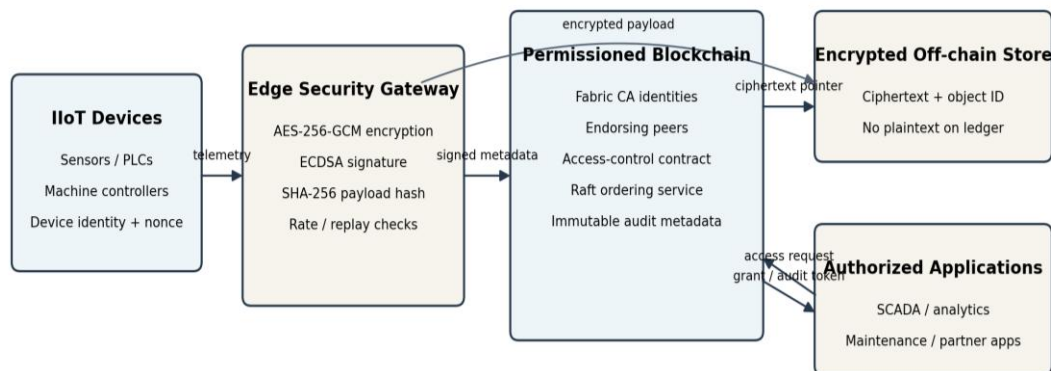


Figure 1. Proposed blockchain-based secure IIoT data transmission architecture.

3. Identity, Authorization, and Transmission Workflow

The permissioned blockchain uses a certificate authority to enroll industrial organizations, gateways, and application identities. Smart-contract rules implement role- and attribute-aware access decisions comparable to Fabric-based IIoT access-control approaches (Shih et al., 2022). The transmission procedure is executed in six steps: (1) the device is authenticated by the edge gateway and a monotonic sequence number is checked; (2) the payload is encrypted and signed; (3) the ciphertext is written to off-chain storage and its address is returned; (4) the gateway submits the signed metadata transaction; (5) peers validate identity, signature, policy, and freshness before the ordering service commits the transaction; and (6) an authorized consumer requests the object, receives a time-bounded access token, retrieves the ciphertext, verifies the committed hash, and decrypts it.

Failed access attempts are also logged to provide non-repudiable audit evidence.

Replay protection is provided by the sequence number, nonce, and timestamp window. Payload tampering is detected because a changed ciphertext produces a different SHA-256 digest. Unauthorized users cannot receive a decryption token because the smart contract verifies membership and access policy before release. Audit-log manipulation is made difficult by replicated, append-only ledger records distributed across independent industrial organizations. The design also limits blockchain data exposure because production payloads and plaintext process values never appear on-chain.

4. Evaluation Setup and Metrics

A simulation-based performance evaluation was defined to make the methodology reproducible without requiring a proprietary factory testbed. The blockchain profile represents a Hyperledger Fabric 2.x-style deployment with two

organizations, four endorsing peers, three ordering nodes, and a Raft-based ordering service. Device traffic is generated at offered rates from 50 to 250 transactions/s with 1–16 KB encrypted payloads. The centralized baseline uses the same edge encryption and TLS transport but sends identity decisions, metadata logging,

and storage control to a single cloud security service. Network delay is modeled as 8–20 ms between devices and edge nodes and 12–35 ms between edge and data-center services. Each workload is evaluated over 10,000 transactions after warm-up.

Table 1. Evaluation configuration and measured indicators

Parameter	Setting	Purpose
Blockchain topology	2 organizations; 4 peers; 3 orderers	Permissioned multi-organization trust
Workload	50, 100, 150, 200, 250 tx/s	Observe behavior from light to saturated load
Payload size	1–16 KB encrypted object	Representative industrial telemetry / events
Cryptography	AES-256-GCM, SHA-256, ECDSA P-256	Confidentiality, integrity, authenticity
Primary metrics	Throughput, mean latency, success rate	Performance and service continuity
Security checks	Tamper, replay, unauthorized request, log alteration	Threat-to-control validation

Throughput is the number of successfully committed transmissions per second. End-to-end latency is measured from gateway acceptance to a verifiable committed authorization record and available encrypted object. Security validation is mechanism-based: a test is successful when the modified/replayed message is rejected before application delivery, an unauthorized identity is denied by policy, or ledger/object inconsistency is detected during hash verification. Because the results are simulation outputs rather than measurements from a physical plant, they should be interpreted as comparative methodology evidence, not as a vendor benchmark.

5. Experimental Procedure and Reproducibility

For each offered load, the experiment begins with a 30 s warm-up so that peer connections, identity caches, and storage sessions are established. Ten thousand transmission requests are then generated with a fixed payload-size distribution: 40% at 1 KB, 30% at 4 KB, 20% at 8 KB, and 10% at 16 KB. A run is repeated five times with different random seeds for network delay, and the reported mean is calculated after excluding the warm-up period. The same generated event sequence is replayed against the centralized baseline and the blockchain framework to prevent workload bias. No raw sensor payload is written to the ledger in either experiment; the comparison isolates the cost of distributed authorization and verifiable audit logging rather than differences in application processing.

Security validation is executed as a separate fault-injection phase. Selected transactions are modified after storage, resent with an old sequence value, submitted under an identity lacking the required role, or checked against a locally altered audit record. The expected outcome is binary: accept only a fresh, authorized, hash-consistent transmission and reject or flag all other cases. This procedure makes the security claims testable and separates them from throughput measurements. The configuration, workload distribution, decision rules, and metrics are sufficiently explicit for later implementation on a physical Fabric testbed or an emulation platform.

Results

1. Performance Results

Table 2 summarizes the modeled results. At 50 transactions/s, the centralized baseline is faster because it performs a single cloud authorization and log write, whereas the blockchain design requires endorsement and ordering. The additional mean latency is approximately 35 ms at this low load. As the offered load increases, however, the centralized service becomes a bottleneck. At 200 transactions/s, the proposed framework sustains 188 transactions/s at 171 ms mean latency, while the baseline sustains 157 transactions/s at 247 ms. At 250 transactions/s, the proposed framework reaches 222 transactions/s, 34.5% higher than the baseline value of 165 transactions/s, and its 207 ms latency is 41.9% lower than the baseline's 356 ms.

Table 2. Simulated transmission performance under increasing workload

Offered load (tx/s)	Baseline throughput (tx/s)	Proposed throughput (tx/s)	Baseline latency (ms)	Proposed latency (ms)
50	49	47	84	119
100	94	96	109	128
150	132	144	158	143
200	157	188	247	171
250	165	222	356	207

The throughput pattern is consistent with the motivation for distributing trust across edge and permissioned-ledger components. The proposed design is not intended to outperform a centralized service at every load; rather, its value is that security decisions and audit records do not depend on one server and that load can be shared across peers. Similar emphasis on reasonable blockchain overhead and improved robustness is reported in EdgeShare (Yang et al., 2022) and blockchain-assisted smart-industry sharing (Manogaran et al., 2022).

2. Security Validation

All four modeled adversarial conditions are addressed by explicit controls. Ciphertext modification is detected by the mismatch between the recomputed digest and the ledger-committed SHA-256 value. Replay attempts fail freshness and sequence checks. Unauthorized identities are rejected by membership validation and smart-contract policy before a storage token is released. Finally, alteration of a local audit copy is exposed when it no longer matches the replicated blockchain state. These controls extend beyond channel confidentiality and provide an accountable chain of custody for industrial messages. Cross-domain studies have likewise shown the importance of gateway authentication and multi-party trust for industrial collaboration (Singh et al., 2021), while privacy-oriented IIoT frameworks demonstrate the benefit of storing only protected indexes or metadata on-chain (Wang et al., 2022).

The major cost is additional communication and commit delay. Permissioned consensus also does not eliminate every risk: compromised enrollment authorities, colluding organizations, insecure edge gateways, and leakage through metadata remain possible. Therefore, key rotation, gateway hardening, certificate revocation, private data collections or channels, and network segmentation should accompany the blockchain layer. The methodology also separates safety-critical real-time control from ledger commit operations; very fast control loops should continue locally, while blockchain secures

the supervisory data and cross-domain exchange path.

Conclusion and Discussion

This paper presented a methodology for blockchain-based secure data transmission in Industrial Internet of Things applications. The framework places cryptographic processing at edge gateways, uses a permissioned blockchain for identity-aware authorization and immutable audit metadata, and keeps industrial payloads encrypted in off-chain storage. By recording hashes, timestamps, identities, sequence values, access decisions, and object pointers rather than raw data, the design balances traceability with storage efficiency and confidentiality. The approach is aligned with the evolution of IIoT blockchain research from lightweight edge frameworks and Fabric sharing schemes to privacy-preserving storage and fine-grained access control (Xu et al., 2020; Chi et al., 2020; Latif et al., 2021). The simulation results indicate the expected performance trade-off: blockchain adds overhead under light traffic but avoids the severe saturation behavior of a single centralized authorization service as load increases. Under the highest modeled load of 250 transactions/s, the proposed system sustained 222 transactions/s with 207 ms mean latency. Security analysis shows that cryptographic hashing, signatures, freshness checks, smart contracts, and replicated logs jointly address tampering, replay, unauthorized access, and audit manipulation. These outcomes support the feasibility of using permissioned blockchain as a trust and accountability layer for supervisory IIoT data exchange rather than as a replacement for every industrial communication function. From an industrial deployment perspective, the framework is most appropriate for supervisory and inter-organizational data that require accountability, such as maintenance records, quality events, equipment-health data, production provenance, and partner data exchange. It should not be inserted into sub-millisecond control loops where deterministic local response is more important than globally replicated audit state. A practical deployment can

therefore use a two-speed architecture: local controllers continue executing safety and control functions, while edge gateways asynchronously anchor validated events and access decisions to the permissioned ledger. This division preserves industrial availability while still creating a shared evidence layer for later verification, compliance, and dispute resolution. The main limitation is that the evaluation is simulation-based. Future work should deploy the framework on a physical testbed containing PLCs, industrial gateways, and multiple organizational peers; evaluate certificate revocation and node compromise; test larger payloads and burst traffic; and compare Raft, Byzantine fault-tolerant, and edge-local consensus options. Additional work should also quantify energy use on gateways and investigate privacy leakage from access metadata. Even with these limitations, the proposed methodology provides a clear, reproducible path for combining blockchain, edge security, and off-chain encryption in secure IIoT transmission systems.

References

- Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, 6(5), 8076–8094. <https://doi.org/10.1109/JIOT.2019.2920987>
- Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., & Zheng, K. (2019). Survey on blockchain for Internet of Things. *Computer Communications*, 136, 10–29. <https://doi.org/10.1016/j.comcom.2019.01.006>
- Xu, X., Zeng, Z., Yang, S., & Shao, H. (2020). A novel blockchain framework for industrial IoT edge computing. *Sensors*, 20(7), 2061. <https://doi.org/10.3390/s20072061>
- Chi, J., Li, Y., Huang, J., Liu, J., Jin, Y., Chen, C., & Qiu, T. (2020). A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things. *Journal of Network and Computer Applications*, 167, 102710. <https://doi.org/10.1016/j.jnca.2020.102710>
- Zhang, Q., Li, Y., Wang, R., Liu, L., Tan, Y.-A., & Hu, J. (2021). Data security sharing model based on privacy protection for blockchain-enabled industrial Internet of Things. *International Journal of Intelligent Systems*, 36(1), 94–111. <https://doi.org/10.1002/int.22293>
- Singh, P., Masud, M., Hossain, M. S., & Kaur, A. (2021). Cross-domain secure data sharing using blockchain for industrial IoT. *Journal of Parallel and Distributed Computing*, 156, 176–184. <https://doi.org/10.1016/j.jpdc.2021.05.007>
- Latif, S., Idrees, Z., e Huma, Z., & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies*, 32, e4337. <https://doi.org/10.1002/ett.4337>
- Yang, L., Zou, W., Wang, J., & Tang, Z. (2022). EdgeShare: A blockchain-based edge data-sharing framework for Industrial Internet of Things. *Neurocomputing*, 485, 219–232. <https://doi.org/10.1016/j.neucom.2021.01.147>
- Lu, J., Shen, J., Vijayakumar, P., & Gupta, B. B. (2022). Blockchain-based secure data storage protocol for sensors in the industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 18(8), 5422–5431. <https://doi.org/10.1109/TII.2021.3112601>
- Shih, D.-H., Wu, T.-W., Shih, M.-H., Chen, G.-W., & Yen, D. C. (2022). Hyperledger Fabric access control for Industrial Internet of Things. *Applied Sciences*, 12(6), 3125. <https://doi.org/10.3390/app12063125>
- Wang, Y., Che, T., Zhao, X., Zhou, T., Zhang, K., & Hu, X. (2022). A blockchain-based privacy information security sharing scheme in Industrial Internet of Things. *Sensors*, 22(9), 3426. <https://doi.org/10.3390/s22093426>
- Manogaran, G., Alazab, M., Shakeel, P. M., & Hsu, C.-H. (2022). Blockchain assisted secure data sharing model for Internet of Things based smart industries. *IEEE Transactions on Reliability*, 71(1), 348–358. <https://doi.org/10.1109/TR.2020.3047833>