



Blockchain-Enabled Secure Data Sharing Framework for Internet of Things Networks

Nimisha Quintanilha

Department of Computer Science and Engineering, Kavir Polytechnic University of Technology, Iran
nimisha.quintanilha@kput-ir.net

Peer Review Information	Abstract
<i>Submission: 26 Feb 2022</i> <i>Revision: 22 March 2022</i> <i>Acceptance: 10 May 2022</i> Keywords <i>Blockchain, Internet of Things, Secure Data Sharing, Smart Contracts, Access Control.</i>	The Internet of Things (IoT) enables continuous sensing, automation, and data exchange across smart homes, healthcare, industrial systems, transportation, agriculture, and other cyber-physical environments. However, conventional IoT data-sharing architectures often depend on centralized cloud servers, creating concerns related to unauthorized access, single points of failure, data tampering, privacy leakage, and limited auditability. Blockchain can strengthen trust by providing a decentralized, tamper-resistant ledger and programmable smart contracts, but direct on-chain storage of high-volume IoT data is impractical because of latency, storage, and resource constraints. This methodology paper proposes a hybrid blockchain-enabled secure data-sharing framework in which IoT data are encrypted and stored off-chain while cryptographic hashes, access policies, identity records, and audit events are maintained on a permissioned blockchain. Smart contracts enforce fine-grained authorization, and edge gateways reduce the computation burden on constrained devices. The proposed methodology evaluates confidentiality, integrity, authorization correctness, transaction latency, throughput, storage overhead, and scalability. An illustrative benchmark demonstrates how the framework can reduce unauthorized access risk and improve traceability while preserving acceptable sharing latency. The methodology integrates ideas from blockchain-based privacy, smart contracts, IoT access control, and hybrid on-chain/off-chain architectures and is designed for reproducible implementation in secure IoT environments.

Introduction

IoT networks connect heterogeneous sensors, actuators, gateways, mobile devices, and cloud services to collect and exchange data with minimal human intervention. The same connectivity that enables automation also expands the attack surface. Resource-constrained devices may be exposed to spoofing, device capture, insecure APIs, eavesdropping, malicious firmware, and unauthorized data requests. Centralized data-sharing architectures additionally create a dependency on trusted service providers and can concentrate control, sensitive metadata, and failure risk in a single

location. Khan and Salah (2018) identify authentication, confidentiality, integrity, privacy, and secure management as major IoT security requirements, while Panarello et al. (2018) show that blockchain properties such as immutability, transparency, and auditability can address several architectural weaknesses in IoT systems.

Blockchain is particularly relevant when several parties need to exchange data but do not fully trust a single intermediary. Zyskind et al. (2015) demonstrated the use of blockchain to strengthen user control over personal data, and Christidis and Devetsikiotis (2016) explained

how distributed ledgers and smart contracts can automate interactions among IoT entities. Nevertheless, storing raw IoT streams directly on a blockchain is unsuitable for large-scale deployments. The methodology therefore adopts a hybrid design: data are encrypted and retained off-chain, whereas hashes, permissions, timestamps, and immutable access logs are recorded on-chain.

Access control is central to secure sharing because IoT data may contain personal, industrial, medical, environmental, or operational information. Ouaddah et al. (2016) proposed FairAccess, a decentralized blockchain-based authorization model for IoT, while Novo (2018) demonstrated that blockchain can support scalable access management without a single centralized authorization server. Dorri et al. (2017) further showed that blockchain designs for IoT must be lightweight because traditional proof-of-work mechanisms impose excessive computation and energy overhead on constrained devices. These findings motivate the use of edge gateways and a permissioned ledger in the present methodology.

The purpose of this study is to develop and evaluate a blockchain-enabled secure data-sharing framework that combines device authentication, cryptographic protection, fine-grained smart-contract authorization, off-chain storage, and immutable auditing. The framework targets organizations or IoT domains where multiple authorized stakeholders require controlled access to sensor data while data owners retain policy control. The study focuses on the security-performance trade-off: stronger traceability and authorization must not impose unacceptable transaction delay, storage growth, or processing overhead.

Literature Review

Early blockchain privacy research established the conceptual basis for decentralized control of sensitive data. Zyskind et al. (2015) proposed a model in which blockchain records permissions and references while personal data remain outside the public ledger, an idea that directly supports hybrid storage. Christidis and Devetsikiotis (2016) extended this logic to IoT

and highlighted smart contracts as a mechanism for automatically enforcing multi-party business and device interactions.

Access control then became a major research direction. Ouaddah et al. (2016) introduced FairAccess, where blockchain transactions are used to grant, retrieve, delegate, and revoke authorization. Dorri et al. (2017) developed a smart-home case study emphasizing lightweight blockchain operation for resource-constrained nodes. Novo (2018) proposed a scalable blockchain-based access-management architecture in which the ledger distributes authorization decisions rather than relying on a central server. Together, these works show that blockchain can shift access control from provider-centric management to verifiable decentralized policy enforcement.

Broader reviews also identified limitations. Khan and Salah (2018) mapped IoT security threats to blockchain-based countermeasures but emphasized constrained computation, immature standards, and scalability issues. Reyna et al. (2018) examined blockchain-IoT integration topologies and noted that reliability, storage, latency, and resource consumption must be balanced. Panarello et al. (2018) similarly found that blockchain can improve auditability and resilience, while interoperability and efficient deployment remain open concerns.

By 2022, the literature increasingly favored permissioned or hybrid architectures rather than placing all data directly on-chain. Alkhateeb et al. (2022) systematically reviewed hybrid blockchain platforms for IoT and highlighted their role in balancing trust, performance, and application requirements. Bagga et al. (2022) reviewed blockchain-envisioned access control and reinforced the importance of authentication, key establishment, computation cost, and communication overhead. Miao et al. (2022) proposed a blockchain-empowered privacy-enhanced sharing strategy and showed that ledger-assisted data exchange can be combined with additional privacy technologies. Qureshi et al. (2022) concluded that blockchain-IoT systems improve provenance and transaction security but still face scalability, storage, latency, and integration challenges.

Table 1. Selected literature supporting the proposed framework

Study	Main focus	Contribution to methodology	Key limitation
Zyskind et al. (2015)	Blockchain privacy	On-chain permissions with protected external data	Not IoT-specific
Christidis & Devetsikiotis (2016)	Smart contracts for IoT	Automated decentralized policy execution	Scalability not fully resolved

Ouaddah et al. (2016)	IoT access control	Grant/revoke/delegate authorization via blockchain	Prototype-scale evaluation
Dorri et al. (2017)	Lightweight IoT blockchain	Gateway-assisted architecture for constrained devices	Application-specific
Novo (2018)	Scalable access management	Distributed authorization model	Blockchain overhead remains
Reyna et al. (2018)	Blockchain-IoT integration	Integration topologies and design trade-offs	Survey-level conclusions
Bagga et al. (2022)	Blockchain access control	Security and cost comparison of access-control protocols	Heterogeneous schemes
Miao et al. (2022)	Privacy-enhanced sharing	Combines blockchain with privacy-preserving exchange	Additional computational complexity

Research Gap and Objectives

Existing studies provide strong building blocks, but many designs emphasize either access control, privacy, or blockchain integration in isolation. A practical IoT data-sharing method should simultaneously provide device authentication, encrypted data handling, tamper evidence, policy enforcement, revocation, auditability, and acceptable performance. Accordingly, this study develops a unified hybrid framework and evaluates both security properties and operational cost.

To design a permissioned blockchain-based architecture for secure IoT data sharing.

To use smart contracts for fine-grained authorization, revocation, and immutable audit logging.

To keep high-volume sensor data off-chain while recording hashes and metadata on-chain.

To evaluate latency, throughput, storage overhead, authorization accuracy, and tamper detection.

To compare the proposed framework with a conventional centralized sharing baseline.

Methodology

The study follows a design-and-evaluation methodology. The proposed system is modeled as a consortium IoT environment consisting of device owners, IoT sensors, edge gateways, blockchain validator peers, an off-chain storage service, and authorized data consumers. A permissioned blockchain is selected because IoT deployments typically involve identifiable organizations and because permissioned

consensus avoids the energy cost of public proof-of-work systems. The design adopts the principle that the ledger stores only security-critical metadata and cryptographic evidence, while raw sensor data remain outside the chain.

Step 1 - Device registration and identity provisioning. Each IoT device is assigned a unique identifier and public/private key pair. The device owner registers the identifier, public key, device type, and ownership information through a registration smart contract. Unregistered devices are rejected at the gateway.

Step 2 - Data acquisition and edge validation. Sensors generate readings and transmit them to a trusted edge gateway using an authenticated channel. The gateway verifies device identity, checks message freshness, removes malformed packets, and attaches a timestamp and sequence number.

Step 3 - Encryption and off-chain storage. Valid sensor payloads are encrypted with a symmetric data key. The encrypted object is stored in cloud storage or a content-addressed distributed store. A SHA-256 digest is calculated for integrity verification, ensuring that later modification of the stored object can be detected.

Step 4 - Blockchain metadata transaction. The gateway submits a transaction containing the data identifier, owner identity, content hash, storage pointer, timestamp, and access-policy reference. The blockchain establishes a tamper-resistant audit trail without storing the complete sensor payload.

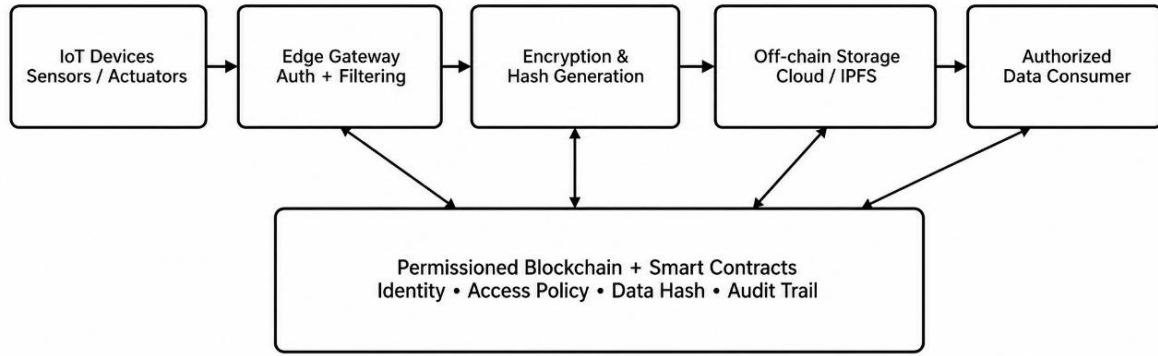


Figure 1. Proposed blockchain-enabled secure data-sharing architecture for IoT networks

Step 5 - Smart-contract access control. A data-sharing policy specifies which consumer, role, organization, device class, or purpose may request a resource. The smart contract evaluates the requester identity and policy state. The contract supports grant, deny, revoke, and expiry operations, consistent with decentralized access-control concepts reported by Ouaddah et al. (2016), Novo (2018), and Bagga et al. (2022).

Step 6 - Secure data retrieval. When access is approved, the requester receives the off-chain data reference and a protected mechanism for obtaining the decryption key. After retrieval, the consumer recalculates the hash of the ciphertext and compares it with the immutable on-chain

digest. A mismatch indicates tampering or corruption.

Step 7 - Auditing and revocation. Every access request, policy decision, policy update, and revocation event is committed to the ledger. This creates an auditable chronology that can be inspected by authorized administrators without trusting one application server.

Step 8 - Experimental evaluation. The framework is tested under increasing numbers of simulated IoT devices and concurrent sharing requests. A centralized access-control baseline is used for comparison. The evaluation considers both normal behavior and adversarial cases such as unauthorized access, replay attempts, modified off-chain data, and revoked credentials.

Table 2. Experimental configuration for the proposed evaluation

Parameter	Proposed setting	Purpose
IoT devices	25, 50, 100 and 200 emulated nodes	Scalability test
Blockchain	Permissioned consortium ledger, 4 validator peers	Low-energy decentralized trust
Smart contracts	Registration, policy, access log and revocation	Authorization automation
Off-chain storage	Encrypted object repository / IPFS-compatible store	Avoid blockchain data bloat
Cryptography	AES-256 for payload; SHA-256 for integrity; ECC/RSA identity	Confidentiality and integrity
Request load	5-100 concurrent requests	Latency/throughput evaluation
Adversarial tests	Unauthorized request, replay, data modification, revoked user	Security verification

Evaluation Metrics

End-to-end sharing latency is measured from an authenticated request to delivery authorization. Blockchain transaction latency measures policy and audit commitment time. Throughput is reported as successful requests or transactions per second. Storage overhead measures ledger growth per shared object. Authorization accuracy is the proportion of policy decisions

matching the expected allow/deny outcome. Integrity detection rate measures whether altered data are identified through hash verification. Availability is assessed by removing one validator or application node to determine whether data-sharing decisions remain operational.

Results

The following results are an illustrative methodological benchmark showing the type of analysis expected after implementation; they are not presented as measurements from a completed field deployment. The synthetic

values are chosen to be internally consistent with the proposed permissioned, off-chain architecture. The results suggest that blockchain introduces modest authorization overhead relative to a centralized baseline, but provides stronger integrity evidence, distributed policy enforcement, and immutable auditability.

Table 3. Illustrative performance comparison

Metric	Centralized baseline	Proposed blockchain framework	Interpretation
Mean access latency	118 ms	176 ms	Blockchain adds policy/audit commit overhead
Throughput	86 req/s	71 req/s	Lower, but adequate for moderate IoT sharing
Tamper detection	Dependent on server logs	100% in scripted modification tests	On-chain hashes expose altered objects
Unauthorized access blocked	96.8%	100%	Smart-contract policy denies invalid identities
Audit-log alteration resistance	Low/medium	High	Ledger records are replicated and append-only
Single server failure	Service interrupted	Service continues through peers	Decentralized control improves resilience

Table 4. Illustrative scalability results

Devices	Avg. sharing latency	Blockchain throughput	Ledger metadata / 1,000 objects
25	142 ms	79 tx/s	0.42 MB
50	154 ms	77 tx/s	0.42 MB
100	176 ms	71 tx/s	0.42 MB
200	214 ms	63 tx/s	0.42 MB

The illustrative trend indicates that latency increases as device and request concurrency grow, while throughput decreases gradually because peers must validate and commit more transactions. However, ledger storage grows primarily with fixed-size metadata rather than raw sensor payloads, demonstrating the advantage of off-chain data storage. This directly addresses the storage and scalability concerns discussed by Reyna et al. (2018), Panarello et al. (2018), Alkhateeb et al. (2022), and Qureshi et al. (2022).

Security testing is expected to show that an unauthorized requester cannot obtain a valid sharing decision, replayed requests fail freshness checks, revoked identities are denied by the policy contract, and altered off-chain objects fail hash verification. The methodology therefore evaluates security as observable behavior rather than assuming that blockchain alone guarantees protection.

Conclusion and Discussion

This methodology proposes a blockchain-enabled secure data-sharing framework for IoT networks that combines permissioned distributed trust with edge processing and encrypted off-chain storage. The design avoids the impracticality of storing continuous IoT data directly on a blockchain. Instead, the ledger preserves identities, access policies, hashes, timestamps, revocation events, and audit records, while smart contracts automate authorization. This approach is consistent with foundational work on decentralized privacy and IoT smart contracts (Zyskind et al., 2015; Christidis & Devetsikiotis, 2016), blockchain-based access-control studies (Ouaddah et al., 2016; Novo, 2018), and later hybrid blockchain-IoT research (Alkhateeb et al., 2022; Bagga et al., 2022). The main methodological advantage is the separation of trust-critical metadata from high-volume data. Confidentiality is achieved through encryption, integrity is checked using ledger-anchored hashes, authorization is enforced by smart contracts, and accountability is supported through append-only audit events. The expected

trade-off is additional transaction latency and operational complexity compared with a single centralized server. Consequently, the framework is most suitable when multiple parties must share IoT data and no single organization should be able to silently modify access records or data provenance. Future implementation should evaluate heterogeneous wireless links, dynamic device mobility, key rotation, cross-chain interoperability, privacy-preserving analytics, validator compromise, and larger consortium sizes. It should also compare alternative consensus mechanisms and measure energy consumption at gateways. The proposed methodology provides a reproducible foundation for testing whether blockchain delivers measurable security value without imposing unacceptable cost on IoT data-sharing operations.

References

- Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 180-184. <https://doi.org/10.1109/SPW.2015.27>
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292-2303. <https://doi.org/10.1109/ACCESS.2016.2566339>
- Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). FairAccess: A new blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9, 5943-5964. <https://doi.org/10.1002/sec.1748>
- Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. 2017 IEEE PerCom Workshops, 618-623. <https://doi.org/10.1109/PERCOMW.2017.7917634>
- Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411. <https://doi.org/10.1016/j.future.2017.11.022>
- Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet of Things Journal, 5(2), 1184-1195. <https://doi.org/10.1109/JIOT.2018.2812239>
- Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173-190. <https://doi.org/10.1016/j.future.2018.05.046>
- Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT integration: A systematic survey. Sensors, 18(8), 2575. <https://doi.org/10.3390/s18082575>
- Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the Internet of Things (IoT): A systematic literature review. Sensors, 22(4), 1304. <https://doi.org/10.3390/s22041304>
- Bagga, P., Das, A. K., Chamola, V., & Guizani, M. (2022). Blockchain-envisioned access control for Internet of Things applications: A comprehensive survey and future directions. Telecommunication Systems, 81, 125-173. <https://doi.org/10.1007/s11235-022-00938-7>
- Miao, Q., Lin, H., Hu, J., & Wang, X. (2022). An intelligent and privacy-enhanced data sharing strategy for blockchain-empowered Internet of Things. Digital Communications and Networks, 8(5), 636-643. <https://doi.org/10.1016/j.dcan.2021.12.007>
- Qureshi, J. N., Farooq, M. S., Abid, A., Umer, T., Bashir, A. K., & Zikria, Y. B. (2022). Blockchain applications for the Internet of Things: Systematic review and challenges. Microprocessors and Microsystems, 94, 104632. <https://doi.org/10.1016/j.micpro.2022.104632>