International Journal of Research and Applied Innovations (IJRAI)

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November–December 2022||

DOI:10.15662/IJRAI.2022.0506001

Blockchain-Enabled Secure Data Sharing in IoT Networks

Raghav Nair Menon

ISL Engineering College, Affiliated to Osmania University, Hyderabad, India

Abstract: The rapid expansion of Internet-of-Things (IoT) networks introduces significant challenges in securely managing data sharing among heterogeneous, resource-constrained devices. Blockchain technology offers a promising solution by enabling decentralized trust, integrity, and authentication for IoT data exchange. This paper reviews and synthesizes key contributions from 2021, addressing how blockchain supports secure data sharing in IoT.

We first examine industrial IoT settings, where blockchain integrated with identity-based cryptography enables sensor-actuator data sharing, as proposed by Meng & Li, ensuring security and data provenance MDPI. Another study employs Hyperledger Fabric within an IoT–big data ecosystem to decentralize provenance tracking, offloading metadata to a blockchain ledger while storing bulk data off-chain for efficiency SpringerOpen.

Architecturally, Brotsis et al. assess blockchain platform suitability — focusing on IoT's stringent requirements for performance, privacy, and resilience. Their findings highlight that many blockchain platforms fail to meet IoT constraints arXiv. Additionally, Pal et al. survey blockchain-based access control mechanisms for IoT, emphasizing decentralized, tamper-resistant control but also noting limitations such as scalability and integration complexity arXiv.

Based on these works, we propose a research methodology that integrates identity-based cryptographic authentication, permissioned blockchain (e.g., Hyperledger), and off-chain storage with integrity validation via IPFS or ledger references. This hybrid approach balances security, latency, and storage constraints for IoT networks. Advantages include immutable audit trails, fine-grained access control, and reduced reliance on central servers. Drawbacks involve limited scalability, increased latency, and complexity of deployment.

This paper concludes by highlighting results demonstrating feasibility of decentralized provenance tracking and secure access control. It positions future work toward optimizing consensus, enhancing lightweight identity and access mechanisms, and improving blockchain–IoT interoperability. The contributions serve as a framework guiding practical, secure IoT data-sharing implementations.

KEYWORDS: Blockchain, Internet of Things, Secure Data Sharing, Identity-Based Cryptography, Hyperledger Fabric, Off-chain Storage, Access Control, IoT Security.

I. INTRODUCTION

The Internet-of-Things (IoT) ecosystem comprises a vast and accelerating array of interconnected devices sharing data to enable automation, smart environments, and analytics. However, the decentralized and resource-constrained nature of IoT poses critical security challenges: ensuring data integrity, authenticity, fine-grained access control, and auditability without centralized trust or heavy computation.

Blockchain technology offers capabilities like tamper-resistance, decentralized consensus, and immutable audit trails—features highly valuable to IoT environments. By combining blockchain with lightweight cryptographic authentication and off-chain storage mechanisms, IoT networks can securely and transparently manage data sharing among untrusted participants. Notably, 2021 has seen several foundational contributions demonstrating blockchain's potential across industrial and large-scale IoT scenarios.

For instance, Meng & Li (2021) propose a mechanism for sensor-actuator data sharing using blockchain-assisted identity-based cryptography, enabling secure and authenticated communication in industrial IoT MDPI. Another study by Pajooh et al. leverages Hyperledger Fabric within a Hadoop-based big data framework to decentralize data provenance tracking:

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November–December 2022||

DOI:10.15662/IJRAI.2022.0506001

metadata stored on-chain, large data kept off-chain for efficiency, and identity managed via peer verification SpringerOpen.

However, the suitability of blockchain platforms for IoT must be carefully evaluated. Brotsis et al. (2021) analyze architectures across security, privacy, and performance dimensions and find that many existing blockchain models cannot sufficiently address IoT constraints arXiv. Similarly, access control via blockchain is promising but faces challenges in scalability and integration, as detailed by Pal et al. (2021) arXiv.

This paper builds upon these insights to frame a secure, scalable architecture for blockchain-enabled data sharing in IoT networks. It outlines methodology, analyzes trade-offs, and suggests appropriate blockchain-IoT configurations suitable for practical deployment.

II. LITERATURE REVIEW

Key 2021 contributions in blockchain-enabled IoT data sharing include:

Identity-Based IoT Security: Meng & Li (2021) designed a blockchain-assisted identity-based cryptography mechanism to securely facilitate data sharing between sensors and actuators in industrial environments MDPI.

Distributed Provenance in Big Data Systems: Pajooh et al. propose a layer-based blockchain design for IoT data lakes, using Hyperledger Fabric to record lightweight verification tags on-chain and storing full datasets in off-chain storage. Their prototype demonstrates feasibility in latency (≤500 ms), throughput (~600 TPS), and resource use (low CPU involvement) SpringerOpen.

Platform Suitability Analyses: Brotsis et al. evaluate various blockchain platforms against IoT requirements—focusing on architecture, security, privacy, and performance—and report that many 1.0/2.0 platforms fall short in key IoT scenarios arXiv.

Access Control via Blockchain: Pal, Dorri, and Jurdak survey blockchain-based access control for IoT, highlighting blockchain's strengths—decentralization, secure storage—but noting limitations around efficiency, scalability, and integration complexity arXiv.

Collectively, these studies acknowledge the potential of blockchain to enhance IoT security and data integrity, but also expose challenges in practical deployment—particularly performance, resource consumption, and system complexity. We build on these insights to propose a balanced architecture integrating identity authentication, permissioned blockchain, and off-chain storage.

III. RESEARCH METHODOLOGY

Objective
Develop a secure, scalable architecture for blockchain-enabled data sharing in IoT networks, preserving data integrity, provenance, and access control while accommodating device constraints.

Component Design
Identity Authentication
Implement identity-based cryptography (IBC) or decentralized identity (DID) for secure device enrollment and authenticatio.
Ensures only authorized devices can participate and generate authenticated data.

Permissioned Blockchain Platform
Use Hyperledger Fabric due to its customizable consensus, private ledger channels, and smart-contract capabilities MDPI.
Each data event triggers a transaction recording metadata or data references; smart contracts enforce access control policies.

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November–December 2022||

DOI:10.15662/IJRAI.2022.0506001

Off-Chain Storage
Integrate off-chain data storage (e.g., IPFS or traditional Big Data systems) for actual data; store only hashes or pointers on-chain to maintain integrity and reduce storage cost SpringerOpen.

Secure Provenance Tracking
When devices publish data, the system records provenance events on-chain.
Retrievable in smart contracts; allows audit and traceability.

Implementation Plan
Prototype Setup
Deploy Hyperledger Fabric network with peer nodes representing IoT gateways or edge servers.
Integrate identity enrollment via IBC or DID.

Data Flow
IoT device sends data → data is hashed & stored off-chain → on-chain transaction created linking to off-chain hash + identity data → smart contract verifies permissions.

Performance Measurement
Metrics: transaction latency, throughput, CPU/memory usage, data retrieval time, provenance trace duration.

Security Evaluation
Threat modeling: unauthorized data injection attempts, identity forgery, ledger tampering.
Ensure smart contracts prevent access violations.

Experimental Scenarios
Deploy small-scale IoT testbed (edge nodes + sensors).
Generate data sharing workflows under varying load (e.g., 50–200 TPS) and measure system responsiveness and resource overhead.
Compare to centralized schemes (no blockchain) to quantify added cost.

Analysis & Optimization
Evaluate access control latency vs scalability.
Optimize block size, consensus parameters, and off-chain retrieval methods.
Refine identity and permissioning models for lightweight IoT contexts.

Ethical & Practical Considerations
Maintain data privacy; ensure sensitive data is encrypted before storage.
Use permissioned blockchain to restrict access.
Document access logs for audit and compliance.

Advantages
Immutable Audit Trails: Blockchain ensures tamper-evident provenance tracking.
Decentralized Trust: Reduces reliance on central authorities; improves resilience.
Fine-Grained Access Control: Smart contracts enforce per-device permissions.
Efficient Storage: Off-chain storage mitigates blockchain bloat.

Disadvantages
Scalability Challenges: Blockchain throughput and latency can limit IoT performance.
Resource Overhead: Extra computational cost for cryptography and communication.
System Complexity: Combining blockchain, off-chain storage, and identity systems increases design complexity.
Interoperability and Standards: Loosely standardized; integration across diverse IoT platforms remains difficult TechTarget.

| ISSN: 2455-1864 | www.ijrai.com | editor@ijrai.com | A Bimonthly, Scholarly and Peer-Reviewed Journal |

||Volume 5, Issue 6, November–December 2022||

DOI:10.15662/IJRAI.2022.0506001

IV. RESULTS AND DISCUSSION

.Prototype evaluations—drawing from similar studies—indicate that IoT provenance recording via Hyperledger achieves acceptable throughput (~600 TPS) with moderate latency (<500 ms) SpringerOpen. Identity-based mechanisms enhance secure authentication with minimal overhead. However, system responsiveness degrades under high loads, and off-chain retrieval introduces additional latency. Results emphasize the need for optimized consensus mechanisms and scalable design choices.

V. CONCLUSION

Blockchain-enabled architectures—combining identity-based auth, permissioned ledgers, and off-chain storage—offer robust frameworks for secure data sharing in IoT networks. They address integrity, provenance, and access control effectively. However, practical adoption requires addressing scalability, resource constraints, and standardization gaps.

VI. FUTURE WORK

- **Lightweight Consensus**: Explore IoT-optimized consensus (e.g., Proof-of-Assignment, DAG-based systems like IOTA) InvestopediaMDPI.
- **Interoperable Standards**: Align with DID and W3C identity standards for cross-chain IoT interoperability Reddit.
- **Adaptive Off-Chain Solutions**: Dynamically cache data to reduce retrieval latency.
- **Edge-AI Integration**: Complement blockchain with local AI-based anomaly detection for access anomalies.

REFERENCES

1. Meng, Y., & Li, J. (2021). Data Sharing Mechanism of Sensors and Actuators of Industrial IoT Based on Blockchain-Assisted Identity-Based Cryptography. *Sensors*, 21(18), 6084. MDPI
2. Pajooh, H. H., Rashid, M. A., et al. (2021). IoT Big Data provenance scheme using blockchain on Hadoop ecosystem. *Journal of Big Data*, 8, 114. SpringerOpen
3. Brotsis, S., Limniotis, K., et al. (2021). On the Suitability of Blockchain Platforms for IoT Applications: Architectures, Security, Privacy, and Performance. *arXiv preprint*. arXiv
4. Pal, S., Dorri, A., & Jurdak, R. (2021). Blockchain for IoT Access Control: Recent Trends and Future Research Directions. *arXiv preprint*. arXiv
5. Survey on challenges: interoperability, governance in IoT-blockchain combos. TechTarget
6. Hyperledger frameworks and IoT relevance. MDPI