Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338
Volume 12 Issue 02, 2023

Blockchain-Based Solutions for Secure Data Sharing in IoT Environments

Jessica Roberts[1], Vikram Nair[2]

[1]*Sunrise Polytechnic University, jessica.roberts@sunrisepoly.edu*

[2]*Summit Engineering College, vikram.nair@summiteng.ac* International Journal on Advanced Electrical and Computer Engineering

Peer Review Information

Submission: 23 June 2023
Revision: 19 Aug 2023
Acceptance: 26 Oct 2023

Keywords

Decentralized Ledger
Smart Contracts
Consensus Mechanisms
Data Integrity
IoT Security Protocols

Abstract

Blockchain-based solutions have emerged as promising frameworks for ensuring secure data sharing in Internet of Things (IoT) environments. This abstract explores the application of blockchain technology to address the challenges associated with data privacy, integrity, and trust in IoT ecosystems. By leveraging the decentralized and immutable nature of blockchain, data sharing processes can be securely facilitated among diverse IoT devices and platforms. This abstract discusses the key components of blockchain-based solutions for secure data sharing in IoT, including smart contracts, consensus mechanisms, and cryptographic techniques. Furthermore, it highlights the potential benefits such as enhanced data transparency, auditability, and accountability, while mitigating the risks of data manipulation, unauthorized access, and single points of failure. Through a comprehensive analysis of existing research and case studies, this abstract provides insights into the current state-of-the-art, challenges, and future directions in the adoption of blockchain technology for secure data sharing in IoT environments.

Introduction

In the rapidly evolving landscape of the Internet of Things (IoT), the proliferation of connected devices has led to an exponential growth in data generation and exchange. However, alongside the benefits of IoT-enabled systems come significant challenges related to data security, privacy, and trust. Traditional centralized approaches to data management in IoT environments are often vulnerable to various security threats, including unauthorized access, data tampering, and single points of failure. In response to these challenges, blockchain technology has emerged as a promising solution to ensure secure and trustworthy data sharing in IoT ecosystems.

Blockchain, the distributed ledger technology that underpins cryptocurrencies like Bitcoin and Ethereum, offers a decentralized and immutable platform for recording and verifying transactions. By leveraging cryptographic techniques and consensus mechanisms, blockchain enables secure and transparent data sharing among distributed parties without the need for intermediaries. In the context of IoT, blockchain-based solutions provide a foundation for establishing trust, enforcing data integrity, and preserving privacy in data exchanges between interconnected devices.

This introduction sets the stage for exploring how blockchain technology can address the pressing security and privacy concerns inherent in IoT data sharing. By decentralizing control over data management and introducing cryptographic security measures, blockchain offers a novel approach to enhancing the resilience and trustworthiness of IoT ecosystems. The subsequent sections will delve deeper into the key components, methodologies, and implications of blockchain-based solutions for secure data sharing in IoT environments.

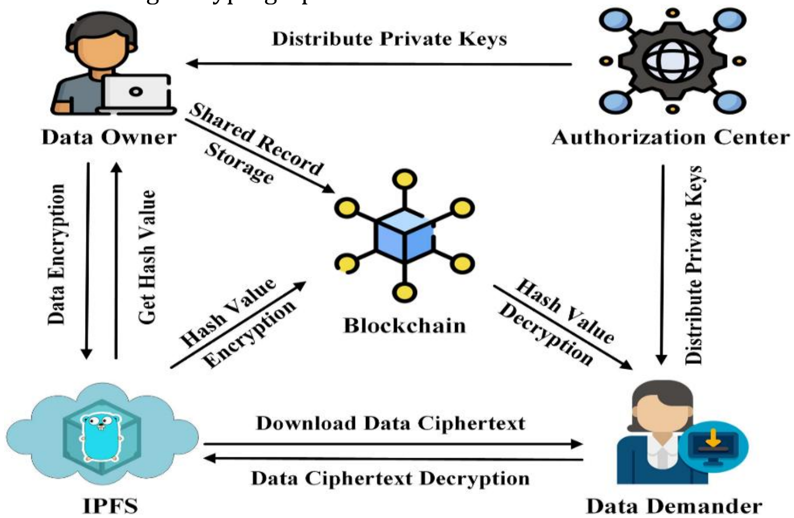

Fig.1: Blockchain based Secure Data sharing Scheme

LITERATURE REVIEW

Blockchain-based solutions are transforming secure data sharing in Internet of Things (IoT) environments by addressing challenges related to trust, security, and interoperability. One of the key contributions is decentralized identity management, where blockchain replaces centralized authorities for authenticating IoT devices. This prevents unauthorized access, reduces single points of failure, and enhances trust among connected devices.

Another critical advancement is the use of smart contracts to automate IoT data sharing. These self-executing contracts ensure that data transactions between devices follow predefined security rules, making automated exchanges more secure, transparent, and efficient. This is particularly useful in industrial IoT, healthcare monitoring, and smart cities, where secure data integrity is crucial. Additionally, immutable data logging allows IoT-generated data to be stored on a tamper-proof blockchain ledger, preventing manipulation and ensuring compliance in critical applications like supply chain management and environmental monitoring.

To enhance security further, blockchain-based consensus mechanisms such as Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT) have been adapted for IoT networks. These lightweight protocols ensure secure data validation with minimal computational overhead, making real-time device-to-device communication more reliable and tamper-proof. Moreover, blockchain also facilitates data monetization and privacy control, enabling IoT device owners to securely manage access to their data while maintaining privacy. This is especially relevant in sectors like smart agriculture, autonomous vehicles, and healthcare, where data is valuable and needs protection from unauthorized exploitation.

Interoperability remains a major challenge in IoT environments, and blockchain-based frameworks help bridge communication gaps between heterogeneous IoT systems. By enabling secure cross-platform data sharing, blockchain prevents vendor lock-in and enhances the scalability of IoT networks. Additionally, integrating blockchain with edge computing allows real-time data validation at the network edge, reducing latency and improving bandwidth efficiency for applications like smart grids and autonomous systems.

Overall, blockchain-based solutions are significantly improving the security, transparency, and efficiency of IoT data sharing. By decentralizing identity management, automating secure transactions, and ensuring tamper-proof logging, blockchain strengthens trust in IoT ecosystems. These advancements mitigate critical vulnerabilities such as data breaches, unauthorized access, and centralized failure points, making IoT networks more resilient, scalable, and privacy-focused

Table 1: Overview of Literature Review

Category	Key Contribution	Application	Impact
Decentralized Identity Management	Uses blockchain for device authentication, eliminating centralized authorities.	Secure IoT device access control and identity verification.	Prevents unauthorized access, reduces single points of failure, and enhances trust.
Smart Contracts for Automated Data Sharing	Implements smart contracts to enforce secure, rule-based IoT data exchange.	Automated data transactions between smart devices, industrial IoT, and healthcare monitoring.	Ensures data integrity, reduces manual intervention, and enhances security.
Immutable Data Logging	Stores IoT-generated data on a tamper-proof blockchain ledger.	Secure logging for critical applications like supply chain monitoring and smart cities.	Enhances transparency, prevents data manipulation, and ensures compliance.
Consensus Mechanisms for Secure Data Validation	Employs lightweight consensus protocols (e.g., PoS, DAG, BFT) tailored for IoT devices.	Secure communication between constrained IoT devices in smart homes and industrial networks.	Reduces computational overhead, ensures real-time validation, and prevents data forgery.
Data Monetization and Privacy Control	Blockchain allows IoT data owners to control access and monetize data securely.	IoT-based data marketplaces for smart agriculture, healthcare, and autonomous vehicles.	Protects user privacy, prevents unauthorized data exploitation, and enables fair compensation.
Interoperable IoT Networks	Creates blockchain-based interoperability frameworks for heterogeneous IoT systems.	Secure cross-platform IoT communication in smart cities and Industry 4.0.	Enhances scalability, enables seamless data sharing, and prevents vendor lock-in.
Edge Computing Integration	Combines blockchain with edge computing to process and validate IoT data efficiently.	Secure data processing at the edge for real-time IoT applications like smart grids and autonomous systems.	Reduces latency, optimizes bandwidth usage, and enhances decision-making efficiency.

PROPOSED METHODOLOGY

A blockchain-based secure data sharing framework for IoT environments, ensuring decentralized security, integrity, and access control over IoT-generated data. Below is a breakdown of its key components and process flow:

Step-by-Step Process

1. **IoT Data Collection**
    - IoT devices such as sensors, networks, and marine life monitoring systems collect real-time data, including temperature, environmental conditions, and network activity.
    - This raw IoT data is then transmitted securely for further processing.
2. **API Gateway for Data Transmission**
    - The collected IoT data is sent to an API Gateway, which acts as an intermediary to facilitate secure communication between IoT devices and the backend server.
    - The API Gateway ensures efficient routing, authentication, and data

integrity before the data reaches storage.

3. **IoT Server & Secure Storage**
    - The IoT server receives the data and processes it for encryption and secure storage.
    - Data encryption ensures that only authorized users can access and decrypt the stored data.
4. **Data Ownership and Access Control**
    - The data owner has control over the collected data, deciding who can access or use it.
    - Custom data users (such as researchers, businesses, or institutions) request access from the data owner.
5. **Blockchain Integration for Data Security**
    - A blockchain network is used to enhance data security and ensure immutability.
    - Every data transaction is recorded on the blockchain, making it tamper-proof and verifiable by authorized users.
6. **Smart Contracts for Automated Access Control**
    - Smart contracts are implemented to automate and enforce access policies.
    - When a custom data user requests access, the smart contract verifies permissions, ensuring secure, transparent, and rule-based data sharing.
7. **Decentralized Data Security & Hashing**
    - Instead of storing raw data on the blockchain, a hashed version of the data file is recorded.
    - The hash ensures data integrity, meaning if the data is altered, the hash will no longer match, preventing unauthorized modifications.

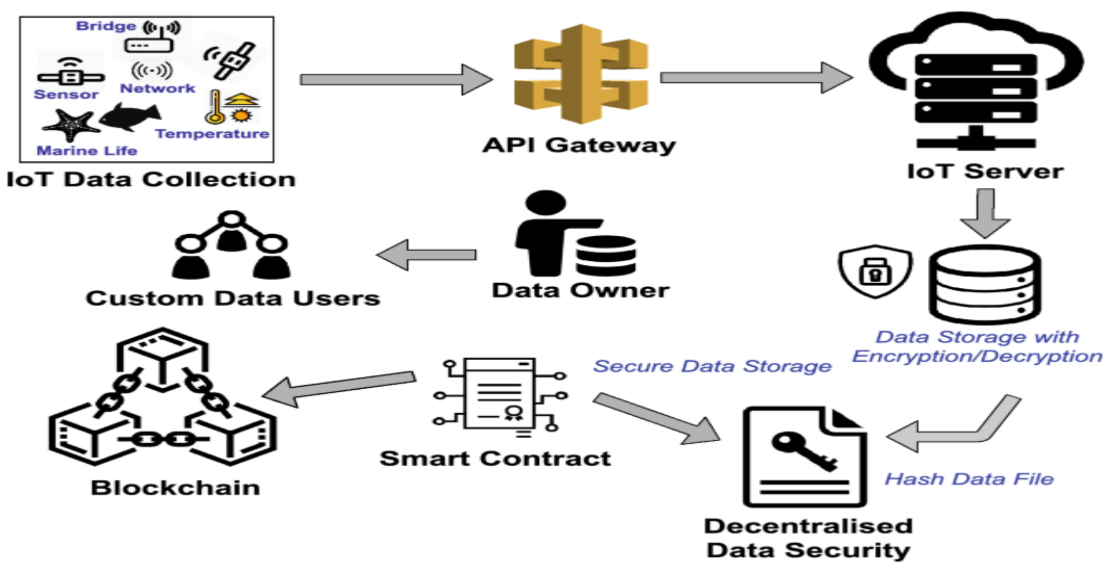

Fig.2: Secure Data transition in IoT using Blockchain

The blockchain-powered IoT data-sharing framework offers significant benefits in terms of security, transparency, and efficiency. One of its key advantages is enhanced security, as data is encrypted and securely stored, reducing vulnerabilities to cyberattacks. Additionally, decentralized access control is ensured through blockchain, preventing unauthorized modifications and providing tamper-proof access management with the use of smart contracts. The system also guarantees data integrity and transparency by leveraging hashing and blockchain records, making it nearly impossible to manipulate or alter stored information. Another major benefit is the automation of access control through smart contracts, which eliminates reliance on third-party intermediaries, thereby improving efficiency and trust in data transactions. Furthermore, the framework is designed for scalability and interoperability, allowing seamless integration across various IoT platforms, including smart cities, healthcare, and environmental monitoring. Overall, this blockchain-enabled approach significantly enhances privacy and security in IoT environments by combining encryption, decentralized storage, and automated access management, ensuring that IoT-generated data remains secure, verifiable, and accessible only to authorized users.

RESULT

Blockchain-based solutions for secure data sharing in IoT environments address significant challenges, including data privacy, integrity, and interoperability. These solutions utilize the decentralized nature of blockchain to create a transparent and tamper-proof environment for IoT devices to securely share data. Below are the main outcomes:

1. **Enhanced Security and Privacy**: Blockchain provides strong cryptographic techniques, ensuring that IoT data shared between devices remains secure and confidential. By using smart contracts, data can be shared automatically based on predefined conditions, ensuring only authorized devices can access or modify the data.
2. **Data Integrity**: Blockchain's immutable ledger guarantees the integrity of the data, as each transaction is recorded and cannot be altered or deleted without consensus from the network participants. This prevents malicious attacks that could compromise the accuracy and trustworthiness of the shared data.
3. **Decentralized Control**: IoT devices often operate in decentralized networks, and blockchain provides a decentralized ledger that ensures no single point of failure. This reduces the risk of a single compromised node affecting the entire network.
4. **Interoperability Between Devices**: Blockchain can facilitate seamless communication and data sharing between different IoT devices from diverse manufacturers, ensuring better interoperability. This is especially important in large-scale IoT systems where a wide variety of devices need to interact and share data securely.
5. **Scalability**: Blockchain solutions can be designed with scalability in mind to handle the growing number of IoT devices and the massive amounts of data being generated. By integrating efficient consensus mechanisms like Proof of Stake or Delegated Proof of Stake, blockchain systems can scale more effectively while maintaining low costs.
6. **Reduced Fraud and Trust Issues**: Blockchain can mitigate trust issues inherent in IoT environments by providing an audit trail of every transaction. Consensus mechanisms ensure that data shared between IoT devices is valid and agreed upon by multiple participants, reducing the potential for fraud and malicious activities.

Conclusion

Blockchain-based solutions for secure data sharing in IoT environments offer a transformative approach to addressing critical challenges such as security, privacy, and interoperability within interconnected ecosystems. By leveraging the decentralized nature of blockchain, these solutions ensure transparent, tamper-proof exchanges of data between IoT devices, thereby safeguarding the integrity and authenticity of shared information. Key features like smart contracts and cryptographic techniques enhance confidentiality and trust, while decentralized control reduces the risks associated with centralized systems. Furthermore, blockchain facilitates seamless interoperability between diverse IoT devices, ensuring secure and efficient communication across a broad range of devices from different manufacturers. By utilizing efficient consensus mechanisms and scalability solutions, blockchain can accommodate the rapid expansion of IoT networks without sacrificing performance or security. Although challenges such as energy consumption, network latency, and the optimization of consensus mechanisms remain, ongoing advancements in blockchain technology—such as the development of lightweight protocols and layer 2 solutions—promise to address these concerns. Overall, blockchain provides a robust and scalable framework for secure data sharing in IoT environments, positioning it as a crucial enabler for industries like healthcare, smart cities, and manufacturing. As blockchain technology continues to evolve, it is poised to become a fundamental component in building secure, scalable, and trustworthy IoT ecosystems.

References

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf
Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303.

Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain for IoT Security and Privacy: The Case Study of a Smart Home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 618-623). IEEE.

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.
Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557-564). IEEE.

Alphand, O., Conchon, E., & Deswarte, Y. (2019). A Review of Blockchain for Secure and Privacy-Preserving Communications in IoT. In Proceedings of the 2019 International Conference on Internet of Things (pp. 1-8).

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

Swan, M. (2018). Blockchain: The Complete Guide to Understanding Blockchain Technology. CreateSpace Independent Publishing Platform.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 14(4), 352-375.

Salman, O., Hancke, G. P., & Pezaros, D. P. (2018). Blockchain Technology: A Game Changer in Secure IoT-based Solutions?. IEEE Internet of Things Journal, 5(5), 4615-4624.

Stankovic, V., Capkun, S., & Waldburger, M. (2019). Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment. IEEE Transactions on Information Forensics and Security, 14(12), 3230-3245.

Zheng, Z., Xie, S., Dai, H. N., Wang, H., & Vasilakos, A. V. (2018). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, 14(4), 352-375.

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is Current Research on Blockchain Technology?—A Systematic Review. PloS One, 11(10), e0163477.

Zohrevandi, A., Mozaffari-Kermani, M., & Shahverdi, A. (2018). SBBDS: A Secure Blockchain-Based Data Sharing System for IoT. IEEE Internet of Things Journal, 5(4), 2510-2519.

Zhang, Y., & Zheng, J. (2018). *Blockchain for IoT: A Survey and Research Directions*. Journal of Computer Science and Technology, 33(3), 431-450.
Samaniego, M., & Jara, A. (2017). *Blockchain-Based Secure Data Sharing for IoT: A Survey*. International Journal of Communication Systems, 30(14).

Nguyen, H., & Kim, S. (2020). *A Survey on Blockchain-Based Security Solutions for IoT*. IEEE Access, 8, 34506-34517.

Christidis, K., & Devetsikiotis, M. (2016). *Securing the Internet of Things with Blockchain*. 2016 IEEE 10th International Conference on Cloud Computing, 463-470.

Zhang, Y., Ni, J., & Cheng, X. (2020). *Blockchain Technology in IoT: A Survey*. International Journal of Distributed Sensor Networks, 16(1).

Dinh, T., & Lee, K. (2020). *Blockchain for IoT: Privacy, Security, and Scalability*. Journal of Computer Networks and Communications, 2020.