"Blockchain-Based Access Control Model for Secure Data Sharing in IoT Networks"

Mrs.S.Suganya,

Assistant Professor ,Surya Engineering College,Erode.

Abstract: In this research, the rapid rise of Internet of Things (IoT) devices has dramatically changed the way we generate, share, and consume data. But with this surge in connectivity comes a host of serious issues around data security, privacy, and trust, particularly because traditional centralized access control systems have their limitations. These older models often suffer from single points of failure, unauthorized access, and a lack of transparency. To tackle these problems, this paper introduces a blockchain-based access control model designed to facilitate secure and decentralized data sharing in IoT settings. By utilizing smart contracts, the model automates access permissions, keeps unchangeable logs, and provides detailed control over data. The framework is built on the Ethereum blockchain using Solidity and tested with simulated IoT data. The experimental findings reveal improved security, better resistance to common attacks, and enhanced auditability when compared to traditional systems. This model offers a scalable and tamper-proof access control solution that fits perfectly with the decentralized nature of IoT systems.

Keywords: Blockchain, Internet of Things (IoT), Access Control, Smart Contracts, Data Security, Decentralized Systems

INTRODUCTION

The Internet of Things (IoT) is shaking up various industries by linking billions of devices and allowing for real-time data collection and communication. From smart homes and cities to industrial automation and healthcare, IoT applications are building extensive ecosystems where data flows non-stop. However, despite its game-changing potential, IoT grapples with significant challenges, particularly around secure data sharing and access control.

Traditional access control models—like Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC)—depend heavily on centralized servers for tasks like authentication, authorization, and auditing. This centralization can lead to vulnerabilities, such as single points of failure, exposure to Distributed Denial of Service (DDoS) attacks, and increased administrative burdens. Additionally, these systems often lack transparency and struggle to provide detailed, tamper-proof access logs, which are essential in the highly distributed and dynamic world of IoT.

Enter blockchain technology, which was originally created for cryptocurrencies but has now surfaced as a promising solution for decentralized security. Its key features—immutability, transparency, consensus-driven validation, and decentralization—make it a great fit for bolstering IoT data security. Blockchain can either replace or enhance existing access control systems by storing access rules and logs on an unchangeable ledger and automating enforcement through smart contracts.

Smart contracts are self-executing pieces of code that run on a blockchain. They automatically implement and enforce access control policies without needing a central authority. This guarantees that data access is granted or denied based on set rules, and every access attempt is permanently logged, allowing for real-time auditing.

In this paper, we introduce a blockchain-based access control model designed for secure data sharing within IoT networks. Our approach leverages the Ethereum blockchain and smart contracts to effectively manage and enforce access control policies in a decentralized way. This means we can do away with a central authority, ensuring that only those who are authorized can access IoT data, all while providing unchangeable logs for auditing purposes.

1. A decentralized access control model that utilizes blockchain technology for IoT systems.
2. The implementation of smart contracts to oversee access rights and maintain access logs.
3. An evaluation of the model's performance through simulated IoT scenarios, with a focus on latency, throughput, gas usage, and security.

The structure of the paper is as follows: Section 2 offers a literature review, Section 3 outlines the theoretical framework, Section 4 goes into detail about the system implementation, Section 5 shares the results and discussion, and Section 6 wraps up the paper with insights on future research directions.

RESEARCH QUESTION

1. How does blockchain technology enhance access control and security in IoT networks?
2. What advantages do smart contracts offer for managing access in IoT settings?
3. How does the suggested blockchain-based model stack up against traditional access control methods when it comes to performance and security?

LITERATURE REVIEW:

Previous studies have shed light on various approaches to securing the Internet of Things (IoT) through blockchain technology. For instance, Zhang et al. (2018) proposed a framework for access control that leverages blockchain to eliminate reliance on centralized servers. Meanwhile, Xu et al. (2020) examined access models based on smart contracts, addressing issues related to latency and storage. Christidis and Devetsikiotis (2016) introduced a conceptual model aimed at decentralized trust management in IoT using blockchain. However, many existing models tend to either concentrate solely on authentication or struggle with scalability in large-scale IoT environments.

This research aims to overcome those challenges by merging smart contracts with access control mechanisms, allowing for detailed permissions and maintaining access logs on the blockchain. A side-by-side comparison with traditional models shows notable enhancements in data integrity, transparency, and resistance to tampering.

THEORETICAL FRAMEWORK

This research is rooted in the concepts of Zero Trust Architecture (ZTA) and Decentralized Access Control Theory.

Zero Trust Architecture is a security framework that operates on the premise that no individual, system, or service can be trusted by default, even if they are within the network's perimeter. Every request for access is thoroughly verified, logged, and audited. Blockchain technology fits seamlessly with ZTA because it mandates verification and logging without the need for a central authority.

On the other hand, Decentralized Access Control Theory posits that access policies should be enforced independently of a central governing body. Blockchain enhances this by facilitating distributed consensus, ensuring immutability, and managing identities in a decentralized manner. Smart contracts play a crucial role by automatically enforcing access policies, which helps to minimize administrative delays and boosts auditability. By merging these theories, the proposed model enables each IoT device or user to authenticate and gain access based on rules stored on the blockchain. Access logs are recorded on the chain for transparency, while smart contracts guarantee that access decisions are made autonomously and securely.

ETHEREUM BLOCKCHAIN

1. Smart Contracts: These are crafted in Solidity and serve to outline access rules, validate requests, and keep a record of actions.
2. IoT Simulation: Using Node-RED and Raspberry Pi devices, we can generate data and function as IoT nodes that request access.
3. Blockchain Node: For deployment and testing, we utilize Ganache, which is a local Ethereum testnet.
4. Web Interface: With ReactJS and Web3.js, users can easily request and keep an eye on access.
5. Backend: The backend is powered by Python and a Flask API that works with Web3.py to interact with the blockchain.

ENFORCEMENT OF ACCESS POLICIES

A fundamental aspect of the model was its ability to enforce fine-grained access control rules automatically. Smart contracts encoded the access permissions for each IoT device, ensuring that any request to access sensitive data was validated against these rules before granting or denying access. The testing phase demonstrated that unauthorized requests were consistently blocked, preventing data breaches or misuse. This reliable enforcement arises from the immutable and autonomous nature of blockchain smart contracts, which do not require human intervention or trusted third-party authorities, thereby significantly reducing the risk of insider threats or policy manipulation.

SECURITY AND TRANSPARENCY

Security improvements stem directly from blockchain's decentralized architecture, which eliminates single points of failure common in centralized access control systems. Traditional systems often depend on centralized servers vulnerable to attacks or failures; in contrast, blockchain nodes collectively maintain a distributed ledger, making unauthorized data tampering nearly impossible. In addition, all access events—whether approvals or denials—were immutably logged on the blockchain with timestamps and user identities. This permanent, transparent audit trail increases accountability, allowing administrators and auditors to trace every access event for compliance with privacy regulations like GDPR or HIPAA.

To assess resistance to common attack vectors, the system was subjected to impersonation attempts, replay attacks, and unauthorized data injection. Thanks to cryptographic signatures and consensus validation, none of these attacks succeeded, confirming the model's robustness in preserving data integrity and user trust.

CONCLUSION

This study introduces a blockchain-based access control framework specifically designed for IoT networks. By utilizing smart contracts and decentralized validation, the model tackles major issues found in current systems—like centralization, a lack of transparency, and poor auditability. It shows a notable enhancement in secure data sharing, resistance to unauthorized access, and clear logging.

While the system holds great potential, there are still hurdles to overcome, such as transaction latency, gas fees, and device compatibility. Future research could aim at optimizing smart contract execution, incorporating off-chain storage, and creating lightweight consensus protocols that are better suited for IoT.

REFERENCE

1. Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., ... & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., & Wan, J. (2018). Smart Contract-Based Access Control for the Internet of Things. IEEE Internet of Things Journal, 6(2), 1594–1605.
2. Xu, R., Chen, W., & Zhu, Y. (2020). Blockchain-Based Data Integrity Service Framework for IoT Data. *IEEE Internet of Things Journal*, 7(5), 4040–4054.
3. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292–2303.
4. Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). *Applications of Blockchains in the Internet of Things: A Comprehensive Survey*. IEEE Communications Surveys & Tutorials, 21(2), 1676–1717.