Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Blockchain-Based Access Control for Secure and Efficient Smart Homes in the Internet of Things (IoT) Era

Mohammed Yasaruddin[1], Dr. M. Subramaniam[2], Dr. Sangeeta Gupta[3]

[1] M.Tech CSE,myasaruddin@gmail.com,CBIT 500075

[2]Professor & Head CSEIOT, msubramaniam_cseiot@cbit.ac.in, CBIT, 500075

[3]Associate Professor CSE, sangeetagupta_cse@cbit.ac.in, CBIT, 500075

Article Info
Page Number: 12736-12740
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received: 25 October 2022
Revised: 30 November 2022
Accepted: 15 December 2022

Abstract
This research paper explores the integration of blockchain technology with smart homes and the Internet of Things (IoT) to enhance security and access control. With the increasing proliferation of IoT devices in modern homes, ensuring secure and authorized access is crucial. Blockchain's decentralized and immutable nature offers a promising solution for addressing security challenges. This project proposes a secure access control system that leverages the blockchain's distributed ledger and cryptographic techniques. It facilitates user authentication, device authorization, and tamper-resistant audit trails. The study aims to enhance the overall security and privacy of smart homes while facilitating seamless interactions with IoT devices. By combining blockchain, smart home technology, and the IoT, this research contributes to the development of robust access control mechanisms for a connected and secure home environment.

Introduction

Blockchain technology, smart homes, and the Internet of Things (IoT) have emerged as significant technological advancements, shaping the way we interact with our living spaces. This research aims to explore the potential of blockchain as a secure and transparent solution for access control in smart homes, leveraging the benefits of the IoT. Blockchain is a decentralized and immutable digital ledger that records transactions across multiple nodes in a network, ensuring transparency, security, and trust. It provides a robust framework for managing and verifying data, without the need for a centralized authority.

Smart homes encompass a network of interconnected devices and systems that provide automation, convenience, and energy efficiency. These devices range from thermostats and lighting systems to security cameras and home appliances. They are designed to enhance the quality of life for homeowners by enabling remote control, monitoring, and efficient management of various functionalities.

The IoT refers to the interconnected network of physical devices embedded with sensors, software, and connectivity, enabling them to collect and exchange data. Within smart homes, IoT devices enable remote control and monitoring, enhancing convenience and flexibility for homeowners. They enable seamless ommunication and interaction between devices, allowing homeowners to control their environment through various interfaces.

Integrating blockchain technology with smart homes and the IoT can establish a robust and secure access control system. The decentralized nature of blockchain reduces the risk of unauthorized access or manipulation. Through the use of smart contracts, user authentication and device authorization can be implemented seamlessly, allowing only authorized individuals to interact with smart home devices.

Blockchain technology also enhances data privacy and integrity in smart homes. The immutability of the blockchain ledger prevents unauthorized tampering, ensuring a high level of security. Audit trails stored on the blockchain provide transparent and traceable records of device interactions, aiding in the identification of suspicious activity.

The objective of this research project is to design and implement a blockchain-based access control system for smart homes, enabling secure and efficient management of IoT devices. By leveraging the strengths of blockchain technology, the project aims to enhance user privacy, strengthen security measures, and provide a seamless user experience when interacting with smart home technologies.

Related work

The Internet of Things (IoT) is witnessing exponential growth as more devices become interconnected through the Internet. Existing literature on IoT security and privacy has explored various mechanisms, often relying on a centralized client/server approach [1]. A case study was conducted to examine access control in an IoT system, which involved a desktop computer, a laptop, and two Raspberry Pi single-board computers [2].

To optimize users' transactive energy management in the IoT while preserving privacy, a privacy-preserving distributed algorithm was developed [3]. This approach integrated blockchain, group signatures, and message authentication code to enable reliable auditing of user access history, anonymous authentication of group members, and efficient authentication of home gateways [4].

In another study, the application of an embedded model in cross-chain exchange scenarios was explored [5]. Additionally, a study proposed a blockchain-based system architecture for Smart Home Systems (SHS), investigating its structure and syncretizing technologies [6]. The study also examined the Real-Time Security-Driven Event-Driven Learning Model (RTS-DELM) methodology implemented in blockchain-based smart homes for detecting malicious activity [7].

Furthermore, a proposed Smart Home Architecture based on Blockchain was carefully evaluated for reliability in terms of essential security aims, including privacy, integrity, and accessibility [8]. Another secure smart home system solution, addressing security constraints, combined Hyperledger Fabric and Hyperledger Composer [9]. This proposed system provided a flexible approach to implementing IoT applications for diverse IoT devices.

The integration of blockchain with IoT was investigated, highlighting the opportunities of Blockchain of Things (BCoT) and outlining its architecture. The BCoT architecture comprised five sublayers: Data, Network, Consensus, Incentive, and Service [10]. A novel

secure, private, and lightweight architecture for IoT based on lockchain technology was proposed to eliminate blockchain overhead while retaining its security and privacy benefits [11].

In conclusion, the related work on IoT security and privacy explores various approaches, including blockchain integration, group signatures, message authentication code, and decentralized architectures. These studies aim to enhance the security, privacy, and reliability of IoT systems, considering the unique challenges and requirements of IoT environments.

Proposed Work

The proposed work aims to develop a secure access control system for smart homes by integrating blockchain technology with the Internet of Things (IoT). Building upon the research conducted in the related work, we will design and implement a robust architecture that leverages blockchain's decentralized nature and cryptographic algorithms to ensure transparent and secure access to IoT devices within the smart home ecosystem.

Our approach will involve the utilization of the blockchain as a distributed and immutable ledger to store access control data and device interactions. Each device within the smart home network will have a unique identifier, and access permissions will be managed through a distributed consensus mechanism. This will ensure that only authorized individuals can interact with the IoT devices, providing enhanced security and privacy.

To enable seamless integration between the blockchain and the IoT devices, we will develop a lightweight and efficient communication protocol. This protocol will facilitate secure data transfer and device authentication, enabling smooth interaction between the smart home ecosystem and external entities such as mobile applications or voice assistants.

Challenges

Implementing a blockchain-based access control system for smart homes poses several challenges. Ensuring scalability and efficiency in handling a large number of IoT devices and user interactions is crucial. The system needs to manage data storage and processing requirements while maintaining acceptable performance levels.

Interoperability among various IoT devices and platforms is another challenge. Smart homes often consist of devices from different manufacturers, requiring seamless integration and communication. Supporting a wide range of IoT protocols and standards is necessary to accommodate diverse device types.

Maintaining the security of the blockchain network is vital. Protecting against potential attacks, such as 51% attacks and malicious nodes, requires robust cryptographic mechanisms and continuous monitoring.

User experience and ease of use are critical factors for smart home adoption. Designing a user-friendly interface that enables homeowners to manage access permissions, monitor device interactions, and configure the system effortlessly is essential.

Addressing these challenges will be key to the successful implementation of the proposed work, ensuring a secure and efficient access control system for smart homes while enhancing the overall user experience.

Conclusion

In conclusion, this research project explores the integration of blockchain technology with smart homes and the Internet of Things (IoT) to develop a secure and transparent access control system. By leveraging the decentralized nature of blockchain and the convenience of IoT devices, the proposed solution aims to enhance user privacy, strengthen security measures, and provide a seamless user experience when interacting with smart home technologies. The related work and proposed architecture highlight the potential benefits and challenges in implementing such a system. Overcoming scalability, interoperability, security, and user experience challenges will be crucial for successful adoption. This work contributes to the advancement of blockchain-based solutions for smart homes, paving the way for a more secure and efficient IoT ecosystem in residential environments.

REFERENCES

1. https://doi.org/10.48550/arXiv.2001.01837
2. Y. Zhang, S. Kasahara, Y. Shen, X. Jiang and J. Wan, "Smart Contract-Based Access Control for the Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594-1605, April 2019, doi: 10.1109/JIOT.2018.2847705.
3. Q. Yang and H. Wang, "Privacy-Preserving Transactive Energy Management for IoT-Aided Smart Homes via Blockchain," in IEEE Internet of Things Journal, vol. 8, no. 14, pp. 11463-11475, 15 July15, 2021, doi: 10.1109/JIOT.2021.3051323.
4. C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar and K. -K. R. Choo, "HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes," in IEEE Internet of Things Journal, vol. 7, no. 2, pp. 818-829, Feb. 2020, doi: 10.1109/JIOT.2019.2944400.
5. H. Su, B. Guo, Y. Shen and X. Suo, "Embedding Smart Contract in Blockchain Transactions to Improve Flexibility for the IoT," in IEEE Internet of Things Journal, vol. 9, no. 19, pp. 19073-19085, 1 Oct.1, 2022, doi: 10.1109/JIOT.2022.3163582.
6. J. Yang and L. Sun, "A Comprehensive Survey of Security Issues of Smart Home System: “Spear” and “Shields,” Theory and Practice," in IEEE Access, vol. 10, pp. 124167-124192, 2022, doi: 10.1109/ACCESS.2022.3224806.
7. Farooq, M.S.; Khan, S.; Rehman, A.; Abbas, S.; Khan, M.A.; Hwang, S.O. Blockchain-Based Smart Home Networks Security Empowered with Fused Machine Learning. Sensors 2022, 22, 4522. https://doi.org/10.3390/s22124522
8. M. A. Khan et al., "A Machine Learning Approach for Blockchain-Based Smart Home Networks Security," in IEEE Network, vol. 35, no. 3, pp. 223-229, May/June 2021, doi: 10.1109/MNET.011.2000514.
9. https://www.hindawi.com/journals/wcmc/2022/4393314/#copyright

10. H. -N. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076-8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.
11. https://arxiv.org/ftp/arxiv/papers/1608/1608.05187.pdf