International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

Blockchain-Driven Security Framework for IoT-Based Home Security Systems: A Comprehensive Case Study

Nalini Tiwari
(Research Scholar)
Dr. Sonal Singla (Associate Professor)
(Research Supervisor)
Glocal School of Technology and Computer Science

ABSTRACT

IoT is a digital network that connects common physical objects. Including smartphones, sensors and various devices. This makes it possible to collect and share information over the internet. The emergence of the Internet of Things (IoT) in smart homes has changed personal security. By providing comfort automation and real-time monitoring. However, these technical improvements include cyber security concerns such as hacking, data breaches, and unauthorized access This is increasingly being threatened by IoT-based home security systems that rely on network-connected devices. This leaves them vulnerable to attack if there is insufficient security. This paper examines the use of blockchain technology in IoT-powered home security systems, presenting a decentralized security framework that improves privacy, integrity, and accuracy of communications. Provides detailed case studies to demonstrate how blockchain can alleviate security issues in smart homes. Including system improvements, stability, data protection. Emphasize the ability to do and strengthen resistance to cyberattacks.

Keywords: Blockchain Security; Internet of Things; Home Security; Data Integrity

1. INTRODUCTION

The Internet of Things (IoT) is comprised of devices that generate, evaluate, and convey massive volumes of vital security and safety data. in addition to personally identifiable information For this reason, they are susceptible to a wide range of cyberattacks, such as those targeting the Internet of Things (IoT) and new Foldable and energy efficient, the majority of

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

network equipment Application tasks should take up the majority of these devices' power and processing resources. Because of this, guaranteeing privacy and security at a reasonable cost is a formidable obstacle. While considering to computing and power usage, traditional Internet of Things security methods might be pricey at times. Furthermore, a large number of cutting-edge security frameworks prioritize Because of the problems with scalability, it is not suited for the Internet of Things. Various models for connection Isolation of a critical component (Al-Turkistani and Alsa'wi) , 2020)

Decentralized ledger technology (BC) blockchain provides a formidable answer to these security concerns. Blockchain guarantees the integrity of data exchanged between IoT devices by facilitating secure, transparent, and irreversible transactions (Khan et al., 2020). This paper examines the possibility of integrating block technology. Chain joins IoT-based home security systems by offering a blockchain-powered security architecture. It is designed to reduce the risk of cyberattacks. Improve system flexibility and protect the privacy and integrity of sensitive information.

2. LITERATURE REVIEW

This table provides a comprehensive summary of the various studies. About integrating blockchain with IoT to enhance security in home security systems These studies address a variety of concerns. From IoT vulnerabilities to blockchain's potential to secure IoT environments.

Table 1: A comprehensive summary of various studies

Author and Year	Methodology	Key Findings
Madakam et al. (2015)	Systematic review of academic publications, business white papers, expert forums, and internet databases	Provides an overview of IoT, architecture, and required technologies. He highlighted the role of IoT in transforming physical objects into intelligent virtual entities. and emphasizes its use in daily life
Khan and Salah (2017)	Survey and evaluation of IoT security concerns, analysis of	Critical security vulnerabilities have been found in IoT devices due to their

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

	IoT layered architecture, and protocols	processing capabilities. Storage space and IoT-constrained networks explore blockchain as a potential solution to security challenges.
Yu et al. (2018)	Examination of security and privacy concerns, framework development for IoT and blockchain integration	Proposed a framework integrating blockchain with IoT to enhance security and privacy. Demonstrated how blockchain could solve IoT security challenges such as authentication, decentralized payment, and scalability using Ethereum.
Hui et al. (2019)	Review of blockchain technologies and their applications in IoT security	Analysis of blockchain's potential in solving IoT data security problems, focusing on addressing challenges such as large scale IoT devices, heterogeneous networks, and limited computing resources through blockchain integration.
Atlam et al. (2020)	Analysis of IoT and blockchain integration, discussion of blockchain's advantages for IoT	It explains in detail how to use blockchain technology with the Internet of Things to solve problems like accurate information, privacy, transparency, and security. Internet of Things (IoT) blockchain service introduction and exploring the impact of AI on IoT and blockchain.

Research Gap

Although current research addresses the theoretical benefits of blockchain in improving IoT security, it lacks insights into its scalability, performance, and practical applications in smart home settings. This article attempts to address this gap by presenting a detailed case study that addresses technical and practical issues.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

3. METHODOLOGY

A case study was undertaken to illustrate the possibilities of blockchain-based security frameworks for IoT home security systems, focusing on the integration of blockchain inside a conventional smart home setting. The solution included many IoT devices, such as cameras, motion detectors, and smart locks, all linked to a blockchain network.

A Case study

Figure 1: Blockchain based architecture

- Security Analysis

Any security architecture must fulfill three primary requirements: The three pillars of CIA are availability, security, and integrity. By design, confidential communications may only be accessed by those with the proper authorization. Each service or piece of data must be available to the user at all times, and integrity makes sure that the message gets there unmodified. To meet the first two requirements, the methods are detailed in Section III. Protecting smart home equipment from malicious queries improves their accessibility. This is achieved by ensuring that only entities who were every computer has generated a shared key are allowed to complete permitted transactions. (Meng et al., 2018).

- Performance Evaluation

To improve security and safety, a BC-based architecture makes smart home gadgets and miners pay more computationally and in packets. An alternative scenario was developed to assess the overhead of the blockchain-based system. This scenario handles transactions independently of

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

blockchain technology, which includes hashing, and encryption. We call this starting point strategy a " foundation method."

Smart safety systems for homes that include blockchain-based components have successfully reduced a number of security risks. The decentralized architecture of blockchain mitigates the danger of data leaks and assaults on a central server. Authentication measures guaranteed that only authorized devices may engage with the system, hence prohibiting unauthorized access. The use of smart contracts automates the execution of security measures, enhancing the system's efficiency and responsiveness.

B. Core Components

- Transactions

A transaction is a dialogue between two or more local devices or overlaid units. The intelligent house in British Columbia is structured with many transactions that serve certain purposes. Devices that store data generate transactions that take place. The house owner or service provider initiates an access activity for receiving data from the cloud (Khvoynitskaya, 2020). In order to routinely evaluate device data, homeowners or contractors might conduct an eye transaction. Genesis transactions allow for the addition of new smart home appliances, while removal transactions allow for the removal of existing ones. To guarantee confidential communication, all of the aforementioned transactions employ a common key that is shared. If the contents of transactions are modified while they are being sent, ultralight hashing can detect this. A private digital ledger in the area records all operations that enter or exit the smart house.

- Local BC

There is a policy header in every smart home's local secret blockchain that controls user permissions for any transaction, both incoming and outgoing. This blockchain keeps tabs on every transaction that takes place. Each device's operations are interconnected as a fixed record within the chain of transactions, starting with the genesis action. A section opener and a rules opener are both included in each part of a local BC. To make assured the blockchain can't be changed, this hash of the preceding block is in this block's header. Device identification and the enforcement of proprietor control rules for resident devices are both handled by the regulations footer.. (Li et al., 2020).

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

- Home miner

Any time money enters or leaves a smart home, a gadget called a "smart home miner" handles it all. A miner's residence's internet gateway is one possible connection point. Alternately, you might connect it to your home gateway using a separate device, such as F-Secure. Similar to the modern central security systems. Transactions are validated, approved, and verified again by miners. Additionally, miners are responsible for something else: Create first purchases. Update and give keys Rearrange the financial dealings Form and oversee teams.

- Local Storage

Devices often use local storage, which is a kind of storage media like a spare drive, to keep data close at hand. Depending on the situation, the storage might be included within the miner or used separately. Each device's data is organized as a ledger connected to the device's origin in the storage, which uses a First-in-First-out (FIFO) mechanism to provide information preservation.

4. CONCLUSION

The security of IoT is now receiving significant interest from both academic and industrial sectors. Current security solutions may not be appropriate for IoT because of significant energy consumption and processing demands. Despite existing obstacles, like scalability and energy consumption, the prospective advantages of blockchain in IoT security render it a significant technology for the future of smart homes. As technology advances, blockchain is expected to assume a progressively vital part in the establishment of safe and dependable IoT-based systems. Future research may concentrate on enhancing blockchain performance in IoT settings, investigating hybrid consensus methods, and doing further case studies to assess the practical use of blockchain in smart homes.

International Journal of Research in IT and Management (IJRIM)
Available online at: http://euroasiapub.org
Vol. 12 Issue 12, December- 2022
ISSN(o): 2231-4334 | ISSN(p): 2349-6517 | Impact Factor: 8.106

References

1. Al-Turkistani, H., & AlSa'awi, N., 2020. Poster: Combination of Blockchains to Secure Smart Home IoT. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), pp. 261-262.

2. Hui, H., An, X., Wang, H., Ju, W., Yang, H., Gao, H., & Lin, F. (2019). Survey on blockchain for IoT. Comput. Commun., 136, 10-29.

3. Khan, M., & Salah, K. (2017). IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst., 82, 395-411.

4. Khan, M.A.; Abbas, S.; Rehman, A.; Saeed, Y.; Zeb, A.; Uddin, M.I.; Nasser, N.; Ali, A. A machine learning approach for blockchain-based smart home networks security. *IEEE Netw.* 2020, *35*, 223–229.
5. Khvoynitskaya, S. The History and Future of the IoT. 2020.
6. Li, X., Jiang, P., Chen, T., Wang, L., & Wen, Q. (2020). A survey on the security of blockchain systems. Future Generation Computer Systems.

7. Madakam, S., Ramaswamy, R., & Tripathi, S., 2015. IoT: A Literature Review. Journal of Computational Chemistry, 3, pp. 164-173.
8. Madakam, S., Ramaswamy, R., & Tripathi, S., 2015. IoT: A Literature Review. Journal of Computational Chemistry, 3, pp. 164-173.

9. Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *IEEE Wirel. Commun.* 2018, *25*, 53–59.

10. Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the IoT. IEEE Wireless Communications, 25, 12-18.