International Journal in Commerce, IT and Social Sciences
Volume 10 Issue 10 Oct 2023 ISSN: 2394-5702 Impact Factor: 6.973
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

Strengthening IoT Security in Smart Homes: Integrating Blockchain for Enhanced Protection

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

ABSTRACT

IoT protocols are critical to enabling communication between components. These protocols enable simultaneous communication between different devices and sensors. IoT protocols ensure that all communications between IoT devices occur within a secure environment. This paper explores the potential of blockchain technology to enhance IoT security by providing a decentralized framework immutable and transparency for communication security Authentication and data integrity in smart homes Using blockchain technology within IoT to analyze branch expansion. The challenges that arise Focusing on security, a blockchain-based smart home framework is also being developed. The results indicate that blockchain integration significantly improves the security of smart homes. Increased resilience to cyberattacks and protect the integrity of user data.

Keywords: Internet of Things Security; Blockchain; Smart Home; Protection

1. INTRODUCTION

“The Internet of Things (IoT)” is a system of interrelated nodes that can exchange data and coordinate their actions with little intervention from a person. Internet of Things (IoT) technology is becoming standard in smart houses. Controls for thermostats, security cameras, and other devices may be integrated. Electrical devices and the lighting system In order to better manage energy, access, and efficiency The widespread use of these type of IoT devices is quite concerning from a security perspective. A lot of the time, the processing power of IoT devices is rather low. thereby leaving it open to assault, data leak, and unauthorized access Hackers may easily take advantage of smart home installations by taking advantage of registration, connection, or information storage flaws. The need for efficient security measures is growing in tandem with the number of IoT devices. (Hassan, 2019).

Increased security breaches Illegal access to information and privacy violations resulting from the integration of IoT devices into smart homes. Despite the benefits and features IoT offers, these devices often lack adequate authentication methods. Insecure communication channels and lack of real-time monitoring Traditional security solutions such as firewalls and encryption are insufficient to address the unique challenges presented by IoT networks (Li et al., 2020), and there is an urgent need for secure, scalable, and more strong To protect smart homes from advanced cyber threats Improving IoT security in smart homes is important to protect user privacy. Prevent data theft and guarantee the reliability of the linked devices. Possible answers to these problems

- To assess the current security challenges faced by IoT devices in smart homes.
- To investigate how blockchain might mitigate IoT security risks, including device authentication, data integrity, and secure communication.
- To propose a blockchain-based framework for IoT security in smart homes.

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**
Granjal et al. (2015)	Systematic review of communication protocols and security methods in IoT	IoT sees a future of widespread collaboration between users, systems, and devices, which requires secure communication. For IoT, IP-based communications are essential. But security

		methods for these communications have not yet been developed.
Payne and Abegaz (2018)	Review of best practices, IoT security incidents, and proposed security frameworks	IoT introduces a wide variety of devices into IP networks, which require improved security protocols. A framework is proposed for secure IoT deployment in residential and commercial networks. It highlights specific examples of cyberattacks.
Cynthia et al. (2018)	Review of IoT protocols and security measures.	IoT's rapid growth necessitates securing networks and data across various industries. Identified a lack of standardization at the manufacturing level, creating vulnerabilities in hardware, software, and data.
Benkhelifa et al. (2018)	Analysis of intrusion detection systems (IDS) and proposed developments	Highlighted challenges in IoT security due to resource constraints and diverse network protocols. Suggested improvements in intrusion detection systems (IDS), emphasizing the inadequacy of current systems in covering the IoT landscape.

The current research highlights substantial security deficiencies in IoT systems, including insufficient security protocols for IP-based communication, vulnerabilities arising from a lack of manufacturing standards, and poor intrusion detection systems. These challenges emphasize the need for a more comprehensive security solution. The integration of blockchain with IoT enhances security by offering decentralized, immutable, and secure mechanisms for communication, authentication, and data integrity, therefore eliminating the weaknesses present in existing IoT security frameworks.

3. METHODOLOGY

In a smart home, intelligent devices may interconnect directly to exchange data for the provision of certain services. The experimental design technique of the study will be as follows:

the detailed operational model of the study project, focussing on the model's architecture and the associated workflow (Marwala and Xing, 2018). Constructed an ARM (Advanced RISC Machine)-based smart home for demonstration purposes. Selected smart home gadgets due to their ARM-based architecture. used economical ARM CPUs with limited computational capabilities (Panarello et al., 2018; Hezam et al., 2020).

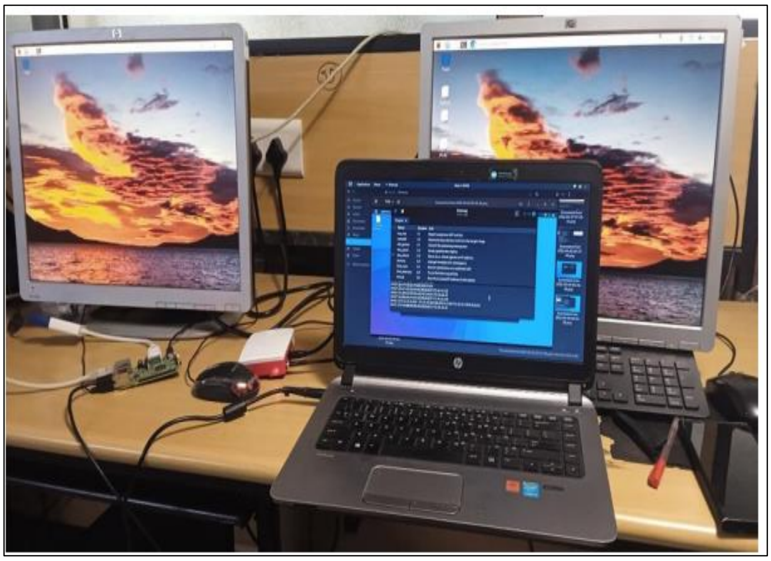


Figure 1: **Experimental Setup**

3.1 **Experiment Components**

- Raspberry Pi (Model-3B)
- Raspberry Pi (Model-4)
- Raspbian OS

4. Machine with Kali Linux

- Ethereum- Ethereum is a distributed, open-source blockchain that supports smart contracts and decentralized governance.

A. **DoS attack on Smart Home Network without Blockchain**

The researcher must assess all logs inside the network's log file. The field delineates the source IP address, destination IP address, source MAC address, destination MAC address, port number, packet, byte, message, and annotations. During a DoS attack on the network, the source ID transmits incessant flooding requests to the destination ID.

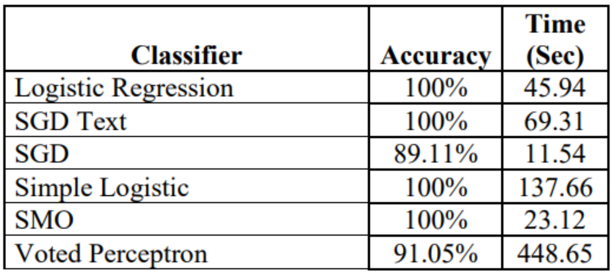
B. **DoS attack on Smart Home Network with Blockchain**

The binary classification outcomes of Logistic Regression, SGD Text, SGD (Stochastic Gradient Descent), Simple Logistic, Sequential Minimal Optimisation, and Voted Perceptron classifiers.

4. RESULT ANALYSIS AND DISCUSSION

A. Result of **DoS attack on Smart Home Network without Blockchain**

Table 2: Results Classification

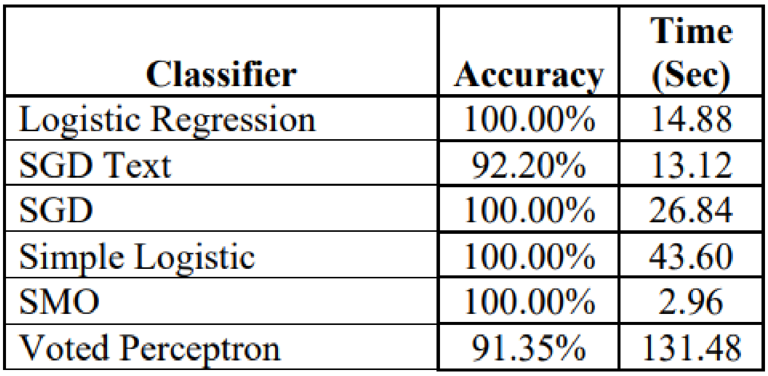


Classifier	Accuracy	Time (Sec)
Logistic Regression	100%	45.94
SGD Text	100%	69.31
SGD	89.11%	11.54
Simple Logistic	100%	137.66
SMO	100%	23.12
Voted Perceptron	91.05%	448.65

The study determined the number of attacks in that file via a machine-learning categorisation method derived from the log. This categorisation approach divides the data into two classifications: assaults and non-attacks. This classification considers many approaches, including the voted perceptron, logistic regression, SGD text, SGD, basic logistic, and SMO (Sequential Minimal Optimization). Utilising our machine-learning categorisation method, this study successfully identified a greater number of attacks occurring inside the network. The machine learning system—Logistic Regression, SGD Text, Simple Logistic, and SMO—achieves a detection accuracy of 100%, although SGD and Voted Perceptron attain accuracies of 89.11% and 91.05%, respectively. SMO attained flawless accuracy in 23.12 seconds, whereas Logistic Regression, SGD Text, and Simple Logistic accomplished it in 45.94, 69.31, and 137.66 seconds, respectively. SGD and Voted Perceptron recorded durations of 11.54 and 448.65 seconds, respectively, to attain accuracies of 89.11% and 91.05%. Consequently, based on the categorisation, study may affirm that the SMO is the superior algorithm regarding accuracy and model-building processes.

B. Result of DoS attack on Smart Home Network with Blockchain

Table 3: Result classification



Classifier	Accuracy	Time (Sec)
Logistic Regression	100.00%	14.88
SGD Text	92.20%	13.12
SGD	100.00%	26.84
Simple Logistic	100.00%	43.60
SMO	100.00%	2.96
Voted Perceptron	91.35%	131.48

Logistic regression, SGD, simple logistic, and sequential minimal optimisation attained optimal accuracy, achieving 100% in 14.88, 26.84, 43.60, and 2.96 seconds, whereas SGD text and voted perceptron recorded accuracies of 92.20% and 91.35% in 13.12 and 131.48 seconds, respectively. This accuracy pertains to non-attack transactions, whilst the others constitute attack transactions. Furthermore, the findings indicate that the SGD has attained exceptional outcomes regarding accuracy and the model development process, which will result in enhanced performance.

The study has classified transactions into attack and non-attack categories for smart home network security, both in the absence of blockchain technology and in the presence of blockchain technology for attack transactions. The frequency of assault transactions decreased subsequent to the implementation of blockchain technology. This signifies that proposed strategy is to enhance security.

5. CONCLUSION

This study employs a scenario for the security of smart home networks. This study have examined numerous kind of DDoS attacks, along with their corresponding reactions and pathways. Thesis have used blockchain technology, with SHA-256, BASH-64, and filtering, in the realm of smart home network security. This study have enhanced the security of smart homes via the use of these methods. To substantiate that our methodology yields superior outcomes compared to current methods, researchers used machine learning-based categorisation and conducted a comparative analysis of transaction, mining, and chaining durations inside blockchain technology. Consequently, the proposed security strategy enhances the existing one. The proposed strategy enhances security more effectively than existing methods.

References

1. Benkhelifa, E., Welsh, T., & Hamouda, W., 2018. A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. IEEE Communications Surveys & Tutorials, 20, pp. 3496-3509.
2. Cynthia, J., Sultana, H., Saroja, M., & Senthil, J., 2018. Security Protocols for IoT. Studies in Big Data.
3. Granjal, J., Monteiro, E., & Silva, J., 2015. Security for the IoT: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials, 17, pp. 1294-1312.
4. Hassan, W.H. Current research on IoT security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
5. Hezam, A., Konstantas, D., & Nijdam, N., 2020. A Novel Methodology for Securing IoT Objects Based on their Security Level Certificates.
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. Marwala, T.; Xing, B. Blockchain and artificial intelligence. *arXiv* **2018**, arXiv:1802.04451.
8. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and iot integration: A systematic survey. *Sensors* **2018**, *18*, 2575.

9. Payne, B., & Abegaz, T., 2018. Securing the IoT: Best Practices for Deploying IoT Devices.pp. 493-506.

10. Tanwar, S., 2018. Blockchain Technology. Blockchain Regulation and Governance in Europe.