Proceedings of the 2nd International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/96/20241332

# Enhancing Smart Home Security and Privacy: Integrating Blockchain and Machine Learning

**Jianwen Sheng**

Northeastern University at Qinhuangdao, Qinhuangdao, 066004, China

1093599303@qq.com

**Abstract.** A smart home is a type of home device connected through the Internet of Things (IoT) technology. With the rapid development of IoT applied to smart homes, this brings great convenience to people and also raises some privacy and security issues. As IoT collects privacy and a large amount of data about users that may be stolen by unscrupulous people through some cyberattacks, people are beginning to pay more and more attention to the security of the smart home. Blockchain is a distributed database technology that stores data in the form of blocks and uses cryptographic methods to ensure the security and integrity of the data. And mechanical learning can detect some network attacks. This study proposes a smart home architecture that integrates blockchain technology and mechanical learning. Combining blockchain technology, machine learning, and smart homes can effectively identify some cyber attacks while ensuring privacy and security so that people can take appropriate measures.

**Keywords:** Data Encryption, Privacy Protection, The Internet of Things, Blockchain.

## 1. Introduction

In recent years, the Internet has been growing rapidly, and the number of Internet users has been increasing exponentially every year. With the increasing demand of users, the Internet of Things (IoT) has also started to develop gradually. The term "Internet of Things" (IoT) was first coined by Kevin Ashton in 1999 [1]. IoT is a technology that enables networks and multiple devices to connect with each other. Currently, IoT technology is now deployed in highly critical areas such as space technology, healthcare, and smart cities [2]. Therefore, security of IoT devices is a critical issue that we are now facing. Smart home is an application based on IoT that intelligently controls and manages household devices and other devices by using advanced information technology. Therefore, the smart home system will also be affected by the security of IoT devices. But smart homes will also face external network attacks while bringing convenience to people's lives. These attacks may lead to the leakage of users' personal privacy, home network security, and other problems.

In this paper, we try to propose an architecture that combines blockchain technology and mechanical learning to protect the security of smart homes. Blockchain technology provides a secure and transparent way to store and share data [3]. Machine learning methods can identify attack patterns based on trained data and can make effective predictions. This will help people to take timely countermeasures to protect the security of smart home systems [2]. The combination of blockchain technology and machine learning has the potential to greatly improve the security of smart homes.

DOI: 10.54254/2755-2721/96/20241332

## 2. Overview of relevant technologies

### *2.1. Blockchain and smart contracts*

Blockchain is a distributed database technology that uses cryptographic techniques to guarantee the security and integrity of data while storing it in blocks. Every block has a fixed quantity of transaction data and is cryptographically connected to the one before it to create a chain that keeps becoming longer. This design makes it impossible for data to be tampered with in the network, as any attempt to modify the data in a block would disrupt the continuity of the entire chain. Blockchain technology is a distributed ledger technology that provides a new solution for the security and data privacy protection of Internet of Things (IoT) devices with its transparency, immutability, and decentralization [4]. Smart contracts are the core technology of blockchain. It runs on the blockchain and must fulfill specific conditions or rules when executed. In the smart home sector, the integration of blockchain technology provides a secure and reliable control mechanism for device interactions in home automation systems in the form of smart contracts. Smart contracts are computer codes that automatically enforce the terms of a contract and can ensure that interactions between devices comply with preset rules and permissions, thus effectively preventing unauthorized access and data leakage [5].

### *2.2. Machine learning*

A subfield of computer science and artificial intelligence known as "machine learning" is concerned with using data and algorithms to simulate human learning processes and progressively increase their accuracy. The application of machine learning technology in the smart home industry is expanding, since it mimics the cognitive and learning functions of the human brain to make smart home systems more automated and intelligent [6].

In addition, machine learning technology plays an important role in improving the security of smart home systems. Smart home systems contain many connected devices that can be targets of cyber attacks. Machine learning algorithms can prevent potential security threats by monitoring network traffic and user behaviour and identifying unusual patterns [2].

### *2.3. Internet of things in the smart homes*

Through the provision of automated and intelligent home services, the smart home industry's use of Internet of Things (IoT) technology is progressively altering people's lifestyles and improving living comfort and ease. The capacity to connect devices, such smart door locks, smart outlets, and lightbulbs, to one another, gather data from sensors, and analyze that data intelligently to provide real-time home environment monitoring and control, is the foundation of Internet of Things technology. The use of IoT technology in smart home systems encompasses several areas, such as data management, remote control, lighting control, air conditioning system control, and security system control, among others.

These technologies are made to make things easier for users to use, boost automation and control over home gadgets, improve security, and enhance usefulness. For example, through IoT technology, users can remotely monitor and regulate the temperature, lighting, and security systems in their homes for efficient management and optimal use of energy [7].

## 3. Common types of network attacks in smart homes and their impacts

While smart home systems provide convenience, they also face a variety of cybersecurity threats. Examples include the security threats of unencrypted inter-device transactions and password cracking, both of which can lead to serious privacy breaches and loss of device control. When data transfers between devices are not encrypted, this information becomes vulnerable to interception and tampering. Attackers can exploit these vulnerabilities to listen in on communications between devices, access sensitive information, and even forge transactions. For example, they may intercept a user's personal data, home surveillance video, or smart lock unlock commands. Password cracking is another common means of attack. Once attackers succeed in cracking passwords, they are able to take full control of these

DOI: 10.54254/2755-2721/96/20241332

devices. This not only violates the user's privacy, but can also lead to property damage or broader security concerns [8].

Regarding data privacy and security, smart home systems, due to their nature as IoT devices, need to communicate with external entities in order to provide services, which makes them vulnerable to malicious attacks. Some home device firmware is regularly updated via the cloud, which provides an opportunity for attackers to obtain a copy of the firmware, reverse engineer it, and take control of USB ports.

In terms of data privacy, smart home devices may collect data without the user's knowledge, which can be stolen by some unscrupulous individuals. Also, smart homes are exposed to a variety of cybersecurity threats. For example, Adversarial Machine Learning (AML) attack is a kind of attack that exploits the vulnerability of machine learning models, including white-box, black-box, and grey-box attacks. In a white-box attack, the attacker understands the internal structure of the model and the training data and is able to design input samples that mislead the model. Black-box attacks, on the other hand, do not require knowledge of the model's internals and infer model behaviour by observing the output. Grey-box attacks fall somewhere in between, where the attacker has some knowledge of the model but it may be incomplete. These attacks may result in the smart home's security system being bypassed, causing security risks. In addition to AML attacks, smart homes may also be subject to Denial of Service (DoS) attacks, which overload the device or network resources by sending a large number of requests, leading to system paralysis, affecting the user's control of the smart device, and even threatening the home's security. MAC/ARP spoofing attacks are, on the other hand, interception or tampering with network traffic by spoofing the network requests, compromising user privacy, or conducting further attacks. Man-in-the-middle (MITM) attacks pose a threat to data confidentiality and integrity by intercepting and modifying communications between devices, where attackers can gain access to sensitive information or control [9].

## 4. Smart home architecture design based on blockchain and machine learning

In order to improve data security and data privacy in smart homes, after reviewing some papers and information, this paper tries to propose an architecture that combines blockchain and machine learning applied to smart homes. The architecture basically consists of three parts, which are the smart home device layer, the blockchain-based P2P (Peer to Peer) network layer, and the cloud data storage layer. Meanwhile, mechanical learning models are deployed in the network layer and cloud data storage layer to improve the security of smart homes.

The Smart Home Device Layer is primarily made up of a variety of IoT devices, such as sensors, cameras, actuators, and other gadgets that gather information from the outside environment, send it to the other components of the system, and carry out operations that make up the device layer of the IoT system architecture. Before being used for decision-making or additional analysis, the frequently disorganized and unprocessed data gathered in this layer may need to be processed or examined. In addition, this layer might be equipped with state-of-the-art technology to handle data locally before forwarding it to higher layers [10].

Blockchain-based P2P Network Layer: the infrastructure required to support data transfer and other basic communications throughout the application is provided by the network layer. Wi-fi, bluetooth, cellular networks, and other communication technologies are some of the elements of the network layer. In this layer there are smart contracts; devices such as laptops or smartphones are nodes of the private blockchain. All nodes are required to execute smart contracts, and these nodes need to be authenticated when controlling access. Also for data security, different types of machine learning models like Support Vector Machine (SVM), Random Forest, Neural Networks etc. can be used for intrusion detection and anomalous behaviour identification. And adding machine learning nodes for double authentication.

The cloud data storage layer is mainly responsible for data storage and data processing. When deploying the smart home architecture, a reliable cloud database should be selected to store the data of the IoT devices and use cloud computing for further processing and analysis of the data. In order to ensure the security of the smart home, a mechanical learning model is added to the cloud storage layer,

DOI: 10.54254/2755-2721/96/20241332

and by deploying the trained model in the cloud, it can analyze the data transmitted from the smart home devices in real time and respond quickly to possible security threats.

## 5. Assessment and analysis

Some security evaluations of hypothetical architectures have been conducted to address some of the common cyber-attacks and threats in smart homes. For example, some password cracking attacks, AML attacks, Dos attacks, etc. The countermeasures for these attacks are listed below.

Password Cracking Attacks: the designed smart home architecture communicates with each other through a private blockchain platform where only authenticated devices are allowed to communicate with each other and each device needs to be individually authenticated. Even if an attacker cracks the password of one device, they will not be able to control other devices.

AML attacks: decentralization of the blockchain through a combination of blockchain and machine learning means there is no single point of control, and AML attacks usually require an attacker to be able to access and manipulate a central server or cloud service [9]. so decentralization can provide protection for blockchain networks. At the same time, smart contracts can prevent unauthorized access, and mechanical learning based intrusion detection systems can learn and identify anomalous patterns in network traffic to detect and prevent AML attacks.

Attacks such as Dos, MAC/ARP, and MITM: in Dos attack, the attacker sends a large number of requests; in MAC/ARP attacks, the attacker spoofs MAC addresses or ARP requests to spoof other devices, and MITM attack intercept the communication between modified devices and disguises them as legitimate devices. However, none of these illegal requests will be verified due to the need to pass smart contracts during the verification process. Meanwhile, the mechanically learned monitoring system is able to detect and prevent these attacks by learning and identifying anomalous patterns in network traffic.

Blockchain's immutability and its unique cryptographic properties can protect smart home data. Combining it with mechanical learning can be more effective in detecting and predicting some network attacks, leading to an adaptive security defence. The combination of the two can effectively improve the privacy and security of smart homes.

## 6. Conclusion

Smart home serves as a platform for integrating devices related to home life, enabling the establishment of a centralized and intelligently controlled residential facility management system that enhances convenience and comfort within households. In this study, the researcher discusses the concept of smart homes along with their susceptibility to common cyber threats. Additionally, the paper also proposes an innovative framework that combines blockchain technology and machine learning techniques to improve the security of smart homes. Blockchain, a distributed database technology that stores data in blocks and uses cryptographic methods to keep the data secure, is employed alongside machine learning algorithms capable of detecting anomalous patterns in networks traffic and user behavior to protectively prevent potential security breaches. By combining blockchain and machine learning, it become feasible to ensure privacy and security while also effectively identifying some cyber-attacks so that users can take appropriate measures.

In order to evaluate the feasibility of the proposed architecture, this paper has evaluated some common cyber-attacks and spoofing attacks. Through analyzing them, the designed architecture in this paper demonstrates the ability to resist and prevent common attacks by providing effective preventive measures. Moving forward, the researchers could aim to implement and test the proposed new system design in order to test the identified security requirements in IoT smart home devices and try to apply this architecture in other domains such as smart health, smart city, etc. to improve data privacy for all.

DOI: 10.54254/2755-2721/96/20241332

## References

[1] Butun, I., Österberg, P., & Song, H. (2020). Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644. https://doi.org/10.1109/COMST.2019.2953364

[2] P. K., K. M., & S. M. V. (2021). Attack and Anomaly Prediction in IoT Networks using Machine Learning Approaches. In 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT) (pp. 1-6). Erode, India. https://doi.org/10.1109/ICECCT52121.2021.9616794

[3] Almasoud, A. S. (2023). Blockchain-Based Secure Storage and Sharing of Medical Data Using Machine Learning. In 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS) (pp. 979-8-3503-1890-6/23/$31.00). IEEE. https://doi.org/10.1109/SNAMS60348.2023.10375435

[4] Arif, S., Khan, M. A., Rehman, S. U. R., Kabir, M. A., & Imran, M. (2020). Investigating Smart Home Security: Is Blockchain the Answer? IEEE Access, 8, 117802-117816. https://doi.org/10.1109/ACCESS.2020.3004662

[5] Al Oliwi, H. H., Al Husain, Z., & Rafeh, R. (2021). Integrating Blockchain and Internet of Things for Smart Homes. 2021 Computing, Communications and IoT Applications (ComComAp). https://doi.org/10.1109/COMCOMAP53641.2021.9652936

[6] Zhang, jiasheng (2023). Research on Smart Home System Based on Machine Learning Methods. Master's thesis, ZheJiang A&F University.

[7] Zhao, Jie. (2024). The Design of Smart Home System Based on Internet of Things Technology. Toys World, (07), 169-171.

[8] Al-Turkistani, H. F., & AlSa'awi, N. K. (2020). Combination of Blockchains to Secure Smart Home Internet of Things. In 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH) (pp. 261-262). IEEE. https://doi.org/10.1109/SMART-TECH49988.2020.00069

[9] Sabra, A., Rmeiti, N., & Atieh, M. (2023). Using Machine Learning Techniques to Detect Cyberattacks in Smart Homes: A Survey. 2023 International Scientific Conference on Computer Science (COMSCI). IEEE. https://doi.org/10.1109/COMSCI59259.2023.10315831

[10] Gomathi, L., Mishra, A. K., & Tyagi, A. K. (2023). Blockchain and Machine Learning Empowered Internet of Things Applications: Current Issues, Challenges and Future Research Opportunities. In Proceedings of the 4th International Conference on Smart Electronics and Communication (ICOSEC) (pp. 637-647). Trichy, India. doi:10.1109/ICOSEC58147.2023.10276385