International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1293-1296 www.ijaem.net ISSN: 2395-5252

Blockchain for Iot Security and Privacy: Smart Home - A Review

Shivam Taneja, Ishita Rana, Shobha Tyagi

Date of Submission: 15-05-2023 Date of Acceptance: 30-05-2023

ABSTRACT: The safety and privacy of the Internet of Things (IoT) remains a major challenge, due to large widespread nature of IoT networks. Blockchain-based methods provide increased security and privacy, this paper provides a review of the main attributes and capabilities of Blockchain and how attacks can be performed on IoT devices at various network levels. Each smart home is equipped with a "miner," a high-performance device that stays online and handles all communications.

Keywords: IoT, Blockchain, Security, Smart Homes, Privacy

I. INTRODUCTION

Among all the data security and privacy tools available, the blockchain is the most efficient due to its architecture such as durability and retrieval. Blockchain is not compatible with data modification [1]. Tools in the Internet of Things (IoT) generate, process, and exchange a lot of valuable data as well as security dataand sensitive information, and that is why they are attractive targets for various cyber-attacks [2].Blockchain is a distributed, flexible ledger that enables recorded transactions and tracking of assets. In a blockchain network, virtually anything with value can be tracked and sold, reducing risk and reducing costs for all victims.

This paper provides an overview of the different attacks done to the OSI layer of network they are running on.

II. LITERATURE REVIEW

Traditional security methods are often more expensive in terms of IoT for power consumption and overhead processing. In addition, many high-level security frameworks are located in the same location and therefore do not qualify for IoT due to the complexity of the scale, multiple environments in one traffic, and one point of failure [3].

Blockchain employs a distinct and distributed structure, as well as cryptographic techniques, making it unique. Where information security and confidentiality are important to the network, blockchain technology is appealingme. In IoT, access control can be effectively achieved through blockchain [4].

The shared ledger provided by Blockchain to record Bitcoin transactions can be used to record any transaction and track the movement of any asset, whether physical, intangible, or digital. Blockchain, for example, allows securities to be resolved in minutes rather than days. It is also used to assist businesses in controlling the delivery of goods and related payments, as well as to allow manufacturers to share production logs with OEMs and regulators to reduce product memory.

Each node can receive or send a function to other nodes, and the data is synced as it travels across the network. Because it eliminates duplication of effort and eliminates the need for intermediaries, the blockchain network is expensive and efficient. And it is less dangerous because it verifies data using compatible models. Jobs are safe, secure, and guaranteed. Both transaction systems have the same participants. What is different now is that the work record is shared and accessible to all stakeholders.

The network of mobile devices, automobiles, household appliances, and other embedded electronic devices, software, sensors, and connections to allow them to connect and exchange data is called Internet of Things (IoT).

Today, blockchain technology is gaining the attention of researchers and scientists for a variety of reasons, including access control, data security, privacy, and wireless seg-mentation. While the blockchain offers a number of benefits such as peer-to-peer technology, anonymity, volume boost, and improved security, its consistent design is the main reason for its popularity. Due to its distributed nature, the blockchain can be used as an important technology to eliminate the role of a trusted third party within connected net-works. The most popular blockchain platforms are presented by IBM Blockchain, thereum, and multichain. An

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1293-1296 www.ijaem.net ISSN: 2395-5252

in-depth study of blockchain use cases will serve as a complex tool for researchers looking to conduct advanced research in the field of blockchain technology.

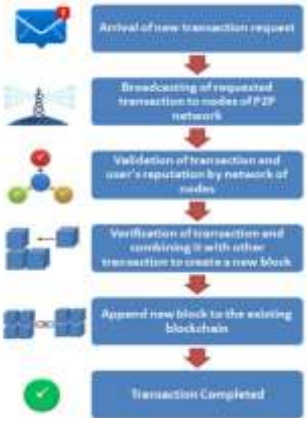

Figure 1. General Workflow of Blockchain

The IoT device should be safe and resistant to intrusion. Wormholes, Denial of Service (DoS) Attacks, and Spoofing, Altering, or Replaying Network Requests are the most common attacks and methods of network attacks against IoT devices.

Let's discuss about the different attacks on different network layers.

1. Physical layer - Jamming or tampering on IoT devices' physical layers can cause radio interference and exhaustion, which can result in the development of compromised nodes.
2. Data link layer - When two nodes transmit at the same time, a collision on the data link may result.
3. Network layer - Selective forwarding, sinkholes, wormholes, and spoofing of routing information can all affect the network level.
4. Transport layer - Generating new requests until the IoT device exhausts all of its resources, and de-synchronization causes flooding.
5. Application layer - Attackers can carry out harmful actions like changing the clock or data exaggerationby acting like regular users in the IoT systems.

III. METHODOLOGY

IoT research has exploded due to the growing number of communications and net-work technologies. Connecting to various smart devices online has many benefits, including data sharing, easy access, and remote monitoring.

IoT's centralized, client-server-based structure is one of the technology's most serious problems. The failure of the entire network can be caused by a lack of trust among participating devices, so a dependable solution is necessary to prevent this issue. In recent years, a number of strategies have been put forth, with blockchain rising to prominence due to its decentralized structure, security, and immutability.

This paper contributes by introducing Blockchain Home Server. Blockchain validates incoming data, builds new Blocks, and adds them to the distributed ledger when parsing it.

Let's discuss about the steps to implement security.

1. Custom home server or hub for all connected smart devices.
2. Adding layer of encryption by preventing communication between a smart device and the internet or between a smart device and the internet. The home server must be used for all communication.
3. Decentralizing the network by incorporating Blockchain Technology which introduces authentication, and extra layer of security because of a distributed ledger which keeps track of all requests to prevent any request made by the devices from being tampered with.

Figure 2. Overview of the proposed BC-based architecture discussed in more details in [6].

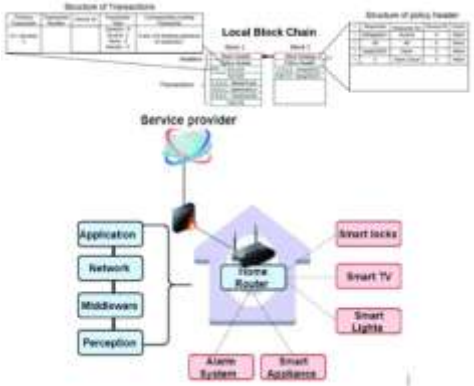

Figure 3. Smart Home Overview

Design security is provided by a number of factors, including: (1) indirect means of accessing devices; (2) various functional structures in a smart home and overlay. Symmetric

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 5 May 2023, pp: 1293-1296 www.ijaem.net ISSN: 2395-5252

encryption is used on smart home devices to achieve lightweight security. We have proposed a solution that involves a custom server, also known as a hub, a home server, a wired or wireless connection to a smart device, and the Blockchain technology to enhance the privacy, security, and access of smart devices.

The main smart home components as shown in the Figure 3 are as follows –

Transactions - Transactions are exchanges of information between nodes. There are several transactions in the smart home in BC, each of which has a particular function. Store transaction is generated by devices to store data. Lightweight hashing [9] is employed to detect any change in transactions' content during transmission. All transactions to or from the smart home are stored in a local private Blockchain (BC).

All of the data that smart devices send to their remote services will be intercepted and parsed by the server. By doing so, it is ensured that no device-related information is disclosed and that the package can be properly encrypted before being sent to the service.

Local Blockchain - There is a local private BC in each smart home that keeps track of all transactions. We are using Blockchain technology to track each network request made by the IoT device in order to intercept data being sent by the IoT device. Each device's exchanges are chained together as an immutable ledger in the BC starting with the genesis transaction.

As shown at the top of Figure 3, each block in the local BC has two headers: a block header and a policy header. To keep the BC immutable, the block header keeps the hash of the previous block. The policy header is used to authorize devices and enforce the owner's home control policy. The policy header has four parameters, as shown in the top right-hand corner of Figure 3.

To determine whether the data being transferred to the distributed ledger is accurate or not, we will use software like Wireshark to determine and sniff which device is sending a request to which server, along with that server's IP address and port.

Local Storage - A storage device used for local data storage, such as a backup drive, is known as local storage. To store data, the storage implements a First-in-First-Out (FIFO) method and stores each device's data as just a ledger chained to the device's starting point.

IV. RESULT AND DICSUSSION

There are three main security requirements that need to be considered by any security design, namely: Privacy, Integrity, and Accessibility, known as the CIA [8].

Confidentiality ensures that only authorized users can read the message. Integrity ensures that the sent message is received at your destination without any change, and availability means that each service or data is available to the user when needed.

Increasing the availability of smart devices protected from malicious programs. This is achieved by limiting the accepted functions in those businesses where each device has created a shared key. Overlay work is authorized by the miner before transferring it to de-vices.

Moreover, this paper contends that limiting direct internet requests can increase the security of smart devices. Requests should all go through the Blockchain interface for authentication, and if they are valid, they should be granted.The device may also be shielded by this interface from unauthorized access to the local network by outside parties.

Table 1. Security Requirement Evaluation

Requirement	Employed Safeguard
Confidentiality	Achieved using symmetric encryption.
Integrity	Hashing is employed to achieve integrity.
Availability	Achieved by limiting acceptable transactions by devices and the miner.
User control	Achieved by logging transactions in local BC.
Authorization	Achieved by using a policy header and shared keys.

V. CONCLUSION AND FUTURE SCOPE

In upcoming work, IPFS will be used to convert the data collected from IoT devices into cryptographic hashes, making it easy to store this data on a blockchain.

In order to add an additional layer of security protection for Internet communication, we also intend to implement a straightforward interface as a security gateway.

REFERENCES

[1]. Christidis, K., &Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4(1), 2292–2303.

[2]. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[3]. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.

[4]. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things. IEEE Access, 6(1), 32979–33001

[5]. Kumar, N. M., &Mallic, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132(1), 1815–1823 Hwang, D., Choi, J., & Kim, K. (2018). Dynamic access control scheme for IoT devices using blockchain.

[6]. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," arXiv preprint arXiv:1608.05187, 2016.

[7]. A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, Bitcoin and cryptocurrency technologies. Princeton University Pres, 2016.

[8]. N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and coun-termeasures," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933–1954, 2014.

[9]. A. Bogdanov, M. Knezevi ˇ c, G. Leander, D. Toz, K. Varıcı, and I. Ver- ´ bauwhede, spongent: A Lightweight Hash Function. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 312–325.