Blockchain based security in IoT

Al-Fareed, Department of Computer Applications and Data Science
Manipal Institute Of Technology, Manipal

Abstract

Blockchain is a cutting-edge technology that functions as a decentralised, distributed, public, and real-time ledger to hold transactions among Internet of Things (IoT) nodes. Every block in a blockchain is connected to the blocks before it. Every block contains its data, the previous block's hash, and the cryptographic hash code. The fundamental units utilised to transport data between Internet of Things nodes are transactions in the blockchain. The Internet of Things nodes are various forms of physical, intelligent devices with built-in sensors, actuators, and software that can communicate with other IoT nodes. The function of blockchain on the Internet of Things is to offer a method for processing safe data records through IoT nodes. Blockchain is a safe technology that is accessible to everyone. This type of technology is necessary for IoT to enable secure communication among IoT nodes in heterogeneous environments. Blockchain is being utilised within IoT to handle device settings, store sensor data, and enable micropayments due to its distributed and decentralised organisational structure. Anyone who is authorised to communicate within the IoT could track and investigate the transactions in the blockchain. IoT with blockchain technology could enhance communication security through the concept of blockchain as a service for IoT by implementing it.

Context

Introduction

What is IoT and Blockchain?

IoT is a system of interrelated devices connected to the internet to share/transfer data with other devices (where device can be general device or sensing device) and Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding).

Problems in to IoT

- **Vulnerabilities**
- **Malware**
- **Escalated cyberattacks**
- **Information theft and unknown exposure**
- **Device mismanagement and misconfiguration**

Why blockchain technology in IoT?

The blockchain technology has shown to be a viable solution in many distributed applications where trust and transparency are essential components. The Internet of Things (IoT) is increasingly being utilised and applied in a variety of industries, including smart cities, banking, self-driving cars, healthcare, smart homes, and marketing. Both IoT deployment and its vulnerabilities are growing. These kinds of apps are crucial, and user data must be safe and confidential. IoT users whose devices lack security measures put their data and privacy at risk of attack.

IoT devices constantly interact with their surroundings to produce various forms of data resources. The data privacy and security of users and devices, however, rely on the prevention of the central server owing to the volume and scale of dispersed IoT device deployment, and the security authentication of device resources confronts enormous obstacles. Another cutting-edge data management system that can guarantee the validity of data stored in a distributed fashion is blockchain. The use of blockchain technology is expanding quickly as it is increasingly expands from digital currency to non-financial industries as a result of the growing maturity of the technology and the continuous implementation of pertinent national technology regulations.

IoT-chain refers to the conception and application of a secure authentication mechanism. IoT-chain can keep records, offer dynamic security certification management, and address security certification challenges on the Internet of Things by utilising a distributed architecture.

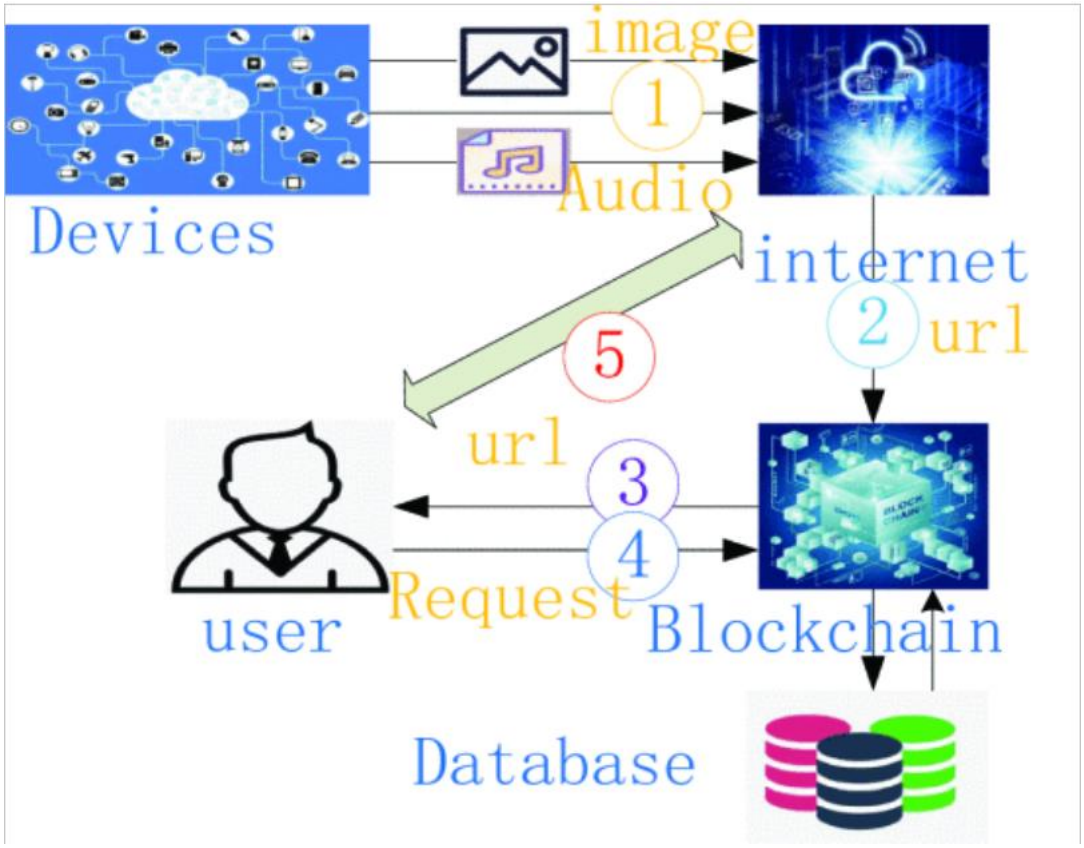
Therefore, adopting blockchain to store IoT data would provide an additional security layer that would be difficult for hackers to go over in order to access the network. Blockchain offers a far higher standard of encryption that essentially prohibits the overwriting of pre-existing data records.

Resource and authentication model

A. Resource model

Sensors gather environmental physical signal data. Direct storage of this gathered data in a relational database is not possible. As a result, a resource URL mapping model has to be created so that the user may access the resource URL based on the blockchain system's verification of their data permissions device→resource→url.

The relationship between the consumer and the gadget is depicted in the following figure below.



• In addition to generating a URL link, the gadget sends other data to the network.

• The blockchain system stores the device's URL data.

• The client asks the blockchain system for authorization.

• The website is distributed to authorised users using the blockchain system.

• The consumer may get pertinent information online based on the website.

B. Authentication model

Three levels make up the Internet of Things architecture: the perception layer, the network layer, and the application layer. Identity identification between devices, devices, and users is a key component of the security of the perception layer. Keys are used in the initial stage of networking to secure identity authentication. The session data of the communicating parties will be obtained by the attacker if the key of one of the communication parties is stolen, resulting in losses for both communicating parties.

According to the characteristics of data generated by IoT devices, the device security authentication strategy model is defined as follows:

P = {User, Device, Authority, Environment}, User = userID,role, group, Device = {deviceID, MAC}, Authority = allow,not, Environment = {createTime, endTime, allowedIP}

Security authentication approach is abbreviated as P. There are four components in this group: AS, AO, AP and AE

User: Represents information about users, including three different sorts of data: group, role, and userID, which uniquely identifies each user (user group).

Device: Displays the name of the device, which is made up of its MAC address or device ID.

Having the legal right to access resources is referred to as having authority.

the environment needed for attribute security authentication is referred to as the environment. The creation time, end time, and authorised IP are the three characteristics of the environment. The start time of the strategy is represented by the creation time. The policy's expiration date is indicated by the end time. The chosen IP might block access to the system from IP addresses outside of the network segment.

System and chain code

A. System structure

Customers, the blockchain, smart gateways, and devices make up the four components of IoT-chain, a blockchain-based IoT security authentication solution.

Customer: Administrators and regular users are the two categories into which the system separates its users. The blockchain system and smart gateway program's maintenance must be managed by the administrator.

The resource URL is made available to regular users, who are the equipment owners, by sending authorization requests to the blockchain system.

The mainstay of the system is the blockchain. It serves three primary purposes.

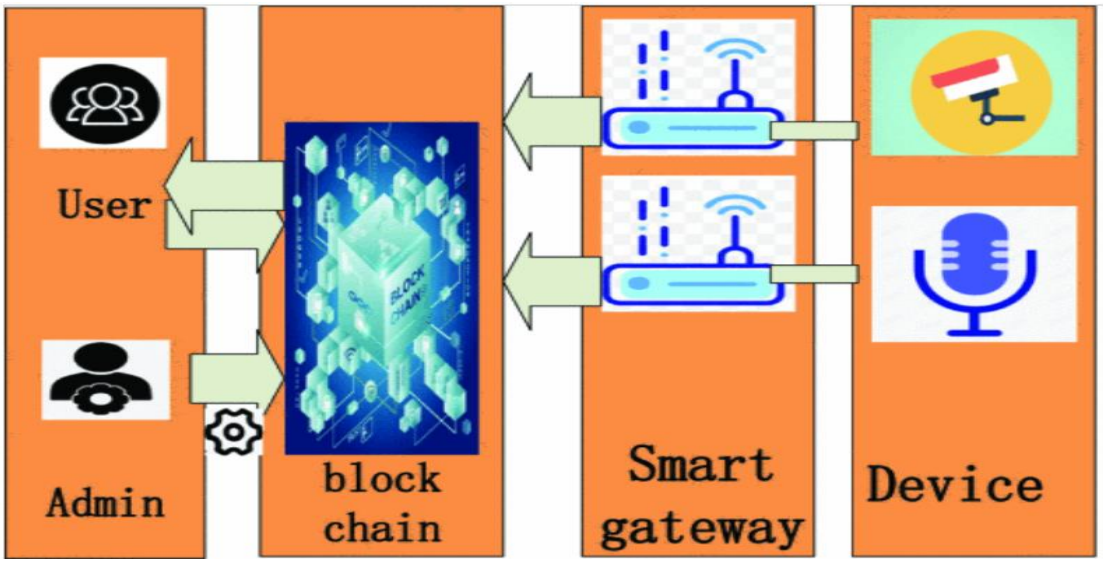
1) Data storing for device resource URLs.

2) Management of customer authority.

3) Confirm the client's request for resources.

Smart gateway: Due to resource limitations, IoT devices cannot be installed directly as peer nodes of the blockchain. In order to reduce the strain on the blockchain system caused by direct access, it can act as a bridge between the device and the blockchain system by receiving the URL from the device and adding it to the block Chain.

IoT devices: Each time an IoT device creates a new resource, the device sends a message URL to the smart gateway that contains the resource.



B. Chaincode

The installation of security certifications is based on smart contracts. Chaincode is the smart contract in Fabric. The system uses three different sorts of chain codes: access codes, device codes, and policy codes.

- Code for the strategy: It offers a way to implement the security authentication technique. The administrator creates the user's security authentication policy and submits a request to the blockchain system to include it. The correctness of the security authentication policy must be verified by the strategy code. User, Device, Authority, and Environment are the four characteristics that must be included in a legal security authentication policy, and each attribute's type must also adhere to the rules.

- Device code: This code is primarily in charge of adding the storage device's resource URL to the State Database of the blockchain system.

- Access Code: Check if the user request complies with the attribute-based access control policy using the access code. The access code, like the policy code, checks the user's signature using the public key to confirm the user's identity once the request data has been signed by the user's private key.

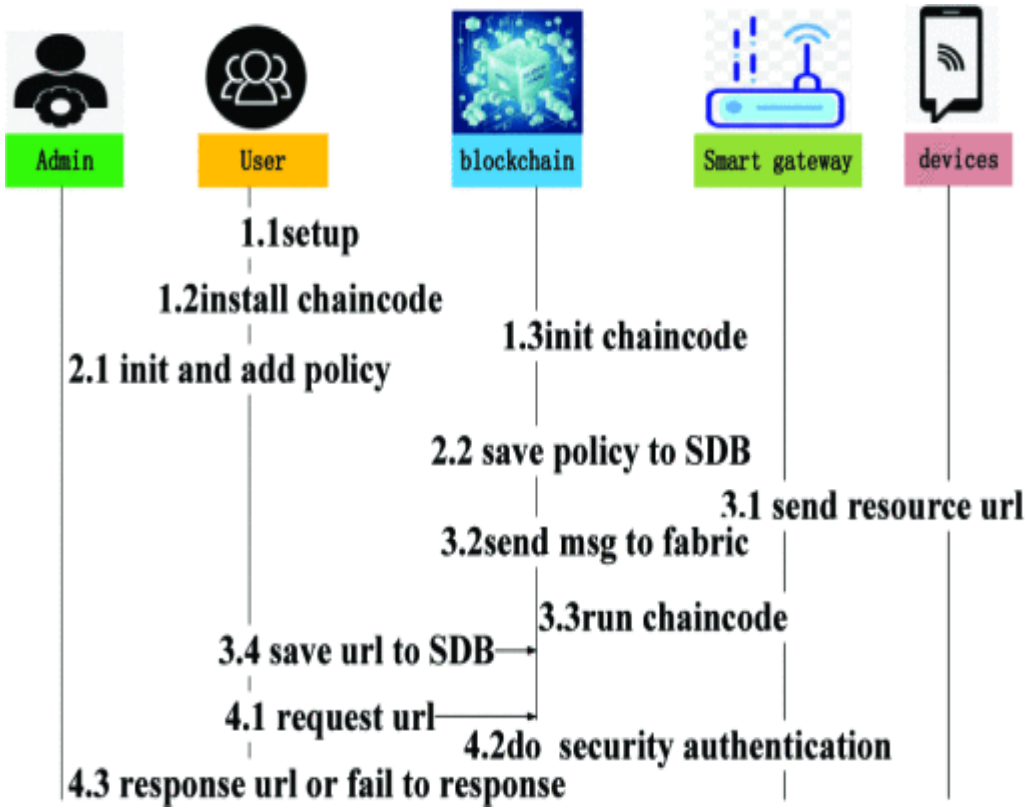
C. System workflow

The four steps that make up the majority of the system's workflow are. These procedures enable the system to authenticate users while converting the resource information from IoT devices into information that users can access on the blockchain. The procedures for each step are described in this section.

- Initializing the blockchain network and installing the chain code is the first phase. These are the fundamental operations of the system. The administrator must use the Intranet to do these tasks. Even if it finishes basic network construction, the administrator initialises and builds the fabric network, which contains data like order nodes, and completes the channel creation. The three chain codes are then installed on the blockchain by the administrator using the SDK, and they are eventually initialised.
- Creating a security authentication technique and saving it to the blockchain system constitute the next stage. The system administrator uploads the access strategy to the blockchain once the user and the administrator jointly decide on it and configure it. By running the chain code, the administrator may then connect to the blockchain to create, edit, and remove policies. This strategy's value is recorded in the state database, and a record of the operation will be made in the ledger for later inspection.
- The third step involves the IOT device reporting the resource URL to the smart gateway, which analyses the resource information using its own programme before uploading it to the blockchain system. The blockchain

system then calls the chain code to parse the URL, parses the URL, and stores the parsed URL data in the state database.

- The user requests website information from the blockchain system in the fourth phase, which is also the system's fundamental step, and engages in interactive security authentication with the blockchain system. The policy chain code saved by the administrator prior to authentication is used by the blockchain system. An error code will be given if the authentication is successful, and the device chain code is then called to deliver URL information to the user.



Conclusion and further work

This addresses the issue that traditional security authentication methods based on centralised design are challenging to meet the security authentication requirements on the Internet of Things by utilising the benefits of blockchain technology, such as decentralisation, tamper-proof, and traceability. Creating and deploying a secure authentication system based on Hyperledger Fabric is another thing to do. The administration of security certifications is provided by this system using a distributed architecture. The following areas can be improved in future:

1. The low consensus efficiency of the current blockchain technology is a problem that will directly impact how quickly an authentication request is processed. The Hyperledger Fabric cluster environment is currently only comprised of a small number of nodes, which reduces the transaction time. The current consensus process, however, is no longer able to satisfy the criteria if it is to be used on a broad scale. Therefore, in order to further increase certification efficiency, the consensus method must be modified.
2. This article's experiment uses two personal PCs. We want to use clusters or implement edge computing services in the future and further analyse the system's distributed performance.

3. More tangible tools can be employed in the future to check the system's dependability and throughput.

4. The members in the alliance chain should be able to amend the smart contract on their own, even though smart contracts might incorporate business logic that is open and challenging to modify. The next phase of study can concentrate on how to implement the self-customization direction while deploying the smart contract to the alliance chain. To enhance this system, future study can strive to create additional smart contracts involving the participants.

REFERENCES:

1.Kashif Naseer Qureshi, Shahid Saeed Rana, Awais Ahmed and Gwanggil Jeon, "A Novel and Secure Attacks Detection Framework for Smart Cities Industrial Internet of Things", *Sustainable Cities and Society*, vol. 2, pp. 3-5, 2020.

2.Tang ChengJun, Cai Guobao, Xu Hui, Zhao Ruwen and Ye Jun, "Blockchain IoT device and wireless access point two-way authentication scheme", *Cyberspace security*, vol. 10, pp. 8-14, 2019.
3.S Niu and Chi H Zhu, "Privacy and authentication protocol far mobile RFID systems", *Wireless Personal Communications.*, vol. 77, pp. 713-1731, 2014.

4.Xiong xiong and Zhang jinyi, "Overview of the application research of blockchain technology in many fields", *Journal of Tianjin University (Social Science Edition)*, vol. 1, pp. 323-369, 2018.
5.B Yu, J Wright and S Nepal, "Establishing Trust in the Internet of Things Ecosystem Using Blockchain", *IEEE Cloud Computing*, vol. 4, pp. 12-23, 2018.

6.M Samaniego and R Deters, "Blockchain as a Service for IoT", *International Conference on Internet of Things*, vol. 2, pp. 433-436, 2017.

7.S Singh and Singh N. Blockchain, "Future of financial and cyber security", *Contemporary Computing and Informatics*, vol. 2, pp. 463-467, 2016.

8.K Christidis and M Devetsikiotis, "Blockchains and smart contracts for the Internet of things", *IEEE Access.*, vol. 4, pp. 2292-2303, 2011.
9.Shao Qifeng, Jin Cheqing and Zhang Shao, "Blockchain technology: architecture and progress", *Chinese Journal of Computers*, vol. 41, pp. 969-988, 2018.

10. Qin Wang, Xinqi Zhu, Yiyang Ni, Li Gu and Hongbo Zhu, "Blockchain for the IoT and industrial IoT A review", *Internet of Things.*, vol. 10, pp. 11-13, 2020.