SECURING IoT WITH BLOCKCHAIN

Kazım Onur Toka[1[0000-0003-2070-9036]], Yılmaz Dikilitaş[1[0000-0002-8892-574X],

Talha Oktay[1[0000-0001-8939-4672]] and Ahmet Sayar[1[0000-0002-6335-459X]]

[1]Department of Computer Engineering, Kocaeli University, Kocaeli, Turkey – (kazim.onurtoka@gmail.com, yilmazdikilitas91@gmail.com, toktay@gmail.com, ahmet.sayar@kocaeli.edu.tr)

KEY WORDS: IoT, Blockchain, Hyperledger, IoT Security, IoT with Blockchain.

ABSTRACT:

IoT is becoming ubiquitous in industry, homes, cities, literally in every aspect of our daily lives. Securing IoT-based systems is difficult because of deficiencies in the very nature of IoT devices such as limited battery power, processing, and storage, etc. Blockchain is a new approach used to securely record transactions and offers potential solutions to computer and internet security issues such as confidentiality, integrity, availability, authentication, authorization, and accountability. Blockchain, as a decentralized ledger consisting of interconnected blocks, can remedy most of the security deficiencies of heavily IoT based systems. The Hyperledger Fabric blockchain network used in this study provides confidentiality, data integrity, authentication, and data security for data obtained from IoT devices. Widely used IoT data transfer MQTT protocol is included in the proposed approach. The approach is demonstrated in a simple demo Hyperledger network with simulated IoT devices. The proposed approach is discussed in terms of network security dimensions. Based on the features of the Hyperledger Blockchain network, it is displayed that the IoT security deficiencies can largely be remedied with the proposed approach.

1. INTRODUCTION

Today, IoT devices are everywhere, in smart homes, wearable devices, smart cities, healthcare, automotive, environment, smart water, and grid applications, etc. IoT solutions are used in many areas for optimizing production and transitioning industries to information technologies. Approximately 46 billion devices will be connected to the Internet of Things by the end of 2021, according to Juniper Research (Juniper Research, 2021).

Despite these great opportunities offered by IoT technologies, ensuring the reliability and accuracy of the data obtained from these technologies remains a problem that has not yet been fully addressed. It is unfortunately easy to capture and manipulate the data transmitted by many IoT devices. Typically, an IoT device is more vulnerable to attacks as it is limited by information processing, storage, and networking capacity (Jyoti and Amarsinh, 2017). It is deemed necessary usage of different designs, different interfaces, or different environments to ensure secure communication.

It is generally regarded as difficult to assure that the data provided from IoT devices has not been tampered with or changed in any way (Alfonso, 2018) specifically in architectures where IoT devices send data to shared servers that keep all records centrally.

Blockchain can be a solution to the security problems of IoT systems (Dikilitas et al. 2021). In the most basic terms, a blockchain can be defined as a decentralized and distributed ledger technology that contains interconnected records. A record can be added to the blockchain ledger with the approval of the majority of all peers on the network. Blockchain's interconnected blocks nature ensures that the data is protected from tampering. This decentralized structure of the blockchain offers security and privacy (Rui et al. 2019). Blockchain technologies can provide a high level of security, privacy, authentication, and device authorization for the data to be recorded and can be used to secure systems that use IoT devices.

However, there is no clear solution in the literature on how to securely transfer data from IoT devices to a blockchain. The main motivation in our study is that the data transfer between these two environments can be done securely with the integration of IoT and blockchain.

The outline of the study is as follows, summary information about IoT and blockchain is included in section II. In section III, the work done on IoT and blockchain integration is summarized. In section IV, the proposed architecture for securely integration IoT and blockchain is discussed and section V provides conclusions.

2. BACKGROUND

2.1 Internet of Things (IoT)

The density of digital data in our lives has started to increase very rapidly because of continuously online devices. Since these data are actively transferred over the internet, they are always accessible. The technology that enables this intensive data transfer between human beings and devices is called IoT.

Standard IoT devices are heterogeneous devices with embedded sensors that connect over a network. IoT devices are uniquely identified in the network. These devices are generally designed to operate with small memory, limited processing capacity, and low power. Networks act as a bridge between IoT devices and users.

IoT devices by nature are small memory, low powered, and limited processing capacity; faced with security weaknesses in

the fields of identity verification, authorization, and accounting. However, IoT's seven-tier architecture (Jasmin, 2016) allows participants to develop IoT devices that are compatible with each other by determining layers in which certain types of transactions can be optimized.

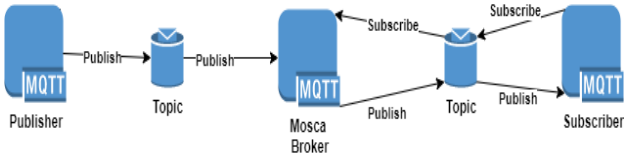

Figure 1. Architecture of MQTT

There are protocols for to transfer of data received from IoT devices (Nitin, 2017). The most widely used one is MQTT. It is an OASIS standard messaging protocol for the IoT. It is designed as an extremely light publish-subscribe messaging transport ideal for connecting remote devices with a small code space and minimal network bandwidth.

The MQTT structure consists of three basic components: "publisher", "subscriber" and "broker". MQTT Publisher posts a message under a specific topic via the MQTT broker. Likewise, the MQTT subscriber can access all the messages published under this topic by subscribing to the topic published by the MQTT publisher via the MQTT broker.

2.2 Blockchain Technology

Blockchain is a decentralized, distributed, immutable and shared ledger that keeps track of assets and transactions on a peer-to-peer network (P2P) (Nabil and Claus, 2018).

One of the most important concepts of blockchain is blocks. Each block contains an encrypted value containing the block information preceding it.

Transactions are a small task unit usually stored in public records within a block. Records are usually added to the blockchain after obtaining the approval of the majority of users participating in the blockchain network (Gareth and Efstathios, 2015). The data processed in the distributed ledger is recorded in the ledger with the consent of all participants in the network. This is called a consensus mechanism.

The first of the features that make Blockchain valuable is the decentralization structure. In a blockchain network, data appears as a distributed ledger database. The same data are kept simultaneously on all other stakeholders in the network. With all these features, blockchain technology provides the highest level of traceability by all stakeholders.
Another important contribution of blockchain technology is the transparency it adds to business processes. This increases the trust between stakeholders and ensures accountability. It allows all stakeholders to monitor the blockchain network in real-time.

Data privacy is an important feature of restricted blockchain networks. In restricted blockchain networks, only users authorized by the node's administrator can view data. This ensures that data coming to the blockchain network is protected. The public key structure of blockchain networks, which protects data modification, largely eliminates integrity problems. The participants and the consensus mechanism of a blockchain network are other factors that increase data security.

Smart contracts are pieces of code that define the business processes between stakeholders in blockchain networks.

Blockchain technology is used on many digital currencies including widespread Bitcoin and Ethereum cryptocurrencies using smart contracts. In the field of corporate blockchain applications, Hyperledger Fabric network is frequently used.

3. RELATED WORKS

In this section, relevant studies about IoT, blockchain integration, and security will be discussed.

At (Nejc, 2019), an approach is presented to integrate IoT and blockchain technologies into supply chain processes. The study proposes a Blockchain-based distributed logistics platform that involves adding actors in a supply chain to the system as a node. A virtual copy of a transported property is created with IoT devices on the proposed platform. Other data such as the location, temperature, and humidity of the transported goods are monitored via the virtual copy and recorded on the blockchain.

At (Thomas, 2017), It is explained that the most important benefit in saving data from IoT devices to a blockchain network using smart contracts is that these data can be evaluated and reported to the sender or receiver automatically. The smart contract running in the system corrects the temperature values coming from the sensors and saves them to the blockchain. Mobile clients communicate with the server using the REST API. Customers can control the data in the system through these mobile clients.

At (Kristi´an, 2019), a blockchain-based network monitoring and management architecture is proposed. The administrators in the network indirectly control the network devices by recording the changes in the device configuration on the blockchain, where they control the updates in the configurations of the network devices.

At (Seyoung et al. 2017), It is aimed to control and configure IoT devices using blockchain. The proposed system includes a smartphone and three raspberry pi. The three raspberry pi in the system act as a meter, air conditioner, and light bulb, respectively. The user can adjust the policy in the system via the smartphone. Configuration changes made via the smart device are recorded on the Ethereum network.

At (Mayra et al. 2016), It is pointed out that blockchain's decentralized and change-resistant nature can be used to solve some of the problems faced by the nature of IoT. The authors present a cloud and fog-based solution to solve this problem. In the study, the Intel Edison Arduino card is used as the IoT device, and the blockchain works separately on the fog and the cloud. In the experiments, the IoT device writes data to the blockchain via a Python server.

Studies in the literature are generally based on IoT and Blockchain integration. However, there is no clarification on how to ensure security in data transfer, which is one of the biggest disadvantages of IoT systems. We propose a solution to this problem in section IV.

4. PROPOSED APPROACH

In this section, a simple approach is presented that integrates IoT devices to any blockchain network securely. In our research, Hyperledger Fabric is used as the blockchain network.

In the proposed architecture presented at figure 2, an IoT device via its sensors captures the data of interest and publish to MQTT message broker. The message broker distributes the received messages to the registered subscribers. In our model implementation "Mosca MQTT broker" is used. The subscriber of the data of interest is an application within the blockchain network which is defined as an authenticated user to the blockchain node. This application creates the necessary transaction on the Hyperledger network based on received data.

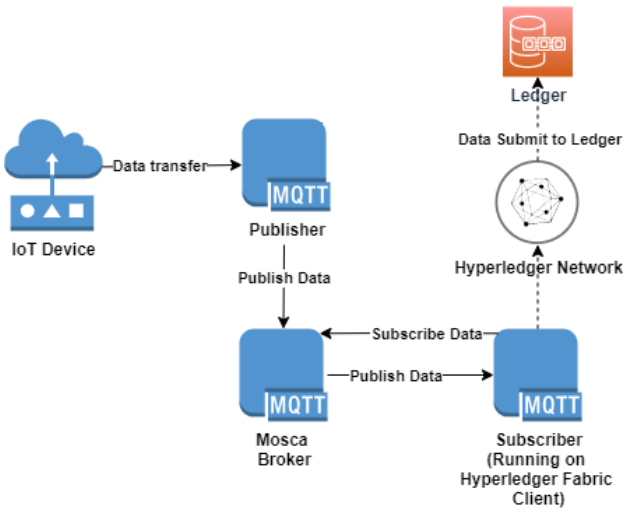

Figure 2. IoT Integration to Hyperledger Network

This approach is simulated in a simple hyperledger network setup. Four Hyperledger Fabric organizations are created on four separate physical machines. Organizations communicate with each other via Docker Swarm Network. Four organizations operate the processes in the network with a channel policy in which they are participants. Three of the four organizations were established to implement the relevant business processes, the fourth organization on the network is Orderer. Organizations in the network each create users to execute the defined processes through smart contracts.

Simulated IOT devices in figure 3 in between organizations trigger events that inform the network of state changes via collected data from sensors. The state changes can be applied to many subjects of interest such as production, transfer of goods in supply-chain processes as production of a material, transfer of materials.

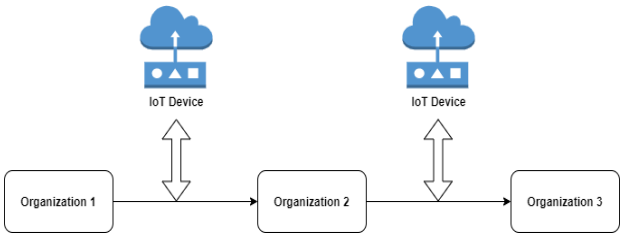

Figure 3. Transaction request flow

With this approach, it is ensured that the data received from the IoT device is transferred to the network over a secure transfer layer through the Hyperledger Fabric user, defined for the IoT device, preventing unauthorized access and modification of the data. The proposed approach satisfies IoT security problems as discussed below in terms of dimensions of network security.

Confidentiality is ensured with the solutions regarding privacy control and data security offered by the Hyperledger Fabric network (IBM, 2021). Hyperledger Fabric only allows transactions between predefined users via authorized channels which prevents unauthorized users are prevented from making transactions within the network.

The integrity of the data is ensured by keeping data of the network in distributed databases called ledgers. Blockchain ledgers consist of all of the transactions called blocks and that are linked together in a chain. This connection is achieved by a block storing a hash value containing the information of the preceding block itself. If a peer wants to intervene directly in the Hyperledger Fabric state database, the data cannot be changed, as other peers will not be convinced that this is the case. Having these distributed databases in all stakeholders ensures data integrity.

In terms of Availability, Hyperledger network provides resilience to failures with its distributed nature and the data will be kept continuously accessible for authorized users. In multiple peers carrying the ledger databases, the data will be available over other healthy peers even when one peer is inaccessible. Hyperledger network also provides a high count of transactions per unit time by using cheaper commodity hardware (Hyperledger, 2021).

Identification, Authentication, and Authorization The MQTT publisher running on the Hyperledger Fabric API server must transact with a previously defined authorized user within the Hyperledger Fabric organizations. At the same time, additional authentication is provided by using the username and password fields provided by MQTT for authorization. With this identification provided by the Hyperledger Fabric user identification and MQTT protocol, the data sent through the protocol will be authenticated, and unauthorized access to the data will be prevented. In addition, the optional MQTT TLS support makes it easy to encrypt messages and authenticate clients using authentication protocols.

In terms of Accountability, all elements that will operate in the proposed architecture will be able to perform these operations with a specific identity, and these transactions will be accountable by answering questions such as from which IoT device, when and from which Hyperledger Fabric user the transaction was made.

5. SUMMARY AND CONCLUSIONS

IoT is becoming ubiquitous in industry, homes, cities, literally in every aspect of our daily lives. Securing IoT-based systems is difficult because of deficiencies in the very nature of IoT devices such as limited processing, storage, etc.

Blockchain is a decentralized ledger consisting of interconnected blocks that can remedy most of the security deficiencies of IoT-based systems. The Hyperledger Fabric blockchain network provides confidentiality, data integrity, authentication, and security for data obtained from IoT devices. Widely used IoT data transfer MQTT protocol is included in the proposed architecture. The proposed approach is demonstrated in a simple Hyperledger Fabric blockchain network with three organizations and simulated IoT devices. Our approach is discussed in terms of dimensions of network security. Based on the features of Hyperledger Fabric blockchain network and the proposed architecture, it is demonstrated that the IoT security deficiencies can largely be remedied.

REFERENCES

Internet of Things' Connected Devices to Triple by 2021, Reaching Over 46 Billion Units, https://www.juniperresearch.com/press/internet-of-things-connected-devices-triple-2021, last accessed 2021/08/10.

Jyoti D. and Amarsinh V.: Security Attacks in IoT: A Survey (2017).

Alfonso P.: Blockchain and IoT Integration: A Systematic Survey. Sensors, 1424-8220 (2018).

Dikilitas Y., Toka K.O. and Sayar A..: Current Research Areas in Blockchain. European Journal of Science and Technology, 26, pp. 488–492 (2021).

Rui Z., Rui X. and Ling Liu.: Security and Privacy on Blockchain (2019).

Jasmin G.: Comparison of IoT platform architectures: A field study based on a reference architecture. 2016 Cloudification of the Internet of Things (CIoT), pp. 1–6 (2016).

Nitin N.: Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. 2017 IEEE International Systems Engineering Symposium (ISSE), pp. 1–7 (2017).

Nabil El I. and Claus P.: A Review of Distributed Ledger Technologies. OTM 2018 Conferences, Vol. 11230, Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, pp. 277–288 (2018).

Gareth P. and Efstathios P.: Understanding Modern Banking Ledgers Through Blockchain Technologies. Future of Transaction Processing and Smart Contracts on the Internet of Money (2015).

Nejc R.: Distributed logistics platform based on Blockchain and IoT. 52nd CIRP Conference on Manufacturing Systems (CMS), pp. 826–831 (2019).

Thomas B.: Blockchains everywhere - a usecase of blockchains in the pharma supply-chain. 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). pp. 772–777 (2017).

Kristi´an K.: Management and Monitoring of IoT Devices Using Blockchain. Sensors 19.4, p. 856 (2019).

Seyoung H., Sangrae C. and Soohyung K.: Managing IoT devices using blockchain platform. 19th International Conference on Advanced Communication Technology (ICACT), pp. 464–467 (2017).

Mayra S., Uurtsaikh J. and Ralph D.: Blockchain as a Service for IoT. IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 433–436 (2016).

The Linux Foundation's Hyperledger Fabric enables confidentiality in blockchain for business Blockchain Pulse: IBM Blockchain Blog, https: //www.ibm.com/blogs/blockchain/2018/04/hyperledgerfabric-enables-confidentiality-in-blockchain-for-business/, last accessed 2021/08/10.

Hyperledger Blockchain Performance Metrics White Paper Hyperledger, https://www.hyperledger.org/learn/publications/blockchain-performance-metrics last accessed 2021/08/10.