Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 4, April 2022, pg.69 – 73

Strengthening IoT Security with Blockchain Integration

Sara Koulali[1]; Mostapha Derfouf[2]

[1]Competitive Intelligence Team (DSCI), National School of Applied Sciences Al-Hoceima, Morocco
[2]OASIS TEAM, Mohammadia School of Engineering (EMI) Rabat, Morocco
[1] skoulali@uae.ac.ma; [2] mostaphaderfouf@research.emi.ac.ma

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i04.009

Abstract— The Internet of Things (IoT) has become one of the major trends in recent years. This new paradigm is at the center of technological innovations and represents a fast-growing sector that is implemented everywhere and aims to facilitate our daily lives. However, security problems related to this new concept remain the most prominent concern since the traditional security architecture adopted for the IoT is still not efficient and reliable. The present paper will discuss the most significant IoT-related security issues and propose a comprehensive approach based on Blockchain to improve IoT security. Integrating Blockchain in IoT aims to increase trust, security, transparency, and data traceability in IoT applications.

Keywords— IOT, IOT security, Blockchain, SmartContract, MultiChain

I. INTRODUCTION

All sectors of the economy are gradually being transformed by the proliferation of connected objects. The Internet of Things can be seen as a source of new opportunities; however the security of IoT devices has been a cause for concern. Identifying them and preventing the security risks targeting the IOT is an essential prerequisite for manufacturers who would like to be part of this new technological revolution.

Our work involves designing a challenging approach based on a private Blockchain architecture, this paper is based on our previous work when we introduced this concept for first time to our best knowledge [1] the added value of this paper is to focus more on security aspects.

By integrating Blockchain in IOT we gain in terms of performance, privacy, cost reduction, confidentiality, integrity, availability, and optimization of administration's tasks.

Our proposed architecture covers two main IOT security issues, which are the security of data exchanged via encryption techniques and the management of access to the IOT network through a permissions control and authentication approach.

The remainder of this paper is organized as follows: next section surveys related work. Section three provides background information and some benefits of integrating Blockchain in IOT architectures, while Section four describes the fruit of our contribution. In section four we will describe the architecture design of our proposed. Finally, Section five draws some conclusions and probable future works

II. RELATED WORKS

IOT is widely discussed in research area, security aspects take an interesting part of these studies. One of these important works is related to IOT security challenges [2], the authors of that paper found that security concerns are still top of-mind for users considering IOT adoption. They pointed out research directions that may be the eventual solutions to the security challenges that IoT encounters. The work of these authors was limited to exposing security vulnerabilities and perspectives without proposing a technical solution to protect against security risks.

The authors in [3] have put the focus on the security side of the IOT, by carrying out an in-depth analysis and a presentation of the security risks linked to the paradigm of the internet of objects. The authors also highlighted the current works and security trends regarding the IOT.

In [4] the authors have listed the various works reflecting the progress regarding IOT security since 2016 to 2018. This paper provides an overview of the current state concerning the IOT security researches, exposes the relevant tools and the mechanisms to make the IOT secure.

The work presented in [5] has dealt with the security problems targeting the IOT by exhibiting several works promoting artificial intelligence techniques, in particular through the implementation of the of Deep learning concept. Indeed, the authors of this article have examined the various works proposing approaches using deep learning algorithms. The analysed approaches were classified according to several criteria in order to identify the shortcomings of each approach.

In [6] gave the authors outlined the concept of edge-centric IoT architecture and its interaction with IOT applications. They presented a comprehensive study of existing solutions based on edge-centric IoT architectures to secure IoT. The analysed designs were classified into five main categories such as intrusion detection, security architecture, authentication and authorization, firewalls, and privacy. Finally the authors of this paper provided an overview on research perspectives aimed at securing IOT environment sandfosting future noveledge-based security designs.

Some researchers [7] outlined security requirements for IoT along with the existing attacks, carried out a detailed inventory of the various attacks and vulnerabilities in IOT environments. They also evoked the concept of the Blockchain while highlighting its advantages and its essential role in solving IoT security issues.

In the same context, other researchers [8], highlighted the concept of the Blockchain by citing the IOT applications that make use of the Blockchain by considering it as a necessary and essential layer for IOT security.

III. THEORETICAL BACKGROUND AND BENEFITS OF THE BLOCKCHAIN APPROACH

A. Blockchain paradigm

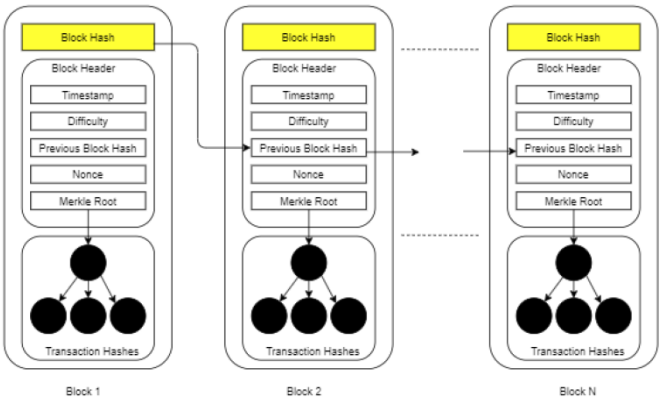

Fig. 1 The Blockchain structure [9]

According to Blockchain Partner, the Blockchain, or chain of blocks, is defined as a “technology of digital storage and transmission at minimal cost, decentralized and completely secure”. This technology appeared in 2008 with the Bitcoin currency, the most well-known use case of the Blockchain. But this concept has many other uses than cryptocurrency transactions [10].

The Blockchain is often compared to a vast public register, a kind of ledger integrating all the exchanges

carried out by its users since its creation. These exchanges are grouped together within blocks ordered from the oldest to the most recent. Each block contains information relating to the previous block so that it is impossible to modify a block without modifying the entire Blockchain downstream, in this case the Blockchain then becomes obsolete, and that is why we say that Bitcoin cannot not be hacked.

To ensure the integrity and authentication of transactions, the Blockchain is based on the use of asymmetric cryptographic keys and hashing algorithms, a sum of checks which will prevent any subsequent modification of the block. Public key cryptography is based on the use of a public key, broadcast, and a private key, kept secret, one allowing to encode the message, the other to decode it. It is with the public key corresponding to the private key used to sign the transaction that the reliability of the operation is checked. Once a transaction is entered in the database, it can no longer be modified; it is incorruptible. It would be necessary to have access to more than half of the servers simultaneously to falsify information.

B. Benefits of implementing Blockchain with IoT

The Blockchain promises us effective data protection, particularly for the transfer and exchange of information. With the IoT and the volume of data, the Blockchain appears to be the most suitable solution for protecting data.

Our approach of integrating Blockchain with the IOT will ensure two advantages that we will demonstrate in the experiment and which can be circumscribed as follows:

- Ensure trust and transparency between IOT devices that typically do not trust each other, through authentication and identification techniques provided by the Blockchain. The proof of authentication in Blockchain is inviolable, tamper-proof and traced in a sustainable way.
- Secure the data exchanged between IOT devices. Indeed, the Blockchain is a technology that is based using public key cryptography to ensure encryption of data that can only be decrypted by an authenticated recipient. The powerful cryptographic algorithm for encrypting sensitive data is one of the reasons why we have opted for the Blockchain to secure the transfer of information between IOT devices.

IV. PROPOSED ARCHITECTURE DESIGN

Our proposed architecture allows users to connect to and interact with each other through a Blockchain network. To design our private Blockchain network we opted for Multichain [11]. The choice of the Multichain platform was made after an in-depth study of the different Blockchain platforms and multichain was chosen as the implementation platform for two following main reasons which respond to our problem and which are as follows:

- It offers a powerful permission management system, so that the Blockchain's activity is only visible to chosen participants.
- It is a private Blockchain and in this case problems relating to scale are easily resolved.

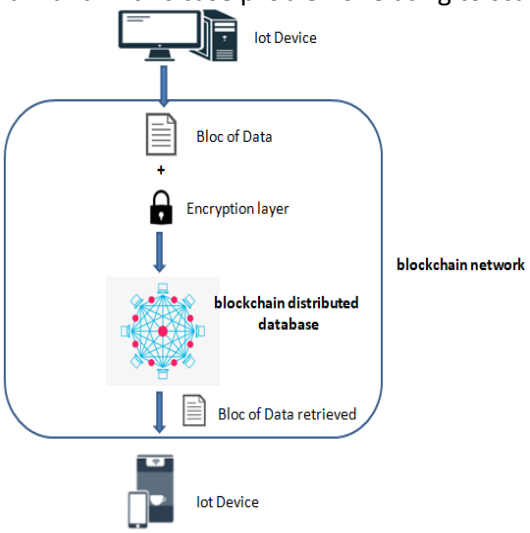

Fig. 2 Design of the proposed architecture

As shown in the figure, the IOT nodes that are equipped with the Multichain client communicate through the Blockchain, no data exchange takes place outside the private Blockchain network. The data exchanged is recorded in transaction blocks and is encrypted and access is limited. Each client holds the addresses of the other nodes and at each new connection of a new device a handshaking process is triggered (See Figure 3).

To solve the access and identity problem, we opted for the “handshaking” process that occurs when two Blockchain nodes connect and which is described in the sequence diagram below:

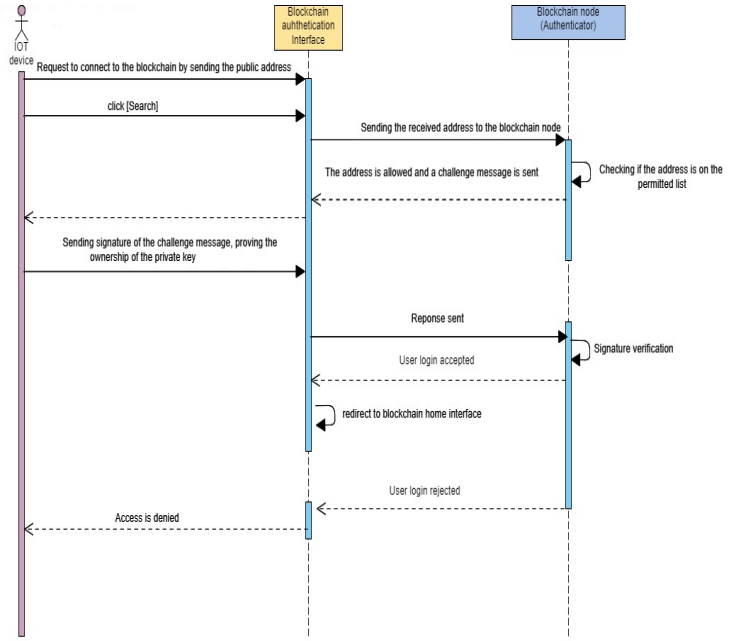

Fig. 3 The process of "handshaking" to manage access to the private Blockchain using Multichain

The diagram shown below details the handshaking process to verify the identity and access rights of each node (IOT device) of the Blockchain. The scenario of connecting a device to the Blockchain looks like this:

- The device wishing to connect to the Blockchain network must first present its public address as an identity.
- Each node of the Blockchain receives the identity of the device and checks if its public address belongs to the list of authorized addresses.
- If the provided address is authorized, a challenge message is sent to the device requesting the connection.
- The device requesting the connection decrypts the challenge message and returns a signature of the challenge message proving that he owns the private key corresponding to the public address he presented.
- Finally the node gets access to the Blockchain and interacts with other nodes in a secure way. In case of rejection of the connection request the node will no longer be able to participate in the blockchain.

V. CONCLUSIONS AND FUTURE WORKS

In this work, we exposed the most important researches and contributions in IOT security. We also presented the strengths relating to the integration of the Blockchain in the IOT through the proposal of a novel architecture that guarantees data security and enhance authentication mechanisms.

As a future work, we will focus consists of implementing the proposed architecture on a virtualized environment consists in implementing the proposed architecture on a virtualized environment using Open source blockchain platform, this will allow us to validate our approach and verify that the expected objectives are achieved

REFERENCES

[1]. KOULALI, Mohammed-Amine, KOULALI, Sara, TEMBINE, Hamidou, et al. Industrial internet of things-based prognostic health management: a mean-field stochastic game approach. IEEE Access, 2018, vol. 6, p. 54388-54395.

[2]. ZHANG, Zhi-Kai, CHO, Michael Cheng Yi, WANG, Chia-Wei, et al. IoT security: ongoing challenges and research opportunities. In : 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014. p. 230-234.

[3]. ROMÁN-CASTRO, Rodrigo, LÓPEZ, Javier, et GRITZALIS, Stefanos. Evolution and trends in IoT security. Computer, 2018, vol. 51, no 7, p. 16-25.

[4]. HASSAN, Wan Haslina, et al. Currentresearch on Internet of Things (IoT) security: A survey. Computer networks, 2019, vol. 148, p. 283-294.

[5]. AVERSANO, Lerina, BERNARDI, Mario Luca, CIMITILE, Marta, et al. A systematicreview on Deep Learning approaches for IoT security. Computer Science Review, 2021, vol. 40, p. 100389.

[6]. SHA, Kewei, YANG, T. Andrew, WEI, Wei, et al. A survey of edgecomputing-based designs for IoT security. Digital Communications and Networks, 2020, vol. 6, no 2, p. 195-202.

[7]. KHAN, Minhaj Ahmad et SALAH, Khaled. IoT security:Review, Blockchain solutions, and open challenges. Future generation computer systems, 2018, vol. 82, p. 395-411.

[8]. MINOLI, Daniel et OCCHIOGROSSO, Benedict. Blockchain mechanisms for IoT security. Internet of Things, 2018, vol. 1, p. 1-13.

[9]. JATOTH, Chandrashekar, JAIN, Rishabh, FIORE, Ugo, et al. Improved Classification of Blockchain Transactions Using Feature Engineering and Ensemble Learning. Future Internet, 2022, vol. 14, no 1, p. 16.

[10]. PLISSON, Claire Fénéron. La Blockchain, un bouleversement économique, juridique voire sociétal. I2D-Information, donnees documents, 2017, vol. 54, no 3, p. 20-22.

[11]. LI, Suisheng, XIAO, Hong, et QIAO, Jingwei. Multi-chain and data-chains partitioning algorithm in intelligent manufacturing CPS. Journal of Cloud Computing, 2021, vol. 10, no 1, p. 1-10.

[12]. GÜRSOY, Gamze, BJORNSON, Robert, GREEN, Molly E., et al. Using Blockchain to log genome dataset access: efficient storage and query. BMC medical genomics, 2020, vol. 13, no 7, p. 1-9.

