https://doi.org/10.26682/sjuod.2023.26.1.25
Journal of University of Duhok., Vol. 26, No.1 (Pure and Engineering Sciences),Pp 256-265, 2023

ETHEREUM BLOCKCHAIN TECHNOLOGY FOR INTERNET OF THINGS AUTHENTICATION

NOOR **S**ALAH **H**ASSAN[*] and **A**HMAD **B**. **A**L-**K**HALIL[**]
[*]Dept. of Information Technology, Technical College of Informatics-Akre,
Duhok Polytechnic University, Kurdistan Region-Iraq
[**]Dept. of Computer Science, College of Science, University of Duhok, Kurdistan Region-Iraq

(Received: January 23, 2023; Accepted for Publication: March 15, 2023)

ABSTRACT

The Internet of Things (IoT) technology has grown rapidly and continuously. The IoT ecosystem comprises an increasing number of smart devices that can sense, act, process, store, and communicate via the Internet. Data within such communication technology is continuously exposed to be hacked or attacked. Therefore, there should be methods to protect the issue of data authentication and increase the security of such large-scale networks. In this article, a method of using a Blockchain network is proposed. The proposed system uses the Ethereum blockchain and benefits from several critical technologies, including distributed consensus, smart contracts, digital signatures, and cryptographic hashes. The whitelist and blacklist are the two lists that are suggested. The approved users who have obtained their private keys are included on the whitelist. The blacklist, on the other hand, is intended to stop illegal users who are flagged as spammers or attacks. According to findings, the Blockchain can drastically save expenses and boost the security of IoT networks.

KEYWORDS: Blockchain, Decentralization, Iot, Security.

1. INTRODUCTION

The Internet of Things (IoT) is a relatively new technology. It creates a global network of physical things that communicate and exchange data. The IoT ecosystem is made up of an increasing number of smart devices that can sense, act, process, store, and communicate via the Internet. These physical devices are spread across several industry verticals, such as transportation, industrial, manufacturing, healthcare, smart homes, and cities [1]. IoT technology offers significant advantages to both consumers and enterprises. It allows for fresh insights and the acquisition of actionable data from huge streams of real-time data. IoT also significantly reduces the human work required to control and monitor the system [2]. Therefore, IoT technologies are well-liked and very successful. However, they require a consistent and safe data transfer and communication mechanism.

The connected physical objects via the internet in the IoT networks, such as embedded sensors, software, and other technologies, can cover every day domiciliary objects to advanced industrial equipment [3]. IoT devices increase operational effectiveness and productivity, support in-the-moment decision-making, and open new business options. These advantages drive an exponential rise in connected devices, which may reach tens of billions soon. Unfortunately, these advantages frequently come with numerous security dangers and difficulties [4]. Therefore, IoTs are a desirable target for attackers due to their open accessibility, security flaws, and the high caliber of data they store.

IoT device security is still under development [5], and the alarming rate of device multiplication makes it more difficult to safeguard them. Due to this, bad hackers can simply use IoT systems to steal personal information, compromise security, and cause severe financial and reputational harm [6]. Therefore, there is a necessity to have some security measures to protect IoT devices from hackers and unauthorized users. Different technologies are used to protect the IoT networks, such as Machine Learning (ML) [7], a credit-based Proof-of-Work (PoW) mechanism [8], Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method [9], Multi-Factor Authentication (MFA) [10], etc... However, many other technologies use to secure IoT, most of them are on the basis of the

Blockchain that also has been used in the proposed system of this paper.

The future of IoT infrastructure makes it clear that it is necessary to take advantage of Blockchain's intrinsic qualities [11], since it gives the ability to make IoT systems feasible. In addition, it allows the development of trust-free, preventative, decentralized, and interoperable systems. Any interaction in the IoT system is legitimated by Blockchain distributed immutability.

The first Blockchain proposal came in 2008 by Nakamoto [12]. A sequence of blocks can be linked to a public ledger that contains all committed transactions. The chain is flexible to be expanded with the addition of more blocks. Combining several essential technologies, such as distributed consensus mechanism, cryptographic hash, and asymmetric cryptography-based digital signature, Blockchain can significantly reduce costs and increase efficiency [13].

2. RELATED WORK

Cyber-attacks on IoT devices have the potential to compromise privacy and security; as a result, IoT requires strong authentication. Blockchain is seen as a new technology and can provide high security. Many researchers in different fields have used Blockchain technology for IoT systems, like the work in [14]. The authors proposed the adoption of Blockchain and provided a fundamental interface to the security gateway design of an IoT device. Data was encrypted using compatible techniques before being sent to external services. Their solution increased the reliability of the data delivered to distant services. In accordance with the network regulations, their interface may also shield the appliance from illegally accessing the local network. However, the storage constraint is associated with the distributed ledger, which must be used to save all Blockchain transactions. Scalability concerns developed as more IoT devices are added to the networks increasing device activity processing time.

The authors in [15] proposed a user authentication approach based on Blockchain-enabled fog nodes. The authentication of users for IoT device access is done via fog nodes communicating with Ethereum smart contracts. They also conducted a security study, demonstrating that the suggested authentication system meets security objectives and is resistant to known threats such as eavesdropping, replay, and denial of service. They implemented their approach in a virtual public Ethereum network. Virtual IoT devices based on Raspberry PI and Arduino had been linked to fog nodes with Ethereum clients installed. The restriction was that the distributed ledger, which had to be used to store all Blockchain nodes, was tied to the storage limitations.

Furthermore, the authentication of IoT in smart cities and smart homes has been covered [16]. The authors proposed an authentication network for the home automation system using Blockchain. In order to employ unified smart home services, the Blockchain technology concept of a smart contract is used for user authentication across different users. They made it possible for users to access services faster and more securely. In the same context, the authors in [17] proposed a combined hyper-ledger fabric and hyper-ledger composer initially proposed by [18]. Their proposed architecture consists of four layers: cloud storage, hyper-ledger fabric, hyper-ledger composer, and a smart home layer. The secrecy, integrity, availability, privacy, authorization, and other related features like transparency and interoperability were all improved by their method for smart homes.

Similarly, the authors in [19] presented a Blockchain-enabled single character frequency-based Exclusive Signature Matching (ESM) to create a verifiable database of malicious payloads in a smart city. They evaluated their strategy's performance under assault in both a simulated and real-world IoT network environment. Their findings demonstrated that increasing the single-character frequency-based ESM's resistance to malicious traffic was successful. There are certain restrictions, too, such as the need to formalize the character padding attack model and confirm how it affects other exclusive matching systems. Furthermore, they relied solely on a virtual consortium Blockchain and tested only with a proof-of-concept (PoC). Thus, this limits the awareness of all types of Blockchain assaults.

The researchers in [20] proposed a high authentication for Edge devices. They have presented a Blockchain for Constrained Edge Devices (BCD). BCD is a revolutionary version of Blockchain technology that allows edge devices to interface with and participate in a Blockchain without needing a trusted intermediary. They suggested an architecture that provided a flexible and extensible

framework allowing multi-party interactions at the network's edge. However, their method required higher storage and processing overhead due to integrating the full nodes of the Blockchain. In the same context, the Global Blockchain Infrastructure method has been proposed in [21] to implement edge devices' traceability. Unique digital fingerprints (device IDs) using SRAM-based Physically Unclonable functions (PUFs) were generated. Registered manufacturers upload an ether key-value store or smart contract instance of Blockchain that is accessible to everyone with a cryptographic hash of each device ID. The end-user checks the hash's presentation in that Blockchain while locally registering or identifying the device to prevent cloning. Their method reduced the possibility of information leakage and sabotage in crucial infrastructure and large-scale deployments (like smart cities) brought on by adversary devices.

For IoT healthcare applications using Blockchain for the secure transmission of healthcare IoT data, researchers in [22] proposed a mathematical framework, an Advanced Signature Based Encryption Algorithm (ASE), an analytical model for healthcare IoT device identification, and Patient Health Data (PHD) authentication. It also proposed a three-tier fog computing Blockchain architecture. Each fog node is given one of the created keys in its model. For secure data conversion in the IoT, the authorized PHD created by IoT devices is stored on fog nodes using Ethereum Blockchain-based PoW technology. Decentralized healthcare data processing at the edge of IoT networks is secured using Blockchain technology.

Moreover, to satisfy security requirements without a trusted third party, Lamport Merkle Digital Signature (LMDS), a Blockchain-assisted extremely secure solution, has been presented by [23]. The authors used a cloud IoT network powered by Blockchain and connected it with patient and hospital healthcare records. Based on their experimental analysis, the suggested LMDS strategy enhanced security and reduced computational overhead and computational time. Rather than researchers in [24] developed a solution based on InterPlanetary File System (IPFS) and Blockchain to secure and protect e-health records. The data from IPFS were distributed among the nodes. The stored records in IPFS have the advantage of being dispersed and thus tamper-proof. The flexibility of the gadget and the reduced computational complexity of the proposed method allowed the patient to receive reliable medical monitoring from the doctors in a secure manner.

In addition, to enhance security, the authors in [25] presented a work to improve energy efficiency for IoT networks. They proposed a framework of software-defined networking (SDN) controller routing protocol with a cluster topology based on Blockchain technology. In the suggested design, private and public Blockchains would take the place of PoW for peer-to-peer (P2P) communication between the IoT devices and the SDN controllers. The proposed protocol could assist in resolving issues with next-generation industrial cyber-physical systems, such as security and energy management. Finally, in [26], the authors presented a Blockchain-based Trusted Network Connection protocol (BTNC). They achieved platform attestation, mutual user authentication, and trustworthy network access across IoT terminals using cryptography, ensuring terminal dependability without the necessity of a reliable third party. This system may enhance the security and viability of trustworthy network connections based on Blockchain, as well as detect unauthorized users, unlawful platforms, and platform replacement attacks.

3. METHODOLOGY

The Internet of Things (IoT) is a network that uses information-sensing devices to link everything to the Internet and conducts data exchange and communication to achieve intelligent identification, administration, monitoring, tracking, and placement. It is one of the technologies advancing the most quickly and has applications in almost every part of our lives, including national security, smart homes, smart gadgets, healthcare, and financial activities. Poor interoperability, security flaws, privacy concerns, and a lack of industry standards are issues that the IoT must deal with. Also, Cyber-attacks on IoT devices have the potential to compromise privacy and security. As a result, the IoT requires strong authentication and more security [27].

Since IoT requires strong authentication, the Blockchain is a promising technology that provides high security. Building a public, transparent, and long-lasting ledger system for data collection using blockchain technology is possible. The authentication of IoT using

Blockchain technology occurred and was managed at a decentralized digital ledger. This improves the speed of data storage in a Blockchain despite the fact that the technology is evolving quickly to address the high latency of the Blockchain nodes certifying transactions.

A Blockchain structure is shown in Figure 1. The genesis block of a Blockchain is the first block and has no parent block each block has a hash code, and each block should contain the previous hash code to connect the blocks.

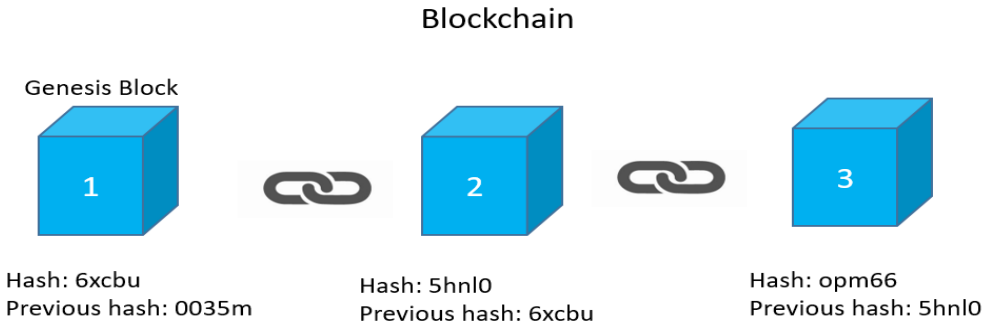

Fig. (1): The Structure of the Blockchain Component (Chain of the Blocks)

The proposed system is developed based on the Blockchain by using smart contracts that use software codes and computational infrastructure to activate the terms and conditions of a particular agreement or contract. They operate alone and enforce themselves.

The proposed system uses a virtual machine (EVMs) as an Ethereum Blockchain platform in which programs are run with arbitrary algorithmic complexity. EVMs are the heart of Ethereum. Every node in the network runs an EVM and puts its suggestions into action. In this paper, Ganache represents the EVM. It translates smart contracts to EVM and passes over nodes [29]. The Blockchain's capacity to handle transactions in a trustless environment makes it the most well-known framework for the execution of smart contracts. Smart contracts are computer programs coded using solidity language that formalizes digital agreements and automatically carries out any predefined conditions using the Blockchain consensus mechanism without needing a reliable third party. Ethereum Blockchain offers secure key pair in which public and private keys should never be transmitted over the network. This mechanism allows the authentication of data of the IoT devices safely and in a decentralized form. The smart contract includes two objects, the Application Binary Interface (ABI) and the bytecode. ABI is an essential object that allows users to understand the functionality of the smart contract. There should be an address to communicate with the deployed smart contract. Any IoT device that wants to use a smart contract's function uses ABI to hash the function and create an EVM bytecode [30]. The Ethereum Blockchain's purpose in this proposed system is to provide security for IoT devices.

Figure 2 depicts how the proposed system solved the data authentication issue in the IoT environment. The proposed system starts its mission when the user needs to add an IoT device. The device should be registered in the Ethereum Blockchain network in advance. During the registration process, the system assigned a private key. Accordingly, the system will ensure that the device is known or not. If the device is registered, then it will be added to the whitelist and will have the privilege to access the IoT network (Figure 2). Otherwise, if the device does not have the private key, it is unknown to the system and was not registered. Therefore, the device will be considered spam and added to the blacklist. The devices in the blacklist cannot access the systems, nevertheless. This is because registering the devices means their addresses are recorded in the smart contract. Therefore, the smart contract will allow connection whenever the registered device needs to access the IoT system. This is how Blockchain Ethereum has been implemented in this thesis. Smart contracts are a valuable part of Ethereum that improves the security of the IoT environment. They act as safeguards to keep data authentication and the security of the IoT network.

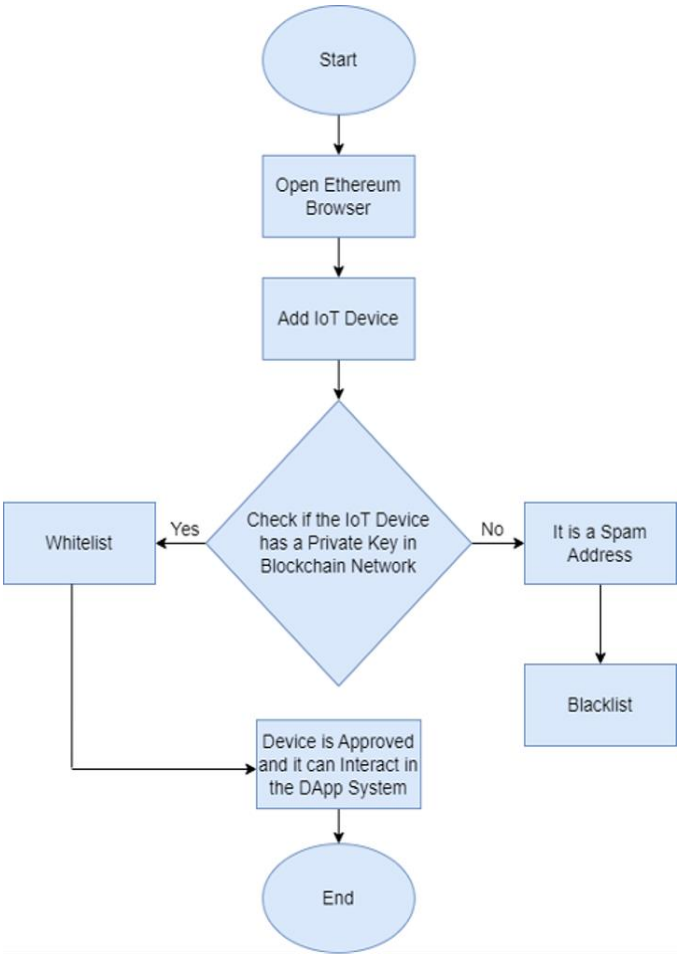

Fig. (2): The Flowchart for the Proposed Solution.

The design of the proposed method and the tools used in the implementation of the proposed method are shown in (Figure 3). The architecture of the proposed system is based on the three layers of the blockchain: the presentation layer, the management layer, and the blockchain layer.

The front-end layer represents the IoT presentation layer. This layer is concerned with the web-based GUI in which users can interact with the Ethereum Blockchain network. The GUI consists of the framework web3.js, Metamask, and contract ABI. Web3.js is a wrapper package for interacting with the JSON-RPC protocol used by Blockchain to prevent low-level conversion, which is prone to failures. Metamask is employed as an Ethereum-related wallet. An Ethereum wallet is needed per each IoT node, including the node's address (public key) and the data exchanged. The Ethereum wallet offers a flexible design that allows smart contracts to be maintained in a different chain code without significantly separating the core system's operation.

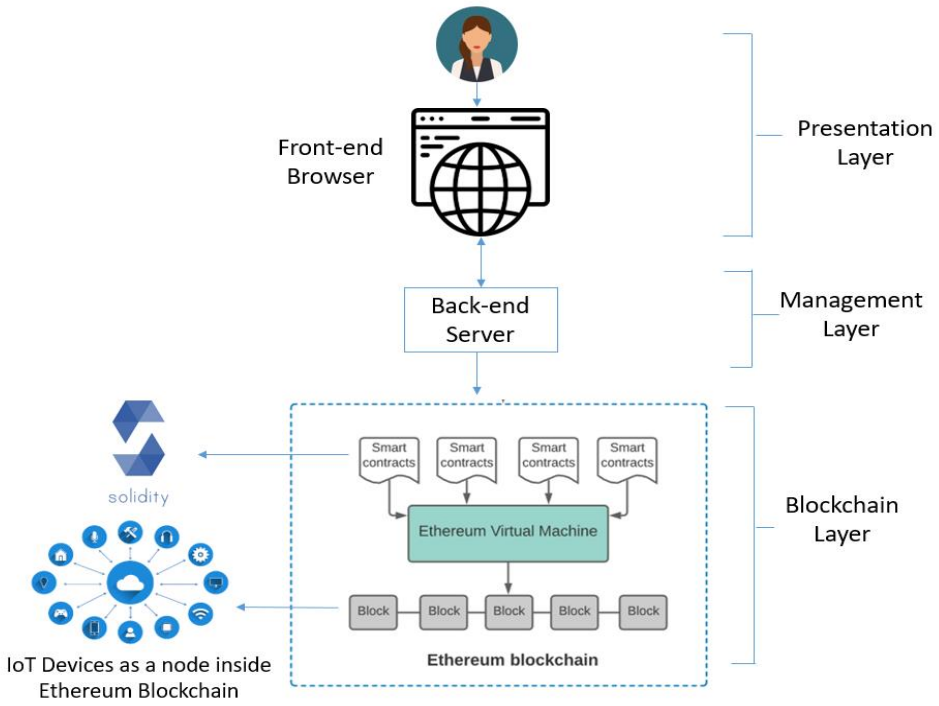

Fig. (3): The Architecture Layers of the Proposed Method.

The second layer is the management layer (back-end server), which links the presentation and blockchain layers. It offers more functionalities, such as a guarantee to do away with the need for callback functions and synchronized exchange of data to give the user complete control by using a private key of each IoT node after a data transfer. This layer uses the node package manager (npm) to deploy the smart contract. The npm is included within Node js. The Node js represents a server that connects the Ethereum Blockchain network with the smart contact via the npm commands.

The third layer in the proposed method is the Blockchain layer. It represents all the block nodes in the Ethereum Blockchain network. In this paper, the blocks represent IoT devices. The block is the small unit in the Blockchain that contains the transmitted/exchanged data within the chain. Cryptographic hash functions are used to hash and sign all transactions. The created hash value links each block together. The Blockchain uses consensus rules to carry out system operations to confirm transaction requests. When an IoT device requests a transaction, a block is transmitted to each node in the network. Each node then performs block validation and admits the block into the chain [31]. The structure of the Blockchain offers an unforgeable log holding a record of all previous transactions. Therefore, each block stores all the transmissions related to – carried out through. As a result, every node synchronizes its replicated state worldwide across the Blockchain in a completely verifiable way by every system user.

4. RESULTS AND DISCUSSION

The proposed system comprises an Ethereum private Blockchain, a front-end application on a local web server, and a smart contract published on the private Blockchain. The smart contract is Dapp's business logic. The contract owner uses her/his Ethereum to deploy the contract on the Blockchain. All IoT nodes (devices) are assumed to function normally during the experiments. The network is also adequately planned for and put in place. Aside from the faults created, especially for the testing scenario, the network devices had no other problems. Additionally, it is believed that all participants in the Blockchain follow the rules and algorithms established by the Ethereum protocol. Furthermore, the proposed system assumes that the users are registered in advance.

Blockchain platforms have scripting languages that are complex and robust enough to develop, secure, and handle a variety of tasks. Additionally, they are used for the beginning and end of transactions and the generation of smart contracts for many applications. This article defined two types of platforms in use. The first is the Cloud platform (real environment), and the

second is the Blockchain EVM Applications (simulation). For implementing the method proposed in this article, the work started to be implemented in a real environment. However, there were significant obstacles in creating the EVM in both Microsoft Azure and Amazon Web Services (AWS). These obstacles include the requirement for high security and a high-quality internet connection. Local internet service providers such as KOREK, ASIACELL, FASTLINK, and FTTH were used to access the URLs. Even with the use of VPN (even those recommended by their companies) and PROXY to access the Ethereum URLs, network accessibility was not possible. Therefore, we moved to an alternative solution: the Blockchain EVM applications using Ganache.

This article suggests two lists: the whitelist and the blacklist. The whitelist is constructed to contain authorized users who have gained their private keys. In contrast, the blacklist is designed to prevent unauthorized users from being classified as spam or attackers (Figure 4). When users attempt to interact with the IoT network, the system will first check their private key. If it is safe, the IoT device address will be added to the whitelist; otherwise, the system will give an alert and add it to the blacklist. The proposed method can be easily used to identify attacks and has fast responses to them.

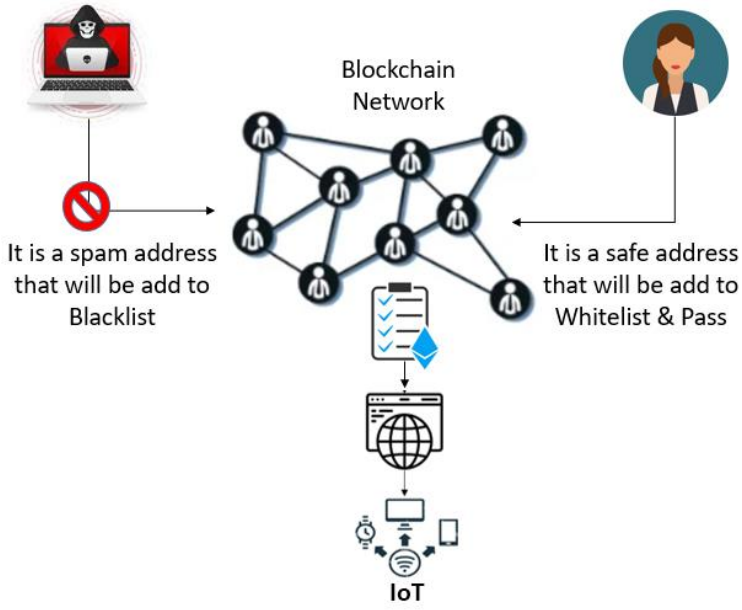

Fig. (4): The Implementation of the Proposed Method.

The smart contracts are implemented upon Solidity, object-oriented language and one of the most widely used in Ganache. The Ganache network can be accessed using the remote procedural call (RPC) server on the port of http://127.0.0.1:7545. This RPC server will be added to the Metamask wallet network to open the Ethereum Blockchain network inside the Dapp.

In this work, ten addresses have been assigned in Ganache to create the IoT network that will be used as a testbed for the proposed system. Each address represents an IoT device with its private key, as shown in Table 1.

Table (1): Registered IoT Devices Address and their Private Keys (Whitelist)

	Device Address	Private Key
1	0x3Bb1539D44194d6FA022e6D72182159D81d44019	bd83e121fd09f287770e74eef8f99d942cdb4154b50ad df87168b510495c1a88
2	0xcB06D88A2DbF6063E0DCb41c8aCafa59D746c3A8	dc1ea7360ded98e522f088916d7f84c2f64864112017 babfef2fc2dfbaaa3ac0
3	0xE0260b6406D18982b64b8F89AfFC0CeF2EA32618	86a8eb2f4cad26cfe505f7f06a966aaffa96d95278ca70 b2b78748090db1d6ed
4	0xb56A4116e71C00F8208d994c4f6DB8F9a2BE4A98	0d12a704329add798ecf562d5b446b5c5118471e1f17 fe32241dc10b47a7cc58

5	0x46933bA5cFfad705006179c1208FD7063a8A8e91	73d92ba3b4a2b19e87be76882d2d628650ce120a53b da28d2b757b4c4783f54c
6	0xC7147B6196708dDbA9CEd2c6035B8B1cd3Ee4Aa9	4c3972d8aab670895094c95faeb77d3b0a3c624887b 78c9369fa60e008a5e544
7	0xA94D30a3A9310BC4C8E5076F462a756CDC012919	c48640a31087bb54ea7f7bd4bba58a5835906fdde336 f43d8c20f8b53226f5de
8	0xF672e59CBc09244F9f530430463ffd5666518e7f	d18229d39745c40c29f6a84d7d24377dac71ac82c3ed 176f3f8c0ba2e0d4e253
9	0xD4F74205a72416108B22665bB5f1E0c987CE3530	7901c22b01dd3bcfbdd837c05be710e1609c739341a d0e859cbe7038309ec70a
10	0x5366f58a591669e558E3719BdB4e531f8ADAEF66	dc7a943b3c9526f34e2cb35645451539a3461a53aa6 3c72a35d3d9ff680c577e

Table 1 represents the whitelist in the proposed system. Once a new IoT device enters the Dapp through Metamask with its address, and private key, the device address and the private key will be checked and compared with the whitelist. If the device is registered, then it is safe, and it will be set to the Whitelist; otherwise, it will be classified as spam and will be added to the Blacklist.

The approach of blockchain technology to secure an IoT system has been implemented in [26]. However, in their method, the authors utilized a publicly distributed Blockchain, which is more expensive for storing large amounts of data. Whereas the method suggested in this article uses a private Ethereum Blockchain, which provides additional privacy, less cost, and efficiency by utilizing smart contracts that never change.

The work in [21] also presented a technique to protect the IoT environment by deploying unique digital fingerprints for device IDs using SRAM-based PUFs. Similarly to our approach, the SRAM generated unique digital fingerprints (in our case, we use the private key). The authors paid attention to one of the many security challenges: the need to track every device before it is used in a system. Additionally, PUF-based solutions have additional costs for helper data storage and protection due to the dependability and security problems intrinsic to PUFs.

The results of implementing the proposed system showed its simplicity in identifying attacks and quick response to them. Therefore, it can be utilized to save the IoT network from attackers and spam addresses. Additionally, the solution also improved authentication in the IoT environment. Furthermore, each Ethereum node stores a copy of the Blockchain data, which reduces storage costs since it takes advantage of the decentralization feature.

5. CONCLUSION

In this paper, a method for data authentication in an IoT system has been proposed. The proposed method is based on the Ethereum Blockchain network's implementation to increase the security of the IoT system during the data authentication process. Blockchain technology provides the IoT system with decentralized, immutable, and transparent features. The proposed method is demonstrated using Ganache (a Blockchain simulation platform). Additionally, the proposed method suggested using two lists in identifying the IoT devices. The whitelist in which the safe IoT devices are registered and the blacklist in which the spam devices will be registered. When a particular device wants to connect to the IoT network, its address will be checked to identify it as a friend device (being saved in the whitelist) or an attacker device (being added to the blacklist). The results showed that the proposed system could protect the IoT network from attackers and spam addresses.

Blockchain can be effective in a simulated IoT system. More research is needed, however, to test models in real-world scenarios and experiment with new types of attacks. In the future, instead of a simulation with real IoT devices, a real Ethereum Blockchain network should be used to protect them from any attack that may damage the IoT environment.

REFERENCES

D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, *IoT fundamentals: networking technologies, protocols, and use cases for the Internet of things*. Indianapolis, Indiana, USA: Cisco Press, 2017.

D. A. Linares, C. Anumba, and N. Roofigari-Esfahan, "Overview of Supporting Technologies for

Cyber-Physical Systems Implementation in the AEC Industry," in *Computing in Civil Engineering 2019*, Atlanta, Georgia, Jun. 2019, pp. 495–504. doi: 10.1061/9780784482438.063.

C. Sauerwein, I. Pekaric, M. Felderer, and R. Breu, "An analysis and classification of public information security data sources used in research and practice," *Comput. Secur.*, vol. 82, pp. 140–155, May 2019, doi: 10.1016/j.cose.2018.12.011.

A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An Energy-Efficient SDN Controller Architecture for IoT Networks With Blockchain-Based Security," *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 625–638, Jul. 2020, doi: 10.1109/TSC.2020.2966970.

V. K. Calastry Ramesh, "Storing IOT Data Securely in a Private Ethereum Blockchain", doi: 10.34917/15778410.

G. Nebbione and M. C. Calzarossa, "Security of IoT Application Layer Protocols: Challenges and Findings," *Future Internet*, vol. 12, no. 3, p. 55, Mar. 2020, doi: 10.3390/fi12030055.

S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine Learning Based Solutions for Security of Internet of Things (IoT): A Survey," *J. Netw. Comput. Appl.*, vol. 161, p. 102630, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3680–3689, Jun. 2019, doi: 10.1109/TII.2019.2903342.

B. Ali and A. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," *Sensors*, vol. 18, no. 3, p. 817, Mar. 2018, doi: 10.3390/s18030817.

W. Alnahari and M. T. Quasim, "Authentication of IoT Device and IoT Server Using Security Key," In Review, preprint, Feb. 2021. doi: 10.21203/rs.3.rs-175858/v2.

L. Vishwakarma and D. Das, "SCAB - IoTA: Secure communication and authentication for IoT applications using blockchain," *J. Parallel Distrib. Comput.*, vol. 154, pp. 94–105, Aug. 2021, doi: 10.1016/j.jpdc.2021.04.003.

Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.095647.

S. F. Aghili, H. Mala, C. Schindelhauer, M. Shojafar, and R. Tafazolli, "Closed-loop and open-loop authentication protocols for blockchain-based IoT systems," *Inf. Process. Manag.*, vol. 58, no. 4, p. 102568, Jul. 2021, doi: 10.1016/j.ipm.2021.102568.

M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, "Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture," *Energy Rep.*, vol. 7, pp. 8075–8082, Nov. 2021, doi: 10.1016/j.egyr.2021.07.078.

R. Almadhoun, M. Kadadha, M. Alhemeiri, M. Alshehhi, and K. Salah, "A User Authentication Scheme of IoT Devices using Blockchain-Enabled Fog Nodes," p. 8.

A. Mukherjee, M. Balachandra, C. Pujari, S. Tiwari, A. Nayar, and S. R. Payyavula, "Unified smart home resource access along with authentication using Blockchain technology," *Glob. Transit. Proc.*, vol. 2, no. 1, pp. 29–34, Jun. 2021, doi: 10.1016/j.gltp.2021.01.005.

R. Martino and A. Cilardo, "Designing a SHA-256 processor for blockchain-based IoT applications," *Internet Things*, vol. 11, p. 100254, Sep. 2020, doi: 10.1016/j.iot.2020.100254.

M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Inf. Process. Manag.*, vol. 58, no. 3, p. 102482, May 2021, doi: 10.1016/j.ipm.2020.102482.

W. Meng, W. Li, S. Tug, and J. Tan, "Towards blockchain-enabled single character frequency-based exclusive signature matching in IoT-assisted smart cities," *J. Parallel Distrib. Comput.*, vol. 144, pp. 268–277, Oct. 2020, doi: 10.1016/j.jpdc.2020.05.013.

A. Douglas, R. Holloway, J. Lohr, E. Morgan, and K. Harfoush, "Blockchains for constrained edge devices," *Blockchain Res. Appl.*, vol. 1, no. 1–2, p. 100004, Dec. 2020, doi: 10.1016/j.bcra.2020.100004.

U. Guin, P. Cui, and A. Skjellum, "Ensuring Proof-of-Authenticity of IoT Edge Devices Using Blockchain Technology," in *2018 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)*, Halifax, NS, Canada, Jul. 2018, pp. 1042–1049. doi: 10.1109/Cybermatics_2018.2018.00193.

S. Shukla, S. Thakur, S. Hussain, J. G. Breslin, and S. M. Jameel, "Identification and Authentication in Healthcare Internet-of-Things Using Integrated Fog Computing Based Blockchain Model," *Internet Things*, vol. 15, p. 100422, Sep. 2021, doi: 10.1016/j.iot.2021.100422.

J. A. Alzubi, "Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare," *Comput. Commun.*, vol. 170, pp. 200–208, Mar. 2021, doi: 10.1016/j.comcom.2021.02.002.

S. Sabu, H. M. Ramalingam, M. Vishaka, H. R. Swapna, and S. Hegde, "Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain," *Glob. Transit. Proc.*, vol. 2, no. 2, pp. 429–433, Nov. 2021, doi: 10.1016/j.gltp.2021.08.033.

S. A. Latif *et al.*, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Comput. Commun.*, vol. 181, pp. 274–283, Jan. 2022, doi: 10.1016/j.comcom.2021.09.029.

J. Zhang, Z. Wang, L. Shang, D. Lu, and J. Ma, "BTNC: A blockchain based trusted network connection protocol in IoT," *J. Parallel Distrib. Comput.*, vol. 143, pp. 1–16, Sep. 2020, doi: 10.1016/j.jpdc.2020.04.004.

F. B. J, R. R, S. M, and G. M. N R, "IoT based Cloud Integrated Smart Classroom for smart and a sustainable Campus," *Procedia Comput. Sci.*, vol. 172, pp. 77–81, 2020, doi: 10.1016/j.procs.2020.05.012.

[28] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020, doi: 10.3390/s20133625.

L. Ante, "Smart Contracts on the Blockchain – A Bibliometric Analysis and Review".

J. J. Hunhevicz, M. Motie, and D. M. Hall, "Digital building twins and blockchain for performance-based (smart) contracts," *Autom. Constr.*, vol. 133, p. 103981, Jan. 2022, doi: 10.1016/j.autcon.2021.103981.

K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, Jul. 2018, doi: 10.1007/s10916-018-0982-x.