Efficient Integrated Blockchain-based Authentication System for IoT

[1]A.Jeevananthan, [2]C.Poongodi, [3]K.Pavithra, [4]M.Vignesan, [5]R.Yuvan shankar
[1,2,3,4,5]Department of Information Technology, Kongu Engineering College, Perundurai-638060, Erode(dt)
[1]jeeva.it@kongu.edu, [2]poongs.it@kongu.edu, [3]pavithrakrishsnamoorthy98@gmail.com, [4]manovicky3799@gmail.com, [5]yuvanshankarit@gmail.com

Abstract

In day-to-day life, the Internet of Things(IoT) plays a major role. Without the human interface, data is stored and shared in IoT. These entities are also implemented in open environments to provide a smarter and easier way of living such as smart homes, smart cities, etc. Because of this complete autonomy, these entities need to be acknowledged and authenticated with each other and therefore ensure the validity of their data exchanged. Otherwise, malicious users and malicious use will target them. Because of the size and features of IoT an efficient centralized authentication system cannot be created. In this paper, the IoT devices have an efficient decentralized authentication and access control framework which applies to a smart hospital.

Keywords: *Blockchain, Lightweight, Internet of Things, Authentication, Smart hospital*

1 Introduction:

The Internet of Things is a collection of interrelated devices with unique identifiers (UIDs) and which can transfer data through a network without involving any interactions neither between the humans nor between the human and a computer. Things like sensors, when connected to the internet can share data from its environment to another device or to the cloud storage. Thus the IoT devices help an individual by making things work more smartly thus reducing the labor costs. Apart from these advantages, major issues have also been raised in the implementation of IoT. Some of the issues in IoT are shown in Figure 1. The first issue being the resource constraint where there has been a limitation to the parameters such as bandwidth, memory in the IoT devices making it inefficient to fulfill the security issues. The centralized system architecture in the IoT devices is posed as the second issue since a failure to the central hub interrupts the whole network. The final issue is the lack of security of the data which is being shared between the devices.

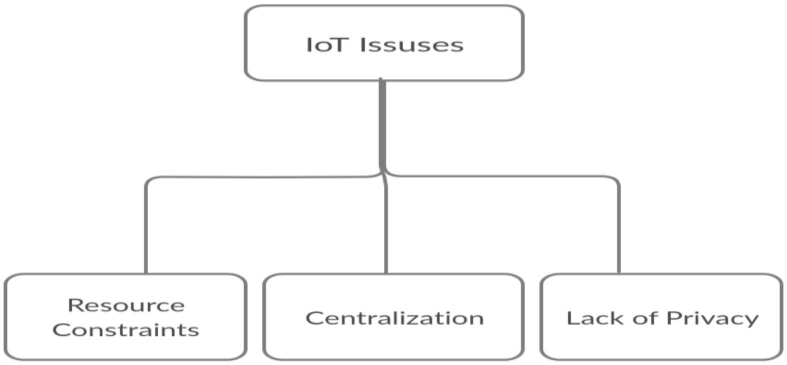

Figure 1. IoT Issues

To overcome these issues, IoT has been integrated with Blockchain Technology. This technology is used since it contains a decentralized architecture, and it also uses a cryptographic hashing algorithm and that makes the digital asset unalterable and as well as transparent. Thus the integration of this technology has improvised the security of the data being shared.

The smart hospital system is taken as a case study due to its significance in the COVID-19 scenario. In the above-proposed system, the centralized IoT system has been converted into a distributed system where the patient's data will be stored securely. For example, when a cured corona infected patient is discharged from the hospital, he/she is advised to be kept under observation for a couple of days. The doctor has mounted the tool for safety monitoring to track and monitor the patient. However, the health monitoring device communicates with the doctor, health department and, also with the devices in smart homes. When there are any abnormalities in the health condition of a patient, an emergency alarm is triggered and a notification is sent to them. A distributed authentication is required, to ensure that only the permitted devices exist in the network. If all these devices authenticate with each other that will cause a delay in time and therefore if one device authenticates with any one of the other devices then that need not be re-authenticated another time.

2 Problem Statement

Authentication is an important aspect that is required to achieve secure communication in a network. High energy is consumed during high overhead communication in the present IoT authentication due to its centralized architecture. These conventional methods are not suitable due to their heterogeneous and resource-constrained nature. To overcome these issues, a lightweight decentralized authentication mechanism that is based on blockchain is proposed which overcomes the above-mentioned issues.

3 Blockchain

Blockchain is a decentralized system. There are multiple numbers of blocks linked to each other forming a blockchain. The data of a particular device is stored in a block along with the header and hash values of the previous block. The hash value in a block is a random number generated for data and header in a block. Any changes made to the data in a block causes a new hash value to be generated. The difference in the new hash value and the previous value stored in its next block indicates the person that his data has been modified. The above-explained process is diagrammatically shown in Figure 2.

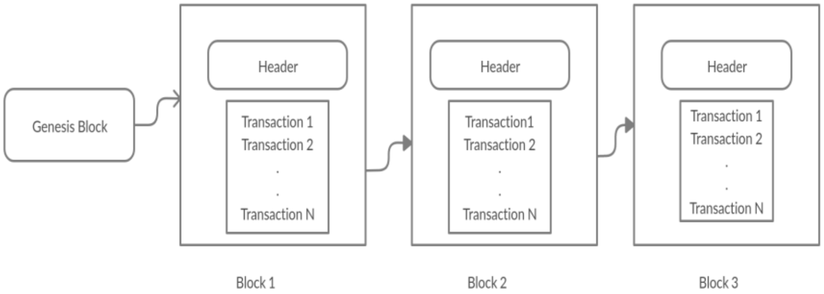

Figure 2. Simple Blockchain Structure

4 Literature Survey

Umair Khalid, Muhammad Asim, in this paper the major problem is more power consumption and centralized authentication. To overcome these problems they go for the lightweight integrated blockchain to reduce the power consumption and enhance the security level [1].

Nadeem Abbas, in this paper the problem is security threats and high energy consumption. To overcome those attacks they go for fog computing. It can minimize security risks and use various cryptographic techniques to reduce energy consumption [2].

Samet Tonyali, Kemal Akkaya, in their paper the problem is privacy when they are dealing with high-frequency data collection. To overcome these problems they go for the two mechanisms: one is secure multiparty computation (secure MPC) and another one is fully homomorphic encryption (FHE) to enhance privacy [3].

Chi Ho Lau,Fan Yan in their paper the major problem is security and more time consumption. To overcome these, an access control mechanism can be used to neglect those security issues and time delay [5].

Bin Liu, in this paper the problem is the third party users can access the device, here we go for the blockchain technology to overcome the security threats[7].

Jongho Won, Elisa Bertino, in their paper the drones will communicate with many different smart entities, such as sensors and built-in devices. Here the problem is security. To overcome these issues they use the efficient certificateless sign encryption algorithm to overcome these issues [9].

Muhammed Naveed Aman, in his paper it represents a great opportunity to link people, knowledge and things, which in effect, will trigger a paradigm shift in how we function, communicate and think. Here the problem is more energy consumption and security problems. Here they use the Physical Unclonable Function (PUF) protocol to overcome the security issues and consumption of energy [11].

5 Proposed Methodology

This mechanism proposes a distributed authentication and authorization over the same system or different systems. Communication can be made in this blockchain-enabled fog node over the same system device or different systems.

5.1. System Architecture

The system architect may deal with smart devices(such as home, hospital and healthcare system) for system authentication and authorization process. First of all the devices connected in the blockchain may transmit data to all the blocks in the blockchain. There are two layers: One is a device layer in which the IoT devices are interconnected for sensing, interacting and authenticating. The other one is the fog layer, which contains the fog nodes. The fog node may communicate data in the blockchain and they transmit it to the respective devices via the network. The devices connected in the blockchain ensure the smart contract (i.e) it has the set of rules that indicate in the blockchain and it also ensures that all devices in the blockchain may transmit data in a distributed manner.

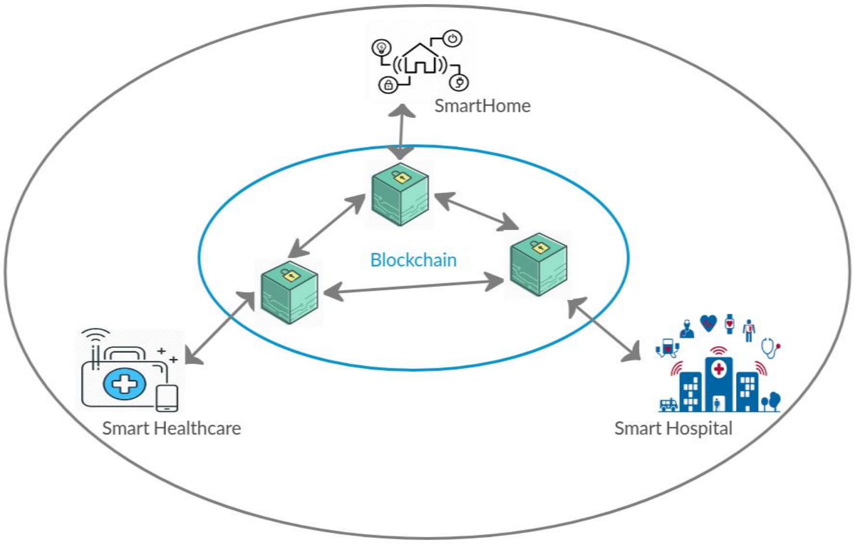

Figure 3. Proposed Function Architecture

5.2. System Functioning

The system functioning may consist of the following steps.

Adding a new device: First of all, we need to add a new system to the network. The network can check the device, whether it has a unique identification or not. After adding a new device then it steps onto the registration process.

Registration process: After the addition of a new device, it should go for the registration process. The registration process should only work for the added devices in the network. The registration process should carry some identification credentials. After the registration process, you can authenticate with the blocks in the blockchain.

Communication process: After registration, you can communicate with the systems either with the same systems or different systems in the blockchain. By using this communication process you exchange data in the blockchain.

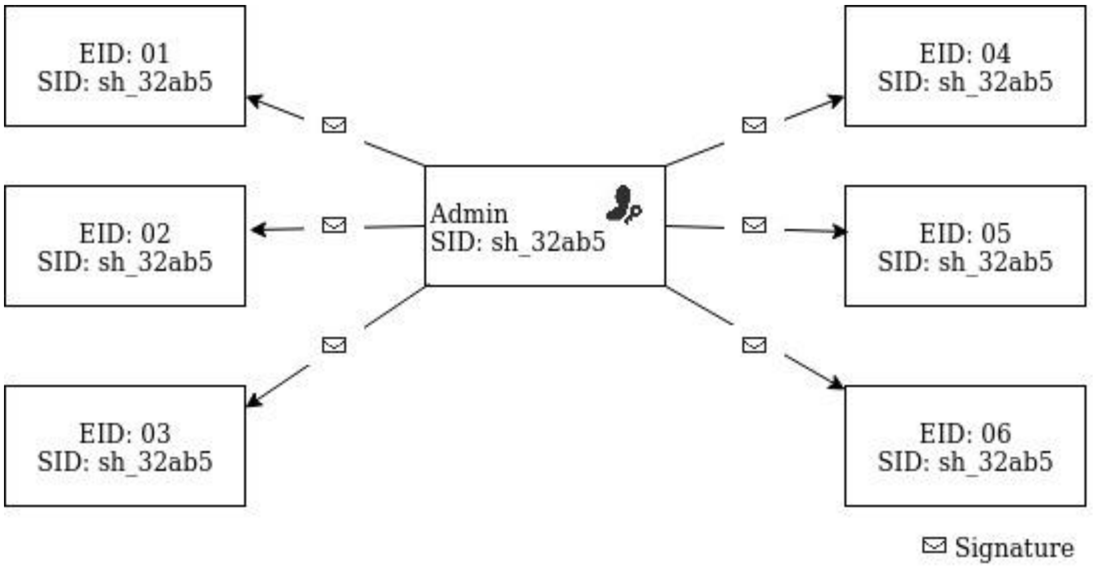

Figure 4. Signature Distribution Among Smart Devices

In Figure 4 shows the distributed signature among devices of smart devices(such as smart home, smart hospital). Admin sharing the signature key from the center to all the blocks. Every block should contain smart devices. The admin shares the token(SID) to each device in the block. Then the smart contract checks the legitimate certificate and existence in the blockchain node. The registration token is available or not in the blockchain and will be checked by the smart contract. After the registration process, we have to map the device between EID and SID. After that, the block is then distributed among the fog nodes enabled with blockchain. This type of authentication process will be used in future.

5.2.1. Types of communication

These two types of communications have been used in this proposed system

1.Device to Device communication: It is a key enabler to facilitate the realization of the internet of things, in which the devices directly communicate with each other. Once it is successfully authenticated, they enable a secure connection and transfer among data.

2.Device to Fog communication: It supports the IoT concept, in which the devices used by humans in daily life may interconnect with each other. The device to fog communication has some methodologies to connect. The first one is to register with the IoT systems and then connect the fog node to the enabled blockchain. Another one is to get authentication to enable secure communication over nodes and devices.

5.2.2. Authentication Mechanism

The authentication mechanism works for authentication and authorization purposes in the blockchain. First of all, a new device should be added to the network in the blockchain. After adding new devices we should go for the registration process, this process should only be valid for devices in the blockchain. After registration, they should get authentication to transmit data over devices. Once they get the authentication they can access the devices. In this authentication mechanism, if someone opens his authentication, the blockchain will check whether it is valid or not. If it is valid it enters into the system. If not it exits out of the system.

5.2.3.Elliptic Curve Digital Signature Algorithm

For key generation, the ECDSA algorithm will generate public keys for the blockchain nodes. In this ECDSA algorithm, the public key bit size will be double the size of the security level. This algorithm needs only less energy, it is a major advantage of this algorithm. In this algorithm, the key used for encryption should be public, thus the name public key. By using this algorithm we enhance the security level and we have to reduce energy consumption.

6 Experiment and evaluation

In this experiment section, the validation purpose is to enhance security and protect against attacks. We predict two approaches i.e time and power consumption in this experiment. These approaches are compared with the state of the art systems.

6.1. Experimental setup

In this experimental setup, the evaluation of 50 experiments validation process can be presented. It holds laptops as a distributed node and raspberry pie as a centralized node. A Connection is made between each fog node with the 2 raspberry pi system. For interaction between the devices, the end nodes were developed by using C++ language. All the communication was done using the JsonRPC library between the nodes. Therefore the description of tools as shown in Table 1.

Tools	Description
Ganache-cli	Ethereum emulator.
QT Framework(IDE)	Node interface development in C++.
JsonRPC	Nodes and blockchain communication interaction.
Truffle	Compilation and deployment of smart contracts.
Remix(IDE)	Developing the smart contract

Table 1. Tools Description

6.2. Evaluation against attack

Masquerade Attack: This attack requires a fake identity like a network identity for an attacker for unauthorized access.

Spoof Attack: When an attacker tries to pretend like a trusted source and gains the attention of the person who is having the secured data.

7 Time consumption

The most important factors for these experiments are the consumption of time and power. We start with time consumption i.e time taken in the minimum amount to complete the authentication process with the rest of the systems. By using this authentication pass we can repeat our authentication with the devices on the same or different systems.

In Figure 5, it indicates the time compared with the bubble of trust and the proposed approach by using the device as a centralized node and distributed node. We take average value for the centralized node and the distributed node. The minimum time required for the bubble of trust is 1.00ms, and the maximum time is 1.42ms. The maximum time taken to generate a data message for the proposed approach is 23.54ms, and the maximum time for the proposed approach is 28.54ms. In this below table the time consumption is comparatively low for the distributed node in both bubble of trust and proposed approach when compared the centralized node. So we propose a distributed one. The below Table 2 shows the time consumption for the centralized node and distributed node.

Approach	Centralised node	Distributed node
Bubble of trust	1.42	1.00
Proposed approach	28.54	23.54

Table 2. Time Comparison

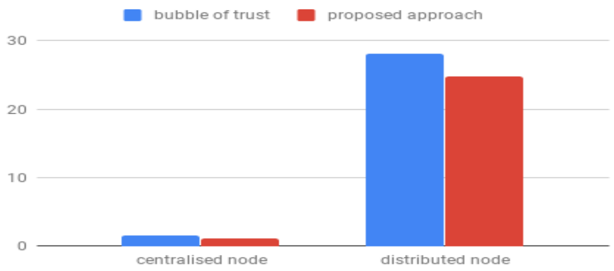

Figure 5. Time Consumption

8 Power Consumption

The next one is power consumption i.e. a minimum amount of energy required by a system to authenticate with the system. Table 2 shows a time comparison with the bubble of trust and the proposed approach by using the device as a centralized node and distributed node. Existing methods consume more power during the registration process by sending many messages.

Figure 6 shows a power comparison with the bubble of trust and the proposed approach. We take average value for the centralized node and the distributed node. The minimum power required for the bubble of trust is 6.25mW, and the maximum power is 8.36mW. The minimum power required to generate a data message for the proposed approach is 57.12mW, and the maximum power for the proposed approach is 62.16mW. Below Table 3 shows the power consumption for the centralized node and distributed node.

Approach	Centralised node	Distributed node
Bubble of trust	8.36	6.25
Proposed approach	62.16	57.12

Table 3. Power Comparison

9 Conclusion

The proposed methodology helps both an individual and the smart hospital workers to track the health condition of the patients. It has been developed in such a way that the patient's data is highly secured and authentication is required for accessing the data. There is no need for a patient to go to the hospital and check for his/her health condition during the pandemic time.

References

1. Umair Khalid, Muhammad Asim, Thar Baker, Patrick C. K. Hung, Muhammad Adnan Tariq, Laura Rafferty: A decentralized lightweight blockchain-based authentication mechanism for IoT systems, Blockchain that provides distributed authentication between hospital and the smart home.
2. Nadeem Abbas, Muhammad Asim, Noshina Tariq, Thar Baker, Abbas, S.: A mechanism for securing IoT-enabled applications at the fog layer. Journal of Sensor and Actuator Networks 8(1):16 (2019).
3. Samet Tonyali, Kemal Akkaya, Saputro, N., Uluagac, A.S., Mehrdad Nojoumian,: Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. Future Gener. Comput. Syst. 78, 547–557 (2018).
4. Mukrimah Nawir, Amiza Amir,, Yaakob, N., Ong Bi Lynn: Internet of Things (IoT): taxonomy of security attacks. In: 2016 3rd International Conference on Electronic Design (ICED), pp. 321–326 (2016).
5. Chi Ho Lau, Alan, K.-H.Y., Fan Yan: Blockchain-Based Authentication in IoT Networks. In: 2018 IEEE Conference on Dependable and Secure Computing (DSC), pp. 1–8 (2018)
6. Fan Wu, Xiong Li, Lili Xu, Kumari, S., Karuppiah, M., Shen, J.:A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud servers. Comput. Electr. Eng. 63, 168–181 (2017).
7. Bin Liu, Xiao Liang Yu, Shiping Chen, Xu, X., Liming Zhu: Blockchain based data integrity service framework for IoT data, Liming. In: 2017 IEEE International Conference on Web Services (ICWS), pp. 468–475 (2017).
8. Khan Muhammad, Rafik Hamza Ahmad, J., Jaime Lloret, Wang, H., Sung Wook Baik: Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans. Ind. Inform. 14, 3679–3689 (2018).
9. Jongho Won, Seo, S.-H., Elisa Bertino: A secure communication protocol for drones and smart objects. In: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, pp. 249–260 (2015).
10. Mrinmoy Barua, Xiaohui Liang, Lu, R., Xuemin Shen ESPAC: Enabling Security and Patient-centric Access Control for e-Health in cloud computing. Int. J. Secur. Netw. 6, 67–76 (2011).
11. Muhammed Naveed Aman, Kee Chaing Chua, Biplab Sikdar.: Mutual authentication in IoT systems using physical unclonable functions. IEEE Internet Things J. 4, 1327–1340 (2017).
12. S.B.Gopal , C.Poongodi, M. Joseph Auxilius Jude, S. Umasri , D.Sumithra, P.Tharani, Minimum Energy Consumption Objective Function For RPL In Internet Of Things. International Journal of Scientific & Technology Research Volume 9, Issue 01, January (2020).
13. Prof.M.Ramalingam, Prof.A.Jeevananthan, P.Keerthana, D.Indumathi, M.Nithyashree, S.ThilakRaj, N.NaveenKumar, R.Harish, Smart Attendance Monitoring System to Avoid Fraudulence by Synchronizing Results of RFID and Face Recognition System. International Journal for Modern Trends in Science and Technology Volume 03, Issue 03, March (2017).