As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology
Volume 9, Issue 10, pages 01-07.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol9issue10.html
DOI: https://doi.org/10.46501/IJMTST0910001

IOT Based Data Monitoring in Secured Block Chain Architecture

Veena P[1] | K. Anugirba[2]

[1]Lecturer, Department of Computer Science and Engineering, NSS Polytechnic College, Pandalam.
veenapadma@gmail.com
[2]Assistant Professor, Department of Computer Science and Engineering,Bethlahem Institute of Engineering, Karungal, Kanyakumari, Tamilnadu, India.
anurimal21@gmail.com

To Cite this Article

Veena P and K. Anugirba. IOT Based Data Monitoring in Secured Block Chain Architecture, International Journal for Modern Trends in Science and Technology, 2023, 9(10), pages. 01-07.https://doi.org/10.46501/IJMTST0910001

Article Info

Received: 12 September 2023; Accepted: 02 October 2023; Published: 06 October 2023.

ABSTRACT

The Internet of Things and blockchain technologies are mostly applied in the field of electronic healthcare. Here, IoT devices have the capacity to deliver patient sensor data in real-time for processing and analysis. Such an approach may result in distrust, data manipulation and tampering, and privacy avoidance as a single point of failure. Blockchain can assist in resolving such problems by providing shared computation and storage for IoT data. There are currently several healthcare solutions that just use IoT technologies. However, they have a centralised database, which is an issue. As a result, the data may not be safe and organizations may charge extra for storage. However, these issues are overcome by the use of blockchain technology, and the user is become the exclusive proprietor of his data. No one else may access the data without his permission. Here, securing and distributing the medical data is essential.

Key words: IoT - Internet of Things, HS – Healthcare System, EHRs – Electronic Healthcare Records, WBAN – Wireless Body Area Network.

1. INTRODUCTION

The IoT which enables remote access and ongoing patient data monitoring, has transformed conventional healthcare systems into intelligent systems. To gather real-time physiological data from patients, such as body temperature, blood glucose levels, and other essential information, wearable devices and other IoT-based medical equipment are employed. Indeed, the Internet of Things was benefit the healthcare sector by enabling quick clinical diagnosis and remote therapy that is successful. But since the IoT nodes in an IoT-enabled HS are constantly linked over an unprotected, open channel, the entire network is susceptible to data manipulation, eavesdropping, and other security-related problems. The lack of security considerations in communication protocols and the rapid growth of hacking techniques, wherein attackers try to undermine the availability, integrity, and dependability of IoT data and devices, are the particular causes of security concerns. These attacks may performed on genuine IoT devices with the intention of limiting their performance, in addition to being carried out on healthcare network components using malware or other malicious software. In order to address privacy concerns in IoT networks, assaults that are both passive and active (such as data poisoning attacks) must compromise sensitive and private data [1]. The breadth of communication between remote devices linked to the internet for data and access transmission has multiplied due to continuous developments in the IoT. As a result, practically every business on the planet has been revolutionized and disrupted by IoT, from the education sector to supply chain management. Decentralizing the IoT network provides a number of benefits, such as decreased costs for maintaining a central database for IoT transactions as well as increased security and privacy, which does away with the requirement for a third party. How these qualities may be used in IoT is still a mystery, though. This is mostly caused by the IoT devices' restrictions in computational capability, power, and storage [2].Blockchain technology is a rapidly expanding area of study that can offer a safe foundation for storing encrypted data in many different industries. Due in large part to the rise of crypto currencies, it is a very common technology to enter a new domain. With its patient-centered approach to the integration of decentralized networks, which includes the accuracy of EHRs blockchain technology has enormous promise in the healthcare sector. It permits the administration of health records in a transparent and open manner. Blockchain technology does not need any centralized management to access EHRs [3].

A distributed shared ledger, often known as a blockchain, is an unchangeable store of data that is encrypted. It enables the interchange and storage of digital assets without the requirement for outside supervision. Devices that download configuration files from a centralized server must have confidence in that authority; otherwise, the device is susceptible. A blockchain eliminates the requirement for a centralized authority. Peer-to-peer is the direct exchange of assets between devices [4]. The blockchain has certain essential features that set it apart from a standard database. First of all, it is given out automatically. It is useless to operate a blockchain network with just one node. The records on the blockchain are also unchangeable, therefore it is impossible to erase or alter them. By doing so, the legitimacy would be compromised. The only way to update a record is to add a brand-new record. Smart contracts are used on the blockchain to guarantee the accurate application of established business rules. An agreement that is executed by nodes on the blockchain is known as a "smart contract." Smart contracts are also used to handle configuration files in IoT environments [5]. IoT systems must provide security for the data they gather, especially in terms of integrity and availability. By integrating a distributed and secure system, such as blockchain, these security aspects may be provided. Some IoT devices might not have the additional computing and storage resources needed for blockchain. However, the availability of edge computing capabilities was meet such requirements and enable the integration of blockchain. IoT devices may communicate and exchange data with users and other IoT devices using a decentralized, reliable, and secure approach that is made possible by combining edge technology with blockchain technology [6].

The WBANs, IoT devices, Big Data, Cloud, and Machine Learning may all be used to integrate blockchain. Together, WBAN and Blockchain technologies guarantee safe data transfer across shorter distance. IoT devices are employed in the Blockchain network to offer anonymity and responsibility for each transitional process. Big data provides countless opportunities for research and development, medical therapies, and personal health monitoring [7]. A copy of every transaction is maintained by all participants on blockchain, which is effectively a decentralized platform. The transactions are visible, making it simple to spot any changes. Think of a smart city where parking spots are displayed to users in real-time. The central database is updated when sensors find a vacant parking place. A system administrator in charge of this database has the ability to reserve a parking spot for himself without disclosing it to anybody else. The sensor data's integrity is at risk in this situation [8]. A blockchain network of connected devices is designed to do away with the need for a third party and, as a result, ensure that the real-time data produced by the sensor may reach every node in the network unaltered. Blockchain also enables IoT devices to connect with one another and make choices on their own [9]. A Prov-chain architecture is used to facilitate data collecting and validation. Prov-chain is required to safeguard private healthcare data, making healthcare more dependable. In a blockchain-based system, the Merkle tree structure offers logs and helps with data upkeep while retaining anonymity. The entries are verified using a timestamp definition, which makes it easier to manage the blockchain [10].

In recent years, blockchain technology has also demonstrated exceptional dependability across a range of industries, including smart homes, healthcare, banking, information storage management, security, and others.The management and processing of the enormous amount of data that the patient is producing must be done while upholding a secure protocol. Furthermore, the Blockchain Network further addresses the implementation of a key module, an access management system, where there are several stakeholders connected to the data being created [11]. The doctor may be given further access to the data, which will be used to help him or her treat the patient's condition appropriately and comprehend it. The wearable devices create data, which is then saved in an external cloud database that is controlled by the blockchain network. Therefore, prefer to suggest the blockchain idea, which is a coalition of many stakeholders such as hospitals, doctors, pharmacies, pathology labs, imaging centres, medical research centres, and insurance companies, for access management and storage of the data was secured to handle the transactions. As a result, such systems might be seen as an important part of raising society through precise and effective healthcare [12].

2. Proposed Work Explanation

IoT devices in the healthcare sector now operate under a centralised server/client approach. The issue with a centralised system is that the hospital controls the fundamental patient data and information, which might result in higher storage costs for consumers. In a centralised system, if there is no adequate backup, the entire database might be lost in the event of a single point of failure. The fact that healthcare data is private raises security issues since it would be simple for hackers to access the data from a centralised system. Another major issue with centralised healthcare approaches is interoperability. Therefore, it was putting up a strategy that addresses all of these issues by using both IoT and blockchain technology.

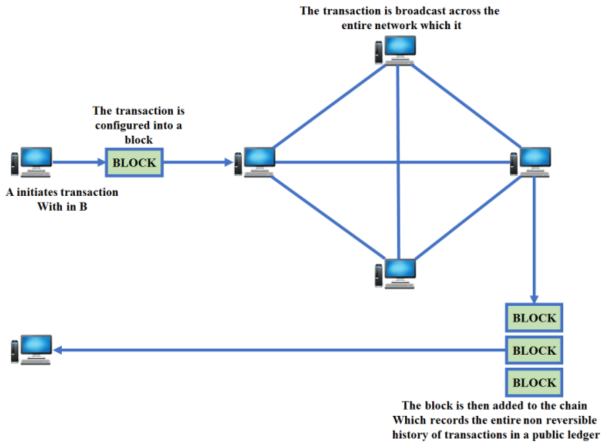
The transaction is broadcast across the entire network which it
The transaction is configured into a block
BLOCK
A initiates transaction With in B
BLOCK
BLOCK
BLOCK
The block is then added to the chain Which records the entire non reversible history of transactions in a public ledger

Fig.1. Proposed Diagram

A chain of blocks can be thought of as blockchain. Data, a hash, and the preceding block's hash are all included in each block. The kind of blockchain determines the data that is held inside a block; for instance, the bit coin blockchain holds information about the sender, recipient, and number of currency. A block's hash may be likened to a fingerprint. It always serves as a unique identifier for the block and all of its contents. The preceding block's hash is used to help create a chain of blocks, and it is this characteristic that makes blockchain so safe. Since it is the first and is referred to as the genesis block, the first block cannot point towards the prior block. A block's hash is determined after it has been produced. Figure 1 shows the block chain transaction through internet.

Transaction in the network can be initiated by any node.

- The first node that wants to do the transaction is the sender node. It creates a transaction and sends it to the network. The transaction message contains the cryptographic public address of the receiver, transaction details, and cryptographic digital signature of the sender.
- Every transaction is authenticated by the sender’s private key until it is transmitted to the network.
- This transaction is broadcasted to every node in the network, and they validate the authenticity of the message by verifying the digital signature. The authenticated transaction is placed in the pool of pending transactions.
- The pending transactions are encapsulated in a block by one of the nodes, and it also alerts all other nodes in the network about the newly built-in block for its validation.
- A great number of computational resources are required for validation. The nodes which validate the

block are called miners, and they are awarded by giving them incentives.

- The multiple systems use specific validation strategies. Bit coin, for example, requires proof of research. The key objective of this technique is to guarantee that any transaction is legitimate and that illegitimate transactions remain impossible. After authentication of all transactions, the new block is combined with previously chained blocks comprising the blockchain.
- The present condition of the ledger is then transmitted to the network.

3. PROPOSED SYSTEM MODELLING

3.1 Internet of Things

The IoT is a paradigm for effective computing that aids us in the operation of many systems utilized in our daily lives. When interactions occur in these IoT systems, the connectivity of multiple devices allows for the interchange of those devices. Mobile phones, smart sensors, and coffee makers are the most widely used IoT devices. IoT systems make it simpler for people and various objects to connect, but because of their fast speeds, they also produce massive amounts of data, making these systems more difficult in terms of data-related issues. In IoT systems, remote-controlled physical items and computer-based systems are integrated with the use of already-existing network infrastructure. IoT technology has reduced the amount of human interaction required to complete any task more accurately and efficiently. IoT systems have the ability to collect data from many types of sensors as well. Due of the cheaper prices of the sensors and actuators utilized in IoT-based technology, several organizations are expressing interest in it. IoT is being used in a number of healthcare management streams. Several applications of IoT in healthcare include:

Clinical Management: IoT-driven, unobtrusive checking can be used to continuously monitor hospitalized patients whose physiological condition demands particular attention.

Remote patient monitoring is made possible by Internet of Things devices, which enable wearable's to transmit medical data from a patient's home and deliver it correctly to a doctor's or nurse's office in a different place. These methods significantly reduce waiting times and make it easier for patients who are unable to travel to hospitals to get there.

Early Intervention/Prevention: IoT-driven checking systems help physically dependent and unwell persons in their everyday tasks. For instance, a senior living alone may require a monitoring sensor that may detect a fall or other obstruction in normal development and alert emergency personnel or family members.

Wireless Sensor Networks (WSNs): WSN is a fundamental IoT enabling technology. Through distant communication, it connects several sensor and actuator hubs to a framework. Through a framework passage, this joins the framework to a larger sum structure. The WSN is built with an IoT application game plan.

3.2 Streams of health care management in blockchain architecture

Clear, Comprehensive Medical Record: Longitudinal medical records-incorporating images, illness databases, test tests, medications can be done via blockchain like inpatient, walking and wearable details, allowing providers to learn for better methods of treatment distribution.

Total Patient List: Regularly records are crossed or copied when managing information on medicinal services is required.

Adjudication of Arguments: Since blockchain takes a shot at a permission-based transaction, cases will obviously be tested where the network fits with the way by which the arrangement is implemented.

Control of Supply Chain: Blockchain-based contracts will allow organizations with medical services to track the supply-request in moving through its entire life cycle. Examples are how the trade takes place or whether the transaction is effective or if there are any delays.

3.3 Working of blockchain

Information exchange in the past relied on centralised infrastructure. The centralised systems have several drawbacks. In distributed systems, the information-sharing process involves every node. Although centralised solutions have been found to be beneficial, they are not scalable or fault-tolerant. Consequently, the necessity to transition to a distributed or decentralized platform was felt. Blockchain is a decentralized network that allows for the secure exchange of information. In a blockchain, transactions are permanently recorded by adding new blocks to the shared ledger. From the genesis block to the most recent block, the blockchain acts as a historical record of all transactions that have ever taken place. Here, the objectives of blockchain in IoT are mentioned below:

a. To build a transparent, aggregated logistic network using blockchain and IoT.

b. The purpose of this paper is to protect client information from infringing parties.

c. This paper offers seven layers of a computational blockchain model.

d. In this paper, propose a blockchain approach and use of Ethereum Smart Contracts to apply IoT details to a mechanized version, including no mediator.

e. This paper involves adaptable network structures, more modules and steps based on the IoT structure.

f. Using blockchain technology to solve a significant problem involving high bandwidth overheads and processing time such that IoT is more suited.

g. This paper extends our knowledge of blockchain technology on the payment network.

3.4 Proposed methodology

IoT devices in the healthcare sector now operate under a centralised server/client approach. The issue with a centralised system is that the hospital controls the fundamental patient data and information, which might result in higher storage costs for consumers. In a centralised system, if there is no adequate backup, the entire database might be lost in the event of a single point of failure. The fact that healthcare data is private raises security issues since it would be simple for hackers to access the data from a centralised system. To avoid these issues the data was stored in the sensors for better security. Sensor data is the output of a device that detects and responds to some type of input from the physical environment. The output may be used to provide information to an end user or as input to another system or to guide a process. Sensors can be used to detect just about any physical element.Sensor data can either be stored local to the sensor node that collected the data (local storage), transmitted to one or more collection points outside of the sensor network (external storage), or transmitted and stored at other nodes in the sensor network (in-network storage).

•The first layer is the physical layer and consists of the patient whose data has to be recorded.

•The second layer is the device layer and consists of mobile phones (having sensors), wearable's, medical devices (CT scan, X-Ray), etc. These devices are used for measuring and transmitting the data from the patient end.

•The third layer is the communication layer. This layer is responsible for the transmission of data that is recorded by devices. The device can communicate directly to cloud through API or devices can communicate using LORA, Zigbee, and Profibus; further, MQTT and COAP are used to transmit data from gateway to cloud.

•The next is cloud interface which involves platform components that are further categorized as real-time engine and blockchain engine.

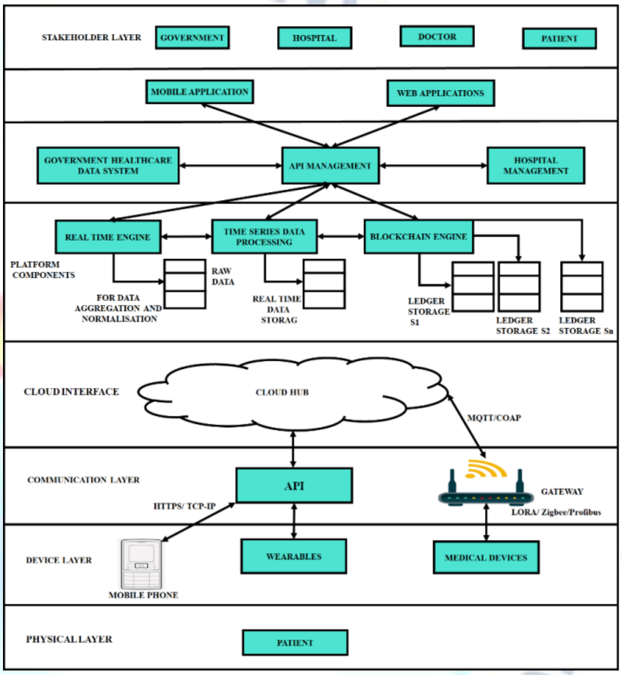

Fig.2. Working of Block chain

The data that is sent to the cloud firstly moves to the real-time engine where raw data is collected, and data aggregation and normalization are done. This data is then fed to blockchain engine which is responsible for the storage of data. Since blockchain is a decentralized technology, data stored in it is in decentralized form. The blockchain stores the records of a patient which is measured and collected by IoT devices. The data is stored is in the form of blocks, and it is also properly secured in it. Through the API management, this data was accessed by the various stakeholderswhich include government regulators, hospitals, doctors, and patients. This data can be accessed by mobile applications or web applications, and this was done by API management shown in the architecture as shown in Fig. 2.

3.5 Scope of Improvement Model

There are number of concerns of the healthcare industry that this model addresses but still there are areas which have to be properly dealt with to get more optimized results. Some of them are:

Mining: Mining of blockchain includes linking transactions to the current blockchain ledger available among all blockchain users. Mining includes forming a hash of a transaction block which cannot be easily manipulated, preserving the credibility of the blockchain as a whole without the need for a central network. Mining is usually done on a specialized computer, need a fast processor, greater usage of power resources and more energy consumed than normal computer operations. The biggest reason for mining is that people opting to use a mining machine would be paid for doing so. Generally, IoT device like Raspberry Pi is a low-end device with quite limiting processing capacity. Unlike higher-end device are not a suitable choice for hashing.

Processing Time: The time needed by the IoT system to perform the appropriate function will be longer, and this reaction period is having further scope to get increased.

4. RESULT AND DISCUSSION

4.1 Energy Consumption

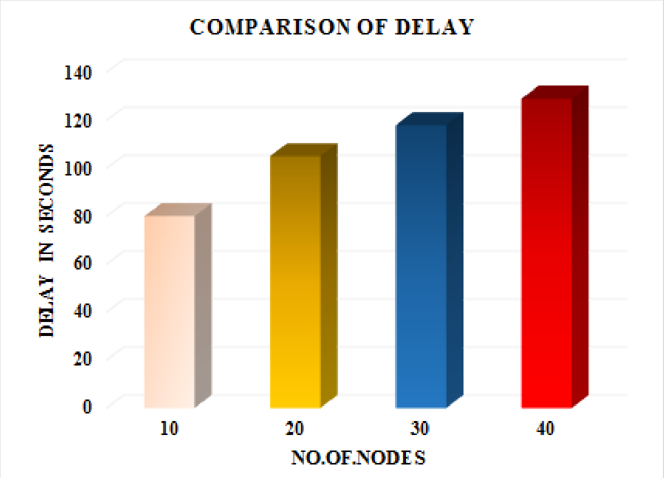

Fig.3. Delay Comparison

The energy consumption graph shows the variations of values between the No.of.Nodes and their respective energy in joules shows in Fig.3.

4.2 Packet Delivery

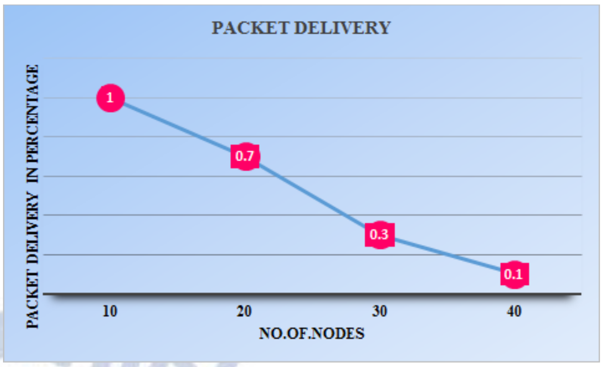

Fig.4. Packet Delivery

This graphs shows the variation between the packet delivery and No.of.Nodes is depicts in the Fig.4.

4.3 Throughput

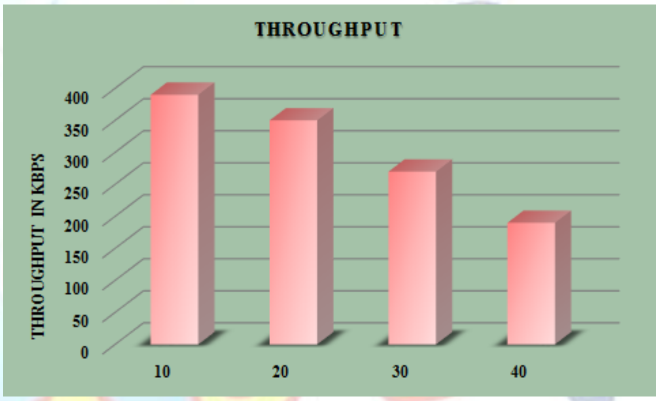

Fig.5. Throughput

The Throughput graphs shows the connection between the No.of.Nodes and the throughput values are shown in Fig.5.

5. CONCLUSION

The study examined how e-Healthcare data and services may be secured using Blockchain and IoT technology. A model for the healthcare sector is put out in this chapter employing both blockchain and IoT technologies. Real-time data is measured and gathered by IoT devices, and this data is subsequently recorded on the blockchain. Due to the decentralised and distributed nature of blockchain technology, the design we have suggested overcomes these issues. Still, there are certain things that might be done better. IoT devices now consume more energy, but as technology advances, this may be decreased, enabling more people to utilize these services at reduced rates. Using speedier, more potent encryption techniques can also reduce the latency of adding a block to a blockchain.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

References

[1] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, Alireza Jolfaei, and AKM Najmul Islam. "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system." Journal of Parallel and Distributed Computing 172 (2023), pp: 69-83

[2] Košťál, Kristián, Pavol Helebrandt, Matej Belluš, Michal Ries, and Ivan Kotuliak. "Management and monitoring of IoT devices using blockchain." Sensors 19, no. 4 (2019), pp: 856.

[3] Alrubei, Subhi M., Edward Ball, and Jonathan M. Rigelsford. "A secure blockchain platform for supporting AI-enabled IoT applications at the edge layer." IEEE Access 10 (2022), pp: 18583-18595.

[4] Mondal, Susmita, Mehak Shafi, Sumeet Gupta, and Sachin Kumar Gupta. "Blockchain based secure architecture for electronic healthcare record management." GMSARN Int J 16, no. 4 (2022), pp: 413-26.

[5] Ratta, Pranav, Amanpreet Kaur, Sparsh Sharma, Mohammad Shabaz, and Gaurav Dhiman. "Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives." Journal of Food Quality 2021 (2021), pp: 1-20.

[6] Dong, Zhaoyang, Fengji Luo, and Gaoqi Liang. "Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems." Journal of Modern Power Systems and Clean Energy 6, no. 5 (2018), pp: 958-967.

[7] Leng, Jiewu, Ziying Chen, Zhiqiang Huang, Xiaofeng Zhu, Hongye Su, Zisheng Lin, and Ding Zhang. "Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions." Machines 10, no. 10 (2022), pp: 858.

[8] Pavithran, Deepa, Khaled Shaalan, Jamal N. Al-Karaki, and Amjad Gawanmeh. "Towards building a blockchain framework for IoT." Cluster Computing 23, no. 3 (2020): 2089-2103.

[9] Hemalatha, P. "Monitoring and securing the healthcare data harnessing IOT and blockchain technology." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12, no. 2 (2021), pp: 2554-2561.

[10] Chakraborty, Sabyasachi, Satyabrata Aich, and Hee-Cheol Kim. "A secure healthcare system design framework using blockchain technology." In 2019 21st International Conference on Advanced Communication Technology (ICACT), IEEE (2019), pp. 260-264.

[11] Singh, Saurabh, In-Ho Ra, Weizhi Meng, Maninder Kaur, and Gi Hwan Cho. "SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology." International Journal of Distributed Sensor Networks 15, no. 4 (2019), pp: 1550147719844159.

[12] Ahmed, Adeel, Saima Abdullah, Muhammad Bukhsh, Israr Ahmad, and Zaigham Mushtaq. "An energy-efficient data aggregation mechanism for IoT secured by blockchain." IEEE Access 10 (2022), pp: 11404-11419.