DOI: 10.53375/ijecer.2022.302

BHC-IoT: A Survey on Healthcare IoT Security Issues and Blockchain-Based Solution

Laraib Javed[1], Bello Musa Yakubu[2*], Muhammad Waleed[3], Zoha Khaliq[4], Abdullahi Binta Suleiman[5], Nura Garba Mato[6,]

[1]Department of Information Security, Faculty of Computing, The Islamia University, Bahawalpur, Pakistan.
Email: laraibrana703@gmail.com
[2]Department of Mathematics and Computer Science, Faculty of Science, Chulalongkorn University, Bangkok, Thailand
Email: *bellomyakubu.cui@gmail.com*
[3]Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan
Email: waleed9809@gmail.com
[4]Department of Computer Science, Bahria University, Islamabad, Pakistan
Email: zohakhaliq.1999@outlook.com
[5]Department of Technical and Vocational Education Islamic University of Technology Gazipur, Bangladesh
Email: abdullahisuleman@iut-dhaka.edu
[6]School of Undergraduate Studies, Federal College of Education, Kano, Nigeria
Email: nuragarbamato@gmail.com
[*] Corresponding author: *bellomyakubu.cui@gmail.com*

Abstract: **In the last decade, the Internet of Things (IoT) has become one of the most used technologies, especially in healthcare systems. With the use of wearable and mobile devices, IoT-based healthcare systems have considerably boosted the value of the healthcare industry, resulting in the effective use of health data interchange for improved, precise, and rapid diagnosis. These devices use wireless and cable connections to interact, process, compute, and monitor real-time settings. These devices are heterogeneous and have restricted memory and processing power. Concerns about security and privacy are raised using IoT systems in healthcare. There is the potential for a privacy breach, privacy leakage, manipulation, etc., due to the presence of sensitive patient information in healthcare records. Recently, blockchain technology has emerged as a possible remedy for such breaches and issues. In this paper, we examine the security implications of the IoT's layered architecture in relation to the adoption of IoT in healthcare for wider practical use. We have classified the different layered security challenges encountered by IoT, as well as the unique threats and security issues faced by IoT-based healthcare systems for communication, computing, and authentication. Then, we explain how blockchain technology could be a crucial facilitator for overcoming several IoT security challenges in healthcare. We reached the conclusion that blockchain offers a safe and efficient method for addressing healthcare challenges.**

Keywords: **Internet of Things (IoT), Blockchain, Healthcare systems, IoT devices' security, Sensory nodes data security and privacy.**

I. INTRODUCTION

It has been observed that technology is tremendously productive. In addition to new techniques and terminology, its creativity has exploded in recent decades. Likewise, the rate of connecting physical things to the internet is growing at an exponential rate. Recent study indicates that around 8.4 billion devices are linked to the Internet worldwide [1]. The number of IoT appliances is incrementing expeditiously day by day. Many applications such as smart tv smartwatches are manipulated in various fields to fabricate smart cities; smart farming becoming part of our lives are originated from IOT, thus making it the future of technology. The revenue initially generated from the IoT industry was $892 billion in 2018, whereas currently, it is expected to raise about $4 trillion in 2025 [2]. A very dominant thread witnessed by customers is related to privacy and trust. Consumers find it intricate to differentiate between more and less assured and secured devices as gadgets vary in terms of protection or the shield they provide. This emerging development of IoT inventions has erected security as an essential issue against cyber-attacks [3].

Technology constantly improves and introduces new platforms in applied sciences, making our lives easier. Furthermore, with the enormous expansion of new technology, the Internet of Things (IoT) may be identified as a facilitating canal of expanding a network of physical items or entities initiating the scheme of utilizing an IP address for internet access. Furthermore, it considers the complexity between the attached devices and numerous vigilante manifestos linked to this relationship and internet-capable utensils [4,5]. Automating manual tasks has become a viable option in nearly every sector in today's fast-paced world. The constantly growing technology also improves IoT in various ways, embracing enhanced connection that extends beyond machine-to-machine settings [6]. As IoT has remarkably persisted and offers a vast array of advantages, it is also observable that researchers are developing advanced clinical applications, such as devices that adapt the feature of remote healthcare monitoring system, which has given rise to contemporary functionalities for recording long-term estimations and providing clinical access to the patient's physiological enlightenment [7,8]. The majority of these proposed remote monitoring frameworks have adopted the idea of building three tiers: the first tier is the body sensor

network tier, which serves as a component for collecting data such as body temperature, heart status, and blood pressure, since it comprises wearable sensors. The second layer assists the manufactured component by including services that gather and transmit sensor data, hence enhancing communication and networking [9,10]. The last layer consists of data processing and evaluation nodes. Fig. 1 depicts the architecture of a healthcare system that depicts a three-step scenario investigation to collect data; the gathered data is then forwarded to the third stage for data analysis and inquiry [11,12].

There are several prototypes of IoT. The primary specification of the IoT is to accommodate its users by allowing and certifying numerous services provided by networks on the World Wide Web to its users and objects [13]. This IoT feature enables the provision of timely, high-quality telemedicine and pharmaceutical services to patients via remote collaboration. To illustrate the concept of telemedicine (Fig. I.), take the example of a clinical practitioner who provides required medical treatments to a patient from a remote location. The patient might be from a remote region, such as the countryside, a village, or the ocean, especially in underdeveloped countries where adequate medical measures are difficult to get due to limited resources and poor transportation infrastructure. Furthermore, it has been observed that the medical options offered in many communities are insufficient. To help them, the concept of circulating healthcare ministrations via telemedicine can increase and improve by leveraging the potential of the IoT [14,15].

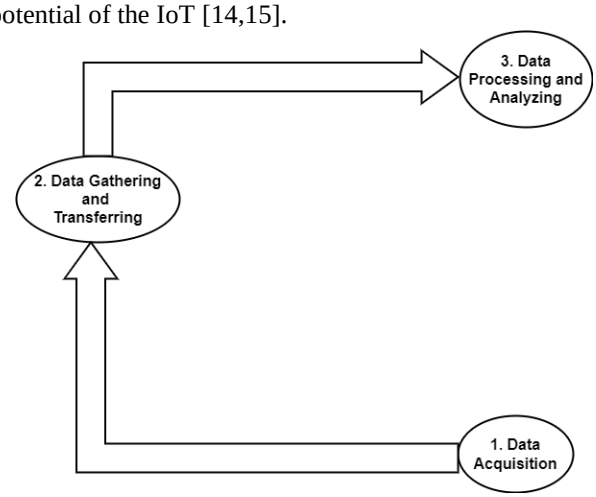

Fig. 1. Flow Diagram of Data Process.

However, launching IoT applications can result in expanding various clinical endeavour and remote health monitoring. A precise and explicit therapy may be performed on the patient by the healthcare provider at the early stages by looking at the patient's condition with the assistance of an example garrisoned on the patient's information [16,17]. Aside from obtaining cynosure existing medical services at hospitals and care institutions, frequent and acceptable medical situations should be prepared to be applied at home. Another crucial effort is the provision of scrupulous medicine by the service contributor. Consequently, different smart devices, such as diverse medical equipment, sensors, and diagnostic and testing utensils, are an essential component of IoT. As a result of this advancement, wearable sensor technology has been seen in hastening the creation of recent and enormous appliances and designs managed in distant medical facilities. This also aids in restricting patients' medical state by providing therapy based on their medical condition using content service applications [18].

However, all medical applications based on IoT are expected to decrease economic rates and focus more on customer satisfaction while improving user experience. Another emphasized finding observed from the medical service providers' viewpoint is that IoT may reduce equipment downtime occurring via remote purchase. To further enhance perceptual intelligence and interoperability, the IoT is being incorporated into clinical applications [19,20], which will result in the IoT expanding at a spectacular and higher rate. The medical services provided based on IoT at an accurate confirmation is fetching and conveying a plethora of valuable services to accelerate the quality of life, render secure and valid within time, initiate cost reductions, and improve the efficiency of medical services by considering technology [21-23].

According to the medical services, devices and techniques are also obliged to consider vital unique particulars such as personal clinical data. In addition, such smart innovations will be linked to a global statistical network, allowing them to be accessible regardless of location or time. Following that, IoT clinical services and accessories may become the target of private information that might accrue from resource-constrained wearable sensors, making isolated concerns susceptible [20,21,24]. Mainly if unlawful and unaccredited access is granted maliciously to clinical authorities' equipment, patients' lives might be endangered [22-24]. However, illegal, and incorrect usage of healthcare sensors and actuators, as well as personal information from a patient's medical report and history, may allow individuals to manipulate IoT-based healthcare services. Despite the certainty that different approaches have been presented to improve IoT safety and privacy, they have failed due to various factors such as secure storage, latency, and scalability [25-27].

The main contribution of this article is providing a basic literature survey on different security threats on IoT-based healthcare systems and how they can be secured using blockchain technology. The article consists of different attacks, security issues, time synchronization, and incentive issues. However, to overcome all these attacks and problems, the research merges blockchain with an IoT-based healthcare system to provide a secure framework in healthcare. Blockchain technology asserts itself to be a robust, tamper-resistant, distributed, and open data format for IoT data that satisfies all these unique requirements and limits all the existing attacks. The remaining paper is organized as follows; section II describes IoT in the healthcare system, and section III discusses the security issues in IoT-based healthcare applications, all different attacks, security issues, time synchronization, and incentive issues. Section IV discusses the IoT and blockchain, section V discusses securing IoT-based healthcare systems using blockchain and finally, section VI concludes the article.

II. IOT IN HEALTHCARE SYSTEMS

There are several advantages to employing an IoT-enabled remote health monitoring system rather than a traditional one. Patients may now check their health with far smaller, more portable sensors. If RFID IDs are reinforced with unique identifiers, they may be used to identify these surveillance devices through the Internet. These devices retrieve data from the physical world and transfer it to the digital one. Patients who are connected to an IoT health monitoring device may be referred to as virtual patients in the real world. The simulated patient's physiological conditions are like those of the real patient. Significant health issues might occur at any moment, which is why a continuous monitoring of a patient's vital signs is crucial and necessary for the patient's safety and well-being. It is feasible to monitor a patient's health state when they are away from a medical institution using the Internet or other technology that is connected to the Internet of Things. This enables major illnesses to be identified early enough for intervention. Additionally, the Internet of Things may aid in the collecting of personal health information. Machines can produce statistical data relating to an individual's health. Therefore, data collection is feasible in ways that would be impossible using conventional methods. Remote health data may be utilized to produce statistics, perform surveillance, and create risk maps for disease [6].

Through IoT, which is a fast-growing sector in the internet environment, things can now be connected to the internet in real-time. As the basic item matures into a smart object, it gains popularity in a variety of fields. This has a long-term effect on patient physiological data monitoring, administration, and clinical treatment. Patients are fitted with sensors and control devices, and the data is sent to a health monitoring unit. Data may be stored in the cloud, which simplifies the process of managing and securing the expanding amount of data. Security is crucial in the IoT since data integrity and confidentiality might be compromised while being transmitted from sensors to the cloud centre, and it is difficult to encrypt data received from low-resource devices [16].

III. SECURITY ISSUES IN IOT-BASED HEALTHCARE APPLICATIONS

The internet of things (or devices connected to the internet) is crucial in healthcare and medical applications. However, there are some significant shortcomings with these devices that must be solved. To earn the trust of people and organizations, IoT devices must have a sufficient level of security. These devices' data must be safeguarded against theft and tampering. For instance, IoT applications may save the results of a patient's health check or a visit to a retail store. While the IoT facilitates communication between devices, scalability, availability, and response time remain concerns. Security is a concern when data is sent securely over the internet. Uncertainty about the IoT ecosystem is increased by issues such as data leakage and sharing [11,12]. This section offers a review of various security issues affecting IoT-based healthcare systems, these include time synchronization, storage, communication, authentication, and sensing layer problems. Most of the techniques employed the use of a sensing layer to protect from various security threats [1]. In time synchronization, time source nodes are employed to prevent malicious nodes from providing incorrect time [3]. The fog and edge layers are used to minimize the burden on the cloud server and make the system more scalable. The following subsections provide detailed discussions on the related issues affecting IoT-based healthcare systems.

A. *Security Threats on Sensing Nodes*

The sensing layer is made up of IoT sensors and actuators which are used to detect physical action around it [28,29]. The sensors detect data in a variety of situations. Figures 2 and 3 describe the node capturing and false data injection code respectively, that is how an attacker performed these malicious activities. Ultrasonic sensors, temperature sensors, and other types of sensors are victims of such threats. The following problems are associated with the sensing layer:

Node Capturing: The first significant difficulty of the sensing layer is node capture. These layers' nodes might be made up of low-power sensors and actuators. From Fig. 2, an attacker may simply hack into these nodes, and quickly replaces or captures their node. While a malicious node functions as a component of IoT systems. With malicious activities, the attacker simply controlled the IoT system [13].

Malicious Code Injection Attack: It allows the attacker to insert malicious code into the node. The attacker injects bogus code into the sensing layer node, allowing him to control and alter the data easily. Using this approach, the attacker may hack the IoT system [30].

False Data Injection Attack: Here, the attacker takes control of the nodes and generates fake IoT system results. All controlled nodes in the IoT system provide misleading and incorrect results, leading to system failure [31].

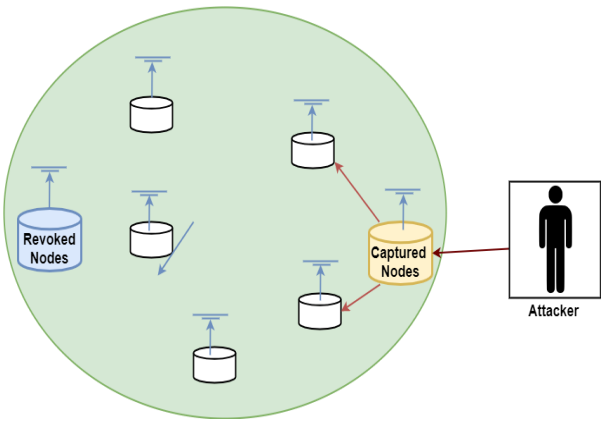

Fig. 2. Node Capturing and False Data Injection Code

Side-Channel Attacks: Side-channel attacks occur when attackers launch direct attacks on nodes, stealing sensitive information from the nodes and passing it on to a third party. Power usage data is also provided to a third party. This is an example of a side-channel attack [32].

Eavesdropping and Interference: Eavesdropping and Interference refer to the attackers' capturing data from many sources and causing interference in various phases such as data transfer and authentication procedures [33].

Sleep Deprivation Attacks: Sleep Deprivation attacks occur when an attacker attacks a node and inserts incorrect code, causing the IoT system to enter an endless loop. The sensing layer comprises sensors that gather data or information as needed, and it has clever small batteries that lose power owing to infinite loops in the sensor [32].

Phishing Site Attack: A phishing site attack implies that the attacker uses the least effort to target many IoT devices. A phishing attempt may occur when a user navigates to a different web page [30].

Access Attack: An access attack occurs when an unauthorized individual gains access to a network. The unauthorized individual takes critical network information during this type of attack [34].

DDoS/DoS Attack: The distributed denial of service (DDoS) attack occurs when an attacker sends unsolicited requests to a network, causing servers on that network to slow down and hang up [35].

Data Transit Attack: Data Transit Attacks occur when data is transferred from one location to another. The attacker simply attacks and steals the network's critical data. It is sometimes referred to as a cyber-attack [34].

Routing Attacks: Routing Attacks imply that a malicious node in the network may attempt to alter the path of all data travelling from one point to another [35].

Data Theft: Data theft refers to data movement through several stages in an adversary's acquisition of users' data. Users will be hesitant to submit their personal information on an IoT application that appears legitimate. These applications are used to steal data effortlessly [35].

Sniffing Attacks: The attackers utilize several applications to monitor the entire network's activity. He also uses the application to steal sensitive data [31].

Reprogram Attack: Because the programming procedure is not secure, attackers may simply reprogram IoT devices [32].

B. *Centralized System Issues*

In many IoT applications such as the medical field, continuous data transmission is critical to keep the patient's health record up to date. Due to the growth in number of IoT devices, the server may slow down and fail to update patients' data effectively, resulting in a loss. Furthermore, with a centralized system, if a problem arises, such as a natural disaster or a fire, the entire system would be affected. Using a centralized storage system may potentially lead to cyber-attacks, resulting in losing patients' sensitive information. In October 2017, for instance, a medical institution inadvertently exposed 47GB of patient data housed in an Amazon database, affecting at least 150,000 individuals [4]. Fig. 3 describes the structure of IoT based network.

In the framework of the personal health data sharing system, the usage of cloud storage systems for outsourcing patient health records has increased significantly. However, these systems can only store and transfer data utilizing the resources of a single, large corporation, which is therefore regarded as a reliable third party. One disadvantage of relying on third-party services is that there may be a single point of failure if the number of connected devices and data volume continue to increase [6]. Multiple IoT devices constantly requesting data may place a strain on centralized storage, for instance. Even if their data availability systems have been backed up, cloud service providers may still experience force majeure [5]. Clients may be unable to access their data as a result.

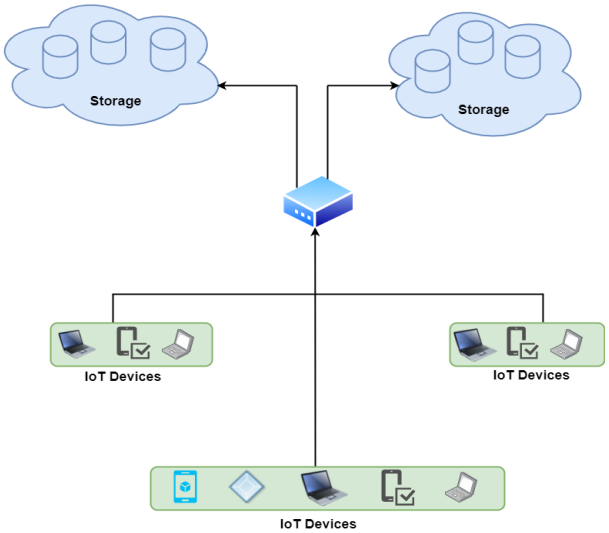

Fig. 3. IoT-Based Network

C. *Time Synchronization and Incentive Issues*

Many IoT applications require time synchronization. In the medical industry, IoT devices such as smartwatches and gadgets are used to keep track of patients' health. This data must be accurately synced in time so that patients' health can be effectively monitored, and proper treatment can be provided. However, due to a rogue node in the network [3], time synchronization is impacted, leading to a severe mishap if a node fails to send data on time. For example, if the patient heart rate data is not synced, the patient may die.

Data is constantly sent and received from service providers. However, because of the significant risk of privacy violations, data providers are hesitant to disclose their information. These providers' services are recognized, but there is no system to reward them for their excellent work to be involved in delivering additional services in the future. These types of issues can be better addressed using blockchain technology [5].

IV. IOT AND BLOCKCHAIN

Blockchain is a distributed ledger that exists as a chronological and time-stamped record of all ingresses. Thus, the hash function aids the scheme by linking each transaction included with the initial transaction. The Merkle tree idea [7] is used to aggregate all transactions, and the root hash is kept in the blockchain. To create a root hash, the hashes of the child nodes are concatenated, and a new hash is generated and stored in the blockchain's interior. Only the root hash must be checked to comply with security requirements since changes to a single transaction would eventually change all hashes. Because each block contains cryptographic hash keys, it is prohibitively time-consuming and impossible for adversaries to tamper with the blocks [9].

Numerous miners often operate against the same transaction, attempting to add it to the blockchain. They engage in mining to gain rewards and improve their reputation. Using these characteristics as the foundation enables blockchain to be tamper-resistant and safe.

Blockchain technology asserts itself to be a robust, tamper-resistant, distributed, and open data format for IoT data that satisfies all these unique requirements [1,26]. Mining is the process of thoroughly and adequately circulating transactions from when they are started until they are committed to the blockchain. Numerous institutions and businesses are developing and creating diverse platforms and configurations to facilitate the creation and maintenance of blockchain systems. Ethereum, Hyperledger, fabric, and Ripple are just a handful of these systems [1,25].

The Linux Foundation introduced Hyperledger Fabric in 2015, which is a blockchain platform with permissioned access. It is a decentralized, distributed, and permissioned ledger system that can be customized to fit a wide range of business needs by virtue of its identity management and access control capabilities. A ledger is a special kind of log that records all the transactions that occur inside an organization. By design, ledgers are immutable and append-only; all participants in a network may independently confirm all transactions. Each participant in a blockchain network has their own copy of the distributed ledger software that underpins the system. By using consensus algorithms, the network ensures that all participants have settled on a common protocol for recording and executing smart contracts and other types of transactions requiring consensus. A transaction or operation is deemed invalid if the consensus requirements are not fulfilled [36,37].

TABLE I. COMPARISON OF BLOCKCHAIN CONSENSUS ALGORITHMS FOR IoT-BASED HEALTHCARE [46]

Characteristic	**PoW (Proof of work)**	**PoS (Proof of stake)**	**DPoS (Delegated proof of stake)**	**PoI (Proof of importance)**	**PBFT (Practical byzantine fault tolerance)**	**PoET (Proof of elapsed time)**
e-health support	Medium	High	High	High	High	High
Energy Consumption	High	Medium	Medium	Medium	Low	High
Computation Cost	High	Low	Medium	Medium	Low	Low
Throughput	Low	Low	High	High	High	High
Application	Bitcoin	Ethereum	BitShare	NEM	Hyperledger	Sawtooth
Scalability	High	High	High	High	Low	High
Latency	High	Medium	Medium	Medium	Low	Low
Leader Selection Based	Hash rate	Stake	Democratic method	Size of Transaction made	Voting Process	Random Timer System

Consensus is used by the peers in a blockchain network to agree on the current state of the distributed ledger. In a distributed computing environment, blockchain networks can withstand attacks and build trust among previously unknown peers by utilizing consensus methods. Simply put, the consensus methods guarantee that each new block added to the blockchain is the only truth upon which all nodes can agree [26]. Each node must participate in the consensus procedure, and achieving consensus is only one of the protocol's many objectives. Therefore, a consensus algorithm seeks a solution that benefits the entire network as a whole [38]. This section provides a summary of popular consensus methods. In Table I, we compare the efficacy of various blockchain consensus methods for IoT-based healthcare.

1. *Proof of Work (PoW):* This consensus method determines which miner is responsible for generating the next set of blocks. The major purpose of this consensus technique is to efficiently answer a difficult mathematical puzzle. The privilege to mine the next block is provided to the first node to solve this mathematical problem, which takes a large amount of computing power. Bitcoin is an example of a blockchain that implements PoW consensus [39].

2. *Proof of Stake (PoS):* Most people favour this method over Proof-of-Work. The Ethereum network has shifted from Proof-of-Work to Proof-of-Stake as its consensus mechanism. Validators invest in the system's currency by locking up a portion of their coins as a stake in this variant of the consensus process, as opposed to acquiring expensive resources to solve a challenging problem. Based on their economic significance to the network, a validator is selected to create a new block. Therefore, PoS uses an incentive mechanism to encourage validators to reach consensus [39].

3. *Delegated Proof of Stake:* In Delegated Proof of Stake (DPoS), a popular variant of the original Proof of Stake (PoS) concept, users of a network cast vote to select delegates who will verify the next block. DPoS enables users to vote for delegates by staking tokens in support of a particular candidate. Instead of sending tokens from one wallet to another, users can utilize a staking service to deposit tokens into a pool where they may earn interest [39].

4. *PoI (Proof of importance):* Proof of Importance (PoI) is a cryptocurrency term attempts to demonstrate the value of nodes in a cryptocurrency system so that they can build blocks [38].

5. *Proof of Elapsed Time (PoET):* PoET is one of the most equitable consensus algorithms due to its emphasis on fairness when deciding which block to create next. It is frequently employed in blockchain

networks that require user authentication. Each network validator has an equal chance of having their block produced using this method. In the proof phase, the winner is the validator with the lowest timer value. In blockchain technology, the winning validator node's block is appended [38].

6. *PBFT (Practical byzantine fault tolerance):* PBFT was created to operate effectively in asynchronous systems with little overhead. Its objective was to solve several concerns with current Byzantine Fault Tolerance approaches [39]. In IoT for intelligent navigation, security concerns arise during communication, consensus, and authentication node insertion. The Byzantine consensus method based on chronology and gossip policy is utilized to eliminate the link between the composition and the authenticity of the harmony. However, the protocol used by the Byzantine consensus algorithm lacks reliable communication and has a high message size set [40]. If the amount of data a node needs to whisper exceeds the message capacity, good delivery will continue to deteriorate since venues will not gossip for specific information items more than an expected number of times [41] even though the suggested method in Hu et al. [42] accomplishes decentralization, tolerance for Byzantine error, and disability. However, the issue of speed remains unaddressed. As a result of its slow processing, the gossip protocol applied with the method slows down the application.

Smart contracts are written in code, and they are often referred to as self-triggered programs. This phenomenon allows them to be read and written on the blockchain in real-time. In the absence of a central administration middleman, smart contracts are used to enforce agreements between contractual parties. The Ethereum blockchain is one kind of distributed ledger that can be used to implement smart contracts. Ethereum is a blockchain-based platform for the distributed and secure execution and verification of smart contracts. On the Ethereum blockchain, the fee associated with completing a transaction is known as gas. Miners set the price of gas, which is needed to execute smart contracts and other transactions, based on the supply and demand for the network's processing capability. The "gas limit" is the maximum amount of Ether a user is prepared to spend on a transaction or smart contract operation on the Ethereum network. The minimum gas limit for an ordinary Ether (ETH) transaction is 21,000 units [34,43].

Merkle Trees are an additional layer of security that can be applied to the blockchain ledger to protect sensitive information stored on IoT devices. Likewise, this would decrease the quantity of new blocks being added to the chain. Except for the leaf nodes, every other node in a Merkle Tree has two children, making it like a binary tree. Therefore, the leaf nodes are responsible for transporting the data and transactions, while the roots are responsible for storing the hash values of the information found on the leaf nodes [7]. The size of the tree determines the number of transactions that must be linked together to get a single root hash. Therefore, each root hash may be considered a block in the chain rather than each transaction, which may reduce the total number of blocks. The several levels of hashing at each tree node also provide an extra degree of protection for the data [36]. Due to the interconnected nature of IoT devices, a possible approach might be to leverage Merkle Tree manipulation in tandem with blockchain technology. In Fig. 4, we see how the blockchain operates and how the message from M1 gets to the M2 device through many intermediaries.

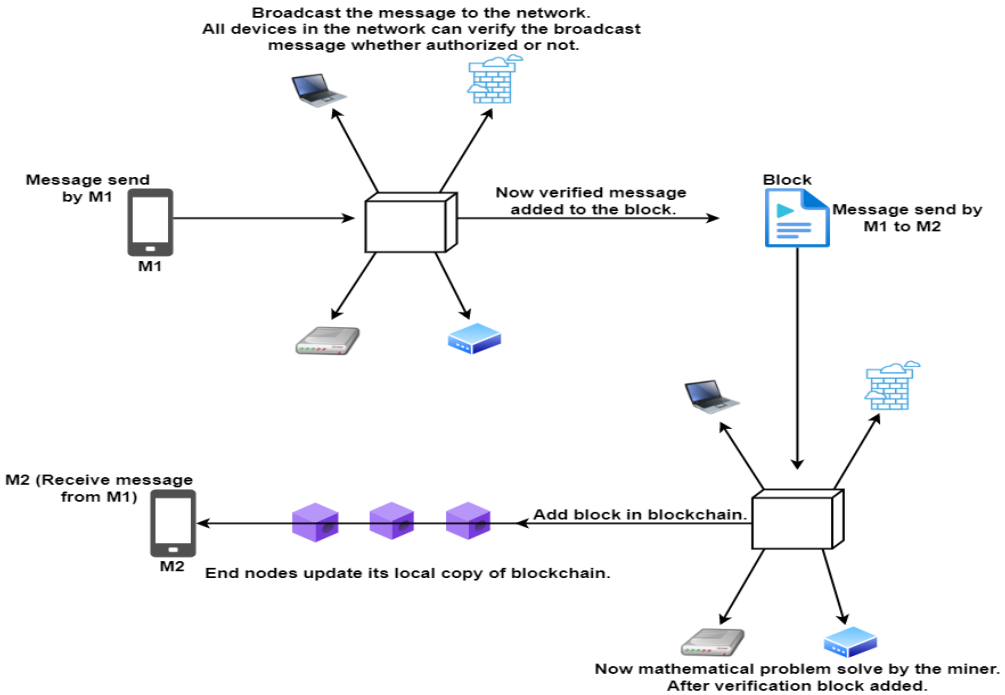

Fig. 4. Working process of blockchain

V. SECURING IOT BASED HEALTHCARE SYSTEMS USING BLOCKCHAIN

A. Securing sensing devices

Using blockchain in IoT provides excellent security. IoT devices are linked to a network of other devices and subsequently to a cloud server, allowing them to communicate from any location. Due to the volume of data being moved, it is less secure and more prone to abuse. Utilizing blockchain technology can ensure data security and integrity since each communication will have its block with a unique hash recorded in the blockchain that cannot be altered. Similarly, IoT devices transmit a vast quantity of data, which may result in a single point of failure due to data being stored on a centralized cloud-based server. This problem may be resolved by distributing and securely storing data through blockchain technology.

Blockchain technology employs hash algorithms (SHA 256) to create hash keys for each piece of data. Rather than storing data on the blockchain, it is first saved on a cloud server and then hashed and put on the blockchain. Changes to the data result in a change to the hash, ensuring the data's security and privacy. Storing hashes on blockchain will not increase the blockchain's size but also decrease the cost. Before data is stored, it is checked by various parties; therefore, the likelihood of storing fraudulent data decreases when utilizing blockchain. An adversary may join a network and participate as an existing user through spoofing, concealing his identity, and easily tampering with data (add and remove). Thus, using blockchain technology resolves this issue since data once added to a block cannot be altered in any manner.

IoT devices often interact, which means that a malicious entity may intervene and transmit incorrect information, resulting in a significant loss. Utilizing blockchain technology resolves this problem since all participants are already registered, and communication occurs through public and private keys. Even if a malicious entity obtains data content, he will not benefit from it since the data is encrypted. Although blockchain has addressed several IoT-related issues, there is still a significant difficulty in IoT. IoT devices have limited resources and are unable to hold huge

ledgers. Using a proxy-based architecture in blockchain technology can assist in resolving this problem. They can be used to store resources encrypted, and the client can simply unload the encrypted contents from the proxy server

B. Security solution to centralized system issues through blockchain

Blockchain technology establishes a decentralized structure that is both safe and trustworthy. Blockchain has been recognized as a revolutionary solution to the centralized storage issue, privacy, and security [30]. It would be helpful in the medical sector since a large quantity of patient data must be kept securely. By using blockchain technology, data would be stored decentralized and dispersed. Furthermore, blockchain technology addresses the primary security issue by replacing centralized cloud storage, which is the primary target of data thieves, with distributed storage, effectively turning the network into a peer-to-peer network. This way, data will be distributed encrypted across the network's nodes. Since blockchain does not use a centralized storage system, it avoids the problem of a single point of failure. Instead, all nodes are distributed randomly, and various devices are linked to different storage nodes. Before data is stored in it, it is encrypted using an encryption technique. Encrypting data would be advantageous in the event of a single point of failure. Even if a single point is attacked, the remainder of the data remains safe since all data on the blockchain is encrypted.

C. Securing time synchronization and incentive issues through blockchain

IoT appliances were initially built with security concerns about time synchronization. A blockchain-based approach was used in IoT devices to address this shortcoming, thus establishing security. The suggested approach is approximate using a publicly verified ledger to document, record, and broadcast time. This innovation may result in a decrease in the number of external threats. Multiple time sources are managed to avoid the difficulties associated with the centralized production of accurate time. Along with centralized generation, the strategy's decentralized composition offers the significant advantage of tolerating changes in network architecture. Time synchronization may be used effectively by developing an improved PBFT (Practical Byzantine Fault Tolerance) consensus method [3].

Although the information is constantly being provided and received from service providers, information providers are hesitant to disclose their data due to the significant risk of security breaches. By using an incentive system, suppliers would be motivated to reveal their knowledge. Once IoT devices get services from service providers, they compensate them for their efforts to ensure that service providers do not offer harmful services and continue to be motivated to engage with devices in the future [2].

D. A solution in Fog and Edge Layers

The Fog Layer implements various solutions for securing data and computing processes across the network. In IoT applications, the fog layer provides real-time services. In order to monitor the network for any suspicious activity, an intrusion detection system has been implemented. The procedure for identity verification is outlined in the fog layer and is implemented using machine learning. With the fog layer, it is possible to securely transmit data from one location to another [33,44]. Edge computing, a form of cloud computing, is utilized by numerous businesses. Edge computing refers to the use of computational and cognitive capabilities at the network's periphery. Between the user and the fog is a tiny edge server. The edge layer undergoes some processing [45]. Edge Computing enables low-cost connectivity and prevents data from sending to the cloud or fog [42]. Different studies have been done to overcome healthcare IoT security issues using blockchain. Several authors have proposed different solutions, and their achievements are as well, but their issues cannot be ignored. Table II describes the issues and solutions for securing healthcare IoT using blockchain.

TABLE II. SOLUTION WITH BLOCKCHAIN

Author	Issues	Solutions
[1] (V. Hassija et al.)	Privacy in IoT devices	The Permissioned blockchain is used to secure privacy in IoT devices.
[2] (Alghamdi et al.)	NO Incentive Mechanism	Incentive mechanism is introduced to boost the service providers.
[3] (K. Fan et al.)	Single point of failure	Decentralized storage resolves the issue of a single point of failure.
[4] (Chen et al.)	Data Manipulation	Devices are interlocked due to blockchain, thus resolving the issue of data manipulation
[5] (Wang et al.)	Unauthorized Access	private and public keys are used along with registration authority to prevent unauthorized access
[7] (D. Koo et al.)	Scalability	The edge layer is used to make the system scalable and cost-effective and reduce the burden on cloud servers.
[12] (B. Lee)	Data encryption	In the blockchain, the Sha-256 key is used to encrypt data.
[16] (M. Hassanalieragh et al.)	Reprogram Attack	All devices are registered, and the record is stored in the blockchain, so it is challenging to reprogram a device, its private key would be required, which is stored in the blockchain.
[17] (C.O. Rolim et al.)	Elimination of cloud	Distributed storage is being used.
[20] (K. Saleem et al.)	Node Capturing	All participants in the network are registered and have their public and private keys so that no node can't be replaced.
[20] (K. Saleem et al.)	Data Size	Decentralized storage IPFS is used along with blockchain data uploaded to IPFS and hash to blockchain so that cost does not increase.
[21] (C. Camara et al.)	Network Layer issues	Using Fog and Edge layer techniques to solve these issues.
[22] (T. Webb et al.)	Side-Channel Attacks	Transactions make up a Merkle tree in case a node gets hacked the chain will break and data will remain secure.
[24] (Hossain et al.)	Malicious Code Injection	Using blockchain no tampering can be done as it is tamper-resistant.
[25] (R. Henry et al.)	Data Transit Attack	Public and Private keys are used to transmit data and there are registered with certified authority to resist the attacks.
[26] (T. Aste et al.)	False Data Injection Attack	A consensus mechanism is being used to verify the data in case malicious data is obtained it will be tracked by other nodes.
[30] (Lu et al.)	Routing Attack	Routing attack is eliminated consensus is made at each level to verify the work.
[31] (C. Kolias, G. Kambourakis et al.)	DDOS Attack	Using blockchain and fog layer this attack is prevented.
[31] (C. Kolias et al.)	Detection of false data	An intrusion detection system is applied to the fog layer, which checks the false data before it gets uploaded to the server.
[32] (S. N. Swamy et al.)	Prevention from data loss and all sensing layer attack.	Using the blockchain, all the IoT devices are registered and quickly identify all devices.
[33] (H. M. Hamad and M. Al-Hoby)	Preventing data loss and temptation	Blockchain resolves this issue as data, once entered, cannot be edited, or deleted.
[34] (APWG.)	Data Theft	Blockchain resolves this problem as it is tamper-resistant.
[35] (C. Li et al.)	Sleep Deprivation Attacks	All devices are registered in the network. It is tough to insert a malicious node into a device as it would be notified through blockchain.
[40] (Hu, W., Hu, et al)	Consensus	A consensus mechanism is used to verify the truthiness of data, and the record is published into the blockchain to make it tamper-resistant.
[46] (Li, Dongxing & Peng et al.)	Authentication issue	Using certified authority authentication issue is resolved.

VI. CONCLUSIONS

IoT-enabled healthcare systems face a unique set of security concerns and threats. Understanding the security requirements of these systems is essential for mitigating the threats, challenges, and constraints. Concerns about multilayer design, time synchronization, single points of failure, and the resource-constrained nature of IoT devices prevent traditional security methods from meeting the demands of IoT-enabled smart healthcare systems. With the advent of blockchain technology, the healthcare industry has recently entered a new era of transparency and safety. This study examines the security challenges posed by IoT-enabled smart healthcare systems, including issues such as time synchronization, storage, communication, consensus, and authentication. In addition, a decentralized, scalable blockchain-based approach is provided for addressing security issues.

REFERENCES

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures" *IEEE Access*, vol. 7, pp. 82721-82743, 2019. DOI: 10.1109/access.2019.2924045.

[2] Alghamdi, T., Ali, I., Javaid, N. and Shafiq, "Secure Service Provisioning Scheme for Lightweight IoT Devices with a Fair Payment System and an Incentive Mechanism Based on Blockchain" *IEEE Access*, vol. 8, pp.1048-1061, 2020. DOI:10.1109/ACCESS.2019.2961612.

[3] K. Fan, "Blockchain-Based Secure Time Protection Scheme in IoT", *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671-4679, 2019. DOI: 10.1109/jiot.2018.2874222.

[4] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-Based Medical Records Secure Storage and Medical Service Framework" *Journal of Medical Systems*, vol. 43, no.4, pp.1-9, 2018. DOI: 10.1007/s10916-018-1121-4.

[5] S. Wang, Y. Zhang, and Y. Zhang, "A Blockchain-Based Framework for Data Sharing with Fine-Grained Access Control in Decentralized Storage Systems" *IEEE Access*, vol. 17, no. 6, pp.38437-38450, 2018. DOI: 10.1109/ACCESS.2018.2851611.

[6] A.R. Rajput, Q. Li, M.T. Ahvanooey, and I. Masood, "EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain" *IEEE Access*, vol. 7, no. 7, pp.84304-84317, 2019. DOI:10.1109/ACCESS.2019.2917976.

[7] D. Koo, Y. Shin, J. Yun, and J. Hur, ``An online data-oriented authentication based on Merkle tree with improved reliability," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, pp. 840-843, 2017. DOI:10.3390/app8122532.

[8] A. Aijaz, A.H. Aghvami, "Cognitive machine-to-machine communications for Internet-of-Things: A protocol stack perspective" *IEEE Internet Things*, vol. 2, no. 2, pp. 103–112, 2017. DOI:10.1109/VTCSpring.2017.8108222.

[9] H. Abie and I. Balasingham, "Risk-based adaptive security for smart IoT in eHealth" in *Proceedings of the 7th International Conference on Body Area Networks*, pp. 269-275, 2012. DOI:10.4108/icst.bodynets.2012.250235.

[10] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 6, pp. 2787-2805, 2010. DOI: 10.1016/ j.comnet.2010.

[11] N. Bui and M. Zorzi, "Healthcare applications: a solution based on the internet of things" in *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, pp. 131-138, 2018. DOI: 10.5958/0974-360X.2018.00580.2.

[12] B. Lee, "Healthcare Framework on the IoT open Platform" Service Model, Architecture, *International Journal of Applied Engineering Research*, vol. 9, no. 2, pp. 29783-29792, 2014. DOI: 10.1016/j.future.2016.02.020.

[13] K. Zhao and L. Ge, "A survey on the internet of things security" in *Computational Intelligence and Security (CIS), 9th International Conference*, pp. 663-667, 2013. DOI: 10.1109/ACCESS.2018.2851611.

[14] S.R. Islam, M.N. Uddin, K.S. Kwak, "The IoT: Exciting possibilities for bettering lives: Special application scenarios" *IEEE Consumer Electron. Mag*, vol. 5, no. 2, pp. 49–57, 2016. DOI: 10.1016/j.future.2017.11.024.

[15] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications*" IEEE Commun. Surveys*, vol. 17, no. 4, pp. 2347–2376, 2015. DOI: 10.2197/ipsjjip.25.23.

[16] M. Hassanalieragh, A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, B. Kantarci, S. Andreescu, "Health monitoring and management using Internetof- Things (IoT) sensing with cloud-based processing: Opportunities and challenges" *IEEE International Conference on Services Computing, SCC, IEEE*, pp. 285–292, 2015. DOI: 10.1109/SCC.2015.47.

[17] C.O. Rolim, F.L. Koch, C.B. Westphall, J. Werner, A. Fracalossi, G.S. Salvador, "A cloud computing solution for patient's data collection in healthcare institutions" *Second International Conference on eHealth, Telemedicine, and Social Medicine, IEEE*, pp. 95–99, 2010. DOI: 10.1007/978-3-030-51517-1-20.

[18] L. Catarinucci, D. De Donno, L. Mainetti, L. Palano, L. Patrono, M.L. Stefanizzi, L. Tarricone, "An iot-aware architecture for smart healthcare systems" *IEEE Internet of Things*, vol. 2, no. 6, pp. 515–526, 2015. DOI: 10.1109/JIOT.2015.2417684.

[19] S.R. Islam, D. Kwak, M.H. Kabir, M. Hossain, K.-S. Kwak, "The internet of things for healthcare: A comprehensive survey" *IEEE Access*, vol. 3, pp. 678–708, 2015. DOI: 10.3390/s20205923.

[20] K. Saleem, Z. Tan, W. Buchanan, "Security for cyber-physical systems in healthcare, in: Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare" *Springer, Cham*, pp. 233–251, 2017. DOI: 10.3390/app9071370.

[21] C. Camara, P. Peris-Lopez, J.E. Tapiador, "Security and privacy issues in implantable medical devices A comprehensive survey" *J. Biomed. Inform*, pp. 272–289, 2015. DOI: 10.1016/j.jbi.2015.04.007.

[22] T. Webb, S. Dayal, "Building the wall: Addressing cybersecurity risks in medical devices in the USA and Australia" *Comput. Law Security Rev*, pp. 231-242, 2017. DOI:10.1016/j.clsr.2017.05.004.

[23] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare" *Future Generation Computer Systems*, vol. 78, no. 9, pp. 659–676, 2017. DOI: 10.1016/j.future.2017.04.036.

[24] M. Hossain, S.M.R. Islam, F. Ali, K.S. Kwak and R. Hasan, "An Internet of Things-based health prescription assistant and its security system design" *Future Generation Computer Systems*, vol. 82, no. 4, pp.422-439, 2018. DOI:10.1016/j.future.2017.11.020.

[25] R. Henry, A. Herzberg, and A. Kate, ``Blockchain access privacy: Challenges and directions" *IEEE Security and Privacy*, vol. 16, no. 4, pp. 38-45, 2018. DOI: 10.1145/ 3133956.3134093.

[26] T. Aste, P. Tasca, and T. D. Matteo, ``Blockchain technologies: The foreseeable impact on society and industry" *Computer*, vol. 50, no. 9, pp. 18-28, 2017. DOI: 10.1109/MC.2017.3571064.

[27] D. Miller, ``Blockchain and the Internet of Things in the industrial sector" *IT Prof.*, vol. 20, no. 3, pp. 15_18, 2018. DOI: 10.1109/MITP.2018.032501742

[28] C. Crisan and B. Butunoi, "An IoT based Smart Home Automation System" *International Symposium on Electronics and Telecommunications ISETC*, vol. 12, no. 4, pp. 321-334, 2021. DOI: 10.3390/s21113784.

[29] K. Salih, T. Rashid and N. Bacanin, "A Comprehensive Survey on the Internet of Things with the Industrial Marketplace" *Sensor*, pp. 321-341, 2022. DOI: 10.3390/s22030730.

[30] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu., "A Privacy-Preserving Trust Model Based on Blockchain for VANETs" *IEEE Access*, vol. 6, no. 4, pp.45655-45664, 2018. DOI: 10.1155/2020/8831611.

[31] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ``DDoS in the IoT: Mirai and other Botnets," *Computer*, vol. 50, no. 7, pp. 80_84, 2017. DOI: 10.1109/MC.2017.201.

[32] S. N. Swamy, D. Jadhav, and N. Kulkarni, ``Security threats in the application layer in IoT applications," in *Proc. Int. Conf. IoT Social, Mobile, Analytics Cloud (I-SMAC)*, pp. 477_480, 2017. DOI: 10.1109/ACCESS.2022.3205351.

[33] H. M. Hamad and M. Al-Hoby, ``Managing intrusion detection as service in cloud networks," *International Journal of Computer Applications*, vol. 41, no. 1, pp. 35_40, 2012. DOI: 10.1372/Access.2021.897765.

[34] APWG. Phishing Activity Trends Report. Accessed: Feb. 12, 2019. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_ report_q4_2017.pdf

[35] C. Li and C. Chen, ``A multi-stage control method application in the ght against phishing attacks" in *Proc. 26th Comput. Secur. Acad. Commun. Across Country*, pp. 145-157, 2021. DOI: 10.3389/fcomp.2021.5630.

[36] J.Wang, M. Li, Y. He, H. Li, K. Xiao, and C.Wang, "A blockchain based privacy-preserving incentive mechanism in crowdsensing applications" *IEEE Access*, vol. 6, pp. 17545-17556, 2018. DOI: 10.1109/ACCESS.2018.2805837.

[37] G. Asma. S. Aafety, "Privacy and Security of sensitive data" *Springer*, pp. 211-221, 2019. DOI: 10.5623/security.2019.2951.

[38] P. Arul and S. Renuka, "Blockchain technology using consensus mechanism for IoT-based e-healthcare system" *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 1055, no. 1, p. 012106, 2021. DOI: 10.1088/1757-899x/1055/1/012106.

[39] A. Jain and D. S. Jat, "A Review on Consensus Protocol of Blockchain Technology" *Lect. Notes Networks Syst.*, vol. 334, pp. 813–829, 2022. DOI: 10.1007/978-981-16-6369-7-72.

[40] W. Hu, Y. Hu, W. Yao and H. Li, "A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles" *IEEE Access*, vol. 7, pp:139703-139711, 2019. DOI: 10.1109/ACCESS.2019.2941507.

[41] A. Panda, D. Soumyashree & M. Bhabend, S. Utkalika, J. Debasish, G. Debasis, P.Kumar, "Study of Blockchain Based Decentralized Consensus Algorithms" In *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, pp. 341-351, 2019. DOI: 10.1109/TENCON.2019.8929439.

[42] E. Oyekanlu, C. Nelatury, A. O. Fatade, O. Alaba, and O. Abass, ``Edge computing for industrial IoT and the smart grid: Channel capacity for M2M communication over the power line" in *Proc. IEEE 3rd Int. Conf. Electro-Technol. Nat. Develop. (NIGERCON)*, pp. 1-11, 2017. DOI: 10.1109/ACCESS.2019.2924045.

[43] R. Kandaswamy and D. Furlonger, "Blockchain-Based Transformation" *WITSC*, pp. 312-334, 2021. https://www.gartner.com/en/doc/3869696-blockchain-based-transformation-a-gartner-trend-insight-report

[44] S. Chandrasekhar and M. Singhal, ``Efficient and scalable query authentication for cloud-based storage systems with multiple data sources," *IEEE Trans. Services Comput.*, vol. 10, no. 4, pp. 520-533, 2015. DOI: 10.1109/ACCESS.2022.3209355.

[45] M. Alrowaily and Z. Lu, ``Secure edge computing in IoT systems: Review and case studies" in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, pp. 440_444, 2018. DOI: 10.1109/SEC.2018.00060.

[46] D. Li, W. Peng, W. Deng, and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT" *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-6, 2018. DOI: 10.1109/ICCCN.2018.8487449.