Secure sharing of healthcare data using a decentralized blockchain network for the Internet of Medical Things (IoMT)- A Review

Vinod Salunkhe [1], Sujatha R. [2]

[1] Research Scholar, Department of School of Electronics Engineering; Vellore Institute of Technology, India, vinod.salunkhe@vit.ac.in.

[2] Associate Professor, Department of School of Electronics Engineering, Vellore Institute of Technology, India; sujatha.r@vit.ac.in.

"Corresponding Author: Sujatha R. (sujathaa.r@vit.ac.in)"

Abstract: Buyers and producers of medical care continue to be worried about the healthcare safety and confidentiality of electronic healthcare records (EHRs). When a medical system is breached, critical medical information is exposed. This information is often maintained in centralized systems, which increases weaknesses and makes cyber-attacks more effective. This review aims to leverage blockchain technology to improve the safety and confidentiality of electronic health records. This study presents a novel architecture that avoids centralized storage concerns by using decentralized databases. In addition, the setup creates a blockchain network based on the Ethereum blockchain to record the hashes of the gathered information and regulate the connection to it while it has been retrieved. The suggested framework based on Blockchain is intended to improve the robustness of healthcare management systems while avoiding security flaws that have been identified in regularly utilized smart healthcare systems

Keywords: Internet of Medical Things, Ethereum Blockchain, Smart Contract, Consensus Algorithm, Healthcare system, Privacy, Security

---

1. Introduction

The Internet of Things (IoT) is a structure of physical devices that includes medical equipment, RFID tags, household appliances, and automobiles [1]. Hospitals, intelligent buildings, retail, transport, automation systems, logistics monitoring systems, and other IoT applications are divided into numerous areas [2], [3]. Healthcare is a very important social issue since this issue is related to improvement in the quality of life, which it may do by solving actual health problems.[4]

The Internet of Medical Things (IoMT) refers to a collection of high-risky, high-value medical devices which are linked to the healthcare networking structure. An IoMT device (an interconnected medical device) generates, collects, and interprets medical information for a patient, as well as transmits that data[5]. In terms of transmission, the IoMT device sends data (such as healthcare or technical details) to the cloud or internal databases via healthcare professional networks to track a patient's health parameters and aid in the prevention, detection, or management of diseases [6]. These collected data add value for the researchers to improve the quality of healthcare devices. But the healthcare data should be treated in a very confidential way as this data is related to the patient's health.

The Internet of Medical Things (IoMT) is a health-related form of (IoT) wherein a doctor may remotely and instantaneously measure various attributes of a patient's health using various sensors put in or on the patient's body[7][8]. Fig. 1 shows a variety of IoMT contexts and entities. This diagram depicts how IoMT technology allows hospital and emergency rooms, medical devices, patients, and doctors to communicate with one another.

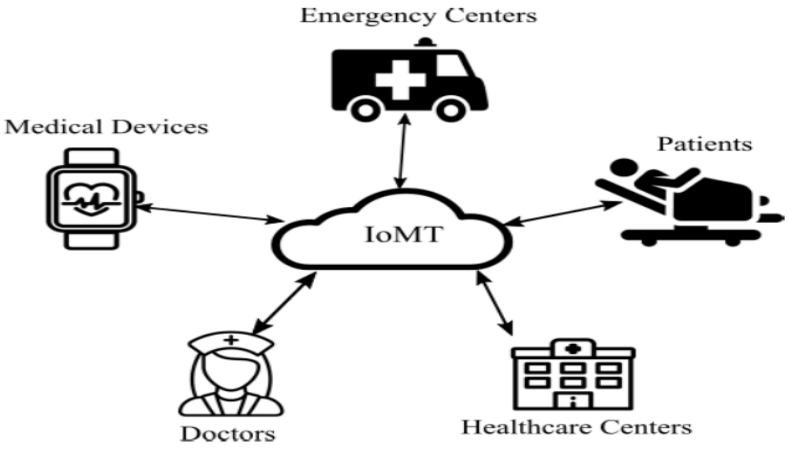

Fig. 1 IoMT Architecture

The Internet of Medical Things (IoMT) is a fast-developing category of the Internet of Things, where medical things are utilized to give a wide range of healthcare services. In recent pandemic situations like COVID-19, where direct contact with humans increases the spreading of diseases. Thus, in that situation, the use of technology without direct human involvement such as blockchain-based Internet of Drone Technology (IoDT) can be used[9]. According to Allied Market Research[10], the worldwide IoT healthcare industry is anticipated to grow by $136.8 billion by 2022. IoT devices are frequently used on the body to capture a variety of personal data. The captured information can be used by healthcare service providers to make critical decisions about a patient's medical situation, but on the other hand, this information is sensitive and personal. As a result, it is very essential to maintain healthcare data private and safe [11]. In recent

In the existing architecture of healthcare systems, devices such as wearable smart devices and sensors are connected through a centralised device called a gateway which further sends the collected data to the cloud[12]. Architecture based on the cloud is shown in Fig. 2. As shown in Fig. 2, nodes of the IoT system such as smart wearables, sensors and mobile devices transmit real-time data to the gateway and then the gateway decides to send the data to the cloud or not. Users of the cloud-based healthcare system access healthcare information from the cloud and can monitor the online. IoMT based on cloud architecture needs to fulfil some requirements such as access control, user authentication, scalability etc.

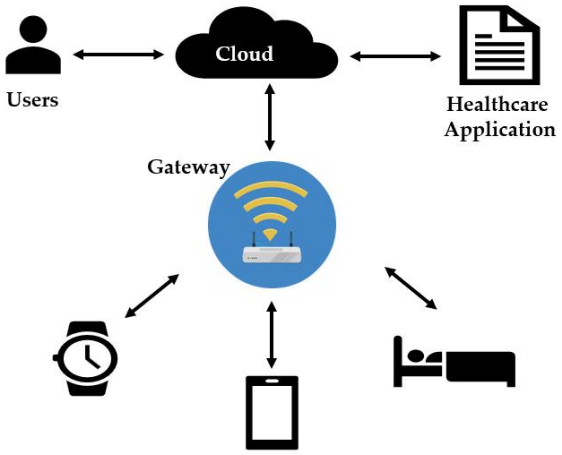

Fig.2 Cloud base architecture of IoMT

Data manipulation, interpretability, security, and privacy are the major problems in the cloud-based Internet of Medical Things [13]. Current equipment's restricted in the scope of resources, and so cannot meet the high resource demands of standard security methods. Moreover, due to the threat of a single point of failure and the considerable scattered structure of IoMT networking, the centralized structure deployed in existing security solutions is not suitable for IoMT [14].

The major concern of cloud-based healthcare systems is the point of failure of centralized cloud. At the time of communication, if the cloud is down, doctors, patients and others will be not able to communicate with the cloud which results in a delay in resolving patients' health-related issues.

Another major concerns of various healthcare companies facing are the protection of patient healthcare data. Similarly, recent reports of cyber-attacks on patient healthcare records have inspired industry persons and researchers to create novel methods to counteract these attacks while keeping user healthcare data secure and private [15]. Interoperability is a significant issue to address because health data integration is typically large and complex. In the following sections, detailed drawbacks of the cloud-based healthcare system and solutions are explained.

This survey presents a unique blockchain technological approach that is specifically enhanced for IoMT to address security concerns and protect IoMT user privacy. Combining blockchain with IoMT is one feasible approach to the privacy and security type of difficulties. Decentralization, reliability, and transparency are the most significant characteristics of blockchain. This shows that blockchain technology can overcome security, privacy, and interoperability concerns. In beginning, the decentralized blockchain can secure patients' private medical information from unauthorized access. As the number of medical sensing devices expands, blockchain's decentralization may assist in avoiding single points of failure and reducing bottlenecks at central servers. Because the blockchain's elements are not dominated by a single party, the medical data and activity logs stored on it are permanent. IoMT data security and traceability will be ensured using blockchain-based IoMT[16]. The processing of different IoMT data can be facilitated through decentralized peer-to-peer (P2P) network design, which also improves IoMT compatibility.

2. Related Work

The Internet of Medical Things (IoMT) is a series of healthcare devices and associated networks, which also include the internet that allows medical personnel and patients to communicate in real time. It enables cloud-based healthcare to store and disseminate large volumes of data to enhance device and overall healthcare system functioning [17]. Results in the collection of the data from medical facilities and forward to a cloud server for analysis. IoMT is having many vulnerable areas to target, such as assault on wireless connectivity, which is used by many IoTs [18]. Furthermore, when new technologies are being deployed on IoMTs, new concerns emerge, which is especially essential in critical illnesses such as COVID-19 [19],[20].

Although most IoMT devices are not concerned about addressing security and privacy, such characteristics are crucial in any eHealth system. Table 1 depicts the many forms of attacks that the IoMT system's perception layer has been subjected to, as reported in previous research findings. To conduct security assaults, criminals take advantage of security flaws in IoT devices and systems.

The fact that IoMT is made up of a range of consumer devices brings new types of threats which cause the root of the issue. Furthermore, conventional security measures are proved ineffective in securing these systems. The eHealth system is made up of several layers, such as network, sensing, and cloud layers. Sybil attack happens in the network layer where IoMT devices communicate the most[21]. Sybil attacks can result in a variety of dangers, including false data supplied to the healthcare system via compromised IoMT. Data could have been created on purpose by the infected device. Identically, data might be created by a compromised node with fake node IDs [22].

IoMT systems are subject to a variety of attacks. Data sent in between IoT devices can be secured using encryption methods inclusive of advanced encryption standards (AES)[23], data encryption standards (DES), and triple DES (3-DES). Device authentication is the most critical IoT security

problem, which is used to prevent object emulation attacks[24]. In terms of device authentication, identity providers can utilize Public Key Encryption (PKI) to handle and manage identity solutions for individuals and medical equipment in decentralized blockchain technology. As a result, attackers go for the identification data that is held off-chain and shared among all users. To prevent crucial IoT information and key management in the cloud database from various threats and attacks, several systems provide security, privacy, and encryption of data.

Eavesdropping attacks rely on the collection of sensitive information. Active and passive eavesdropping attacks are the two types of eavesdropping. Wireless accessing nodes are checked by active eavesdropping to see whether healthcare devices are linked to them or not. In passive eavesdropping, on the other hand, the attackers can keep eye on the data sent and theft the data during transmission. Then attackers use this information to obtain a large amount of data in a more efficient and timely manner[25].

In a man-in-middle attack, the attacker blocks the data and sends it afterwards while performing an attack. This allows intermediates to listen in to Address Resolution Protocols (ARP) to capture handshakes. If ARP captures it, the attacker utilizes it to get unauthorized access to a system and medical records, as well as encryption keys [26].

When an attacker wants to achieve his purpose, such a message tamper attack aims to tamper with the data reliability of delivered communications, which can result in doctors taking incorrect decisions that could hurt patients [27].

A legal entity is developed in the modification attack that can give the system authentication. This attack has had a significant impact on IoMT systems, resulting in the death of patients by sending a message containing misleading information to doctors and hospital databases. Furthermore, the attacker intercepts a legitimate user's correct and accurate message before injecting the incorrect message into the system[28].

Wireless networks are specifically targeted in the jamming attack on medical equipment. The attacker prevents patients and hospitals from communicating with one another. The most common target is wireless networks [29]. DoS attacks send out continuous packets and interrupt all data transmission on any protected channel. The nature of these jamming attacks might be selective or nonselective [30]. As indicated in [31], the impact of this attack can be mitigated by altering the frequency and moving between frequencies.

By flooding and injecting methods, attackers can steal the credentials using wrong info and fake request [32]. These types of attacks aim to overload the medical system and exhaust its capacity of it. An ICMP FLOOD is started by delivering a considerable number of ICMP packets to a distant host. As a result, the resources of the affected system will be used for handling the assaulting packets, rendering the system unavailable to other clients[33].

Due to Transmission Control Protocols (TCPs), a hacker would often perform this SYN flood attack on IoMT networks that are used by the user at a larger capacity. (For example, a webserver/email). The attacker consumes healthcare data from the server to approve the connection which is not insecure for a future attack and it is the major purpose of such attacks. With this attack, the attacker targets CPUs and firewalls, preventing patients and medical workers from carrying Internet traffic through the local area network (LAN) [34].

To find the correct password, a dictionary attack [18]finds and tries all possible passwords. To guess passwords, these techniques use a set of dictionary words. In terms of time and resources, this type of attack might last anywhere from minutes to hours to days. They accomplish this by analyzing every available keyword to acquire access to data for criminal motives such as collecting patient credentials or healthcare records. This assault affects a wide range of devices, including remote medical sensors used by patients [35].

The attacker makes use of the weak node to move the wireless network for various nefarious objectives. It keeps sending false alarms to sirens that were supposed to be used in emergency medical circumstances. The provision of medical services for patients within a hospital may be impacted by a smart grid attack [36]. These attacks permit attackers to change the patient's documented healthcare record, which might result in the wrong medicine or excess amounts of medicine being administered, potentially resulting in death.

In the replay attack, the attacker can send a signal to the network and alter the control commands delivered to other medical equipment. As he redirects the information to another site, the attackers can intercept and steal it. Medical systems may suffer physical harm as a result of this [37]. The network links are stored first and then replayed at the end device. The hacker intends to steal, leak, and reveal patients' private information, get unauthorized control of certain healthcare systems, and gain a high level of privilege within them. [38].

When the security mechanisms for the IoT device are not strong enough and access medical systems without authorization [39], the dictionary attack happens. To guess passwords, these techniques use a set of dictionary words. In terms of time and resources, this type of attack might last anywhere from minutes to hours to days. They use a set of numerals termed the Personal Identification Number in this attack (PIN).

Because two passwords may have the same hash, users frequently rely on weak hashes. In a birthday attack, the hacker takes advantage of this flaw and gains unauthorized access to medical systems[27]. Using secure hash algorithm techniques is the best way to protect devices from such threats as SHA-3) and (SHA-512 [6].

Worms are the type of malware considered the most harmful and damaging type of category found in things [40]. They can use the connected device to self-reproduce and target the device's weaknesses without the need for human participation. It impacts all medical devices and information security services, resulting in information loss and, in certain cases, affecting patients' health and even causing human life loss. They are set up to interfere with specific industrial control systems [41]. In one of the publications [42], harmful Internet worms attacking a network were explained.

A worm can be used to assault an IoMT device to collect and steal data and destruct that medical equipment. Assume that an attacker infects an IoMT and implants vulnerable devices. In such instances, by infecting them with worms, the entire healthcare system can go into danger, as worms automatically spread across the system when they exploit flaws. Worms collaborate with other destructive species, such as botnets and ransomware, to expand throughout the whole IoMT network[43]. Table 1 summarizes the different attacks on IoT.

Table 1: Various Threats & Attacks of an IoMT device

Ref	Attack Description	Architecture	Challenges
[25]	A busybody that silently acts in the medium may lose a data substance known as an eavesdropping attack. When dealing with medical concerns, for example, a patient's privacy may be compromised. Passive information collecting is another name for this type of attack.	Group send receive model	1. Can't monitor sudden disease. 2. Diagnosis system is not reliable.
[27]	Malicious data injection attacks are one of the most common and dead types of web application threats. They may lead to information theft, information leakage, data integrity degradation,	Data extrapolation and threshold algorithm.	The accuracy for finding insider attacks is less.

	denial of service attacks, and even complete system compromise.		
[28]	Malicious script injection, or XSS, seems to be an internet vulnerability that permits a hacker to insert malicious code into a seemingly harmless link.	SQL injection attack prevention using machine learning.	Not able to predict different types of SQL injections.
[29]	In a wireless jamming attack, the attacker deploys a signal jammer to interrupt & deform the IoMT node, leading to a denial-of-service assault.	Packet Send Ratio and Packet delivery ratio.	Do not ensure security for ad hoc networks.
[33]	ICMP is a flooding attack where the attacker floods the target's network infrastructure with considerable ICMP packets, ICMP echo request (ping) packets, and other forms of ICMP to jam and slow it down significantly.	EDOS-IDM system model.	The algorithm is not prepared for given ICMP further attacks.
[34]	Through SYN flooding, the attacker periodically sends requests with a spoofed source IP address towards the server that the victim is already on. Those SYN requests look like they are valid. The address that was spoofed refers to the client system that does not work.	Adaptive threshold algorithm and cumulative sum algorithm.	Dependency on selected parameters only.
[36], [37]	Traffic analysis is a way to find out the secret information that is needed for the authentication protocol and is known as a Brute force attack. It uses the messages that were heard when the reader and the tag were talking to each other.	Decision tree model with two different variables.	1. Only one dataset is used to find brute-force attacks. 2. Solution only limited to SSH and FTP brute force attack.
[31]	A masquerade attack takes place if a person guesses the node identity and commits fraud in the name of the victim for utilizing authorized sources. This form of attack is most often used to gain unauthorized access to the victim's network, this type of attack happens.	Audit Record Repository model framework.	The proposed work does not work for unexpected distribution and low sample sizes.
[38], [39]	A replay attack seems to be a network threat when an attacker detects a data transaction and then fraudulently delays or repeats it. The data is intercepted and retransmitted by the sender or a hostile entity, causing the data transfer to be delayed or repeated.	The framework consists of globally unique identification, a battery depletion rate monitor, and a timestamp.	1. Need to increase the scalability. 2. Need for adoption in the framework of a replay attack.
[40]	A dictionary attack includes trying a considerable number of common terms and their basic variants to guess a password. Such an attack's name came from the fact that hackers use massive	SHA-512 algorithm	Additional security is required to increase efficiency.

	databases of the most commonly used passwords, famous pet names, imaginary characters, or simply basic dictionary terms.		
[41]	Birthday attacks are based on a one-of-a-kind problem with hashing algorithms termed the Birthday Paradox.	Digital signature susceptibility technique.	1. Lack of complexity in encryption 2. Security is based on the integrity of people.
[42]	Malicious code may be utilized by an adversary to harm the system. These viruses are propagated through email attachments and file downloads from the Internet in the form of spyware, trojan horses, and worms.	Wormhole Attack Neighbor Discovery.	1. Inherent nature of versatility and security. 2. Another issue of trust is code reuse.
[43]	IoMT devices are accessed from remote locations through insured localization. As a result, attackers can access the program and use it to connect to IoMT devices.	The proposed protocol validates the reliability of local information.	Only a small percentage of black hole attacks are taken into account.
[44]	Hardware IoMT devices are having a variety of threats and attacks, for example, DoS, key exchange, eavesdropping, jamming, Sybil attack, collisions, and manipulation.	Hardware-Based Ciphers Through KATAN Algorithm.	Work only on a few metrics and investigate the protection performance.
[45]	In a tampering attack, the attacker is trying to steal critical healthcare data out of an IoMT node, like in an encryption key.	Anomaly detection of IoT threats using machine learning.	Devices from remote areas are not attended to.
[30]	In a Sybil attack, a malicious node assumes the identities of many nodes and acts as them in this attack. Every single node in such a Wireless Sensor Network, for example, may vote many times.	Cross-platform intrusion detection.	1. Higher processing requirement. 2. Weak resistance for node compromise.
[31]	DDoS Attacks are conducted by flooding the target or victim with traffic, forcing the victim to become overburdened. Many attackers in separate areas launch assaults on one or more targets at the same time. Since the attack locations are dispersed across the network, it is referred to as a DoS attack.	1. Network traffic detection. 2. System workflow detection.	1. Insufficient validation and authorization. 2. No bandwidth limitation.
[26]	Man-in-middle attack detects the transported encrypted information within the source and destination for extracting the plain text. This approach places the hacker in the middle of two hosts, enabling all interaction between them to be routed via him.	Robust cross-layer security framework	1. Majority of tests are intrusive which is inconvenient for the clients. 2. Additional flow with a trusted server.

3. Overview of Blockchain

Satoshi Nakamoto invented the Blockchain data structure and first used it with Bitcoin in 2008 to build a digital record that allows for immutable and irreversible transactions. Blockchain is a distributed computing and data-sharing architecture shown in Fig. 3, which works on a peer-to-peer basis. Even if they do not trust one another, unidentified parties can conduct transactions on the blockchain network. A blockchain is a form of data structure that helps in monitoring and storing data from a large number of devices without relying on a centralized server [44].

Blockchain is a tamper-resistant digital ledger that can store a growing volume of data. The centralized system approach has been eliminated from the blockchain. The use of public key cryptography for processing transactions between nodes is used in this system. A ledger is made up of a series of blocks. The completed transactions are then registered on the ledger. The data blocks that have been recorded on the blockchain ledger cannot be altered or erased[45].

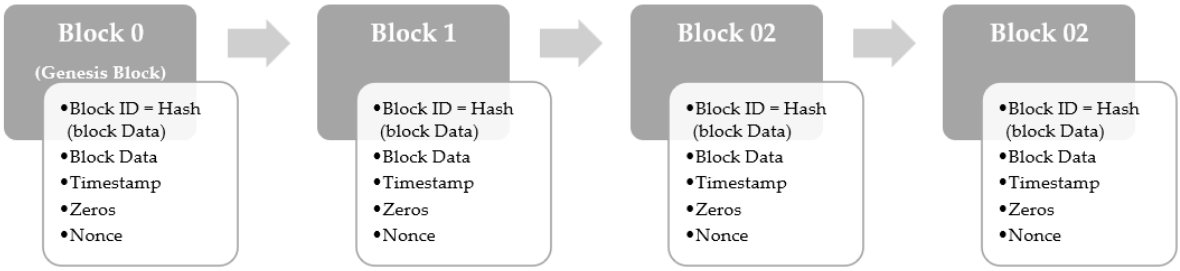

Fig.3 Blockchain Architecture

The use of blockchain technology is not limited to Bitcoin as its use is not limited to specific applications. The characteristics of Blockchain are safe, decentralized, and autonomous, making it a feasible alternative to Bitcoin for IoMT security concerns[46].

To use blockchain technology, you need to know how to use asymmetric encryption techniques, how to store and share information across computers, and how to make sure everyone agrees. Smart contracts are another important technology that has been introduced to blockchain technology as a function of the growing demand and development of the technology. This section provides a comprehensive overview of these four technological fundamentals.

3.1. Cryptographic hash function:

A hashing operation H is a function that converts an input of any size to an output of a specific size. The following are some more characteristics of cryptographic hash functions: a) Collision resistance: Finding two inputs a and b such that H(a) = H(b) is challenging; b) Preimage resistance also it is very challenging to find out the input 'a' for the output 'y' such as H(a) = y and c) Second preimage resistance. It is difficult to locate a second input b such that H(b) = y for an input a given and an output y = H(a).

Blockchain users use Cryptographic hash functions [47] for different purposes:

1. To solve the cryptographic puzzle as the proof-of-work technique used in Bitcoin.
2. To generate the address for public and private keys.
3. To reduce the size of public addresses.
4. Message configuration in signature.

In the blockchain, SHA 2 is one of the most used hash functions, especially the SHA 256 hash algorithm that produces 256 bits output. Few of the thoroughly examined hash functions from the NIST SHA-3 competition and standardization were used in the later phases of that process. A few of the

current blockchain designs created their cryptographic hash function termed Curl-P, which garnered extremely unfavourable and critical feedback from the cryptocurrency community.

Blockchain designs cryptographic hashing algorithms in the form of an operation mode, which is a mix of several same or various hash functions. For instance, SHA256 is used twice in Bitcoin [1], and this design is known as SHA256d, i.e.

$$\text{SHA256d(message)} = \text{SHA256(SHA256(message))} \quad (1)$$

A new block in the blockchain is created by the process of mining, and the person who resolves the cryptographic problem first is referred to as the block's miner. As in the Bitcoin PoW puzzle, a miner has to find the Nonce to generate the next block in the blockchain. The puzzle looks like this:

$$\text{SHA256d(Ver}||\text{HashPrevBlock}||\ldots||\text{Nonce)} \leq T \quad (2)$$

Where T is the 256-bit target value.

Understanding why mining is challenging in PoW may be done by looking at the percentage of SHA256d outputs that are smaller than the targeted value T for various possible values in Table 2. Specifically, the chances of discovering a nonce that will result in the block as a whole having a hash that is lower than the desired value are:

$$\Pr[\text{SHA256d(Block)} \leq T\ ] \approx \frac{T}{2^{256}}$$

Table 2:

Target Value of T	**Fraction of SHA256d values ≤ T**
0x7FFFF FFFF…. FFFF 63 Times	$\frac{1}{2}$
0x0FFFF FFFF…. FFFF 63 Times	$\frac{1}{16}$
0x00……00FFFF FFFF…. FFFF 16 times 48 times	$\frac{1}{2^{64}}$

SHA -256d is pre-image resistant, as for given hash (h), hard to find the message (m) such that h =hash(m). Also, it is collision-resistant, as it performs hash(m1) = hash(m2). It is very difficult for two distinct documents to coincidentally have the same hash result when using SHA-256d since there are 2256 potential hash values. Technology experts mostly employ SHA-256d because it is safe and has not been "broken," unlike some other well-known hashing algorithms. It also has no known weaknesses that make it insecure.

3.2. Hash Implementation:

The hashing algorithm is among the most significant functions in PKI. A hashing function converts the volume of data to a specific size. The SHA-256 [48] hash algorithm is applied to bitcoin, which can generate a 256-bit hash (32 bytes). This is shown in Fig 4

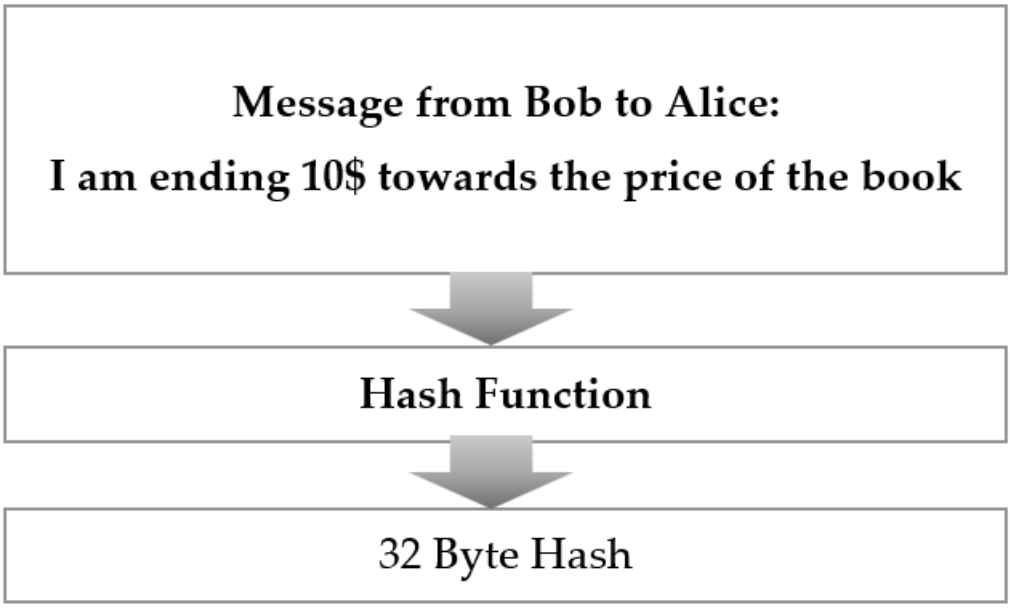

Fig 4 Hash algorithm

Bob sends a text like the one seen above when making an order with Lisa. This message is hashed using a 32-byte hash using hash algorithm. The benefit of this hash is that it (the 256-bit value) is treated uniquely for the contents of the message for all practical reasons. The hash function will change if the message is changed. Not only that, but given a hash function, reconstructing the original message is impossible as shown in Fig 5.

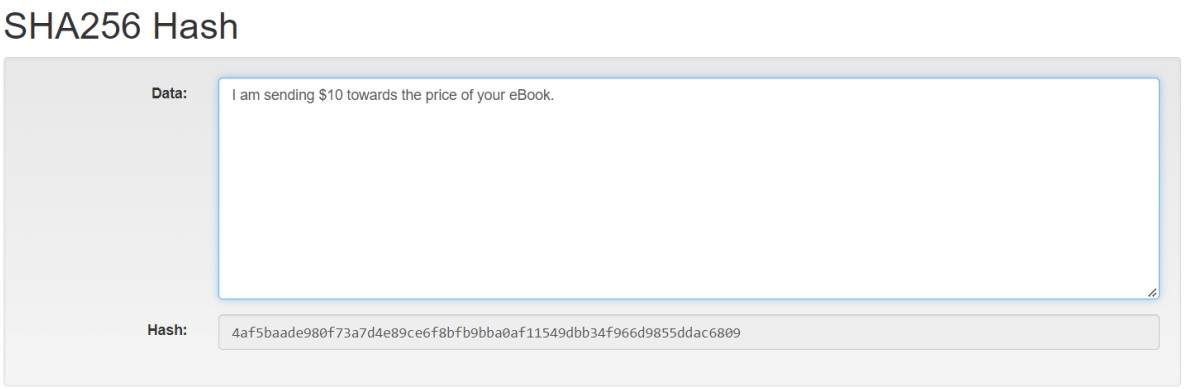

Fig 5. Construction of SHA256

Hashing process:

Software created by Anders Brownworth is available for reference for the hashing algorithm. If a change in any character in the data sections as shown in Fig. 6, results in a change in a relevant cryptographic hash in the hash area.

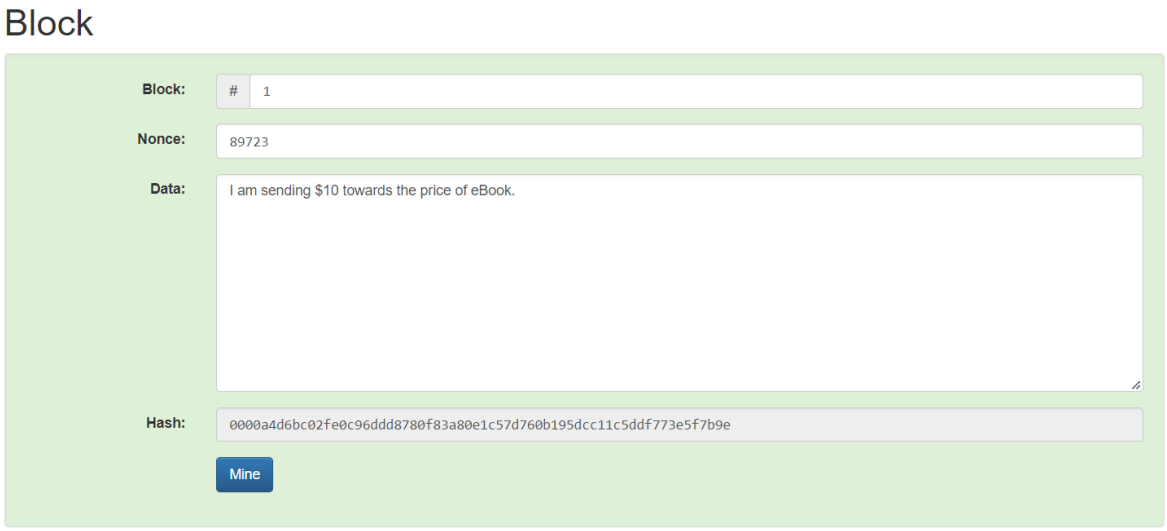

Fig. 6 Creation of block

If we make a small change in the input, the equivalent hash produced will be entirely different as shown in Fig 7.

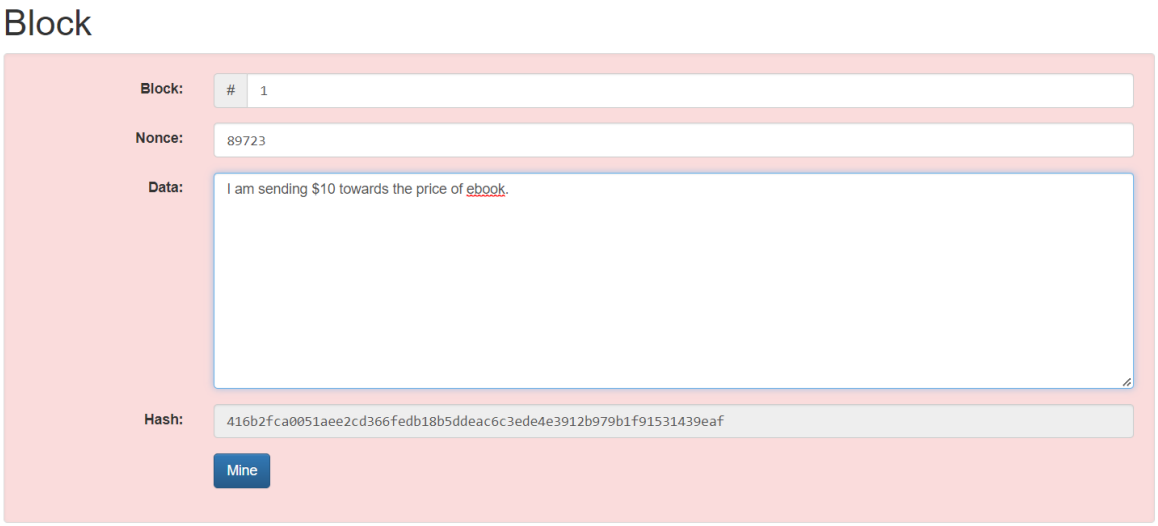

Fig. 7 Demo of change in hash function of block

It is a challenging, but not impossible task, to recover the original string from the corresponding original hash. "Brute-force" is the single way to identify the first string from its hash. “Brute force” basically takes arbitrary inputs, hashes them, and compares them to the desired hash.

3.3. SHA 256 Algorithm Implementation:

According to the common meaning of the term, SHA-256d [49] retains to be a safe pseudo-random function. A distinguisher that can break SHA-256d can be converted into one that can break SHA-256 with just twice as many queries, proving the conventional argument. This protocol, for instance, is intended to give mutual confirmation that every party has performed at least a certain number of evaluations of a certain 256-bit hash function H. (Note: Bob does the next even step once Alice completes the odd steps, and with roles reversed.):

1. Alice generates a 256-bit A_0 randomly and gives it to Bob along with the minimal quantity $k_A \in [2^4 \ldots 2^{14}]$ of assessment of H that she wants Bob to complete the task;
2. Bob generates a 256-bit B_0 randomly and gives it to Bob along with the minimal quantity $k_B \in [2^4 \ldots 2^{14}]$ of assessment of H that she wants Bob to complete the task;
3. In step 2, Alice determines $\hat{B}_0$ and $\hat{K}_B$. If $\hat{K}_B \geq 2^{18}$ then the protocol is terminated with failure by Alice.

4. In step 1, Bob determined $\hat{A}_0$ and $\hat{K}_A$. If $\hat{K}_A \geq 2^{18}$ then the protocol is terminated with failure by Bob.

5. Alice repeats for j=1…max (k_A, $\hat{k}_B$):
    a. If $A_{j-1} = B_0$, terminate the protocol with failure;
    b. compute $A_j = H(A_{j-1})$;
    c. compute $\hat{B}_j = H(\hat{B}_{j-1})$;
6. Bob repeats for j=1…max (k_B, $\hat{k}_A$):
    a. If $B_{j-1} = A_0$, terminate the protocol with failure;
    b. compute $B_j = H(B_{j-1})$;
    c. compute $\hat{A}_j = H(\hat{A}_{j-1})$;
7. Alice sends $\hat{B}$ & $\hat{k}_B$ to bob;
8. Bob sends $\hat{A}$ & $\hat{k}_A$ to Alice;
9. Alice ends the protocol with rejection if the result she received at step 8 differs from A & k_A; else, she reports success.
10. Bob ends the protocol with rejection if the result he received at step 7 differs from B & k_B; else, he reports success.

3.4. Distributed Data Storage

The ability of each contributing node to store information separately is referred to as distributed storage. To synchronize data from remote systems, and preserve data consistency, data from remote systems must be synchronized. After analyzing all data from all devices of the IoT system, the blockchain stores each transaction in the Merkle tree data structure. A Merkle Tree (Fig.8) consists of leaf nodes, root nodes, and intermediate nodes. This tree-like database model helps a lot when it comes to quickly induce and checking the integrity of vast volumes of data. The Merkel tree source is the hash value of the whole transaction set[50] & it is used to represent all transactions within the block.

Blockchain creators should remember the hash of the root node. In the process of verification, if the root node gets tampered with the value of the source node will not be equal to the original value. In the Merkel tree, the smallest leaf node is the hash value of the data block. The hash of the root node will not match in the verification process; if any, one of the nodes in the Merkle tree is manipulated. The Merkel tree is scalable because it can be created irrespective of the kind or size of transaction records, and locating transactions takes a very short amount of time. The Merkel tree can locate and verify whether a transaction exists or not.

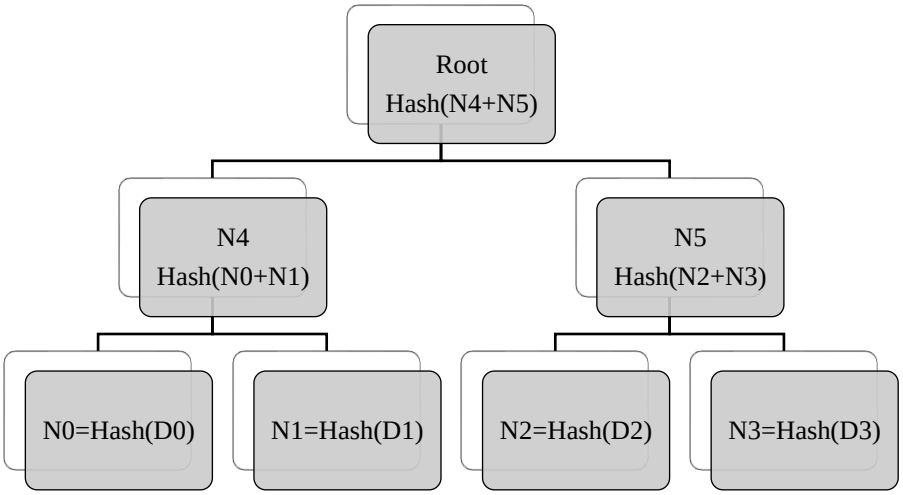

Fig.8. Merkel tree structure

3.5. Consensus algorithm

The blockchain digital ledger is distributed in nature. The Bitcoin blockchain makes use of the proof-of-work (PoW) technique that depends on the computational capacity of each node to verify that the Bitcoin network's distributed accounting is safe. This method is called proof of work (PoW). To increase the computational efficiency of resources, researchers have produced different consensus algorithms. This section provides a quick overview and comparison of several consensus methods to better appreciate their distinctions[51].

I. Proof of work (POW)

Moni Naor and Cynthia Dwork introduced the idea of Proof of Work (PoW)[52]. At the beginning of the PoW work process, the node responds to data records transmitted over the whole network. After the basic authentication check, the information is temporarily saved. The active node then uses its computational capacity to attempt various random numbers for hash computation to get a result that matches called “Mining". The "miner" that solved the issue first was given the option to enter the competition in the third part, resulting in the development of fresh block data.

In the next step, the node sends this newly created block to the outside world. Later, while completing the verification, newly created nodes are inserted into the original chain. In the end, all nodes start another cycle of mining. Using a competitive algorithm approach to solve the issue of possession of accounting copyrights in distributed accounting is the benefit of POW. As a result, it has become one of the most often-used cryptocurrency consensus algorithms. The disadvantages are equally obvious. Because of the large quantity of resource waste generated by mining activities and the duration of time, application areas are difficult to satisfy.

II. Proof of Stake

While implementing PoS, users are not needed to generate a random value in a void of space. It is an organisation that pays you interest depending on how much digital money you maintain and how long you keep it. The PoS method makes it easier to mine for nodes by using an algorithm that accelerates the search for arbitrary integers. The benefit of PoS is that it eliminates the concern of resource wastage. Still, because of the cheap price of mining, the risk of threat is increased. It is difficult to employ them in a business context since network nodes do mining calculations [53].

III. Practical Byzantine Fault Tolerance Algorithm mechanism (PBFT)

As in history, the generals of Byzantium are a subject on which everyone agrees. The Byzantine Empire's generals must decide whether or not to attack a hostile force unanimously [50]. The difficulty is that all generals are geographically isolated, and information can only be conveyed between them through messengers. If there is a traitor among the generals, the traitor may lead to a conclusion that is not shared by all generals. The activities made in response to this decision had to be ineffective.

Nodes are like soldiers in a battle and the system's communication network acts as a messenger. The creation of new blocks is a lot like attacking the other side's forces. A distributed file copy system is the subject of the algorithm. The system has "3f + 1" replication nodes, with "f " Byzantine error nodes at most. Each of the system's replication nodes can perform multiple tasks and execute a copy of the finite state machine. As a result, PBFT nodes only require a short period to justify their validity, and spam and false messages are less likely to spread among nodes[54].

3.6. Smart contract

Participants in the network collaborate to create smart contracts. To conduct a peer-to-peer transaction or transfer, each participant prepares a smart contract together. After the completion of the transaction, a similar block is created & saved inside the network. The transaction information can be checked by participating online traders to guarantee the security of the transaction details. Smart contracts run both the program and participant code automatically. They can respond to the information received promptly, as well as assemble and save the transaction's value. According to the predefined rules, when all requirements are satisfied, the smart contract runs the code and records the resultant sensitive information into the blockchain by monitoring the trigger conditions frequently.

Smart contracts, in comparison to traditional contracts, benefit from the blockchain's trusted environment, which allows them to deliver improved safety and lower contract-related transaction costs.[55]

3.7. IPFS (Interplanetary File System):

The proposed system suggested storage nodes are connected to an IPFS network with a distributed file system. Before being stored on the IPFS system, patient health information is encrypted[56]. Then, hashed encrypted health data is used as an index to locate data that is stored in the file system. The hash value serves as an IPFS address. Without decryption, even if unauthorized users manage to access IPFS information using its address, they may not be able to recover plain data or extract any useful information from it. Therefore, even if an access manager finds the file in the IPFS system, it serves as an additional layer of protection. Due to the system's architecture's distributed and decentralized nature, massive amounts of data could be stored with no scalability problems impairing the system's effectiveness[57].

4. IoMT for Blockchain:

Storage and management of electronic healthcare data (EHR) and Patient Remote Monitoring data in local databases is always a risk factor[58]. But at the same time, local databases increase data privacy, data integrity, data interpretability, security threats for data, and information security. To deal with these security threats, Blockchain (BC) technology will support the validation and authentication of information, as well as the distribution of data inside the system and among many medical institutions. Blockchain eliminates the need for a mediator or centralized authority through the transparent and decentralized network, which improves the cost and data quality. Two more benefits offered by BC are accurate authentication procedures and effective data access for the authorized components of the BC system[24].

The blockchain serves as the key component in this architecture, linking the various parts of IoMT. Cryptographic techniques (such as digital signatures and public encryption), smart contracts, distributed consensus, peer-to-peer networks, and a chain of blocks are all included in blockchains [59]. As a result, the IoMT can benefit from the blockchain's security. Adding authentication, homomorphic obfuscation, and group signing to blockchains can help protect IoMT data privacy even further. Furthermore, blockchain systems' multilayer P2P networks can connect numerous sectors in the IoMT, improving interoperability across the board.

Patients' medical records include personal and delicate information that tempts people from all walks of life, including criminals and retaliators. This data would be protected and transmitted in a controlled manner. IoMT devices need a big storage system for real-time processing of the large volume of medical files. The majority of IoMT organisations are currently storing and deploying their application systems on the cloud (Fig. 9). Like previously indicated, data privacy and security are the major concerns when adopting IoMT in the cloud [60]. We cannot risk it since data could be destroyed or altered if cloud servers aren't trustworthy. Important data is shared between devices, and data leakage is unavoidable.

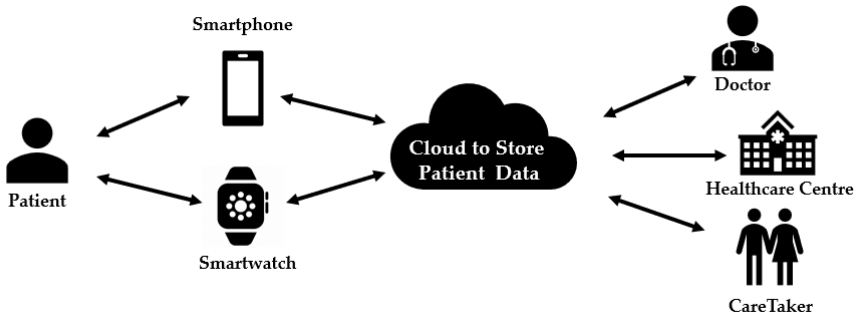

Fig. 9. Cloud-Based IoMT Architecture

A blockchain-based database structure is made up of nearly incorruptible cryptographically connected blocks that can be utilized to store critical patient records [61]. To build the blockchain-based structure, the computers of all participants should be connected. The blockchain-based system is constructed by interconnecting all the computers of participants. Figure 10 explains the blockchain-based healthcare system. Blockchain technology helps doctors to sit in a remote location to assist patients virtually and analyse the patient reports generated in remote diagnosis centres. The medical representative at the diagnostic centre uploads electronic medical reports (EMRs), and later updated them in the patient's medical record[62].

Real-time detailed medical reports are generated and exchanged with a distributed ledger in some clinics, where the health provider reviews them. Wearable tracking devices are also used by the practitioner to keep an eye on the patient. Real-time monitored data received from wearable gadgets attached to the patient's body and sent to the concerned doctor. According to the information received from the patient, the doctor advises the patient. The medical history of the patient is also available to the patient's guardians. Any node in the patient network can read the patient's reports and treatment because they are stored on the distributed ledger.

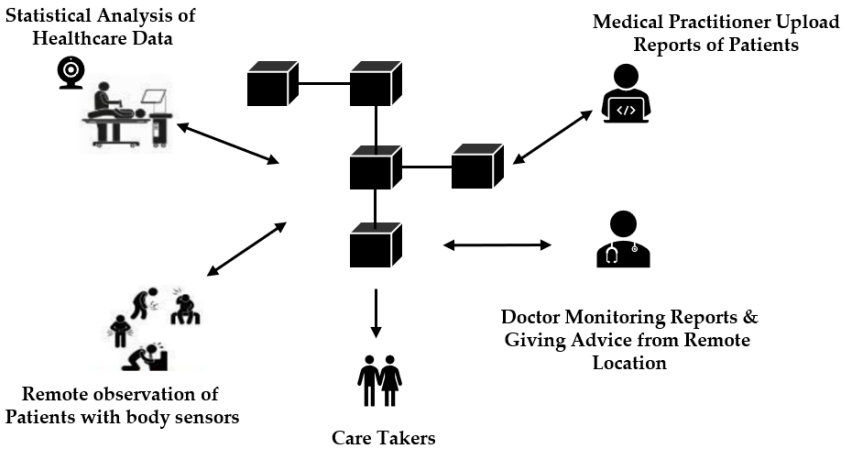

Fig.10. Blockchain-Based IoMT Architecture

Healthcare providers utilise wearables to keep track of their patient's health. These devices have sensors that can continuously monitor the patient and convey vital information to medical specialists via IoMT.

EMRs (electronic medical reports) are mostly patient-related clinical data that a patient sends to a physician or other healthcare professional. These EMRs are confidential and are required to provide the best possible care to the patient. In the diagnosis lab, electronic medical reports will be generated

and the assistant of the diagnosis lab, who is a member of the IoMT network, can able to add these electronic medical records (EMRs) to the blockchain. The patient network receives a fresh block of data when a new patient record is established.

The researcher developed and tried out a mobile app for cognitive behavioural insomnia therapy[27]. The information gathered by the app was transferred to a private Hyperledger Fabric blockchain network. The network of Electronic Medical Records (EMR) has been proven secure and tamper-resistant because of the blockchain's functionality as an immutable distributed ledger. The conclusion of this article is, Blockchain can be used to create a tamper-proof database. The suggested system verifies data integrity; however, the gathered healthcare information is recorded directly in the blockchain, making a considerable scaling challenge due to the ledger's limited storage capacity.

A private Ethereum blockchain was used by the creators of [63]. In the proposed method, sensors connect to a smart device (phone or tablet), which interacts with smart contracts directly. The latter provided information gets examined and sends out alerts to patients and healthcare professionals. Only valid transactions get recorded into the ledger, as a result, a valid RPM is offered. The suggested solution, however, faces a fundamental constraint in terms of data transfer latency from smart devices to blockchain nodes. Integrity, confidentiality, reliability, privacy, and transparency are among the security requirements addressed. However, the proposed approach does not justify scalability.

MedBlock [64] and MedChain [65] are distributed ledger blockchain technology-based information management solutions that offer secure and rapid access to electronic medical data. From a distributed blockchain ledger, medical data was extracted. MedBlock is a technique for distributing healthcare data for diagnosis reasons, as described by the authors in [58]. MedBlock permits people to access their electronic health records (EHRs). However, because the adopted approach relates to local hospital databases, data privacy is not completely assured.

Furthermore, MedBlock maintains only hospital medical data collected via physical checks and does not retain information about patients' physiological conditions. To resolve this problem, the authors of [59] suggested MedChain, a blockchain-dependent session-based architecture for exchanging healthcare data. MedChain enables users to manage and communicate not just electronic health records (EHRs) for their patients, but also physiological data acquired by IoMT devices linked to their bodies. Data integrity and confidentiality are provided via MedChain, however, availability and scalability are severely limited. Because information sharing and information uploading on a blockchain are both manual operations, the sharing service's availability is dependent on the patient's desire to do these tasks. Furthermore, the proposed approach does not allow for the expansion of healthcare practitioners from other organizations.

The authors of [66] proposed a decentralised architecture for monitoring and tracking changes to IoT device settings. They used a private blockchain to store the device configuration information as well as any changes that might arise. The modification history is saved and made available to administrators. As a result, this architecture promotes security by monitoring and auditing the setup of IoT devices. However, since IoT device-configured files are maintained inside the blockchain ledger, the suggested method has a big problem with scaling.

According to [67], a blockchain-based architecture can be used to keep track of patients who are not in a hospital. They suggested two blockchains, one for medical equipment and another for consultations, both of which would hold the patient's whole medical record history. In addition, in the event of an emergency, a monitoring system is employed to track the situation in real time and send out fast alerts. Wearable health devices also gather the data and store it on the medical equipment blockchain ledger. The authors recommend using the NDN paradigm to collect data from patient sensors. Implementation of the suggested architecture is based on the Hyperledger Fabric framework. Security criteria such as integrity, confidentiality, accessibility, transparency, and data privacy are covered in the proposed methodology. However, because the blockchain ledger has a limited storage capacity, storing the gathered medical data directly in it causes a severe scalability issue.

The authors came up with new cryptographic algorithms to keep data and transactions safe through the Ethereum Blockchain network. [68]. The given architecture addresses security problems such as consistency, confidentiality, reliability, data privacy, and scalability.

The authors proposed BiiMED, a blockchain-based framework technique, in [16]. Ethereum is a blockchain architecture that has been used to organize and verify shared data among healthcare professionals that exchange patient EHRs and publish healthcare data in the cloud. This technique established the Trusted Third-Party Auditor (TTPA), a blockchain-based entity responsible for authorising data transfers. While exchanging EHR, the suggested method maintains data interoperability and integrity. An access management module is used by the suggested BiiMED to identify and authenticate members. As a result, secrecy is ensured. Furthermore, the proposed system accommodates a considerable population of patients, according to scalability testing. The authors, on the other hand, do not assess availability, traceability, or data privacy.

The author [69] defined and implemented multiple medical processes for healthcare management by applying Ethereum smart contract framework. A lot of complicated medical procedures have been used in such healthcare workflows to make sure that the data is kept safe and that it can be traced back to the right person when it is shared with other people. The scalability of the suggested system processes, on the other hand, is questionable.

The authors of [70] described a blockchain-based IoT platform for a safety monitoring system of physiological indicators in patients. The suggested architecture employs a permissioned blockchain system that relies on Hyperledger Fabric. Hyperledger Composer is a tool for creating and implementing smart contracts that manage access to the ledger. The proposed solution solves problems with integrity, anonymity, accessibility, traceability, and data protection because Fabric Blockchain has built-in features that help. However, scalability is not achieved because this method stores patients' medical sensitive data from IoMT devices in the blockchain network, which requires a lot of space.

For healthcare tracking, the author of [17] uses the Ethereum blockchain. The authors suggested a four-tier healthcare system consisting of an application layer, a layer of blockchain-based services, a cloud layer, and an IoT device layer. Healthcare data is securely uploaded to the cloud with a blockchain-based distributed ledger. To evaluate the performance of the system, the efficacy of the Hybrid Ethereum Blockchain is compared to that of other prior systems. The proposed healthcare system surpasses the competitiveness in terms of response time, computational cost, and flexibility, however patient data privacy is not guaranteed.

The authors of [71] demonstrated how blockchain technology could be utilized to construct components of smart cities, for example, intelligent health services, intelligent energy, intelligent transportation, and intelligent agriculture. The authors underlined the benefits of blockchain technology in the context of resolving security and privacy issues. Inside the smart healthcare market, they introduced a blockchain-based infrastructure to monitor the patient’s essential parameters like blood sugar level, heart rate, and blood pressure. According to the design, all patient healthcare data is kept on the blockchain platform. Based on the analysis of the stored data, a set of instructions will be sent to the patient's mobile. The scalability issue is not resolved.

4.1. Related state of work & novelty of proposed architecture:

The proposed system is based on a blockchain system integrated with Interplanetary File System (IPFS). In the proposed system healthcare data will not be shared with IPFS directly. In most IPFS-based blockchain systems, healthcare data is shared first with IPFS and then forwarded to the blockchain, or data will be shared with IPFS and blockchain simultaneously. This will lead to the duplication of the data and double spending. Users who get access to the IPFS from outside sources cause data loss. The use of the IPFS as per the proposed system to store blockchain data helps to make a drastic improvement in the scalability of data.

A comparison of the related work is depicted in Table 3 explaining their contributions, the consensus algorithm types used in the proposed solution followed by the storage and data types applied in the proposed system, the type of framework, and blockchain used, and the tools used.

Table 3: Comparative study of existing system & proposed IoMT using Blockchain

Contribution/ Purpose	**Consensus**	**Storage**	**Framework**	**BC Type**	**Tools Used**	**Limitations**
Monitoring of patient's critical health parameters [63]	POW	Blockchain Database	Distributed Ledger Technology	Private	Solidity, Ganache	Scalability issue with storage of the data.
Patient Healthcare information monitoring and sharing [66]	POS	Cloud Storage	Ethereum Blockchain	Consortium	JavaScript, HTML, REST API	Storage is inside the BC ledger so scalability issues will arise.
Real-time monitoring of critical medical parameters [67]	PBFT	Distributed Ledger Technology	Hyperledger Fabric	Private	Hyperledger composer + Caliper	The larger amount of data produced at the nodes in BC causes delays in the transactions and scalability issues.
EHR Medical information sharing with a Trusted Third-Party Auditor (TTPA) [16]	AWS	Cloud database	Ethereum Platform	Private	Solidity language, test net of Ethereum	Lack of data transparency. No assurance of data traceability.
Decentralized Privacy Preserving Healthcare [69]	PoW	Cloud Storage	Ethereum	Private	Overlay network, solidity language	Data computation is high at the nodes of BC. The scalability issue is questionable.
IoT-Blockchain architecture for Healthcare Monitoring [70]	PBFT	Blockchain Database	Hyperledger Fabric	Private	Go language, SDK Application	Storage of transactions at the BC nodes creates space issues.
Tamper Resistant mobile health technology using Hyperledger [27]	PBFT	Blockchain Database	Hyperledger	Public	Data masking, java-based framework	Scalability issue. Outdated technology.
Medical Information Sharing [17]	PoW & PoS	BigData Storage (HDFS)	Ethereum, Hyperledger or	Consortium	Implementing using Java	Based on the public blockchain, privacy is not guaranteed.
Effective Healthcare Data Sharing using Medchain [65]	BFT-SMaRt	Local Database	Java	Consortium blockchain	Implementing using Java	Only limited practitioners are allowed in the blockchain.

Proposed Work	POW	IPFS	Ethereum	Private	Metamask, Remix, Ganache, Truffle	Scalability & data privacy issues were solved through the IPFS network.

5. System Model:

The proposed system is based on the storage of healthcare data & use of the IPFS network to solve the scalability issue of the blockchain shown in Fig. 10.

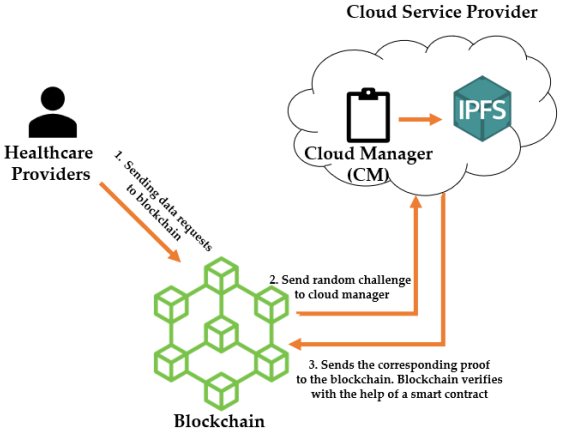

Fig. 10 Proposed Architecture for IoMT using Blockchain

To avoid fake doctor and hospital node attacks, doctors and hospitals upload their data using the private key and public key into the system. Data may contain critical information about the patient or scanned reports. Data will upload with the front-end web application with the patient's public key. The data will be for the patient with his public key. The data will be moved to the blockchain through the patient end device. Whenever the doctor wants to see the data during the next visit, the patient share data on a requirement basis. Nodes assigned to the patient are full user nodes, they can generate transactions, participate in mining and also broadcast them. Doctor's nodes are lightweight, and they will not participate in the mining process.

Each node in the blockchain creates a transaction and generates a block that should create a nounce with difficult calculations using the proof of work (PoW) algorithm. This is the basic concept used in bitcoin to avoid Sybil's attack. Blockchain data will send to the IPFS network to avoid the scalability of the blockchain. Blockchain sends a random challenge to the cloud manager to check the security of the data. Cloud manages to send back the corresponding proof to the blockchain in the form of a smart contract.

Selection of the blockchain technology is done based on community availability, cost, consensus mechanism, history and reputation in the industry, ease of use and languages, level of support and learning material of the blockchain[72].

The whole system is built on Ethereum blockchain technology and it is organized into several areas, which include doctors, patients, pharmaceutical shops, and insurance agencies. For the private Ethereum blockchain development, personal blockchain environments like Ethereum and distributed blockchain environment tools are used for the blockchain implementation. In Ethereum, Truffle Suite is used as a programming framework. It handles the whole smart contract lifecycle, from custom installations to library integration to complicated Ethereum applications. To create accounts and

transfer cryptocurrencies, a meta-mask account is used in dApp. The smart contracts are developed and tested using the remix online solidity compiler, which is built in the Solidity programming language as shown in Fig. 11. The system's front-end applications are created using reactJS.

Home healthcare.sol 5

```
30    address[] public patientList;
31    address[] public doctorList;
32    address[] public insurerList;
33
34    mapping (address => patient) patientInfo;
35    mapping (address => doctor) doctorInfo;
36    mapping (address => insurer) insurerInfo;
37    mapping (address => address) Patient_Insurer;
38    // might not be necessary
39    mapping (address => string) internal patientRecords;
40
41    function add_agent(string memory _name, uint _age, uint _designation, string memory _hash) public {
42        address addr = msg.sender;
43
44        if(_designation == 0){
45            patientInfo[addr].name = _name;
46            patientInfo[addr].age = _age;
47            patientInfo[addr].record = _hash;
48            patientList.push(addr);
49        }
50       else if (_designation == 1){
51            doctorInfo[addr].name = _name;
52            doctorInfo[addr].age = _age;
53            doctorList.push(addr);
54       }
55       else if(_designation == 2){
56           insurerInfo[addr].name = _name;
57           insurerList.push(addr);
58       }
59       else{
60           revert();
61       }
62    }
```

Fig.11 Smart contract for the proposed model

5.1. Smart Contract for medical prescription:

The main purpose of creating a smart contract for medicine prescriptions is to decrease the number of errors caused by doctor misinterpretations by eliminating long wait times, preventing fraud, and expediting the medical prescription process. A smart contract is used by a doctor to prescribe drugs for a patient and add it to the patient's medical record. The pharmacy subsequently gets the prescription via an Ethereum smart contract, which is subject to the approval of both the primary doctor and the patient. The pharmacy provides the drug after obtaining the prescription, which is subsequently uploaded to the patient's medical records through smart contracts, together with the medicine's expiration date and dose usage, and the medicine is available for pickup by the patient.

The advanced feature of smart contracts allows doctors and pharmacy retailers to organize medicine consumption. As part of the consultation, doctors do not spend as much time talking about pharmaceutical requests or talking to drug stores in general. As shown in Fig. 12, the patient, main doctor, and pharmacist are all involved in the process of providing a medical prescription. It also includes information on the prescription, such as the pharmaceutical ID, expiration date, and patient ID.

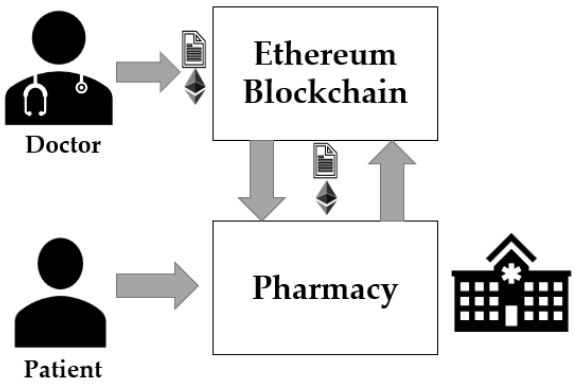

Fig. 12 Smart contract for doctors & pharmacy retailers

a. Smart contracts for Laboratory test data:

As shown in Fig. 13, the primary objective of the creation of a smart contract for laboratory results is to exchange information using blockchain distributed ledger technology, enabling laboratories, doctors, primary hospitals, and other partners to efficiently obtain and disseminate a patient's medical data within many investors.

Consider a scenario in which a patient goes to a lab to have a blood test. Patients will be notified through the Ethereum blockchain when their test findings have been analyzed and entered into their medical records. They will also have the choice to let their data be encoded and stored on the Ethereum blockchain.

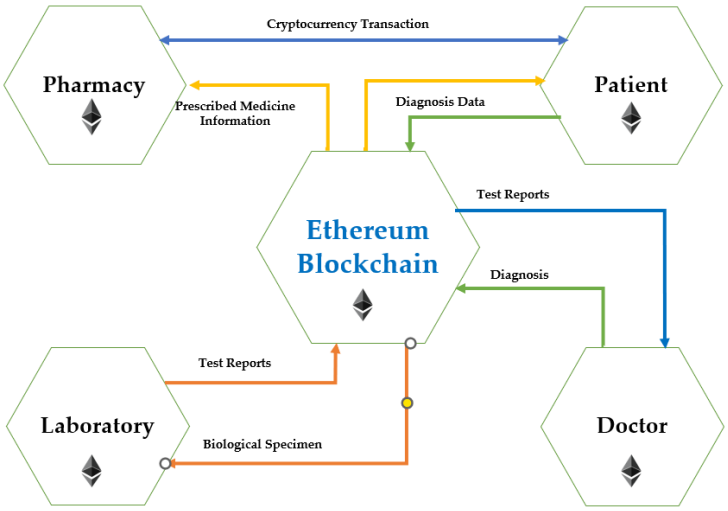

Fig.13 Smart Contract for sharing lab results

b. Smart contracts for patients and service providers:

Fig. 14 shows a patient's demand for immediate medical attention. By using the smart contract method, this request is forwarded to the head doctor as soon as possible. A doctor must evaluate the request and provide a recommendation. If necessary, send the patient to a specialist for further treatment. The EHR should include all information regarding a patient's treatment history. Note that the patient's healthcare data is saved locally in a database with severe constraints on who has the authority to access it and to what extent, all of which are managed via Ethereum smart contracts.

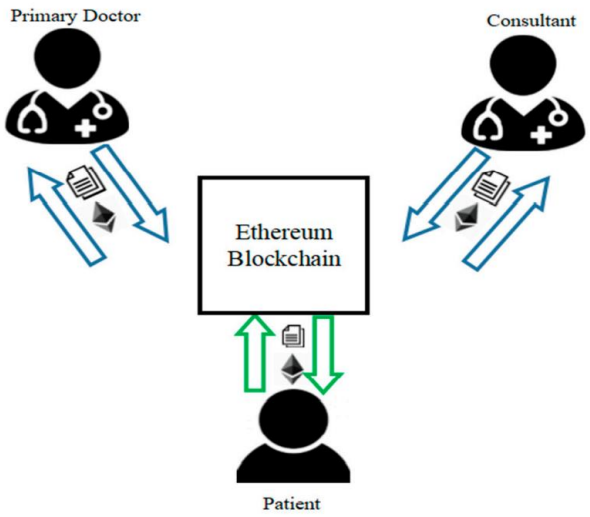

Fig. 14 smart contract between Patients and Service Providers

6. Results & Discussion:

This review's focus is on the use of blockchain for healthcare data management and includes a discussion of its applications on the internet of things and healthcare. It also evaluates the integration techniques used for blockchain and IoT integration. As a result, security attacks on IoT application is reviewed in integration with blockchain techniques. Moreover, data security provisions such as data analysis, processing and security for different healthcare applications are demonstrated. Along with the solution to the storage issue of the blockchain, the transaction speed issue can be solved through the zero-knowledge ledger to reduce the transaction period[73].

6.1. Solution on scalability issue of blockchain:

IPFS model of the blockchain helps in solving storage issues of the blockchain which will be a critical issue in near future for all the blockchain systems. For comparison purposes, consider blockchain without an IPFS network. Let us consider 100 block transactions for evaluation. The blocks will be incremented by 100 to 1000. Data stored in the off-chain blocks is 132 bytes and in contrast storage of data on the blocks consumes 15360 bytes. The maximum capacity of the block is 1 MB, thus the 8286 transactions can hold on the 100 blocks on-chain and 794315 transactions on off-chain. A single block of off-chain can store more transactions compared to the on-chain storage model.

6.2. Attacks on IoMT:

The success of healthcare depends upon security measures taken for the prevention of attacks. Wireless medical sensors are very much prone to security attacks in IoT systems. This review provides a detailed study of attacks on the physical layer and perception layer of the system. Security threats in healthcare are more significant as in wireless sensor range of the attacks is not confined. However, major work is to be done in the area of healthcare security and privacy, since the data can be accessed, monitored and modified which turns into a life-threatening risk. In the current research, it appears there is very less awareness of the attacks on the medical internet of things. Most of the healthcare research either covers the security or privacy of patient's healthcare-related data. Federated learning-based data accumulation schemes help to improve data security in privacy in remote areas with the help of drones based on blockchain technology[74].

6.3. Data Privacy solution through blockchain:

The public blockchain networks may not be too much concerned about data privacy. Still, extra care needs to be taken while dealing with personal data to prevent its misuse. Access to personal data

must be controlled across nodes in the blockchain. In other situations, where no personal information is involved, releasing the information might disclose trade secrets. In healthcare applications, the most essential element is patient identification. In the proposed healthcare architecture, patient data will not be published on the blockchain network, without the permission of the patient. Instead of using the cloud or a hospital data centre, blockchain maintains the information locally on a device that is closest to the owner of the information. In the proposed model, IPFS stores the patient's healthcare information. Access policies of the data will be stored in another private blockchain. This will ensure, the information owner's access policies will not be altered, and access to the data will be in full control.

6.4. IoMT and Blockchain integration:

An integration of IoMT and blockchain is useful for a wide application. The qualitative benefit of both systems is reflected in the system. According to the review, blockchain technology is used for data management, more notably for data security. In data security, blockchain ensures data integrity, privacy preservation, and access control. Blockchain-based data management gives authority to the patient over their data. Blockchain gives authority to access the data and track who can access it. The success of data management is depended upon authentication provided by the blockchain through the public key allocation. Further, smart contracts and user-friendly architecture are created for the blockchain. The number of smart contracts used in the system is inconsistent in number. According to this article, there is no fixed strategy for access control, storage of data and privacy preservation. However, on the aspect of the speed of transactions, storage of data and participation flexibility, established platform like Ethereum is used for access control.

7. Conclusion

We reviewed and develop a system architecture based on the Blockchain platform for distributed healthcare data management in this paper. To provide an effective and secure electronic healthcare data management system, the suggested solution integrates Blockchain technology alongside healthcare IoT devices with the help of an IPFS storage system. The suggested system's design is based on using decentralised storage and a permissioned blockchain network for monitoring the patient's critical data. The proposed system creates blockchain services for main healthcare components, for example, doctors, pharmacies, and patients will have different blockchains. Future directions for this research might include incorporating critical attacks and blockchain solutions with an approach to the analysis of medical data and automation of healthcare diagnostic choices.

Conflict of Interest: Sujatha R. declares that she has no conflict of interest, and Vinod S. declares that he has no conflict of interest. This article does not contain any studies with human participants performed by any of the authors.

References:

[1] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10250–10276, 2020, doi: 10.1109/JIOT.2020.2997651.

[2] W. Lin *et al.*, "Blockchain Technology in Current Agricultural Systems: From Techniques to Applications," *IEEE Access*, vol. 8, pp. 143920–143937, 2020, doi: 10.1109/ACCESS.2020.3014522.

[3] T. Kumar, A. Braeken, V. Ramani, I. Ahmad, E. Harjula, and M. Ylianttila, "SEC-BlockEdge: Security Threats in Blockchain-Edge based Industrial IoT Networks," *Proc. 2019 11th Int. Work. Resilient Networks Des. Model. RNDM 2019*, pp. 1–7, 2019, doi: 10.1109/RNDM48015.2019.8949107.

[4] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of Blockchains in the Internet of Things: A Comprehensive Survey," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019, doi: 10.1109/COMST.2018.2886932.

[5] A. Adavoudi Jolfaei, S. F. Aghili, and D. Singelee, "A Survey on Blockchain-Based IoMT Systems: Towards Scalability," *IEEE Access*, vol. 9, pp. 148948–148975, 2021, doi: 10.1109/ACCESS.2021.3117662.

[6] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020, doi: 10.1109/ACCESS.2020.2995917.

[7] A. H. Sodhro, S. Pirbhulal, and A. K. Sangaiah, "Convergence of IoT and product lifecycle management in medical health care," *Futur. Gener. Comput. Syst.*, vol. 86, pp. 380–391, 2018, doi: 10.1016/j.future.2018.03.052.

[8] L. Haoyu, L. Jianxing, N. Arunkumar, A. F. Hussein, and M. M. Jaber, "An IoMT cloud-based real time sleep apnea detection scheme by using the SpO2 estimation supported by heart rate variability," *Futur. Gener. Comput. Syst.*, vol. 98, pp. 69–77, 2019, doi: 10.1016/j.future.2018.12.001.

[9] A. Islam, T. Rahim, Masuduzzaman, and S. Y. Shin, "A Blockchain-Based Artificial Intelligence-Empowered Contagious Pandemic Situation Supervision Scheme Using Internet

of Drone Things," *IEEE Wirel. Commun.*, vol. 28, no. 4, pp. 166–173, 2021, doi: 10.1109/MWC.001.2000429.

[10] K. Szczypiorski, A. Janicki, and S. Wendzel, "'The good, the bad and the ugly': Evaluation of Wi-Fi steganography," *J. Commun.*, vol. 10, no. 10, pp. 747–752, 2015, doi: 10.12720/jcm.v.n.p-p.

[11] Y. Sun, F. P. W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, pp. 183339–183355, 2019, doi: 10.1109/ACCESS.2019.2960617.

[12] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, no. September 2018, pp. 45–58, 2019, doi: 10.1016/j.jnca.2018.10.020.

[13] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/5978636.

[14] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," *Comput. Networks*, vol. 200, no. September, p. 108500, 2021, doi: 10.1016/j.comnet.2021.108500.

[15] G. Tripathi, M. A. Ahad, and S. Paiva, "S2HS- A blockchain based approach for smart healthcare system," *Healthcare*, vol. 8, no. 1, p. 100391, 2020, doi: 10.1016/j.hjdsi.2019.100391.

[16] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," *2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020*, pp. 310–317, 2020, doi: 10.1109/ICIoT48696.2020.9089570.

[17] D. H. Wang, "IoT based Clinical Sensor Data Management and Transfer using Blockchain Technology," *J. ISMAC*, vol. 2, no. 3, pp. 154–159, 2020, doi: 10.36548/jismac.2020.3.003.

[18] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," *2017 IEEE Int. Conf. Intell. Secur. Informatics Secur. Big Data, ISI 2017*, pp. 176–178, 2017, doi: 10.1109/ISI.2017.8004903.

[19] X. Li, B. Tao, H. N. Dai, M. Imran, D. Wan, and D. Li, "Is blockchain for Internet of Medical Things a panacea for COVID-19 pandemic?," *Pervasive Mob. Comput.*, vol. 75, p. 101434, 2021, doi: 10.1016/j.pmcj.2021.101434.

[20] M. A. Ferrag, L. Shu, and K. K. R. Choo, "Fighting COVID-19 and Future Pandemics with the Internet of Things: Security and Privacy Perspectives," *IEEE/CAA J. Autom. Sin.*, vol. 8, no. 9, pp. 1477–1499, 2021, doi: 10.1109/JAS.2021.1004087.

[21] B. Zaabar *et al.*, "FTM-IoMT: Fuzzy-Based Trust Management for Preventing Sybil Attacks in Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4485–4497, 2021, doi: 10.1109/ACCESS.2019.2960412.

[22] C. W. Yang *et al.*, "Detection and Prevention of ICMP Flood DDOS Attack," *Comput. Commun.*, vol. 13, no. 3, p. 263333, 2017, doi: 10.1016/j.ijpe.2015.11.008.

[23] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 2015, doi: 10.1016/j.comnet.2014.11.008.

[24] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris, "A Blockchain-enabled Architecture for IoMT Device Authentication," *2nd IEEE Eurasia Conf. IOT, Commun. Eng. 2020, ECICE 2020*, pp. 89–92, 2020, doi: 10.1109/ECICE50847.2020.9301913.

[25] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.

[26] O. Salem, K. Alsubhi, A. Shaafi, M. Gheryani, A. Mehaoua, and R. Boutaba, "Man-in-the-Middle Attack Mitigation in Internet of Medical Things," *IEEE Trans. Ind. Informatics*, vol. 18, no. 3, pp. 2053–2062, 2022, doi: 10.1109/TII.2021.3089462.

[27] D. Ichikawa, M. Kashiyama, and T. Ueno, "Tamper-resistant mobile health using blockchain technology," *JMIR mHealth uHealth*, vol. 5, no. 7, pp. 1–11, 2017, doi: 10.2196/mhealth.7938.

[28] C. W. Yang, T. Hwang, and T. H. Lin, "Modification Attack on QSDC with Authentication and the Improvement," *Int. J. Theor. Phys.*, vol. 52, no. 7, pp. 2230–2234, 2013, doi: 10.1007/s10773-013-1498-2.

[29] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *Int. J. Prod. Econ.*, vol. 172, pp. 76–94, 2016, doi: 10.1016/j.ijpe.2015.11.008.

[30] A. Proaño and L. Lazos, "Selective jamming attacks in wireless networks," *IEEE Int. Conf. Commun.*, pp. 0–5, 2010, doi: 10.1109/ICC.2010.5502322.

[31] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 17, no. 4, pp. 197–215, 2014, doi: 10.1504/IJAHUC.2014.066419.

[32] Harshita and R. Nayyar, "Detection of ICMP Flood DDoS Attack," *Int. J. New Technol. Res.*, vol. 5, no. 2, pp. 199–205, 2017, [Online]. Available: www.ijcstjournal.org/volume-5/issue-2/IJCST-V5I2P39.pdf.

[33] M. Bogdanoski, T. Shuminoski, and A. Risteski, "Analysis of the SYN Flood DoS Attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 5, no. 8, pp. 15–11, 2013, doi: 10.5815/ijcnis.2013.08.01.

[34] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst. Man, Cybern. Part ASystems Humans*, vol. 40, no. 4, pp. 853–865, 2010, doi: 10.1109/TSMCA.2010.2048028.

[35] P. Kumar and H. J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012, doi: 10.3390/s120100055.

[36] Z. A. Baig and A. R. Amoudi, "An analysis of smart grid attacks and countermeasures," *J. Commun.*, vol. 8, no. 8, pp. 473–479, 2013, doi: 10.12720/jcm.8.8.473-479.

[37] A. Gupta and A. Anand, "Ethical Hacking and Hacking Attacks," *Int. J. Eng. Comput. Sci.*, no. May, 2017, doi: 10.18535/ijecs/v6i4.42.

[38] A. Yogeshwar and S. Kamalakkannan, "Healthcare domain in IoT with blockchain based security- A researcher's perspectives," *Proc. - 5th Int. Conf. Intell. Comput. Control Syst. ICICCS 2021*, no. Iciccs, pp. 440–448, 2021, doi: 10.1109/ICICCS51141.2021.9432198.

[39] J. Nam, J. Paik, H. K. Kang, U. M. Kim, and D. Won, "An off-line dictionary attack on a simple three-party key exchange protocol," *IEEE Commun. Lett.*, vol. 13, no. 3, pp. 205–207, 2009, doi: 10.1109/LCOMM.2009.081609.

[40] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty, and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," *IEEE Access*, vol. 7, pp. 182459–182476, 2019, doi: 10.1109/ACCESS.2019.2960412.

[41] J. Deogirikar, "Security Attacks inIoT : A Survey," pp. 32–37, 2017.

[42] E. Cooke, F. Jahanian, and D. McPherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," *Steps to Reducing Unwanted Traffic Internet Work. SRUTI 2005*, pp. 39–44, 2005.

[43] Z. A. Solangi, Y. A. Solangi, S. Chandio, M. B. S. A. Aziz, M. S. Bin Hamzah, and A. Shah, "The future of data privacy and security concerns in Internet of Things," *2018 IEEE Int. Conf. Innov. Res. Dev. ICIRD 2018*, no. May, pp. 1–4, 2018, doi: 10.1109/ICIRD.2018.8376320.

[44] "Blockchain basics: Utilizing blockchain to improve sustainable supply chains in fashion," *Strateg. Dir.*, vol. 37, no. 5, pp. 25–27, 2021, doi: 10.1108/SD-03-2021-0028.

[45] D. Pramulia and B. Anggorojati, "Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask," *Proc. - 2nd Int. Conf. Informatics, Multimedia, Cyber, Inf. Syst. ICIMCIS 2020*, pp. 18–23, 2020, doi: 10.1109/ICIMCIS51567.2020.9354310.

[46] A. Yogeshwar *et al.*, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 8, no. 2, pp. 1–4, 2020, doi: 10.1016/j.comcom.2020.02.018.

[47] D. Romano and G. Schmid, "Beyond bitcoin: Recent trends and perspectives in distributed ledger technology," *Cryptography*, vol. 5, no. 4, 2021, doi: 10.3390/cryptography5040036.

[48] M. Turan, R. Perlner, and L. Bassham, "Status report on the second round of the SHA-3 cryptographic hash algorithm competition," *… Interag. Rep.*, 2011, [Online]. Available: http://csrc.nist.gov/publications/nistir/ir7764/nistir-7764.pdf.

[49] E. Heilman *et al.*, "Cryptanalysis of curl-p and other attacks on the iota cryptocurrency," *IACR Trans. Symmetric Cryptol.*, vol. 2020, no. 3, pp. 367–391, 2020, doi: 10.13154/tosc.v2020.i3.367-391.

[50] Y. Fan, H. Wu, and H. Y. Paik, "DR-BFT: A consensus algorithm for blockchain-based multi-layer data integrity framework in dynamic edge computing system," *Futur. Gener. Comput. Syst.*, vol. 124, pp. 33–48, 2021, doi: 10.1016/j.future.2021.04.020.

[51] S. S. Panda, B. K. Mohanta, U. Satapathy, D. Jena, D. Gountia, and T. K. Patra, "Study of Blockchain Based Decentralized Consensus Algorithms," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2019-Octob, pp. 908–913, 2019, doi: 10.1109/TENCON.2019.8929439.

[52] C. Dwork and M. Naor, "Pricing via processing or combatting junk mail," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 740 LNCS, pp. 139–147, 1993, doi: 10.1007/3-540-48071-4_10.

[53] S. Maximiliano and M. Enio, "Explaining Blockchain Technology and Working with Hyperledger."

[54] I. Eluubek kyzy, H. Song, A. Vajdi, Y. Wang, and J. Zhou, "Blockchain for consortium: A practical paradigm in agricultural supply chain system," *Expert Syst. Appl.*, vol. 184, no. June, p. 115425, 2021, doi: 10.1016/j.eswa.2021.115425.

[55] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electron.*, vol. 9, no. 1, 2020, doi: 10.3390/electronics9010094.

[56] A. D. Dwivedi, "Brisk: Dynamic encryption based cipher for long term security," *Sensors*, vol. 21, no. 17, 2021, doi: 10.3390/s21175744.

[57] S. Dhar, A. Khare, and R. Singh, "Advanced security model for multimedia data sharing in Internet of Things," *Trans. Emerg. Telecommun. Technol.*, no. June, pp. 1–17, 2022, doi: 10.1002/ett.4621.

[58] B. Zaabar, O. Cheikhrouhou, M. Ammi, A. I. Awad, and M. Abid, "Secure and Privacy-aware Blockchain-based Remote Patient Monitoring System for Internet of Healthcare Things," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, vol. 2021-Octob, pp. 200–205, 2021, doi: 10.1109/WiMob52687.2021.9606362.

[59] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C. M. Cheng, and K. Sakurai, "A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity," *Cryptography*, vol. 6, no. 1, pp. 1–22, 2022, doi: 10.3390/cryptography6010003.

[60] S. Padmaja and E. Kesavulu Reddy Asst Professor, "Security and Privacy in Cloud-Assisted Wireless Wearable Communications; Security and Privacy in Cloud-Assisted Wireless Wearable Communications," *Int. J. Eng. Res. Technol.*, vol. 8, no. 2, pp. 44–46, 2020, [Online]. Available: www.ijert.org.

[61] M. Raikwar, D. Gligoroski, and K. Kralevska, "SoK of Used Cryptography in Blockchain," *IEEE Access*, vol. 7, pp. 148550–148575, 2019, doi: 10.1109/ACCESS.2019.2946983.

[62] S.-H. Han *et al.*, "Towards a remote monitoring of patient vital signs based on iot-based blockchain integrity management platforms in smart hospitals," *Sensors (Switzerland)*, vol. 9, no. 7, pp. 1–11, 2019, doi: 10.2196/mhealth.7938.

[63] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring," *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, 2018, doi: 10.1007/s10916-018-0982-x.

[64] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "SYSTEMS-LEVEL QUALITY IMPROVEMENT

MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," *J. Med. Syst.*, vol. 42, pp. 1–11, 2018, [Online]. Available: https://doi.org/10.1007/s10916-018-0993-7.

[65] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," *Appl. Sci.*, vol. 9, no. 6, 2019, doi: 10.3390/app9061207.

[66] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of IoT devices using blockchain," *Sensors (Switzerland)*, vol. 19, no. 4, 2019, doi: 10.3390/s19040856.

[67] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application," *2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work.*, pp. 19–23, 2019, doi: 10.1109/NTMS.2019.8763849.

[68] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[69] Y. Nakamura, Y. Zhang, M. Sasabe, and S. Kasahara, "Exploiting smart contracts for capability-based access control in the internet of things," *Sensors (Switzerland)*, vol. 20, no. 6, 2020, doi: 10.3390/s20061793.

[70] A. H. Mohammed, A. A. Abdulateef, and I. A. Abdulateef, "Hyperledger, Ethereum and Blockchain Technology: A Short Overview," *HORA 2021 - 3rd Int. Congr. Human-Computer Interact. Optim. Robot. Appl. Proc.*, 2021, doi: 10.1109/HORA52670.2021.9461294.

[71] *A comprehensive proposal for blockchain-oriented smart city*, vol. 308, no. January. 2021.

[72] S. Nanayakkara, M. N. N. Rodrigo, S. Perera, G. T. Weerasuriya, and A. A. Hijazi, "A methodology for selection of a Blockchain platform to develop an enterprise system," *J. Ind. Inf. Integr.*, vol. 23, no. September 2020, p. 100215, 2021, doi: 10.1016/j.jii.2021.100215.

[73] R. Singh, A. D. Dwivedi, R. R. Mukkamala, and W. S. Alnumay, "Privacy-preserving ledger for blockchain and Internet of Things-enabled cyber-physical systems," *Comput. Electr. Eng.*, vol. 103, no. August, p. 108290, 2022, doi: 10.1016/j.compeleceng.2022.108290.

[74] A. Islam, A. Al Amin, and S. Y. Shin, "FBI: A Federated Learning-Based Blockchain-Embedded Data Accumulation Scheme Using Drones for Internet of Things," *IEEE Wirel. Commun. Lett.*, vol. 11, no. 5, pp. 972–976, 2022, doi: 10.1109/LWC.2022.3151873.