

# A SURVEY ON HEALTH CARE PRIVACY APPROACH USING BLOCKCHAIN TECHNOLOGY

Varsha Chavan<sup>1</sup>, Suvarna Mane<sup>2</sup>, Poonam Adake<sup>3</sup>, Anannya Garud<sup>4</sup>, Prof. S. A. Nalawade<sup>5</sup>

<sup>1</sup>Student, Dept. of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri-Pune, Maharashtra, India

<sup>2</sup>Student, Dept. of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri-Pune, Maharashtra, India

<sup>3</sup>Student, Dept. of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri-Pune, Maharashtra, India

<sup>4</sup>Student, Dept. of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri-Pune, Maharashtra, India

<sup>5</sup> Guide, Dept. of Information Technology, Dr. D. Y. Patil Institute of Technology, Pimpri-Pune, Maharashtra, India.

\*\*\*

**Abstract** - In a computer network huge data is generated by numerous applications. The data is constantly rising, based on comprehensive operating conditions. Applications generate a torrent of data, disrupting the cloud's previously dependable data processing and analytics capabilities, which had previously been handled successfully prior to the introduction of Big-Data. Blockchain technology helps to eliminate the need for centralization and maintain information integrity and ownership, as well as to mediate transactions and the exchange of digital assets by enabling safe and pseudo-anonymous transactions. It promotes direct agreements between participants. It includes crucial characteristics such as immutability, decentralization and openness, which could help in resolving critical concerns and challenges such as incomplete records at the point of service and limited access to patient's own health data. Interoperability in Blockchain enables software apps and technology platforms to connect, share, and use data across organizations and app vendors in a secure and seamless manner, resulting in a more efficient and effective healthcare system. Due to a lack of interoperability in healthcare systems it is suffering from compartmentalized and fragmented data, delayed connectivity, and disparate workflow tools. Blockchain technology allows for safe and pseudo-anonymous access to longitudinal, complete, and tamper-resistant medical records held in fragmented systems. Fog computing, also known as fogging, relocates computer applications, data, and services away from the centralized cloud and onto the network edge's logical stream.

**Key Words:** Block chain, Big-Data, Decentralized, Interoperability, Immutability.

## 1. INTRODUCTION

In hospitals, it is common for workers to use their hands to collect patient information. Papers and books are used to maintain patient's record manually. A fundamental disadvantage of this method is the enormous amount of storage and retrieval space it necessitates. In this method keeping track of all of the information is a complex process. Computers in every field are becoming more common. Every day, an increasing number of people keep and access medical records. When it comes to persuading individuals to alter their opinions, it fails miserably. Self-awareness has become progressively essential. In terms of protecting the patient's right, to hold the doctor and the institution accountable if something goes wrong, patient's records must always be kept confidential. There's a chance that a loss of paper documents may lead to more issues in treating patient.

Improving one's physical health has the ability to improve both own happiness and social well-being. A strong economy is essential to the country's general well-being. According to industry standards, health care practitioners are expected to diagnose and treat diseases and illnesses that arise on a regular basis. This is something to which people are used. Clinical data concerning a patient's health that a doctor has to maintain and entered in a medical record is known as a health record. There are several elements to consider when assessing a patient's overall health, both emotionally and physically. A patient's health record contains detailed information about their medical history. A physical examination, diagnosis, therapy and the results of laboratory testing are all part of it. Scan findings, allergy alarms, and other vital things are also included in these medical records. Manually handling records needs to combine with digital copies with security using a computer. It is feasible to design a computer architecture that does not contain all of its components in a single location. This is useful for programmers that really need to know the exact time and

position at all times. The data can be encrypted for security. If someone trying to gain access to such a cryptographic database without credentials is almost impossible.

In order to ensure the safety of all parties engaged. In this part, we'll look at how Blockchain technology is currently being used in the healthcare business. It is like we are preventing patients from receiving their data anytime they need. We shouldn't be using this strategy inside this situation since it requires a great deal of physical labor. It's indeed possible to send or fax records due to their dispersed location. They're neither concentrated nor dispersed. Furthermore, you have the right to request access to your medical records from the government. In their professional life, doctors have a limited amount of influence.

## 2.LITERATURE SURVEY

[1] In situations of medical negligence or medical conflicts, electronic medical data can assist prevent sickness, enhance cure rates, and give proof. However, worries concerning the integrity and security of electronic medical data remain unanswered. In this post, we discuss how to store and distribute electronic medical records using interplanetary file system. This was done via attribute-based encryption. They employ blockchain technology to secure the ciphertext using attribute-based encryption mechanism and the IPFS storage environment. Our method uses ciphertext policy attribute-based encryption to protect electronic medical records while permitting fast retrieval. Interplanetary File System (IPFS) safeguards the storage platform and has no single point of failure.

[2] Blockchain is a technology that offers the ability to create new business models and solves trust issues in a more efficient way. It leads to many research opportunities and business innovations. Academia and industry proposed many blockchain based software solutions within a wide range of domains. In this paper we present a system design where blockchain technology is proposed to be used in the healthcare system, where the vital information regarding the medical analysis is shared between hospitals, clinics and research institutes based on access policies defined by the patients. In order to protect confidential data, our solution involves the use of two types of chains: a private one, the sidechain, which keeps information about real ID of the patients and a public one,

the main chain, which stores information about patients' health data marked with a temporary ID. To test it, the authors have developed the design using Hyperledger Fabric framework.

[3] A healthy population is necessary for global progress, and health data may be used to predict future health. Patient information is centralized, which leads to data breaches. This number comes from the Ponemon cost of data breach Study, which was released in 2017. A healthcare data breach costs an average of \$380 per compromised record. According to the 2016 Breach Barometer Report, patient data was compromised in 27,314,647 records. As a result, institutional expectations may lead us to return to our prior record-keeping practices. This was a promising indication. Without the patient's awareness or consent, the information is likely to be used. Smart contracts, rather than traditional contracts, may be able to speed up some medical procedures. To create and validate data, it will be critical to use the Blockchain, a distributed ledger. Smart contracts might be utilized to establish a Blockchain-based record-keeping system that is patient-driven. The author anticipates more research and practical applications as long as the study scope is large enough.

[4] An electronic health record is often used to track the trajectory of disease occurrence, development, and treatment (EHR). As a result, it has a high therapeutic value. Data sharing and privacy preservation are key difficulties in EHR since medical data is confidential and sensitive for patients. Blockchain technology, due to its decentralization and tamper resistance, may be a viable solution to the aforementioned difficulties. To improve the hospital's electronic health system, The authors propose a medical data sharing and protection strategy based on the hospital's private blockchain in this paper. To begin, the system can satisfy a number of security criteria, including decentralization, openness, and tamper resistance. A dependable mechanism for doctors to preserve medical data or retrieve patient historical data while respecting patient privacy is designed. A mechanism for matching symptoms between patients is also offered. It allows patients who have similar symptoms to complete mutual authentication and generate a session key for future illness communication

[5] The most burning topic of today, calls for a solution that is reliable, secure and cost-effective cloud storage that can tide over the turbulent conditions of the rapidly budding digital storage technologies. This promotes for a

devoted solution in the form of an individualized, patient-centric care - IoMT (Internet of medical things) that augments precise disease identification, reduction in errors, and reduction in costs of care through the support of technology. It allows patients to direct health information data to doctors, manage medicines and drugs, keep Personal Health Records, caters to remote medical supports care, provides proactive approach to preserving good health, improves and accelerates clinician workflows, empowers extreme connectivity due to better automation and perceptions in the DNA of IoMT functions. But IoMT adoption is like constraints of increased administrative costs, deficiency of universal data access in present-day electronic medical records.

### 3. PROPOSED SYSTEM ARCHITECTURE

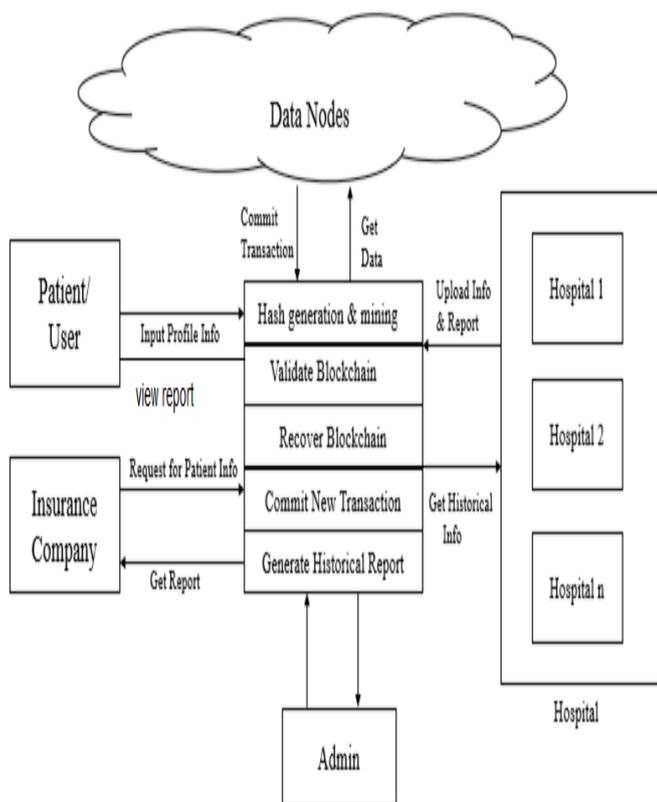


FIGURE: -1

Data from various health-care transactions will be stored in distinct data nodes, with each node containing a unique transaction block.

Before committing a block, the system must validate the prior block.

Each block that has been altered by a third-party attacker

or an unauthorized user must show that the existing blockchain is invalid during a transaction.

Detecting and resolving runtime server risks, as well as restoring the server.

The system will validate all server transactions.

### Modules

The system is made up of the following parts:

A hospital is a service center interacts with patients in order to get the information for each patient's record.

An insurance company that needs to refer patient's medical records.

Patients have to sign up for the system, download and send their records and answer as per doctors' data requests.

The Administrator, who manages the system and ensures smooth functioning.

### 4. ALGORITHM

#### Algorithm1: Protocol for Peer Verification

Step 1: User generate the any transaction DDL, DML or DCL query

Step 2: Get current IP address

For each (read IP address)

If (connection (IP) equals (true))

Flag =true

Else

Flag =false

End for

Step 4: if (Flag == true)

Peer to Peer Verification valid

Else

Peer to Peer Verification is Invalid

End if

End for

**Algorithm 2: Hash Generation**

- Step 1 : Input data as d
- Step 2 : Apply SHA 256 from SHA family
- Step 3 :Current\_Hash= SHA256(d)
- Step 4 : Return Current\_Hash

**Algorithm 3: Mining algorithm**

- Step 1 : User generate a transaction DDL, DML or DCL query
- Step 2 : Get current server blockchain
  - CchainCnode[Chain]
- Step 3: Foreach (read I into NodeChain)
  - If (!.equals NodeChain[i] with (Cchain))
  - Flag =1
  - Else
  - Continue Commit query
- Step 4: if (Flag == 1)
  - Count = SimilaryNodesBlockchain()
- Step 5: Calculate the majority of server
  - Recover invalid blockchain from specific node
- Step 6: End if
  - End for

**5. APPLICATIONS**

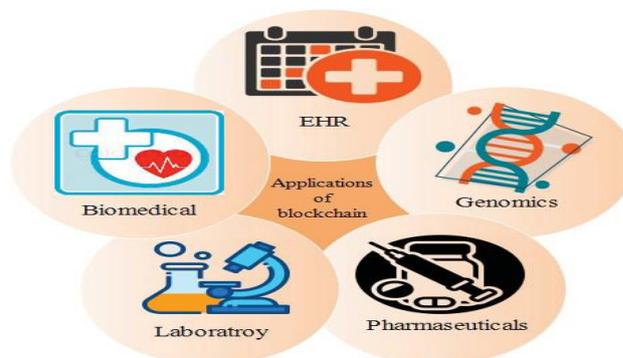


FIGURE: -2

•**Electronic Health Record (EHR):** Decentralized ledger in EHR means that data cannot be held by any intruder. In blockchain, each node has an updated copy of the ledger, and each node validate the copy thus intruder cannot get control all over the ledger. In a Permissioned blockchain, doctor, hospital, Labs can access the patient’s data after taking permission from the patient.

•**Biomedical:** In a blockchain-based medical application, alteration and replication were not allowed in a transaction. Blockchain only allows the secure and transparent transaction.

•**Laboratories:** Blockchain creates a secure decentralized structure for laboratory-related information which only happens with blockchain and that data can be shared securely with researcher groups.

•**Pharmaceuticals:** Blockchain is used to traced the pharmaceuticals in detail and also keeps eye on every phase of the pharmaceutical supply chain of the medicine and its components are regularly detected at each phase to avoid the replacement of any goods.

•**Genomics:** Blockchain technology can help to create a genomics data revolution by reducing the individual genome sequencing costs, democratizing genomic data ownership, and enabling transparent genomic data sharing.

## 6. RESEARCH CHALLENGES

In this section, we present the challenges of blockchain and how these challenges lead to research. The solutions to the challenges are described.

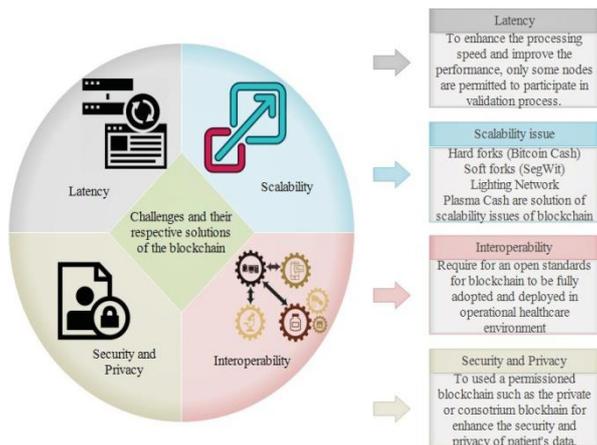


FIGURE: -3

**Latency:** In a public blockchain, all nodes are participating in the validation process which takes more time. To solve this problem, only a few nodes allowed to participate in the validation process which preserves time so improve the processing speed as well as the performance of the system.

**Scalability:** There are various solutions available like Hard fork (Bitcoin Cash), Soft fork, Lighting network, and plasma cash.

**Interoperability:** Requirement for an open standard for blockchain to be fully adopted and deployed in operational healthcare environment.

**Security and Privacy:** In a Permission-less blockchain, Intruder has a chance to attack in a network and create a major problem. To solve this problem, it is required to use a Permissioned blockchain like a private or consortium blockchain to secure the data and preserve the privacy of the patient. Blockchain uses the smart-contracts which allows the execution of transactions without considering the third-party user. These transactions are irreversible and traceable.

## 7. CONCLUSIONS

In this paper we provide insights to the blockchain based system for healthcare sector. The survey provided presents ways to overcome the security and privacy issues of traditional system. Finally, we highlighted various research challenges of blockchain in healthcare sector. Future study aims to look at developing a more efficient and diverse blockchain for smart healthcare governance framework that considers diverse culture and technical backgrounds.

## REFERENCES

- [1] Mohammad Moussa Madine, (member, IEEE), Ammar Ayman Battah, Ibrar Yaqoob, (senior member, IEEE), "Blockchain for Giving Patients Control Over Their Medical Records" [2020] DOI:10.1109/ACCESS.2020.3032553
- [2] LiviuHirtan, "Blockchain-based approach for e-health data access management with privacy protection" [2019] DOI:10.1109/CAMAD.2019.8858469
- [3] Harshini V M, Shreevani Danai, Usha H R, Manjunath R Kounte "Health Record Management through Blockchain Technology" [2019] DOI:10.1109/ICOEI.2019.8862594
- [4] Xiaoguang liu, ziqingwang, chunhuajin, fagenli,(member, ieee), and gaoping li "A Blockchain-based Medical Data Sharing and Protection Scheme"[2019] DOI:10.1109/ACCESS.2019.2937685
- [5] Blockchain based Internet of medical things for uninterrupted, ubiquitous, user friendly, unflappable, unblemished, unlimited health care service s(BC IOMT U6 HCS) [2020] DOI:10.1109/ACCESS.2020.30