A SURVEY ON PRIVACY PRESERVING METHODS OF ELECTRONIC MEDICAL RECORD USING BLOCKCHAIN

Yogesh Sharma¹, B. Balamurugan²

¹,²School of Computer Science and Engineering, Galgotias University
Plot No. 2, Yamuna Expressway, Opposite, Buddha International Circuit,
Sector 17A, Greater Noida, Uttar Pradesh

¹yogeshsharma027@gmail.com, ²kadavulai@gmail.com

Corresponding Author: Yogesh Sharma
Email: yogeshsharma027@gmail.com

https://doi.org/10.26782/jmcms.2020.02.00004

Abstract

A blockchain technology is one of the types of decentralized technology and is based on distributed ledger technology. A blockchain technology is a tamper proof and secure technology which make the technology suitable for data store. However, there are some question from the critics with the issues related to technical challenges like the storage space of blockchain and some security issues but the technology has shown the benefit in multiple sectors. Electronic Health Records (EHR), Electronic Medical Record (EMR), Patient Health Record (PHR) are the patients record that are need to be monitored continuously after the patient get discharged from the hospital specially the patients with heart diseases or cancer. The electronic medical record proves to be a great help for the patient and for the concerned doctor as well. These medical records need more security and privacy against the leak or misuse by some other person. There have been some incidents where it has seen the security breach in the electronic medical records of a patient. In order to provide privacy to these records blockchain technology can be beneficial. In this paper, we will provide a comprehensive survey of different methods for preserving the privacy of EMR using the blockchain technology.

Keywords: Blockchain, Decentralized Technology, Electronic Medical Record, Patient, Security, Privacy

I. Introduction

A blockchain technology is a decentralized, temper evident and a temper resistant technology [V]. A blockchain technology is based upon the concept of distributed ledger technology where every node connected in the network maintains a copy of ledger. Blockchain technology came into light in year 2008 when satoshinakamo to gave the concept of cryptocurrencies and the idea was implemented in 2009 [XVIII], Since then blockchain technology has evolved many folds and
because of many advantages the technology is being used in many sectors. Many organizations are getting benefits of security and privacy with the implementation of blockchain technology. A blockchain technology ensure the integrity and redundancy of the data stored and ensure that once the data gets stored in the blockchain it cannot be changed or modified from its original content.

The healthcare industry is one such industry where the blockchain technology can be very useful. The healthcare industry produces enormous amount of data every minute and every day in form of patient’s laboratory test, X-rays, MRI, CT-scans, financial document, previous medications given, previous medical history and last appointments with the clinicians. All these information’s are private information of any person most importantly when the information is an electronic information, thus, need proper security and privacy in order to protect it from leakage and misuse by some unauthorized persons. The electronic medical records are the records of a person, which can be stored electronically on any device. The electronic medical records are important for the patient as it frees the person from carrying the multiple documents from one doctor to another and one hospital to another. The accessibility of the health records can be done in real time from anywhere and remains with the person everywhere. However, with the advancement of the electronic medical information some kind of risks and liability are also involved where the privacy and false information are at the greatest risk involved with EHR [XVI]. Thus, the blockchain technology has the power of preserving the medical records of a patient. Here in this paper we make the survey of papers that developed some methods or framework for preserving the privacy of the medical records using the blockchain technology. In the paper we will first discuss the preliminaries of the blockchain, in the next section we will discuss about electronic medical records and related work done for preserving the privacy of the electronic medical records. In next section we will see few challenges associated with the work done in electronic medical record. In the next section will we compare and contrast the methods used in privacy of the medical records. Then, we will conclude the survey in the last section.

II. Preliminaries of Blockchain

A peer to peer network is a distributed network, which stores and transfers the data without any involvement of the central server. A blockchain network is built up on the P2P network technology having no central point of storage making the information on the network less vulnerable to be hacked.

A distributed network can be thought of a network in which two or more nodes are working together on the same information in coordination with each other and produces the same output. The output thus produced by the distributed network will look to all the users a single logical platform. But the major challenge with a distributed system is in the coordination of the nodes they are working and the fault tolerance. In a distributed system any participating node can continue to perform with the same intensity and obtain the desired output even if any one of the nodes fails or if any link to the network fails.

Thus, on the basis of the concept of distributed system, came the concept of Distributed Ledger. These distributed ledgers are fast and decentralized and above all
are cryptographically secured. We can now define “A distributed ledger is a ledger in which all the transactions, information and records are recorded from different nodes from multiple locations and the data can be shared and synchronized across distributed network thus eliminating the need of a central authority. All the information and records are cryptographically secured and can be accessible only by the keys with cryptographic signatures. With the distributed ledger any changes made in the ledger or the document will get reflected across all the participating nodes in few minutes or seconds and the involved parties can check in their ledger about the changes made and use the updated record.

Since it becomes sometime inefficient to be constantly updating and synchronizing the data across many centralized databases, thus by putting the databases on a shared ledger it would become easier to access and view the updated database on demand when needed. A blockchain technology is one form of Distributed Ledger Technology (DLT) but it is not necessary that a distributed ledger system employs a chain of blocks in order to successfully provide a secure distributed ledger. Although each DLT is different from very other DLT in terms of data used by the DLT or the technology used, but all types of DLT are based on are based on three well-known technologies, public key cryptography, distributed peer-to-peer networks, and consensus mechanisms [XVII].

**Blockchain Technology**

Blockchain is a technology that came in early 2008 when satoshinakamoto came with the concept of bitcoin [XVIII] the cryptocurrency. The blockchain technology has grown since then and the technology is being used in various different sectors of industry as well.

A blockchain is a distributed, decentralized and a tamper proof technology based on Distributed Ledger Technology (DLT). These qualities have made the technology more useful in many of the organisations. A blockchain technology is like linked list type of data structure where in nodes are connected with a pointer. Similarly, a blockchain is a chain of blocks connected with each other current one referring to previous ones. In the blockchain all the transactions are stored in a block and each block is cryptographically secured by SHA-256. Each block thus creates a unique value known as Hash Value. For each block created, a unique hash value gets created for that transaction, the block gets added in to the chain with that hash value. For all the subsequent block created consists of newly generated hash value and the hash value of the previous block along with other transaction details. The first block created and added into the block chain is called as Genesis block and this block does not have any pervious hash value. Each node or a user can create a block of transaction and send it to the blockchain network. The users of the blockchain network must go for a consensus in order to add this block in the chain of blocks depending upon the consensus algorithm deployed on the chain. The blockchain network is an immutable network that means once any transaction or information is added on to a blockchain that information can never be changed or if any node tries to change the information, other nodes gets the information that there is a change in the transactions (since it will change all the hash values stored previously in the blockchain) and that block will get rejected from the chain of blocks. For this reason,
many organisation and industries are moving their existing network to the blockchain network, as the blockchain network provide better security, better privacy and above all transparency between the users.

However, blockchain technology is still in its growing phase and organisations should investigate how the industry-based problems can be fitted into blockchain technology before moving onto blockchain network.

**Structure of a Block**

The blocks are the containers which are connected with each other forming a chain like structure. This chain of blocks is termed as a blockchain. a block connected in the chain stores the data in it. The data stored could be inform of a text, a number, a program that can execute or most importantly it could be transaction in case of any cryptocurrency. Since the blockchain technology is a type of distributed ledger technology so all the blocks are distributed on all the machine connected in the network and would not be possible to manipulate the content of any block. The blocks are protected with the strong hashing algorithm known as Secure Hash Algorithm-256 or SHA-256 and each block produces a hash value of the transaction or data stored in the block. The hash value is generated automatically for each transaction done in the block. Thus, changing the content of the block would in turn changes the corresponding hash value of the block and since all the successive blocks uses the previous hash value, so the is miss-match is the previous hash value in all the blocks as shown in the figure block #2 the previous hash value is the one generated by the Block#1.

The structure of the block consists of fields like Block Number which shows the number of blocks in the chain, Time Stamp field tells about the time of creation of the block, the Transaction is the actual data, information or any transaction value created by the user and stored in the block. The Previous hash and the Current hash are the hash value created for the transaction made in the block. It is to mention that the current hash value of the newly created block will become,a previous hash value for the next block created and added into the chain
Blockchain Process

A blockchain process is based on the consensus mechanism for a transaction to be verified and valid. A blockchain network consists of various nodes connected in a distributed and decentralized fashion. Any node that need to perform a transaction has to write the transaction in a block. A block can be thought of a container like data structure that can consists of about 500 transactions on an average however the size of a block can be up to 1MB.[XIV] The node performs a transaction in a block and sent to other nodes which are connected in a distributed network. Since the blockchain network is decentralized the block of transaction created by the node, hence the block is being broadcasted to all the nodes present in the network. The blockchain network is a consensus-based network meaning all the nodes present has to agree on transaction made based on consensus algorithm. Consensus Algorithm is a process by which multiple nodes present in a distributed network agreed upon a decision [XXV]. The consensus algorithm provide reliability to a distributed network. There are many consensus algorithms, few of them are Proof of work, Proof of stake, Byzantine Fault Tolerance. Thus, a block created is added to the chain of the blocks already present in the blockchain once it is verified and validated by all the nodes present in the network as shown in the figure. The newly added block will always refer the previous block in the chain which will make the chain more secure. Once the block is added on to the chain of blocks the receiver node can now update the ledger with the new information.

Types of Blockchain

A network designed using blockchain technology can be classified into three types of blockchain a public blockchain, private blockchain and a consortium type of blockchain. The design of the blockchain network depends upon the processing of the transactions and the accessibility of the data by the users of the network. These types of blockchain network be of great use when an organisation thought of shifting existing database on to a newly created blockchain network or thought of creating a completely new network based on the blockchain technology. the three types of
blockchain plays an important role in progress of any organisation depending up on the functionality of the organisation.

1. Public Blockchain

A public blockchain is a type of blockchain which is open to all. Any user can connect to public blockchain and no permission is required to join the network. A public blockchain is an open blockchain for any user who wish to join the network. With a public blockchain any user who joins the network has the access to read the transactions made on to the blockchain, any use connected with the public blockchain has the permission to make any legitimate changes on to the blockchain or if wanted to add any new transaction or a block into the existing chain of blocks. The biggest advantage of the public blockchain come with the fact that a public blockchain can accommodate any anonymous user in the network. A public blockchain can be very useful in generating cryptocurrencies. Bit Coin and Ethereum network is the best example for a public blockchain. The disadvantages of the public blockchain are the transaction fees incurred for joining the blockchain network and scalability issues of the network.

![Public Blockchain Network](image)

2. Private Blockchain

Unlike a public blockchain, in a private blockchain, any user wishes to join the network need to take permission to get added into the network. A private blockchain can be built by any organisation, who wish to add only trusted users in the network and no unauthorized user is allowed to join the network. In a private blockchain some limited users are connected in the network and only authorized users have the access of the network. Unlike a public blockchain, the person who creates the private blockchain network will be the administrator or the validator of the network who has the authority to add the trusted users only in the network. The administrator or the validator has the access to the transactions of the network and can even put rules in the network. Hyperledger, Ripple are the example of a private blockchain.
3. Consortium Blockchain

A consortium blockchain is a mix of both the public and private blockchain. A consortium blockchain allows the users to join the network without any permission like in a public blockchain but when the users joins the network, the ownership of the network does not goes into the hand of a single owner or a company like in the private blockchain rather the few users out of the all the users can be assigned the job of administrators or validators who can validate the transactions performed by the users of the network and also holds the authoritative rules of the network.

Cryptography in Blockchain

Under Distributed Ledger Technology, blockchain technology is considered to be one of the most exciting technology and also considered to be most secure technology [XXVI] in recent decade. Cryptography techniques make the blockchain technology more secure and provide privacy to the information placed in the blockchain. There are primarily two objectives of cryptography: first is security, which prevents the unauthorized access to the data and second is the authenticity and integrity which protect the data from modification. The biggest concern with any network is the three basic things: Confidentiality, Integrity, Authentication and Non-Repudiation[XII]. A blockchain network need all these four things to be included in order to provide privacy and security to the records/information/transaction stored in the blockchain. There could be many ways to provide the security and privacy to the information using cryptography. We have the private and public keys, hashing techniques, digital signature etc. which could be beneficial for the blockchain network.

Security

The data security has always been the top priority of any technology and efforts are still made in order to make a secure network so that nodes could communicate with each other in a secure manner. Blockchain technology uses the encryption and hashing techniques so that the stored data will remain immutable.
Although the blockchain technology has better security as compared with other existing technologies because of the fact that the blockchain is a decentralized technology and does not require a single authority to control the network, while maintaining the trust between the nodes of the network. With the blockchain technology in use there have been some improvement in storing and sharing of the information securely among other nodes using the encryption techniques which gives the user the complete authority to control the information[XXIII]. The security of the data would be necessary specially when the data is either a transaction or an electronic medical data. The electronic medical record of any patient is a critical and personal information, a security breach of this information could lead to disclosure of patient’s information to any unauthorized person, therefore this information needs to be secure from manipulations, unauthorized access. The techniques that can be used for securing the data in a network could be a digital signature or hashing technique. The digital signature however secures the document which is digitally signed in a public domain and remains in a documented format. Whereas, the hashing techniques will create a secret value of the data called hash value, for any given data making it immutable thus protecting the data from modification while maintaining the authenticity and integrity of the information.

**Hashing**

A large document when passes through a hash function it produces a fix length output that too in a hexadecimal format. This fixed length output is the hash value generated for the document. A hash function is a mathematical function maps the data into smaller message digest. A hash value thus created by the hash function could use to provide security to the information. The hash value of any input value will always be a different value and can never be a same value. Any changes made in the input value will change the corresponding hash value. the user can then detect that there is some change made to the original input value.

With the emergence of cryptography, the cryptographic hash function has gained popularity in the field of security and privacy. The hashing techniques are proving to be securer than other technologies.

[XXVIII] has given the definition of hash function as:

A function HF() that produces a fixed length message digest MD from any arbitrary length message M is considered as One-Way Hash Function, if it satisfies the following conditions:

1. The Function HF() should be publicly known and there should be no secret information associated with the operation of this function.
2. For the given message M, it should be easy to calculate HF(M).
3. With the given Message Digest MD it would be difficult to find the message M such that HF(M)= MD, with given HF() and M, it would be difficult to extract a message M’ ≠ M such that HF(M’) = HF(M).

There are number of hash functions methods created for securing the information namely SHA0(1993), SHA1(1995), SHA2(2001), SHA3(2014) and latest is...
SHA256 encrypts the data with a unique quality of hash function and creates a fixed length output differently for different input value. SHA256 is the most recent and popular method that is being used in blockchain technology, supported by the Microsoft Enhanced RSA and AES Cryptographic Provider (One-way Hash Function, n.d.). Almost all the blockchain network uses SHA-256 cryptographic algorithm with output size of 256 bits produces an output of 32 bytes represented by 64 characters of hexadecimal string, which means that SHA256 has $2^{256} \approx 10^{77}$ possible digest values. Out of all the SHA algorithms, SHA-256 is said to be collision resistant, as in order to find a collision in SHA-256, on an average the algorithm has to be executed, about $2^{128}$ times which becomes very difficult for the hacker to crack. Thus, SHA256 is used in blockchain technology which makes the technology more secure with increased privacy compared with any other technology.

For example, we have used an online hash value calculator using a website https://www.fileformat.info. We have given an input text value to the function and the function returned a corresponding hash value:

**Original Text:** Hello, how are you, I have high cholesterol value.

**SHA256 Value:** 1fa6e4f59486f72e3e504cfca9981416297213541967c2c4682791e161106be0

**Modified Text:** Hello, how are you, I have low cholesterol value.

**SHA256 Value:** 26bccd725246b89cbdd74cca64014ed399ccf0c24011068ab89a9eabf4dcef5b

Here we have seen modifying small text in the document could modify the complete hash value of the document. This shows how important is the hash algorithm in data security and privacy.

**Privacy**

In this era of big data, data is the new currency. Any e-commerce or a social media are generating huge amount of data every second. The users of these websites are giving their full information without knowing that there could be information leak any time. According to a report published in Forbes on an average around 1.5 billion of people are active on Facebook in a day, every second 5 new users create their profile on Facebook and around 300 million of users post their photographs in a single day. There are other digital and electronic records such as medical records, transactions, supply chain information, data generated by IOT devices, which are getting stored on cloud and in a database of an organisation. The privacy of this private information must be kept preserve so as to protect it from leak and thereby protecting them from misuse. The user should have the authority to own and control its private information so the security and privacy should not be compromised. [VIII] has developed a platform where in the data is stored on an offline blockchain. The user has the information of data collection about the user and how this data would be used in an offline blockchain. In the proposed platform, the blockchain can...

---

*Copyright reserved © J. Mech. Cont. & Math. Sci.*

*Yogesh Sharma et al*
spot the authenticated user of the data there by providing the security and privacy to
the personal data of the user.

Blockchain provides a way to safeguard and support healthcare. Privacy being the
most desired factor when using the electronic medical records of a patient. Electronic
medical records are the private information for any person so the security and privacy
of these records is a major concern. There are some primary problems that arises when
a patient visits multiple healthcare organization be it a hospital or a doctor’s clinic.
The patient has to keep track of all his documents and medical reports whenever
visiting a doctor. The situation gives pain to the patients when he is not able to track
the medical history or the required documents. There are some situations when the
patients have to repeat some of the test due to unavailability of the test done earlier.
The healthcare data is considered to be most sensitive data to any person and the
process of managing this sensitive data is even more cumbersome. Still, there are no
systems available for the preserving the privacy of the electronic medical records.
The biggest restriction with managing the electronic medical records is that the
nodes identities could be known to the other nodes in the network so that the
malicious behaviour could be detected, which would not be possible in a
Permissionless network. [III] has proposed a framework for secure and trustable
electronic medical record sharing. The system developed on a permissioned network
so that the patient and doctor could be in a same secure network. The framework uses
a membership service for registering the different users of the network. The patient
could generate a symmetric key (SKAES P) for encryption and decryption of the data
from. For sharing the data to the doctor, the patient could share the symmetric key
using the encryption public key of the corresponding clinician (PKED). thus, making
the data sharing trustable and secure.

**Electronic Medical Record**

Electronic medical record (EMR) is a crucial form of healthcare data, currently drawing a lot of attention. Sharing health data is considered to be a critical approach to improve the quality of healthcare service and reduce medical costs. EMRs are often highly sensitive private information for clinical diagnosis and treatment in healthcare. EMRs sharing are considered to be a promising approach to improve the quality of healthcare services, accelerate biomedical discoveries, and reduce medical costs [X]. Private Health Information, Electronic Medical Records and Electronic Health Records have emerged as assets with the potential to affect the quality of life of individuals all over the world. World Health Organization reports have already identified personal health information as assets where sharing goes far beyond their primary medical use [XXIX]. Sharing of healthcare data will help us to become smarter, for instance, better understanding of patterns and trends in public health and disease to ensure better quality care [XX]; better recommendations for exercising or doctors [XXXV] plan services that make the best of limited national health service budgets for the health and wellbeing of everyone, and so on [XXXI]. Medical data is scattered throughout various medical institutions, and the data standards of different medical institutions are not uniform, resulting in a low level of interoperability of medical information systems among agencies. Under the current
medical data management system oriented by medical institutions, there is no guarantee of the integrity and reliability of patient data. The risks of medical data loss or hacking are inevitable, and these data are always facing data security, personal privacy leaks and other issues. Most medical data are stored in medical institutions in a centralized manner, which is vulnerable to different threats, such as malicious tampering, hacking and natural disasters, which can lead to the leakage and loss of medical data.

To handle health data sharing between institutions, there is a need for a secure data sharing infrastructure. However, there are several challenges related to privacy, security, and interoperability. First, health data are highly privacy-sensitive, especially as more data are storing in a public cloud, raising the risks of data exposure. Second, current systems use centralized architecture, which requires centralized trust. Moreover, the effective integration of health data and the interoperability between healthcare systems remain a challenging task. Another challenge is that users have little control over their personal health data [XXXIII]. Challenges associated with data processing, privacy and security continue to rise concurrently, since the healthcare industry highly relies on the data. Health data privacy implies securely and privately processing of the patient data or the need for authorisation to access the data. Besides, security refers to safeguarding sensitive data from intruders and even listeners [I]. By giving the required tool to establish consensus among spread entities without depending on a single reliable party, the Blockchain technique will ensure the data security, the control over sensitive data, and will facilitate healthcare data supervision for the patient as well as different actors in medical area[II]. Blockchain can be used to facilitate secure data management or to enhance the security level in a particular application and enhance the security of trading data in their decentralized smart grid energy trading approach. More specifically, these approaches use a series of Blockchain-oriented techniques to achieve privacy protection in multi-signature, anonymous messaging encryption, anonymous negotiable energy trading, and other applications. Blockchain is used to enable content delivery management [XIV].

III. Related Work

Existing research in the blockchain for the healthcare field mainly includes medical information protection, medical data storage and sharing, medical data application, forecast analysis and illustrated possible influences, goals and potentials connected to blockchain technologies in healthcare. In [XXXI]a Healthcare Data Gateway based on the blockchain was devised. The architecture not only enabled the patient to own, control and share their own data easily and securely but also enabled untrusted third parties to process medical and health data while ensuring patient privacy through introducing secure multifactor computing. In[IV], the Enigma encryption platform was devised to work with blockchain technology to create a secure environment for storing and analysing medical data. Some methods and systems based on the blockchain are proposed for storing and managing patient medical records. In[XXV], a blockchain-based data sharing framework was devised which poses the capability to address the access control challenges associated with sensitive data stored in the cloud using immutability and built-in autonomy properties.

Copyright reserved © J. Mech. Cont.& Math. Sci.
Yogesh Sharma et al
of the blockchain. In [XI], a blockchain-based approach was devised to sharing patient data and used blockchain network technology to create an interinstitutional medical health prediction model. A privacy preserving medical data platform based on blockchain in [I] in which the data is encrypted and stored in a federation blockchain, and a data user needs to get the decryption key from a data owner. In [XXXI], health care data gateway architecture was devised for privacy preservation in which the data is encrypted and stored in a private blockchain cloud. A patient download encrypted data, decrypts it and decides whether to share the data. When the data is shared, it is encrypted again, and the ciphertext and decryption key are sent to the receiver.

### Literature Review

| Authors          | Methods                                      | Advantages                                                                 | Disadvantages                                                                 |
|------------------|----------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------|
| Yue, X et al. [XXXI] | Healthcare Data Gateway (HGD) architecture   | Enable patient to own, control and share their own data easily and securely without violating privacy. | Privacy-aware data access policies cannot be easily achieved by traditional access control models and needs complex computations. |
| Chen, Y et al. [XXXIV] | Storage scheme and service framework based on the Blockchain | Make it a potential solution for healthcare data systems that concerns both sharing and patient privacy. | Did not consider a medical Blockchain network to connect several medical and health institutions. |
| Al Omar et al.[I] | Patient centric healthcare data management system | Encrypt patient’s data to ensure pseudonymity and helps to attain privacy with less cost. | Unable to handle key-theft/loss mechanisms or key distribution techniques. |
| Hussein, A.F et al. [II] | Blockchain-based data sharing system | System is robust, efficient, immune and scalable offers dependable data privacy. | Processing time may increase. |
| Daghera, G.G et al. [VII] | Blockchain-based framework named Ancile | Cost and storage effective. | Did not meet legislative standards for medical data and protection of patient privacy. |
| Zhang, A. and Lin, X [XXXVI] | Blockchain-based secure and privacy-preserving PHI sharing (BSPP) scheme | Time cost increases slowly with the growth of the package length. | Can meet the security goals. |
| Tian, H etal. [XXX] | Sibling Intractable Function Families (SIFF) | Guarantee the privacy, availability and integrity of medical data. | Communication cost increases linearly. |
| Zhu, L et al. [XXXVII] | Controllable Blockchain data management (CBDM) model | Allows one to terminate any malicious actions under any type of attack. | Unable to process on real-world environment. |

### IV. Challenges with the Work done

A big challenge for healthcare data systems is how to gather, store and analyse personal healthcare data without raising privacy violations. For such systems, privacy concerns have proved barriers to adopt and the lack of adequate security
measures has resulted in numerous data breaches, leaving patients exposed to economic threats, mental anguish and possible social stigma [XXXI].

Most medical data are stored in medical institutions in a centralized manner, which is vulnerable to different threats, such as malicious tampering, hacking and natural disasters, which can lead to the leakage and loss of medical data [XXXIV].

In[II], Blockchain-based data sharing system is proposed for privacy protection and the secure storage of medical data using immutability and autonomy properties of the Blockchain, but the methods associated with Blockchain initiates several challenges like immutability of Blockchain, and access control leaks.

Centralized medical data management system is difficult to ensure the integrity of medical data. In such a system, medical data are often stored in a database of a medical centre in which the attacker can delete or modify the data after obtaining the corresponding permissions of the database [IX].

In [XIV], a Controllable Blockchain Data Management (CBDM) model was devised for providing privacy preservation in medical data using Blockchain. The Blockchain is considered a secure platform, since all actions made by system participants are recorded on the chain, but the expanding chain makes it computationally challenging to change any block without detection.

V. Conclusion

The blockchain technology has emerged from cryptocurrency to various other fields. The major focus of using the technology in various sectors is the security and the privacy provided by the technology. Different types of blockchain networks could be used based on the use of technology. It is the strong cryptography that is used in the blockchain technology which made the technology more secure and privacy preserving technology as compared to other secure networks. Healthcare is one of those sectors which is moving on to blockchain technology in order to provide security and privacy to the patients record. The amount of data generations today in the healthcare sector is humongous, although we have the technology to store this huge amount of data but the security and privacy need for such data is not appropriate specially when we talk about the Electronic Medical Record(EMR) for any patient. These kinds of records are private to any patient and any patient does not want his private record to get leaked or get misuse by any other person. Thus, blockchain network could be very useful. Researches have been conducted regarding the privacy of the records. The survey conducted on preserving the privacy of the Electronic Medical Record using Blockchain Technology has shown that many researches has been done till now, some of the researchers has provided strong methods to protect and preserve the medical record of a patient but there are still few challenges associated with some methods. In future we will plan and work on stronger method to preserve the privacy of the medical records using blockchain technology of the patient.
VI. Acknowledgment

It gives me immense pleasure to express my deepest sense of gratitude and sincere thanks to my expected guide Prof. B. Balamurugan, Professor SCSE, Galgotias University, Greater Noida, for his valuable guidance, encouragement and help for completing this work. His useful suggestions for this whole work and co-operative behaviour are sincerely acknowledged.

I am also grateful to Prof. Raju Shanmugam, Dean SCSE, Galgotias University, Greater Noida, for his constant support and guidance.

I also wish to express my indebtedness to my parents as well as my family members whose blessings and support always helped me to face the challenges.

References

I. Abdullah Al Omar, M. S. (2017.). MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, (pp. pp. 534-543).

II. Ahmed Faeq Hussein, A. N.-G. (2018). A Medical Records Managing and Securing Blockchain Based System Supported by a Genetic Algorithm and Discrete Wavelet Transform. Cognitive Systems Research, (pp. 1-11).

III. Alevtina Dubovitskaya, Z. X. (2017). Secure and Trustable Electronic Medical Records Sharing using Blockchain. Annual Symposium proceedings. AMIA.

IV. Allison Ackerman Shrier, A. C.-t. (2017, August 19). "Blockchain and Health IT: Algorithms, Privacy, and Data,". Retrieved from http://www.truevaluemetrics.org: http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf,

V. Dylan Yaga, P. M. (2018). Blockchain Technology Overview. NISTIR 8202.

VI. Dylan Yaga, P. M. (2018, October). Blockchain Technology Overview. Retrieved from https://csrc.nist.gov: https://csrc.nist.gov/publications/detail/nistir/8202/final

VII. Gaby G. Daghera, J. M. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society, 283-297.

VIII. Guy Zyskind, O. N. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE CS Security and Privacy Workshops (pp. 180-184). IEEE.
IX. Haibo Tian, J. Y. (2019). Medical Data Management on Blockchain with Privacy. Journal of Medical Systems, 26.

X. Jingwei Liu, X. L. (2018). BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records. Global Communications,, (pp. pp. 1-6).

XI. Kevin Peterson, R. D. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.

XII. Kessler, G. C. (2019). An Overview of Cryptography.

XIII. Licheng Wang, X. S. (2019). Cryptographic primitives in blockchains. Journal of Network and Computer Applications, Pages 43-58.

XIV. Liehuang Zhu, Y. W.-K. (2018). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 527-535.

XV. Madeira, A. (2016, November 29). What is the Block Size Limit. Retrieved from https://www.cryptocompare.com/coins/guides/what-is-the-block-size-limit/

XVI. Marr, B. (2018, May 21). How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Retrieved from forbes.com: https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5fa0d7e60ba9

XVII. Minal Thakkar, D. C. (2006). Risks, Barriers, and Benefits of EHR Systems: A Comparative Study Based on Size of Hospital. Perspectives in Health Information Management.

XVIII. Nabil El Ioini, C. P. (2018). A Review of Distributed Ledger Technologies. OTM 2018 Conferences - Cloud and Trusted Computing (C&TC 2018).

XIX. Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from www.bitcoin.org.

XX. Neesha Jothia, N. A. (2015). Data Mining in Healthcare – A Review. Procedia Computer Science. Penang Malaysia.

XXI. One-way Hash Function. (n.d.). Retrieved from http://www.aspencrypt.com: http://www.aspencrypt.com/crypto101_hash.html

XXII. P. Gareth, P. E. (November, 2015). “Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money.” SSRN Electronic Journal.

XXIII. Paul J. Taylor, T. D.-K. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks.
XXIV. Popov, S. (2018, July 19). The Tangle. Retrieved from https://iota.org: https://iota.org/IOTA Whitepaper.pdf

XXV. Qi Xia, E. B. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information.

XXVI. Rouse, M. (2017, August). consensus algorithm. Retrieved from whatis.techtarget.com: https://whatis.techtarget.com/definition/consensus-algorithm

XXVII. RUI ZHANG, R. X. (2019). Security and Privacy on Blockchain. ACM Computing Surveys, Vol.1, 1-35.

XXVIII. S. Bakhtiari, R. S.-N. (2005). Cryptographic Hash Function: A Survey.

XXIX. Sandro Amofa, E. B.-B. (2018). A Blockchain-based Architecture Framework for Secure Sharing of Personal Health Data. International Conference on e-Health Networking, Applications and Services.

XXX. Tian, H., He, J. and Ding, Y., "Medical Data Management on Blockchain with Privacy," Journal of medical systems, vol.43, no.2, pp.26, 2019.

XXXI. Xiao Yue, H. W. (2016). Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. Journal of medical systems, 218.

XXXII. Xiaodong Lin, A. (2018). Towards Secure and Privacy-Preserving Data Sharing in Health System via Consortium Blockchain. Journal of medical Systems, 140.

XXXIII. Xueping Liang, J. Z. (2017). Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications. Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (pp. 1-5). IEEE.

XXXIV. Yi Chen, S. D. (2018). Blockchain-Based Medical Records Secure Storage and Medical Service Framework. Journal of Medical Systems, 5.

XXXV. Yin Zhang, M. C. (2015). iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization. Future Generation Computer Systems.

XXXVI. Zhang, A. and Lin, X., "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of medical systems, vol.42, no.8, pp.140, 2018.

XXXVII. Zhu, L., Wu, Y., Gai, K. and Choo, K.K.R., "Controllable and trustworthy blockchain-based cloud data management," Future Generation Computer Systems, vol.91, pp.527-535, 2019.