IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure electronic healthcare (EHC) system using blockchain Technique

Ms. Nilima V. Pardakhe
Research Scholar
CSE Dept
P.R.M.I.T.&R.,Badnera
pardakhenilima@gmail.com

Dr. V. M. Deshmukh
Associate Professor
CSE Dept
P.R.M.I.T.&R.,Badnera

Abstract-

Information systems and computerization nowadays need very faster, secure & easier data analysis techniques. The modern healthcare systems are extremely complex, expensive and face problems concerning data privacy, security and integrity. However, better monitoring and management of electronic health records will reduce these issues regarding complexity and security. Blockchain with its decentralized and trustworthy nature has established massive potentials in healthcare sector. Primary problems in healthcare delivery include lack of data management, and how data can be made verifiable, immutable, and distributed. One of the key benefits of using blockchain technology in the healthcare database is because of its potential to update medical interoperability systems which provides better access to patient records, medication tracking, drug systems and hospital assets etc. Access to patient's medical histories is essential to correctly prescribe medication, with blockchain being able to dramatically enhance the healthcare services framework. In this work, various solutions to improve current healthcare system vulnerabilities using blockchain technology including frameworks and methods are addressed. The main aim of the proposed research work is to design blockchain based framework for preserving & securing electronic medical healthcare data efficiently in comparison with conventional EHR systems. In addition, framework store medical prescription, laboratory report and emergency data which could encompass data regarding medical history of the patients, the medicine details in database for future use providing EHR system which includes scalable, secure and integral blockchain-based solution.

Keywords-- Blockchain, Healthcare System, EHR, Security

I. INTRODUCTION

In this era of computerization of business, organizations focus is mainly on future predication by considering the historical data. The ever growing growth of the Internet of Things (IoT), cloud and edge computing and big data demands rapidly new solutions for distributed and decentralized systems management. Performance metrics like lag, system performance and round- trip time (RTT) were also optimized for blockchain networks to achieve enhanced results with safe data access. The suggested framework uses blockchain to increase efficiency and security of data sharing in comparison with conventional EHR systems using client-server architecture.

The steady growth of Internet of Things (IoT), Cloud and Edge Computing, and Big Data is rapidly requiring novel solutions for managing distributed and decentralized systems. Nevertheless, most private clinics and hospitals typically use their internal network to monitor their patients but do not share data with other medical institutions, which results in a medical service challenge and costly, and the Knowledge Island phenomenon. A stable data storage Network needs to be built to deal with these problems of the current healthcare system.

A. Security in healthcare

Health data needs a large amount of degree of protection and confidentiality. Privacy applies to individuals who have the freedom to authorize or transmit personal data to other people. This involves the cooperation between healthcare professionals and regulatory bodies and the establishment of rules and procedures that have been approved. Nevertheless, most private clinics and hospitals typically use their internal network to monitor their patients but do not share data with other medical institutions, which results in a medical service challenge and costly, and the Knowledge Island phenomenon. A stable data storage Network needs to be built to deal with these problems of the current healthcare system.

Health data needs a large amount of degree of protection and confidentiality. Privacy applies to individuals who have the freedom to authorize or transmit personal data to other people this involves the cooperation between healthcare professionals and regulatory bodies and the establishment of rules and procedures that have been approved. As a result, security guidelines and legislation to protect their health care records were drawn up for the United States and other nations.

B. Why security is important in healthcare?

Healthcare providers have become increasingly reliant on smart technologies since the dawn of Healthcare 4.0. Such tools help monitor and identify patient conditions, allowing patient information to be shared, accessed and processed for the management of medical records. The quality of data collected in HR systems serves a key role in the success of a health care provider [6]. Therefore data should always be secure and endangered. In the absence of these conditions, the systems used are not capable of functioning correctly or are considered false. The size and complexity of health records are that and are not yet standardized with the advent of broad data. Records are also duplicated, malaligned by different ID / Naming conventions and made available on various networks and directories for health care systems. You may include addresses, phone numbers, full names, and so on. Privacy of patient data is critical for successful healthcare management [7]. In light of these issues, numerous states have started or established regulated medical system standards to prevent cyber threats which improve the privacy and security of patient data and increase trust in patient-provider relationships.

Many health systems today utilize centralized customer-serve structures with full access to the system by a central authority. In this case, privacy or security vulnerabilities can lead to system failure, which can lead to cyber intruders having possible access to patient data. Fortunately, an emerging blockchain technology offers a brand-new approach to solve decentralized architecture security issues.

C. Blockchain technology

Work on blockchain and smart ledgers has become more popular in recent years as a consequence of the growth of cryptocurrencies like Bitcoin and Ethereum. Blockchain collects and shares information in such a decentralized, stable, and unchangeable way that eliminates intermediaries without needing a core test dependence [8,9]. Blockchain Transparency provides a less complex network access approach. It connects to a number of computer capabilities in the blockchain network from a number of nodes and allows the calculation speed extremely efficient [10].

Blockchain consists of many technologies and utilities, including Consensus, Hash, Immutable Ledger, Distributed P2P Networking, and Mining which have recently been implemented in large details: Blockchain:

• Consensus Protocol: All customers have personal access rights to system-updated transactions, defined as a Consensus Protocol in a

blockchain network. A block chain uses SHA256 hash to incorporate transactions.

• Hash encryption. The NSA has 64 characters and is created. Hash algorithms contain characteristics like one-way encryption, deterministic faster estimation, avalanche effect and collisions.

• Immutable ledger: Every transaction is recorded in a blockchain network, whereas the shared ledger cannot be changed/altered.

• P2P network distributed: - All transactions are transmitted through the network and are distributed and modified to various users.

• Mining: - miners use nonce blocks for network hash values. To achieve and obtain the award, this requires high calibration speed. A blockchain network may be duplicated at a different venue, e.g. within the same facility or health network or as part of a regional or international knowledge exchange mechanism.

D. Research contributions

This paper 's principal contributions are defined as follows. Firstly, we suggest network architecture for a patient-centered approach using distributed ledger technology with key cryptography to provide an access control policy for the particular healthcare provider. We propose a cryptographic solution based on blockchain for implementing a permission-based EHR sharing framework using the blockchain principle. The proposed program is then evaluated theoretically to determine whether it serves the needs of patients, health care professionals and other stakeholders. Finally, we agree on the best approach for the metrics on performance optimization of the blockchain-based cryptographic framework using parameters of latency and throughput, network scalability, and security.

Remaining section of this paper discuss as follows, section II gives the details review of exiting system with their advantages & disadvantages, In section III explain the motivation of using this system, section IV discuss current research gap in traditional system use by person ,after the motivation we are going the discuss the proposed model with working of system in details in section IV, and in last section V going to conclude the all expectation with expected outcome of proposed work followed by references.

II. LITERATURE REVIEW

This section summarizes existing methods employed by authors and research gaps developed for Healthcare system, Machine Learning, Blockchain & Security and How to Store & utilize various inputs data. For the pilot literature survey, we gathered different research papers from ACM, Elsevier, Springer, IEEE and IJAT databases for period 2017 to 2019. Out of those literature papers, some papers identified as relevant references for proposed study. Finally, to identify key research gaps. Also, latest papers are shortlisted for existing algorithm reference.

Anurag Agrahari et al.2017[1] developed, using Big Data to identify human behavior with a wearable sensor system, the Hidden Markov Model (HMM) which uses Big Data to track elderly people's health. In fact, the program was suggested that can accommodate vast volumes of data without any public health system issues.

The use of the cloud computing framework for big data analytics was suggested by Rupali Jagadale et al. 2018[2]. Authors built a link between cloud computing and big data and compared a variety of large data cloud systems with regard to storage , data mining machine learning techniques and cloud resources. Speak about the Hadoop idea as well. It is used for compiling high amount of information, it is very cost-effective and it can handle large quantity of data in order to process it efficiently, and in case of a system malfunction it can also produce a duplicate copy of data and prevent data loss.

Big data generation from various applications and decision-making support systems to easily access

extracted data from everywhere are the result of the emerging technologies for the handling of cloud computing.

Sabyasachi Dash et al. 2019[3] author proposes an architecture focused on the healthcare sector, which includes hospital records, patient medical records, medical test results and website-based tools. Biomedical research provides a large part of the public health big data as well. These data require careful management and analysis for useful information to be obtained. If not, it is easy to find a solution by analyzing large amounts to locate a diamond in the rough. Only using high-end computer solutions for big data analysis will the through stage in the big data cycle be overtaken. That is why healthcare providers must be fully equipped with the infrastructure needed to generate, evaluate Big Data routinely and offer effective public health changes solutions. The efficient control, analysis and understanding of large data may improve the dynamic by opening new avenues for modern medical care. This is precisely why major companies, such as the healthcare industry, take stringent measures to turn this capacity into better facilities and financial advantages. Modern health institutions, with a clear integration of scientific and clinical data, will revolutionize medical care and personalized medicine. Discuss early disease alerts and novel biomarkers and insightful prevention approaches for improving the quality of life.

An comprehensive research on broad healthcare data has been made by Karim Abouelmehdi et al. 2018[4]. To discuss potential for patient outcomes improvement, the prediction of outbreaks, usefull insights, preventable diseases, cost reduction and improvement in overall quality of life. Modern health institutions, with a clear integration of scientific and clinical data, will vastly improve medical care and personalized medicine. Discuss early disease alerts and novel biomarkers and insightful prevention approaches for improving the quality of life.

Blockchain was identified as a form of database that is used to store data in a distributed system by the Pinyaphat Tasatanattakool et al. 2018 [07]. The distinctions between Blockchain and Bitcoin were also explained and potential work on Blockchain Technology for electronic medical records has been based. We should discuss whether an unauthorized party (unauthorized stake holder) can access or request a patient's health records from the hospital or health authority without contravening patient privacy.

The authors of Zibin Zheng et al. 2017 [08] argue that blockchain networks are classified into 3 kinds: public blockchain, private blockchain and blockchain consortium. All documents can be seen in public in blockchain, and everybody can engage in the process of consensus. Otherwise, a consensus mechanism for a blockchain consortium will only include a group of pre-selected nodes. Only those nodes from a specific organization may join the consensus process as far as private blockchain is concerned. A private blockchain is considered a centralized network as it is operated solely by one entity. The blockchain consortium developed by various organizations is partly decentralized, as only a limited number of nodes are chosen for the consensus.

Already blockchain-based applications are evolving and, in the future, they plan to do comprehensive work in blockchain- based applications.

No.	Techniques	Application	Advantages	Disadvantages
1	Group signature	JUZIX	It can prevent linkage of user addresses.	The centralized services may have privacy leakage risk of the users.
2	Ring signature	CryptoNote , Monero Ethereum	Within a group of users, the signer identity can be concealed. In the event of a dispute, the signatory 's identity can be disclosed	A trustworthy third - party to serve as managers are needed
3	ABE	None	Signer identity can be concealed within a group of users. No need to get some trusted third party involved	In the case of a dispute, the signer 's identity cannot be revealed.
4	HE	Ethereum	At the same time, it can obtain data confidentiality and fine-grained access control	The issuance and revocation of attribute certificates must also be resolved in a distributed environment.
5	SMPC	Enigma	It can achieve computation that protects privacy by running computations directly on ciphertext	Only certain types of operations, like the addition and multiplication, can be performed efficiently. Computational efficiency is very weak for complex Functions
6	NIZK	Zcash	It enables multiple parties to perform any computation simultaneously over their private data inputs without violating the privacy of their inputs	Only some basic functions can be supported, and less efficient are the complex functions.
7	TEE-based solutions	Ekiden, Enigma	With NIZK a user can easily prove that he has ample balance for the transfer, without the account balance being disclosed	Efficiency is less
8	GameBased solutions	TrueBit , Arbitrum	The privacy of smart contracts can be protected by running these in TEE	The computing nodes need to be fitted with a CPU that has TEE, like Intel SGX. SGX attacks still need to be resolved

Table: 01 Summaries of Security and Privacy Techniques

P.K. Kavitha et al . 2017 [16] Address various methods of encryption and decryption of images in this Paper. Today, image security is extremely important. Various encryption methods are researched and analyzed to support the encryption recital. The original picture is incorporated and encrypted in all processes and then sent to the recipient. Every algorithm is special, the method is uniquely implemented. The new technique of encryption is changing every day. High-security encryption methods are still working out.

Javaria Tahir et al. 2017[17] The data is the most precious commodity, they claim. Internet markets are increasingly exchanging data. These markets allow data owners to publish their information sets and data users to find suitable services. Data are a special

commodity, however, rather than conventional items such as clothes and food. It is very difficult to protect copyright and privacy for emerging data exchange markets. Moreover, the management of data resources requires specific IT techniques, something that is difficult for many organizations, including hospitals, government agencies, planetariums and banks, that have big datasets. A decentralized way to share big data is proposed in this paper. This approach aims to build an environment where all participants will participate in the peer-to-peer sharing of data. The main part is to use blockchain technology to archive transaction records and other important documents. Our solution does not need third parties, unlike current data exchange markets. It also provides data owners with a simple way to verify the use of data and protect the rights and privacy of data. They will discuss the environment and the technological problems and solutions.

Eranga Bandara et al . [18] With Mystiko, a high transaction capacity, high scalability and high availability blockchain has been developed. The distributed storage is used as the background storage framework by Apache Cassandra. We introduced full text search functionality to Mystiko by indexing transactions and blocks in Elasticsearch. Our micro-service architecture from Docker and Kubernetes makes scaling simpler and more scalable. Mystiko is a storage system with these features that supports data. It has been demonstrated with empirical tests in terms of scalability and transaction throughput. Mystiko has been integrated in the banking and financial fields of development graduation applications. The implementations are Mystiko as an ideal Big Data and Cloud Storage blockchain network.

Massoud Sokouti et al. 2016 [19]- The Goldreich Halevi Goldwasser (GGH) algorithm is used in the numerical frames for the encryption of medical images. Thus both algorithms and confidential information may be used.In addition, the GGH algorithm does not increase the image size and thus its complexity remains as straightforward as O(n2). However, the Chosen Chipher Text attack is one of the drawbacks of using the GGH algorithm. This deficiency in the GGH algorithm was resolved and improved in our strategy by using padding (i.e., snail tour XORing) before the GGH encoding process. Three measurement parameters are considered for measuring their efficiency, including I the number of pixels changing rate (NPCR), (ii) Unified average intensity change (UACI) and (iii) the effect of Avalanche. The tests on three different imagery sizes showed that the GGH padding strategy, as opposed to the regular GGH algorithm, has improved by approximately 100%, 35%, and 45%. The findings also allow the padding of the GGH resist the cipher text, the cipher text selected and statistical attacks. However, the improvement of more than 50% in the avalanche effects is a positive achievement compared to the more complicated encryption and decryption processes of the proposed system.

Vidhya Ramani et al. 2018[21]The author discusses secure mechanisms for access to information, which can provide patients with access only by authorized entities. This paper therefore considers that blockchain technology safeguards data on health care systems as a distributed approach. This work proposes that patients and doctors in a given medical system have a safe and efficient data accessibility mechanism based on blockchain. A program that can also protect patient's privacy is also suggested. Our security review shows that it can withstand common attacks and maintain system integrity. In order to check the viability of our proposed program, an Ethereum-based implementation was also used.

Explanting EMRs through decentralized hospitals, this is hampering knowledge exchange and jeopardizing the privacy of patients [22],

Jingwei Liu et al. 2018 [23]. In order to solve these problems, we suggest a data sharing network known as BPDS based on blockchain privacy. In BPDS, the initial EMRs are safely stored in the cloud and the indexes are held in a blockchain consortium which is manipulated. This will dramatically reduce the risk of medical data leakage while, at the same time, ensuring that blockchain indexes cannot be unilaterally updated throughout the EMRs. According to the predefined patient access privileges, the secure data sharing can be done automatically via the intelligent blockchain contracts. Furthermore, the CPABE-based framework for access controls and the Content Signature extraction Scheme ensure that data sharing maintains good privacy. Security analysis shows that BPDS is a secure and efficient way to share EMR data.

Table :02 The research gaps studied are shown in following table

Sr No.	Author	Method	Pros	Cons
1	Hongyu Li et al. (2018) [25]	cryptographic algorithms (SHA-256, ECC)	Unchanging cryptographic and memory management algorithms helps to handle the leaked data.	Paper-based documents have a sluggish, low memory and are easily lost.
2	Wang and Song et al. (2018) [26]	Combined attribute-based/identity-based encryption and Signature (C-AB/IB-ES)	Encryption based on identity, guarantees confidentiality and traceability to encrypt databases.	Not yet applied theoretical clarification.
3	Guo et al. (2018) [27]	multiple authorities are introduced into ABS	Unchanging the details booklet.	Interoperability and privacy. Interoperability.
4	Uddin et al. (2018) [28]	Patient-Centric Agent based Healthcare	Single point of failure security and lightweight encryption and authentication.	Delay from end-to-end.
5	Lanxiang Chen et al. (2019) [29]	blockchain based searchable encryption for EHRs	Searchable encryption algorithm for security research.	Have a problem with scalability.
6	DINH C. NGUYEN et al. (2019) [30]	Uses cryptography key & Design access control policy algorithm with mobile cloud computing and blockchain.	Attain system efficiency optimization.	Hard to understand dynamic structure.
7	Shuai Wang et al. (2018) [31]	framework of parallel healthcare systems (PHSs) based on	Use for Data Security	Use for limited disease treatments.

		the artificial systems + computational experiments + parallel execution (ACP) approach		
8	Abdullah Algarni et al. (2017) [32]	1) attacks against the healthcare physical devices, 2) attacks on communication between healthcare devices, 3) attacks against healthcare providers or equipment manufacturers, and 4) attacks against patients. Energy-efficient and secure key management hybrid scheme using sensor energy.	Can be used for Medical data authorization and recovery in case of lost token.	Different attack on healthcare data
9	B D Deebak et al. (2017) [33]	Secure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS) is proposed to ensure secure communication in healthcare applications.	Enhanced resource efficiency for the development of intelligent e-health systems, such as storage, computation and communication.	Difficult to comprehend.
10	Wencheng Yang et al. (2018) [34]	biometric cryptographic technique, i.e. cancelable finger-vein based bio-cryptosystem	Ensure good protection.	There is a complex fra mework required for good data s tore protection.
11	Hina Abrar et al. (2018) [35]	Clouded based key Security method	Can be used for cloud security	Simple

III. MOTIVATION

The In tandem with the continuous participation of the patients in their own health care, the large-scale use of mobiles, assisted by an growing abundance of medical devices and remote access to healthcare facilities, led to the introduction of enormous quantities of clinical knowledge. You must safely send, archive and view your own files. This study refers to an approach that promotes privacy and clinical data protection by using a decentralized blockchain network and the authorization mechanism for access control based on attributes. Differing degrees of authorization are necessary for certain areas of the personal dossier, since personal medical records are often used by different entities (e.g. medical doctors, pharmacists, nurses, etc.). Reasonable blockchain instruments are given for partial

visibility and legitimate security on approved components to protect eHealth data's hierarchical privacy.

IV. RESEARCH GAP IN EHR

This Section going to details research gap in EHR in traditional system,

1. Basic problems in the provision of healthcare include the lack of data protection and how data can be checked, reliable and transmitted.

2. Data Ownership, data protection and Privacy

In various hospitals there are already more than three million patient records. The Ministry of Health has decided that the broad data kit that meets data protection and privacy needs to be properly managed (Sri Lanka Ministry of Health 2016). However, it is impossible to ensure data protection through routine information systems audits and empirical research in that field of security.

3. Data analysis and decision-making The main benefit for healthcare is the best treatment of patients on the basis of well-analyzed data and forecasts. The evaluation report suggested inclusion of data mining tools and intelligent business instruments that allow health sector decision-making support (DSS) at the provincial and national levels. Therefore, a report must be conducted about how such patient data can be used to improve healthcare.

4. Restrictions on remote access and review personnel.

5. Sharing of Inaccurate Information due to unavailability of online healthcare data.

V. OBJECTIVE:

This research work will focus on maintaining the privacy and security of EHR. The research work will look to meet some or all of the following objectives.

- To study various blockchain based frameworks for securing electronic health records.
- To design an efficient cryptographic authentication algorithm to prevent electronic health records from unauthorized access.
- To develop an algorithm for data validation for improving the classification accuracy using machine learning.
- To develop an efficient access control policy method to manage access to distributed electronic health records.
- To develop an enhanced blockchain based security and privacy preserving model and analyze the system performance.

VI. PROPOSED WORK

The proposed system stores crucial Medical prescription, laboratory report and emergency data which could encompass data regarding medical history of the patients, the medicine details in virtual database for future use. This data could be made available whenever needed by the patient & doctor through their login. In this system blockchain based cryptographic algorithm method is used securing the stored data from unauthorized access.

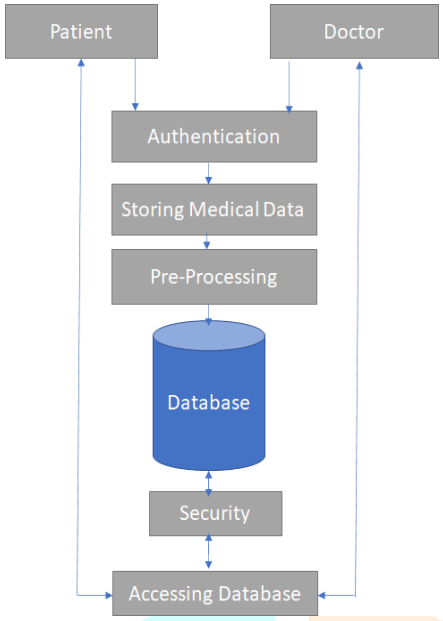

Fig 1: Block Diagram for Proposed Methodology

This research work proposes different modules for providing security and privacy to electronic healthcare data using blockchain technology.

- Healthcare database is accessible for patients as well as medicos from anywhere for patients' diagnosis.
- For both patient and medico staff authentication and validitation step is required.
- Electronic healthcare data such as details of treatment with all proofs of X- rays scan repots, subscription, images etc. with date and time wise detail as preprocessing will be required to store data into database.
- Data Preparation is required. Data pre-processing is the most important step that helps in building model more accurately.
- For accessing the electronic healthcare data blockchain security and privacy method is required to implement. In case of access by medicos need to get consent from patient.
- Patient medical histological database is important for their proper diagnosis & can be needed by healthcare provider at any time, therefore need to propose above framework.

VII. CONCLUSION

The use of blockchain in healthcare systems plays a critical role in present health care industry, according to the study and the way the blockchain is embraced by different sectors. This may contribute to automated processes for data collection and reviewing, correcting and aggregating data from multiple sources that are permanent, tamper-resistant and provide safe data that have a lower risk of cybercrime. It supports distributed data with redundancy and device fault tolerance. In this research, the healthcare industry is addressing current issues. In order to achieve privacy and protection for patient information within the EHR program, we suggest a system architecture and access control policy algorithm based on blockchain based cryptographic method for participants & accessing the data securely. Implementation of a blockchain network-based EHR sharing framework. The research suggested removes the central authority and the system's inherent failure. System protection is accomplished by secure technology, as the ledger cannot be changed by any person as proposed system uses the keys for sharing and accessing the data. The caliper performance evaluations of the proposed system are completed with the configuration of block size, block build time, endorsement policies, and the proposed optimization of

assessment methods, such as latency, capacity, and network safety to achieve better results, for various scenarios.

In future we are trying to implement our proposed system and capture the expected outcome in real life scenario.

References:

[1] Shuyun Shi, Debiao Hea,, Li Lia, Neeraj Kumar, Muhammad Khurram Khan, Kim-Kwang Raymond Choo "Applications of Blockchain in Ensuring the Security and Privacy of Electronic Health Record Systems: A Survey." *Computers & Security* (2020), doi:https://doi.org/10.1016/j.cose.2020.101966.

[2] AYESHA SHAHNAZ, USMAN QAMAR, AND AYESHA KHALID. "Using Blockchain for Electronic Health Records." IEEE Access, vol. 7, pp. 147782–147795, 2019.

[3] Sabyasachi Dash, Sushil Kumar Shakyawar , Mohit Sharma and Sandeep Kaushik, "Big data in healthcare: management, analysis and future prospects", https://doi.org/10.1186/s40537-019-0217-0,springer 2019.

[4] Karim Abouelmehdi, Abderrahim BeniHessane and Hayat Khaloufi, "Big healthcare data: preserving security and privacy", https://doi.org/10.1186/s40537-017-0110-7,2018.

[5] [5]Kashif Saleem, Xiaodong Yang, Abdelouahid Derhab, Mehmet A. Orgun, Waseem Iqbal, Imran Rashid, And Asif Yaseen "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions", October 30, 2017, 10.1109/ACCESS.2017.2767561.

[6] Tareq Ahram, Arman Sargolzaei, Saman Sargolzaei, Jeff Daniels, and Ben Amaba, "Blockchain Technology Innovations", 978-1-5090-1114-8/17/$31.00 ©2017 IEEE.

[7] Pinyaphat Tasatanattakool, Chian Techapanupreeda, "Blockchain: Challenges and Applications", 978-1-5386-2290-2/18/$31.00 ©2018 IEEE.

[8] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 978-1-5386-1996-4/17 $31.00 © 2017 IEEE DOI 10.1109/BigDataCongress.2017.85.

[9] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Member, IEEE, Abdelouahid Derhab, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", 2327-4662 (c) 2018 IEEE.

[10] P. Otte, M. de Vos, and J. Pouwelse, "TrustChain: A Sybil-resistant scalable blockchain," Futur. Gener. Comput. Syst., sep 2017.

[11] Q. Wang, B. Qin, J. Hu, and F. Xiao, "Preserving transaction privacy in bitcoin," Futur. Gener. Comput. Syst., sep 2017.

[12] J.-H. Lee, "BIDaaS: Blockchain Based ID As a Service," IEEE Access, vol. 6, pp. 2274–2278, 2018.

[13] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," IET Commun., vol. 12, no. 5, pp. 527–532, Mar. 2018.

[14] Q. Lin, H. Yan, Z. Huang, W. Chen, J. Shen, and Y. Tang, "An IDbased linearly homomorphic signature scheme and its application in blockchain," IEEE Access, pp. 1–1, 2018.

[15] Mohamed Elhoseny , Gustavo Ramírez-González, Osama M. Abu-Elnasr , Shihab A. Shawkat, Arunkumar N, And Ahmed Farouk, "Secure Medical Data Transmission Model for iot-Based Healthcare Systems" , 2169-3536 2018 IEEE..

[16] P.K. Kavitha, P. Vidhya Saraswathi, "A Survey on Medical Image Encryption", ICASCT2501 | ICASCT | March-April-2017 [(3) 5 : 01-08]

[17] Javaria Tahir ,Nadeem Javaid, "Bootstrapping a Blockchain Based Ecosystem for Big Data Exchange", 978-1-5386-1996-4/17 $31.00 © 2017 IEEE DOI 10.1109/BigDataCongress. 2017.67

[18] SHANGPING WANG , DAN ZHANG , AND YALING ZHANG." Blockchain-Based Personal Health Records Sharing Scheme With Data Integrity Verifiable." IEEE Access, vol. 7, pp. 102888–102901, 2019.

[19] Massoud Sokouti, Ali Zakerolhosseini and Babak Sokouti, "Medical Image Encryption: An Application for Improved Padding Based GGH Encryption Algorithm" , The Open Medical Informatics Journal, 2016, 10, 11-22.

[20] Alexandru Soceanu, Maksym Vasylenko, "Managing the Privacy and Security of ehealth Data", 978-1-4799-1780-8/15 $31.00 © 2015 IEEE ,DOI 10.1109/CSCS.2015.76.

[21] Vidhya Ramani, Tanesh Kumar, An Braeken, Madhusanka Liyanage, Mika Ylianttila, "Secure and Efficient Data Accessibility in Blockchain based Healthcare Systems", December 2018 DOI: 10.1109/GLOCOM.2018.8647221.

[22] Jingwei Liu_, Xiaolu Li_, Lin Yey, Hongli Zhangy, Xiaojiang Duz, and Mohsen Guizanix, "BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records", 978-1-5386-4727-1/18/$31.00 ©2018 IEEE.

[23] HYUNIL KIM, SEUNG-HYUN KIM, JUNG YEON HWANG, AND CHANGHO SEO." Efficient Privacy-Preserving Machine Learning for Blockchain Network." IEEE Access, vol. 7, pp. 136481–136495, 2019.

[24] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang , "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" , 2017 IEEE 6th International Congress on Big Data.

[25] Hongyu Li, Liehuang Zhu, Meng Shen, Feng Gao, Xiaoling Tao, Sheng Liu ,"Blockchain-Based Data Preservation System for Medical Data", https://doi.org/10.1007/s10916-018-0997-3,2018.

[26] HaoWang, Yujiao Song, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain", https://doi.org/10.1007/s10916-018-0994-6, 12 June 2018.

[27] RUI GUO, HUIXIAN SHI, QINGLAN ZHAO, AND DONG ZHENG, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems", 2169-3536, 2018 IEEE.

[28] MD. ASHRAF UDDIN , ANDREW STRANIERI, IQBAL GONDAL, AND VENKI BALASUBRAMANIAN, " Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture", 2169-3536 2018 IEEE.

[29]Lanxiang Chen , Wai-Kong Lee , Chin-Chen Chang , Kim-Kwang Raymond Choo , Nan Zhang, "Blockchain based searchable encryption for electronic health record Sharing", ©2019 Elsevier.

[30] DINH C. NGUYEN, PUBUDU N. PATHIRANA, MING DING AND ARUNA SENEVIRATNE, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems", 2169-3536 2019 IEEE.

[31] Shuai Wang , Jing Wang, Xiao Wang , Member, Tianyu Qiu, Yong Yuan , Senior Member, Liwei Ouyang, Yuanyuan Guo, and Fei-Yue Wang, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach", 2329-924X © 2018 IEEE.

[32] XIAODONG YANG, TING LI, XIZHEN PEI ,LONG WEN, AND CAIFEN WANG." Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology." IEEE Access, vol. 8, pp. 45468–45476, 2020.

[33] XIAOFANG LI, YURONG MEI, JING GONG3, FENG XIANG, AND ZHIXIN SUN." A Blockchain Privacy Protection Scheme Based on Ring Signature." IEEE Access, vol. 8, pp. 76765–76772, 2020.

[34] BIN LIU, LIJUN XIAO, JING LONG, MINGDONG TANG, AND OSAMA HOSAM." Secure Digital Certificate-Based Data Access Control Scheme in Blockchain." IEEE Access, vol. 8, pp. 91751–91760, 2020.

[35] Hina Abrar, Syed Jawad Hussain, Junaid Chaudhry, Kashif Saleem, Mehmet A. Orgun, Jalal Al-Muhtadi, Craig Valli, "Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry", IEEE Access 2018.

[36] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, p. 218, 2016.

[37] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Proc. of International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.