# SECURITY ASPECTS OF USING BLOCKCHAIN IN MANAGINGHEALTHCARE INFORMATION

**Liz George**

*St.Josephs College of Engineering & Technology, Kottayam, Kerala*

**Jubilant J Kizhakkethottam**

*Saintgits College of Engineering, Kottayam, Kerala*

***Abstract***

*Blockchain has come a long way since its introduction in 2009, as the underlying technology which implements the perception of distributed ledger in the first digitalcurrency, bitcoin, proposed by Satoshi Nakomoto. The immutable and decentralized nature, along with the security it provides by means of the cryptographic concepts caused the upsurge of blockchain, makes it apt to apply in many thriving domains like finance, supply chain, education healthcare etc. Digitization in healthcare have resulted in massive volume of electronic records about patients. Popularity of IoT technology andcloudcomputing provided betteroptions in the collection and storageofmedical data. The security of health information in cloud systems has always beena concern. The security and privacy of the medical records, its easy access and controlby patients in transparent way can be realized by using blockchain technology. This article analyses the possibilities of integrating blockchain technology to various healthcare applications and various approaches adopted to ensure the security and privacy ofdata.*

***Keywords:*** *blockchain, healthcare, security, interoperability, privacy*

## 1. INTRODUCTION

Innovation of technology in the past decade has prompted and brought progressive changes in health care domain. Incorporating IoT technology in health care has witnessed the implementation of remote health monitoring, using sensors attached to patient's body [1].Automation of medical records and medical insurance claims has improvised the data management and guaranteed better health care service to patients. These new changes in the clinical field have resulted in producing huge volume of medical data. The storage, security and interoperability of this data became a primary concern. The cloud computing services have been incorporated tostore these large volumeofmedicaldata. Butthesecurity and interoperability of this data in the cloud has been a major challenge. Numerous solutions werere commended from time-to- time toresolve theissue. Butmostof these solutions relayed on a centralized system [2] and doesn't guarantee the security of the medical data whilst sharing it.

The blockchain era is cutting-edge in this regard. The decentralized and immutable nature ofblockchain, alongside the cryptographic techniques used to secure records makes it suitable for handling medical records in a secure way and warrant its interoperability. Interoperability facilitate the trade of health-related information among healthcare providers and patients consistently, securely and efficiently [3]. Depending upon the requirements of the different participants in health care applications (patients, doctors, Insurance companies, hospitals), blockchain applications can be designed to be public, private or hybrid to cater their respective needs. The implementation of interoperability of the medical data ought to be in compliance with the regulations specified by HIPPA or GDPR. [4]

## 2. MAJOR CHALLENGES IN HEALTH CARE APPLICATIONS

Theprivacyofpatient'spersonalhealthrecordisutmostcrucial, andtherearelegalrights and Acts like HIPPA or GDPR instilled for safeguarding patients medical information. The adoptionof cloud storage for maintaining medicalrecords andwideusage ofmobiledevices likesensorshavemadethe data more vulnerable to various malicious attacks and amplified the hazard of compromising personal information while sharing. [5]

### 2.1. Data Security

The medical data is subjected to many types of attack from time to time due to its high commercial value. Managing the security of information has become one of the greatest challenges in health care sector. Tampering of medical data to reap monetary benefit may have extreme consequences, compromising patient's trust and organization's credibility [6].The security techniques currently implemented in this sector is weak and vulnerable and are subjected to malware attack. The requests for accessing healthcare records should be strictly monitored and permitted based only on assigned access rights, minimizing the risk of data tampering or copying.[7]Secure sharing of data is indispensable for many research institutions to conduct disease research.

The incorporation of IoT in medical field enables real time monitoring of vital signs and conditions of patients and medication management in a cost effective way. It also manages remote patient monitoringsaving hospitalization charges. Asmultiple devicesareinvolved inaccumulating sensitiveandpersonaldata, privacy concerns are compounded, as this data is shared among mobile applications and cloud services connected to device. [8] The use of cloud services for data storage is another major concern in the context of security. The need for high level data integration and interoperability of health care data, requires multiple organizations to share their information on internet based environment provided by the cloud service provider, making the data prone to all forms of cyber attacks like fraud,hacking etc.[9] Advanced Persistent Attack (APT) executed via an intruder or a group of intruders for a long time on a system can greatly damage healthcare networks. [10]

### 2.2. Interoperability

Interoperability is the method of sharing and transferring data

among diverse sources. [11]. In medical arena, the data sharing by medical institutions is significant for scientific research, to reduce healthcare cost and to improve quality of health care delivery. Interoperability in healthcare aimstoexchange medicalinformation between health care providers and patients so that they can be shared throughout the environment. [12] The main issue in interoperability is the usage of centralized storage by medical institutions which stores data in different formats and structures.The use of standards for communication, for rep- resenting clinical information and images have been proposed and implemented to ensure interoperability. [13] However these standards are often too general and subject to local interpretation and implementation. Rather than conferring to a single standard, health care organizations uses different standards leading to confusion [14].Legacy systems implemented prior to the introduction of standards, which are nonetheless in use, has limited interoperability as they were designed for a particular task. [15] There has been a recent shift in the focus of interoperability from the 'data exchange between healthcare organizations' to 'patient driven interoperability', controlled by patients. [16].This new approach has also introduced challenges related toprivacy,security, technology, governance etc. manyof them are yet to be resolved in traditional interoperability approach.

## 3. SCOPE OF BLOCKCHAIN IN HEALTH CARE APPLICATIONS

There is an exponential growth in the available medical data, mainly due to the incorporation of mobile devices and technologies like Internet of Things (IoT) in Health care Industry. The centralized nature of available storage concepts doesn't comply with the requirements like availability, scalability and security of data. The decentralized and distributed nature of blockchain with features like immutability and scalability, makes it a suitable candidate to alleviate the currently existing challenges in Health care.

The immutable nature of the records in blockchain ensures the integrity of the data, conforming that the information is not tampered with, which is highly required in the case of medical data, while used for medical research and providing healthcare services to patients. The decentralized storage of blockchain records helps in faster retrieval of data, system interoperability and improved data quality. The cryptographic techniques used for data management inblockchain ensures the privacy of the data. The consensus mechanism and encryption schemes incorporated ensures the authentication of information stored. [17] Another significant feature of blockchain is smart contracts, a set of rules specifying the conditions that are agreed upon by various parties involved, while performing interactions.[18] The implementation of smart contracts in blockchain made it more convenient to manage the access control of various participants in the healthcare applications and monitor it.

### 3.1. Implementing blockchain in Health care Applications

Realizing the scope of blockchain in building efficient healthcare applications, numerous schemes incorporating blockchain technology were derived and implemented, depending upon the specific requirements of applications. These schemes were able to conquer many of the shortcomings and challenges of present healthcare applications. Public or private blockchain can be used based on requirement regarding the visibility of the medical data/information to the participants. Consensus algorithms are protocol sets which provide a technique with the help of which the users or machines can coordinate in a distributed and decentralized setting. [19] There are different consensus protocols like Proof of work, Proof of stake, Proof of Elapsed Time etc. available, which validates the transactions and enforce security and trust in blockchain.

### 3.2. Schemes for ensuring privacy

Ensuring security of the medical data and measures to keep the privacy of the patients is very critical in health care applications, which has been specified as a mandatory requirement through legal acts like HIPPA. Medical records can be shared among several entities involved- patients, research in- situations and semi-trusted cloud servers where the concept of Zero knowledge is used to verify whether the medical data of the patient meets criteria of research institute without revealing the private data of the patient. [20] Healthcare Data Gateway (HGD), an implementation based on the blockchain architecture, enables sharing client's data easily without compromising privacy,canbe incorporated inhealthcare applicationsto maintain patient's privacy. [21] Zhangetal. proposed a scheme comprising consortium blockchain and private blockchain, incorporating the technology of keyword search, guaranteeing the privacyand protection of patient's data. [22] Haibo Tian et al. proposes a scheme in blockchain is used to store the data in the diagnosis and treatment process by encrypting the data and using the shared key. Authentic parties can be reconstruct theshared key before the process of diagnosis and treatment begins. [23]

Alevtina et al. proposed a medical record sharing systembased on blockchain in which patient's data is encrypted and stored in a cloud server. When the data is to be used, it is necessarytoobtain the decryption key from the data owner ensuring privacy of the data [24]. Antonio Emerson et al. proposed a blockchain based solution for data storage and a light weight Non-Interactive zero- Knowledge proof Scheme for authenticating the mobile devices used to collect the health care data. Attribute based Encryption is used to protect the shared data. [25].MedBlock, a blockchain- based information management system, handle patients' information, with an improved consensus mechanism and achieves consensus in an efficient and cost effective way. It alsoprovide high security for data by combining customized access control protocols and symmetric cryptography [26]

### 3.3. Schemes ensuring Interoperability

Gaby G. Dagher et al. proposed a framework which utilizes smart contracts in an Ethereum- based blockchain called Ancile. It guarantees efficient, secure and interoperable, access to medical records by patients, providers, and third parties. [27]. Rateb Jabbar et al. proposed BiiMED: a Blockchain framework for Enhancing Data Interoperability and Integrity in EHR- sharing, which includes an access management system, allowing the exchange of EHRs between different medical providers and a decentralized Trusted Third Party Auditor. [28] Xia et al. developed BBDS [16], a high-level Blockchain-based framework,

which allows data owners and users to access medical records from a shared repository after successful authentication of the keys and identities. [29] OmniPHR: a distributed architecture model that integrates Personal Health Records for patients and Healthcare providers, incorporating blockchain technology. Patients are provided with a unified view of their scattered health records, and healthcare providers are given access to up-to-date data regarding their patients. [30]

## 4. CHALLENGES

Despite of all these features, implementation of blockchain has numerous disadvantages. Lack of standardization is an important challenge that hinders the wide acceptance of blockchain as solution in many domains including healthcare. [31] Even though decentralized architecture is suitable for ensuring the interoperability in health care applications, there is a potential threat about the privacy as the data is stored and retrieved from a public ledger. IoT Based blockchain solutions are popular in healthcare sector due to the wide use of mobile devices in remote health monitoring. But these solutions provide limited scalability, computationally expensive and provides additional overhead due to inadequate computational capacity of IoT devices like sensors. [32] The management of keys, used by cryptographic techniques for ensuring the data privacy in blockchain applications is another issue that is yet to be resolved.[33]. There are few vulnerabilities specific to system's implementation and architecture like 51% attacks, double spending attacks, selfish mining attacks, eclipse attacks, block discarding attack etc. [34]

## 5. CONCLUSION

The adoption of blockchain technology in healthcare domain has redesigned the aspect of healthcare applications. Demand for clinical data has been increased in past few years due to its extensive use by researchers to identify and find cure for diseases. Usage of blockchain helps to time stamp the records so that no one can tamper with it. It gives the patient the right to decide regarding who should have access to data and the how much information should be shared. The immutable and secure nature of the blockchain guarantees that the researcher will be getting the required relevant data, meanwhile patients can hold back their personal information. The use of blockchain has great impact on health applications involving IoT technology, providing better data management and secure data sharing. Still there are certain areas in healthcare that needs improvements. While implementing healthcare applications that involve cross borders, data sharing is one of the major concerns as the privacy policies adopted by governments in different countries are unique. Blockchain is not a solution to all the challenges faced by health industry. While developing an application, we need to scrutinize and evaluate the requirements, making the decision regarding whether incorporating blockchain can improvise the performance of the application. Only a fraction healthcare organizations, especially multinational organizations, have taken the initiative to understand the benefits of blockchain and put the effort to implement it. Majority of the medium and small scale organizations are still oblivious about its advantages. More initiatives and campaigns are required to popularize and encourage the use of this technology for building better applications.

## REFERENCES


[1] D.D.K.S.N. K.P.P. Ray, "Blockchain for IoT-based healthcare: Background, consensus, platforms, and use cases,"," IEEE Systems Journal, pp. 1-10, 2020.

[2] L.D.B.M.S.J.S.X.C.A. Shen J, "Secure verifiable database supporting efficient dynamic operations in cloud computing," IEEE Trans Emerg Top Comput, vol. 8, no. 2, pp. 280- 290, 2017.

[3] M.M.A.Y.B. Seyednima Khezr, "Blockchain technology in healthcare: A comprehensive review and directions for future research," Appl. Sci, vol. 9, no. 9, p. 1736, 2019.

[4] T.-T.K.B.G.K.A.C.G.C.D.G. Tim K. Mackey, "Fit-for-purpose?' – challenges and opportunities for applications of blockchain technology in the future of healthcare," BMCMedicine, 2019.

[5] K.-K.R.C.C.Z.L.D.H. Thomas McGhin, "Blockchain in healthcare applications: Research challenges and opportunities," Journal of Network and Computer Applications,vol. 135, pp. 62-75, 2019.

[6] J.M.A.V.R. Chakraborty, "Security and fault tolerance in Internet of things," Signal and Communication., 2019.

[7] S.M.J. Suzuki, "Blockchain as an audit-able communication channel.," in 41st IEEE Annual Conference on Computer Software and Applications , 2017.

[8] P.A.H. Williams and V. McCauley, "Always Connected: The Security Challenges of the Healthcare Internet of Things," in IEEE 3rd World Forum on Internet of Things (WF- IoT), 2016.

[9] M.G.J.F.S.M. Esmaeil Mehraeen, "Security Challenges in Healthcare Cloud Computing: A Systematic Review," Global Journal of Health Science;, vol. 9, no. 3, 2017.

[10] A.I.Y.B.A.K.M.M.A.A.A.R.K.R.A.K.A.K. Pandey, "Key Issues in Healthcare Data Integrity: Analysis and Recommendations," IEEE Access, no. 8, pp. 15847-15865, 2020.

[11] A.E.V.L. Asaph Azaria, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in 2nd International Conference on Open and Big Data, Vienna, 2016.

[12] F.M.F.P.M.S.A. Luciana Cardoso, "The Next Generation of Interoperability Agents in Healthcare," International Journal of Environmental Research and Public Health, vol. 11, pp. 5349-5371, 2014.

[13] M.J.A.Mykkänen, "An evaluation and selection framework for interoperability information and Software Technology, vol. 50, no. 3, pp. 176-197, 2008.

[14] S.S.L.M.Lau, "Towards Data Interoperability: Practical Issues in Terminology Implementation and Mapping",," in 77th AHIMA Conventionand Exhibit , 2005.

[15] A.S.I.G.J.O. Olaronke Iroju, "Interoperability in Healthcare: Benefits, Challenges andResolutions," InternationalJournalof Innovationand Applied Studies, vol. 3, pp. 262-270, 2013.

[16] C.C. William J. Gordon, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-

Driven Interoperability," Computational and Structural Biotechnology Journal, vol. 16, pp. 224-230, 2018.

[17] F.R.Y.S.Y.Y.Z. Ruizhe Yang, "Integrated Blockchain and edge computing systems: A survey, some research issues and challenges.," IEEE Communications Surveys & Tutorials, vol. 29, no. 2, pp. 1502-1538, 2019.

[18] C.C.G. Daniel Macrinici, "Smart contract applications within blockchain technology: A systematic mapping study," Telematics and Informatics, vol. 35, no. 8, pp. 2337-2354, 2018.

[19] S.C.A.S.J.K. Sivleen Kaur, "A Research Survey on Applications of Consensus Protocols in Blockchain," Security and Communication Networks, 2021.

[20] P.Z.,F.X.X.S.Q.H. Haiping Huang, "A blockchain-based scheme for privacy- preserving and secure sharing of medical data," computers &se curity , vol. 99, 2020.

[21] H.W.J. Xiaoning Yue, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," Journal of Medical Systems, vol. 40, no. 10,pp. 1-8, 2016.

[22] A.Z. Xiaodong Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of Medical Systems, vol. 42, 2018.

[23] J.H.Y.D. Haibo Tian, "Medical Data Management on Blockchain with Privacy," Journal of Medical Systems, vol. 43, 2019.

[24] A. Dubovitskaya, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," in AMIA - Annual Symposium proceedings, 2017

[25] J.C.D.N.S.H. Antonio Emerson Barros Tomaz, "Preserving Privacy in Mobile Health Systems Using Non-Interactive Zero-Knowledge Proof and Blockchain," IEEE Access, vol. 8, pp. 204441 - 204458, 2020

[26] S.W.Y.R.L.Y.Y. Kai Fan, "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain," Journal of Medical Systems, vol. 42, 2018.

[27] M.M.B. M. Gaby G.Daghera Jordan Mohler, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," Sustainable Cities and Society , vol. 39, pp. 283-297, 2018.

[28] N.F.K.K.B. Rateb Jabbar, "Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity," in IEEE International Conference on Informatics, IoT, and Enabling Technologies, Doha, 2020.

[29] E.B.S.A.S.S.A.X.Z.Q. Xia, "BBDS:Blockchain-based data sharing for electronic medical records in cloud environments," Information, vol. 8, no. 2, p. 44, 2017.

[30] C.A.C.R.R.R. Alex Roehrs, "Omni PHR: A distributed architecture model to integrate personal health records," Journal of Bioinformatics, vol. 71, pp. 70-81, 2017.

[31] J.U.J. Svein Ølnes, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," vernment Information Quarterly, vol. 34, no. 2, pp. 355-364, 2017.

[32] H. Hou, "The Application of Blockchain Technology in E-Government in China," in 26th International Conference on Computer Communication and Networks, Vancouver, 2017.

[33] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "Overview of blockchain technology: architecture, consensus and future trends.," in IEEE International Congress on Big Data,2017.

[34] J. J. Xu, "Are blockchains immune to all malicious attacks?," Financial Innovation, vol. 25, no. 2, 2016.

*Proceedings of*

# International Conference on Cyber Security and Ethical Hacking in Blockchain Technology (ICCSEHBT)

## Sponsored by AICTE

**29th September - 1st October 2021**

Hosted by

SCMS SCHOOL OF TECHNOLOGY AND MANAGEMENT (SSTM)

# Contents



## ICCSEHBT Papers

13 **NEW APPLICATION IN BLOCKCHAIN TECHNOLOGY**
**Harshini P U, Devashree S P and Dr.Anitha D**

14 **FRAUD DETECTION AND FINANCIAL CRIME PREVENTION**
**Jeevitha Ranjani Madheswaran and Dharani Kumar**

15 **SECURITY ASPECTS OF USING BLOCKCHAIN IN MANAGING HEALTHCARE INFORMATION**
**Liz George and Jubilant J Kizhakkethottam**

16 **SECURE HASH ALGORITHMS FOR SECURING IoT**
**Pranoti Shingote**

17 **INTELLIGENT BLOCKCHAIN**
**Jini Shaji Varughese, Anju Pratap and Jerrin Sebastian**

18 **SYNTHETIC IMAGE GENERATION USING GANs**
**Anupriya S, Dr. Santhosh P Mathew and Veena A Kuma**

19 **DATA PROTECTON AND PRIVACY PRESERVING USING BLOCKCHAIN IN HEALTHCARE**
**Renji Rajan, Gokulnath G and Jubilant J Kizhakkethottam**

20 **BLOCKCHAIN AIDED COVID 19 VACCINE SUPPLY-CHAIN AND CERTIFICATE ISSUANCE**
**Arshith Suresh, Justin Mathew and Jubilant J Kizhakkethottam**

21 **HASH FUNCTIONS IN BLOCKCHAIN SYSTEMS**
**Reshma K. R, Mrudula Raju, Smitha Anu Thomas and Smitha Vinod**

22 **FRAUD DETECTION IN BLOCK CHAIN SYSTEMS**
**Ashitha Bhaskaran, Jilu Varghese, Smitha Anu Thomas and Smitha Vinod**

23 **DATA ENCRYPTION USING DIGITAL SIGNATURE IN BLOCKCHAIN TRANSACTIONS**
**Gayathri N. S., Jilta John, Smitha Anu Thomas and Smitha Vinod**

24 **IMPLANTED MEDICAL DEVICES SECURITY**
**Aathira Mohanan Pillai, Hari M and Jubiliant J Kizhakethottam**

25 **CYBERCRIME CLASSIFICATION USING MACHINE LEARNING**
**Nikitha Abraham, Dr. Arun Madhu and Ria Mathews**

26 **MFT- THE DIGITAL MASKING TOOL**
**Aathira Mohanan Pillai, Hari M and Jubilant J Kizhakethottam**

27 **A REVIEW ON THE EFFECTS OF ENERGY CONSUMPTION ON PoW BLOCKCHAINS**
**Sheril Dcouto and Edsel Correya**

28 **DATA PROTECTION USING BLOCKCHAIN TECHNOLOGY**
**Anoop Pauly, Deepa Mary Mathews and Prasad J C**