International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

A Block Chain Technology based Data Security in Medical Report for Healthcares

Parameswari M[1], Alwin Mathew M[2], Akilesh M[3], Aravind N[4]

[1]*Assistant Professor, Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Tamilnadu, India*
[2,3,4]*Final Year Student , Department of Computer Science and Engineering, Dhirajlal Gandhi College of Technology, Tamilnadu, India*

Abstract - *Healthcare has been the industry with the highest growth in terms of both revenue and data. With so much of electronic health records, the security has been the need of the hour. One of the predominant requirements in today's health care systems is to protect the patient's medical report against potential attackers. To make this critical information more secure, there has been an urge to use some encryption technique. So, we have proposed Block chain technology as a disbursed approach to grant security in accessing the medical report of a patient. It's composed of three namely Authentication, Encryption and Data Retrieval using Block Chain technology. This proposed framework may likewise ensure the protection of the patients and moreover keeps the security and trustworthiness of the health care system.*

KeyWords: **Block chain, Medical Report,Data Accessibility, Security, Privacy, Authentication, Encryption, Data Retrieval.**

1. INTRODUCTION

The Block chain is the fastest growing technology through various applications in a secure manner. The various implementations make use of this block chain technology among stakeholders. Mainly, block chain technology plays a significat role within the medical and healthcare system. Because of the decentralized and distributed technology. The centralized design in current health care services is not so secure among the various medical services, which provides a delay in accessing the data and it has a major risk in leakage of information. In such a case, the medical reports may be archived without the knowledge of the patient. Accessing the information in a very secure manner within the network is the major issue in current health care maintaining system. Electronic, Health/Medical Record (EHR/EMR) is the presentt online healthcare services which play a key role in maintaining and storing the data, which has a major issue in leakage of patient's information. This becomes the major reason for the development of Block chain technology. In Block chain technology, not only provides security and easy accessibility, but also gives other production elements in the administrations and furthermore pursues privacy, respectability, and verification.

2. Literature Survey

The medical report of a patient is viewed as relatively sensitive and wants a secure and safer ability to guard the data. In this manner, the putting away, sharing and overseeing restorative reports can be executed in secure ways[1-2]. These problems are already proposed by using a number of mechanisms, for example, numerous authentication schemes,[3-5] which leads to fulfilling the need of efficient and secure access of medical reports, manageability, and other safety requirements. These options had been useful in providing a variety of protection necessities under preferred healthcare scenarios. But these strategies in current healthcare technology are no longer enough due to the fact the patient has been exploited by means of various entities via distinct means except their consent[6-7].

In this research, is to discover a variety of security solutions based on block chain based health care approaches[8]. There have been a variety of research studies associated with efficient utilization of block chain in healthcare[9-10]. Electronic medical remedy approaches for manual and remote access of medical reports and protecting the privacy of the records are the most essential fields of application where Block chain technology can create value[11]. The MedRec in which a decentralized method for utilizing block chain mechanical skill is received to deal with the EHR/EMR[12-14] and furthermore gives a potential contextual analysis of block chain usage in social insurance, which gives a model to EHR/EMR. Moreover,[15-16] MedShare gives the trustless method for sharing the clinical reports among an assortment of specialist organizations utilizing block chain. Thus, the examination network characterizes the exceptional systems for accessing the records safely utilizing block chain innovation.

3. PROPOSED SYSTEM

The main aim of this research is to provide secure management in accessing the medical records using block chain technology by unique identification of the data security. Using Block Chain Crypto System Algorithm the laboratory test data and basic information of patients are Encrypted. The clinical dataset is an information system that offers knowledge and personalized information to users in

enhancing health and healthcare outcomes. Using Crypto System the data of each patient are secured with crypto currency encryption process. A novel framework is proposed for retrieving the most relevant information of patients from multiple data sources.

3.1 Register and Login

Register as user by providing first name, last name, user name and password, etc.. Initially, the patient must register their personal details in the registry and unique identification is created for the new user. If the patient already exists, then he/she can directly login to their medical account by using unique identification of the respective patient. The private key is generated for each registered patient with the help of ID. Login operation can be done Using User Name and Password. Thus the registration process is completed.

A. Generate New ID for Patient

if(patient == new user)
then Register with personal information
create unique ID(idp),
public key(Pkp),
private key(Skp)
login(idp, Skp, Pkd)
else directly login using ID(idp)

Fig. 1 shows the registration process should be done. If the patient is a new user then they should register their personal information in a separate account.

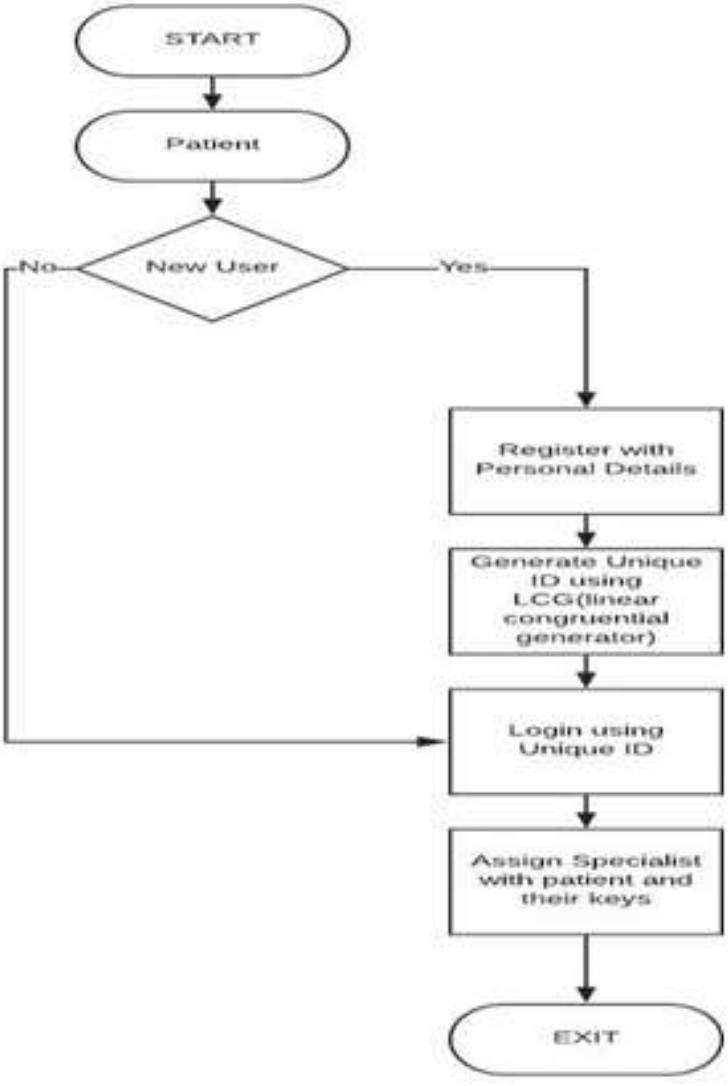

Fig -1: Registration for a new patient

B. Authenticate the doctor

Doctor's medical history should be maintained by the administration of the hospital and public key for the doctor is generated. Then doctor's public key is used as a key for the authentication.

Generate Authenticate ID for Doctor if doctor wants to add details then get permission from patient

This Step authenticates the doctor and only those authorized doctor's can add or retrieve the patient's medical report. Unauthorized doctor will not be permitted to access the medical report of particular patient. By this we can protect the patient medical report effectively.

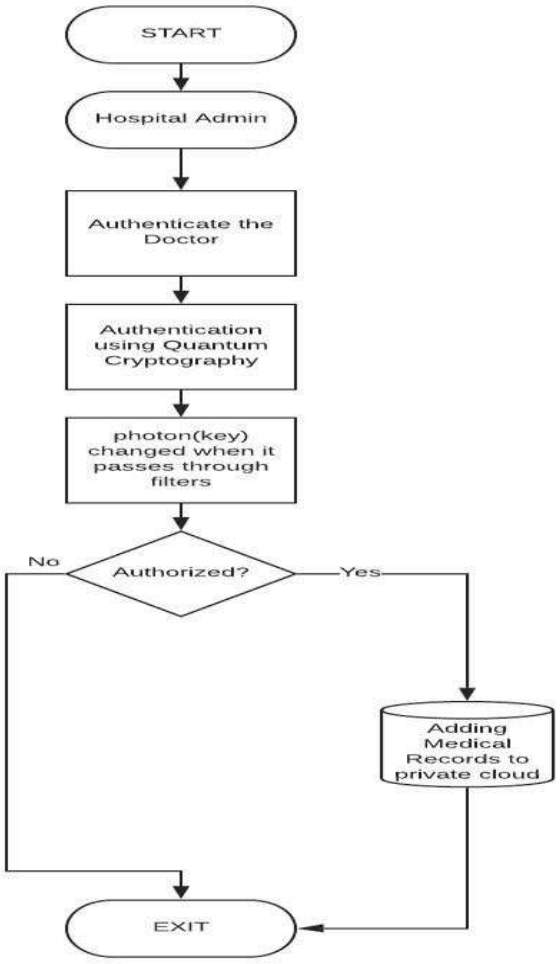

Fig -2: Authenticate the Doctor

3.2 Health Care Data

Patient health care data like height, weight, blood pressure, temperature, heart beat rate, Diseases Symptoms will be given as input. Considering the likely complications due to multiple medical diseases (conditions), Crypto system algorithm is proposed for multi-label learning, by using correlations among labels dataset and for anticipating more potential diseases of a patient, so that a list of diseases can be recommended to the physician simultaneously.

3.3 Block Chain Crypto System Algorithm

Using Block chain Algorithm data of each patient will be Encrypted Based on Cryptographic technique. Encrypted data from database is shown to appropriate doctor and patient with decrypted format.

C. Encrypt the medical report

The encryption process can be done with the help of AES algorithm. AES is a symmetric encryption algorithm which has a specification in encryption of electronic data. For encryption, plain text and secret key is required in AES engine and also the same secret key is used for decryption. The data's are encrypted with the patient's private key Ek(PR, k). The private key of the patient is used to prevent the medical record in a secure manner. Thus, the encrypted data Ek(PR, k) is stored in a private cloud(PC) with the timestamp(T) and PC(PR, T). The address of the encrypted data which is stored in private cloud is added to the block chain(BC).

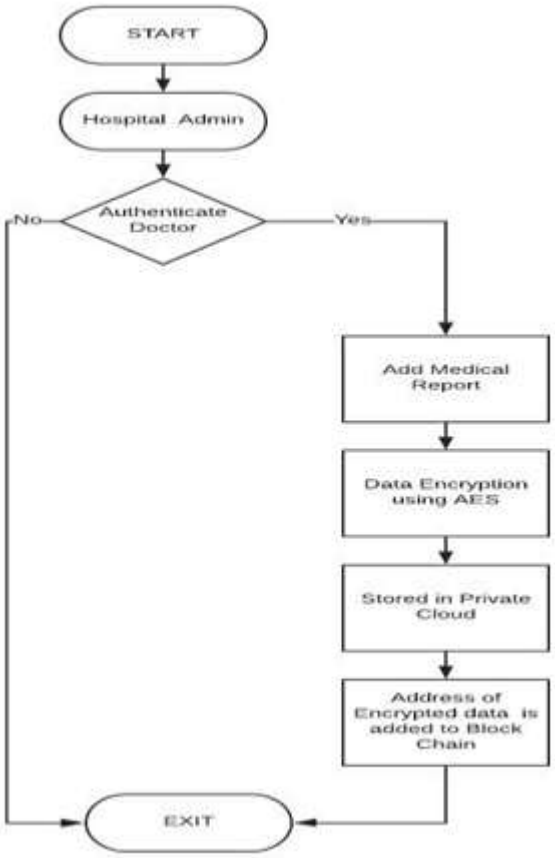

Fig -3: Encrypt the Medical Report

D.Retrieve the Medical Report

The data can be retrieving only by the authorized doctor. The authenticated doctor can perform data retrieval using SHA algorithm. SHA is a cryptographic hash function, there is no direct way decode. Hashed data is very easy and efficient to decrypt.

if(authentication == true)
then retrieve address of the record from BC

3.4 Multilevel Learning Algorithm

Using Multilevel Learning Algorithm data of each patient will be compared with symptoms of previous dataset and stored in database. Using Recommend Diagnosis Analyze pattern matching we have do string matching with disease dataset then the finalized analyzing disease status will be updated.

4. CONCLUSIONS

The block chain technology is gaining rapid attention from individuals, as well as organizations of nearly all kinds and dimensions. It is capable of transforming the traditional industry with all its features, which include decentralization, anonymity, persistency, and auditability. The block chain technology is expected to reshape the healthcare ecosystem. Not only the process will be transparent and secure, but also the quality of healthcare will be increased at significantly very low cost. In this paper, we discussed various block chain applications in the healthcare industry and identified the major research initiatives as well as future research opportunities. Specifically, we presented the present research on health data management and how block chain will empower patients and stream line the sharing process of health data. We found that there is a consensus among researchers that, with block chain technology, patient's data will be truly owned and controlled by its rightful owner, i.e., the patients. The block chain makes the health records to be time-stamped so that no one can tamper with them after becoming part of the distributor ledger. The patients can have the right to decide who can and cannot access their data and for what purposes. However, there are still several open challenges that has to be further investigated.

REFERENCES

[1] M. Puppala, T. He, X. Yu, S. Chen, R. Ogunti, and S. T. C. Wong, "Data security and privacy management in healthcare applications and clinical data warehouse environment," in2016 IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI), Feb 2016, pp. 5– 8.

[2] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. Saadi, "Big data security and privacy in healthcare: A review," Procedia Computer Science, vol. 113, pp. 73 – 80, 2017, the 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017) / The 7th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2017) / Affiliated Workshops.

[3] N. Kahani, K. Elgazzar, and J. R. Cordy, "Authentication and access control in e-health systems in the cloud," in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security ril 2016, pp. 13–23.

[4] Christo MS, Meenakshi S. Enhancing security properties of Rumor Riding protocol under various attacks scenario in P2P network. In2016 International Conference on Communication and Signal Processing (ICCSP) 2016 Apr 6 (pp. 1130-1135).

[5] Christo, M.S. and Meenakshi, S., 2018. Enhancing Rumor Riding protocol in P2P network with Cryptographic puzzle through challenge question method. Computers & Electrical Engineering, 65, pp.122-138.

[6] Christo, M.S. and Rathinam, J.J., 2018, April. Enhancing Authenticated Intermediate Node in Rumor Riding Protocol. In 2018 International Conference on Communication and Signal Processing (ICCSP) (pp. 0023-0027). IEEE..

[7] F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust C. Esposito, A. D. Santis, G. Tortora, H. Chang, and K. K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, Jan 2018. S.P.Bingulac, "On the compatibility of adaptive controllers (Published Conference Proceedings style)," in Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory, New York, 1994, pp. 8–16.

[8] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralizedapps," in 2017 IEEE 19th International Conference one-Health Networking, Applications and Services (Healthcom),Oct 2017, pp. 1–4..

[9] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in 2016 IEEE 18th International Conferenceon e-Health Networking, Applications and Services (Healthcom),Sept 2016, pp. 1–3.G.W. Juette and L. E. Zeffanella, "Radio noise currents n short sections on bundle conductors (Presented Conference Paper style)," presented at the IEEE Summer power Meeting, Dallas, TX, June 22–27, 1990, Paper 90 SM 690-0 PWRS.

[10] W. Liu, S. Zhu, T. Mundie, and U. Krieger, "Advanced blockchain architecture for e-health systems," in e-Health Networking,Applications and Services (Healthcom), 2017 IEEE 19thInternational Conference on. IEEE, 2017, pp. 1–6..

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permissionmanagement," in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 25–30.

[12] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "Medshare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, vol. 5,pp. 14 757–14 767, 2017.IEEE Criteria for Class IE Electric Systems (Standards style), IEEE Standard 308, 1969.

[13] G.Wood,"Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp.1–32, 2014.

[14] M. Wohrer and U. Zdun, "Smart contracts: security patterns in the ethereum ecosystem and solidity," in Blockchain Oriented Software Engineering (IWBOSE), 2018 International Workshop on. IEEE, 2018, pp. 2–8.

[15] P. Zhang, J. White, D. C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability in blockchainbased healthcare apps," arXiv preprint arXiv:1706.03700,2017.

[16] Christo, Mary Subaja, S. Meenakshi, and R. Subhashini. "An intelligent fuzzy beta reputation model for securing information in P2P health care applications." (2017).

[17] Mary Subaja Christo, Anigo Merjora A, Partha Sarathy G, Priyanka C and Raj Kumari M. "An Efficient Data Security in Medical Report using Block Chain Technology in International Conference on Communication and Signal Processing, 2019"

BIOGRAPHIES

Ms. Parameswari Marimuthu is currently working as Assistant Professor in the Department of Computer Science Engineering in Dhirajlal Gandhi College of Technology, Salem. She obtained M.Tech and B.Tech (Information Technology) from Sona College of Technology, Salem, affiliated to Anna University, Chennai. Her current research interests include Image processing and Cryptography and Network Security.

Mr. Alwin Mathew is currently a Final Year Student in Departement of Computer Science Engineering in Dhirajlal Gandhi College of Technology, Salem, affiliated to Anna University, Chennai. His current intrerests include Data Analytics and Network Security.

Mr. Akhilesh Mani is currently a Final Year Student in Departement of Computer Science Engineering in Dhirajlal Gandhi College of Technology, Salem, affiliated to Anna University, Chennai. His current intrerests include Salesforce and Cloud Computing.

Mr. Aravind Narayanan is currently a Final Year Student in Departement of Computer Science Engineering in Dhirajlal Gandhi College of Technology, Salem, affiliated to Anna University, Chennai. His current intrerests include Data Security and Big Data.