IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EHR using Blockchain

[1]Abdul Rashid Reshamwala, [2]Sayed Heena , [3]Nadim Khatri,[4]Dr.Sampath A.K., [5]Dr.Varsha Shah

[1]Student, [2]Student,
[3]Student,[4]Professor, [5]Principal

[1]Computer Engineering,
[1]Rizvi College of Engineering, Mumbai, India.

Abstract: Medical data is one of the most sensitive types of data.Secure storage and making full use of personal medical records has always been a concern for the general population. The emergence of blockchain technology brings a new idea to solve this problem. The current way of sharing medical data is mostly done by physically transporting the document or sharing it online via email. These methods are prone to MTM (Man in the Middle) attacks where an unauthorized person might get access to medical records. Also in case if the transportation medium is compromised our data will also be compromised. Our solution is to develop a storage scheme to manage personal medical data based on blockchain and cloud storage. The system can be used by both patients and doctors.The patient can choose which report they want to share with the doctor. The Files would first be used by an OCR (optical Character Recognition) pass which will extract the important data from the files using keyword filtering .The data will then encrypted using AES which can only be decrypted with a special key which can only be used by the patient or doctor who is authorised by the patient.

The system would also have different analytical tools to help the doctor in recognizing different illnesses or take a second opinion. The system will have different endpoints through which they can avail different facilities such as Detection of pneumonia in chest x-rays.

Index Terms **- Medical, blockchain , MTM, cloud storage, patient, doctors, OCR, AES.**

I. INTRODUCTION

The current way of sharing medical data is mostly done by physically transporting the document or sharing it online via email. These methods are prone to MTM (Man in the Middle) attacks where an unauthorized person might get access to medical records. Also in case if the transportation medium is compromised our data will also be compromised.So,for the security reason the the Files would first be used by an OCR (optical Character Recognition) pass which will extract the important data from the files using keyword filtering .The data will then encrypted using AES which can only be decrypted with a special key which can only be used by the patient or doctor who is authorised by the patient. The foundational design of electronic healthcare records (EHRs) failed to anticipate the need for the management of multi-institutional, lifetime healthcare records. The regular change of healthcare providers renders patient data sparsely trailed across numerous sources. Consequently, patients often lack easy access to their historic data, while providers retain primary ownership. Defining healthcare data exchange mechanisms and pathways is particularly challenging, but promises highly positive feedbacks for healthcare system operations and medical research . Privacy concerns are ubiquitous among healthcare institutions and are often the main driver for their closed-data policies , along with the threat of data disclosure to their competitive advantage . In addition to privacy concerns, the required technical infrastructure poses a challenge considering the large Youssef Wehbe is with the Department of Civil Infrastructure and Environmental Engineering, Khalifa University of Science and disparities in the field. The evident lack of coordination among stakeholders involved in healthcare record transactions is the primary driver for their fragmentation and devaluation . Healthcare record data is the primary source of information and the foundation for medical research. Ekblaw et al.

.

II. EXISTED DESIGNS

2.1. Survey Existing system:

In this section of existing system survey, we have highlight the various attempts which was made to safeguard the health records, its challenges, and the possible solutions.

a) Towards using the Blockchain technology for eHealth data access management: In the paper we found entitled ”Towards using Blockchain technology for e-Health data access management”

The authors had highlighted the benefits and importance of Blockchain and the specific problems which are associated with it that helps for the secure deployment of the health record and it also provides a scalable solution in order to obtain the best

performance and results. They have also proposed an important architecture to address-Health application relations challenges where Doctors and hospitals are considered as nodes which are also connected to the eHealth Blockchain with the smart contract even an off-chain database is also maintained. Patient's can also interact with the Blockchain and medical sensors through the data gateway. This paper which is to be published also proves that with the use of correct tools, models, protocols and the Blockchain technology may fully functional systems are yet to be implemented to
revolutionized the future applications.

b) Decentralized the e-Health Architecture for boosting health-care Analytics: In this paper titled" Decentralized e-Health Architecture for boosting Healthcare Analytics" authors have
It also summarised the problem which is integrated and designated with the analysis and include security of medical data. They have also tried to provide a solution that improves the quality of medical services. They have proposed and generated a Blockchain solution for state-scale in healthcare which is also based on the Exonum framework, which consists of nodes connected through peer-to-peer connections and where all nodes are authenticated by using the public key. They have also told that Blockchain will be used to deal with very large volumes of clinical data and also to maintain the security, confidentiality of medical data. There is one more advantage is Blockchain can be used to create a data-based market where the patients will get a data monitoring tool through which they can participate in medical analytics and if they provide their data to the medical institution, research institutions they can even get rewards.

c) Blockchain technology: Is this the solution to our research EMR interoperability and security issues in developing countries: The paper " Is this the solution to EMR interoperability and security issues in developing countries" tells and conclude that the use of Blockchain in EMR safeguards continuous availability and access to real-time data. Taking the case study of EMR in Kenya, the authors have discussed the existing method of maintaining the health record and they have highlighted the importance of Blockchain technology as it increases the interoperability and security of the system. Blockchain helps the patient to have full access to the data and control on how data is shared. Further Blockchain depends on cryptographic
Proceedings of the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019) IEEE Xplore Part Number: CFP19J32-ART; ISBN: 978-1-5386-9439-8
978-1-5386-9439-8/19/$31.00 ©2019 IEEE 1412 techniques to interact in a network without pre-existing trust between the parties.. When the patient's information is passed between stakeholders, the patients' privacy is preserved because of the encryption of information.

d) Introducing Blockchain for Healthcare: In the paper titled "Introducing Blockchain for Healthcare," the authors have focussed on different Blockchain structures, existing of various challenges of Blockchain and there possible solutions. Even though Blockchain is used to create smart contracts and many more between healthcare providers and to provide access to certain data or patient records there arises a problem that who is accessing the data and the person who is accessing is authorized to do so or not. One more security issue is Sybil attack which can be solved by forcing each of the miner nodes to involve themselves in solving a mathematical problem before a new block is added to Blockchain by the attacker [7]. Another issue is the inference of private and secure data because of these issues the author and researcher have suggested the scientists come up with new architecture design for Blockchain which does not rely on a current cryptographic algorithm.

.

III. LIMITATION OF EXISTING SYSTEMS

A systematic literature review which also facilitates the identification of numerous challenges and limitations alongside the disadvantages of adopting or using blockchain technology, particularly in our healthcare domain. The research gaps and
Future in which research directions are based on the identified challenges, limitations, and disadvantages Once the provider has a patient's data, they could possess it permanently by any other means, and it although the patient may not want it.
Patients who are not much aware of this new technology. Apparently, that there would be confusion on where the data would be stored and also who can have access to this private data.

IV. SYSTEM IMPLEMENTATION

The goal of our major project is to develop an automated advance system in which Blockchain could also reinvent the way patient's electronic health records are shared and also stored by providing safer and secure mechanisms for patient health information exchange of medical data in the healthcare and medical industry, by securing it over a decentralized peer-to-peer network.

3.1Designed Details

The system design would also have different analytical tools which would help the doctor in recognizing different types of illnesses or take second opinion. This system will have different endpoints through which they can avail different facilities such as Detection of pneumonia in chest x-rays.

Technologies:

Secure Encrypted Locker:

1.Ethereum Blockchain network for storage of keys

2.Solidity language for writing and managing smart contracts

3.Python for Backend

4.AES hashing algorithm for encryption

5.ReactJS for Front End

Hashing Scheme

1 . Finding way to secure the files using blockchain:

The solution we used is a 2 way encryption system where the files are first encrypted with a random key generated by our backend after that the key is then encrypted using a salt present on our backend and then sent to the server this allows us store the files on any cloud service without having to worry about giving access to any un authorized user.

Also we can make sure we never store any files in an un encrypted format

This allows us to store a large number of files without putting a lot of stress on the blockchain network

2. Extracting useful data from large and unorganized medical records:

To solve that issue we used a fine tuned version of bert trained specially on medical data which allows us to extract all references to medical conditions and drugs mentioned we find the Medical Subject Headings (MeSH) id of the conditions which allows us to provide the patient with more information about the conditions and give an evaluation based on the report without need for any doctor

3. Providing users the complete control over their data:

We wanted to make sure the users have complete control over their data and our application follows all data privacy laws world-wide to do that all the data we store are anonymous in the following ways:

-> Before storing any information on our database we remove all personal information that may be present on the reports

->Providing users the choice to censor any data that they don't want to share

->Nobody (Not even the super admin) can view any data unless the user allows it

4. Removing the complexity from storing Blockchain based D' apps:

Most of the users would find the application experience if they have to manage their own personal keys or install 3rd part software like meta-mask to make our app work on all browsers we have custom made a blockchain wallet that handle all this for the user and many more could not added due to char limit

Smart disease detection:

1. Pytorch for implementing Machine learning algorithm.
2. OpenCV2 for Image processing.
3. Python (Flask) as Backend.
4. MongoDB for database.
5. ReactJS for Frontend.

The healthcare sector stands to benefit immensely from the blockchain technology due to security, privacy, confidentiality and decentralization. Nevertheless, the Electronic Health Record (EHR) systems face problems regarding data security, integrity and management.

To understand the blockchain architecture let us use the following figure 1 that explains the whole process of a transaction being send from a user on the blockchain network.

1.A new transaction being sent by a user on the blockchain network suggests that a new block is created. A block in the blockchain is used for keeping transactions in them and these blocks are distributed to all of the connected nodes in the network. That transaction placed inside a block is broadcasted to all of the nodes in the network. All the nodes in the network have a copy of the complete blockchain that helps them in verification process. When a block containing the user transaction is broadcasted to all of the connected nodes, they verify that the block is not tampered by any means. If this verification results in success then the nodes add that block in their own copy of blockchain.

2. This whole process of the block being added on the blockchain is done by the nodes reaching upon a consensus where they decide which blocks are valid to be added on the blockchain and which are not. This validation is performed by the connected nodes using some known algorithms to verify the transaction and to ensure that sender is an authenticated part of the network. When a node succeeds in performing the validation that node is rewarded with crypto-currency. This process of validating the transaction is known as mining and the node performing this validation is known as miner.

3. After validation is done that block is added to the blockchain.

4. After the whole process of validation is performed the transaction is completed.

.

3.2 Methodology

The systematic literature review is selected as the methodology of this study. The aim of the systematic literature review is identifying the previous research on the topic, which is blockchain for healthcare in our case, and then defining the research gaps and future research directions. We firstly identified two research questions:

1. What are the research topics that have been studied on blockchain in healthcare? Through scrutinizing all relevant papers in the literature, we built a comprehensive understanding of current research of blockchain in healthcare domain. We also mentioned applications of blockchain technology in healthcare to comprehend its current and potential impact.

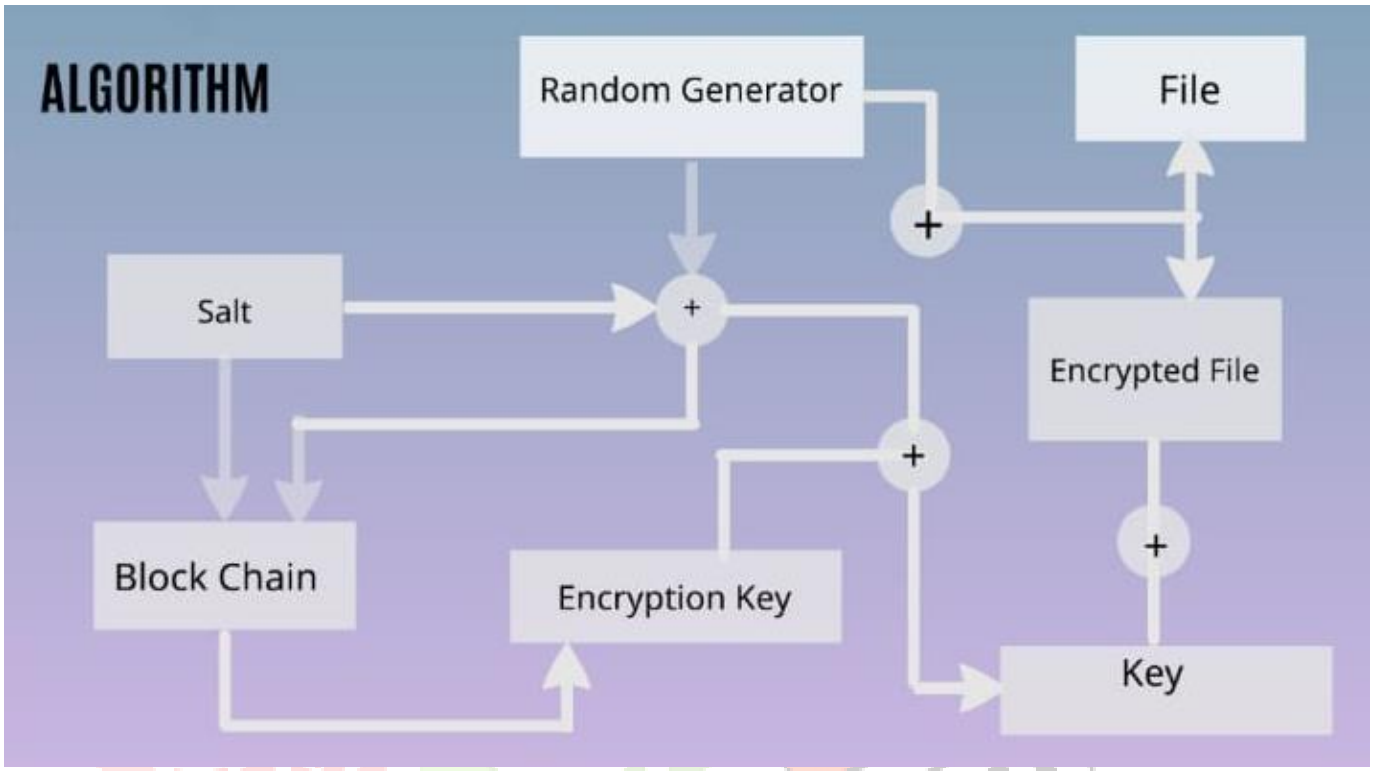
2. What are the research gaps and future research directions in blockchain technology in healthcare research?

A systematic literature review facilitates the identification of challenges and limitations alongside disadvantages of adopting blockchain technology, particularly in healthcare domain. The research gaps and future research directions are based on the identified challenges, limitations, and disadvantages.

This work is conducted using a systematic literature review methodology. A systematic literature review (often referred to as a systematic review) is a method for identifying, evaluating, and interpreting all available research that is relevant to a research question, topic area, or phenomenon of interest.[5] Most research begins with a literature review. However, unless a literature review is thorough and fair, it is of little scientific value. This is the main rationale for undertaking systematic reviews. A systematic review synthesizes existing work in a manner that is fair and is considered fair.

All reviewed articles in this systematic literature review were identified by searching reliable academic repositories such as PubMed, Google Scholar, ACM, Science Direct, and IEEE . These databases index research articles and abstracts from most major academic publishers and repositories worldwide, including both free and subscription sources

3.3 Algorithm



Step1: If User exist then go to step2.

Step2: Start the ChatBot process by acquiring information from the user.

Step3: Generate knowledge by interacting with user.

Step4: Compare the answer with data stored in database. If present then go to step5 else go to step2.

Step5: Process the information, learn, and recommend activities.

Step6: Send notification.

Step7: If review results then go to next step, otherwise go to step2.

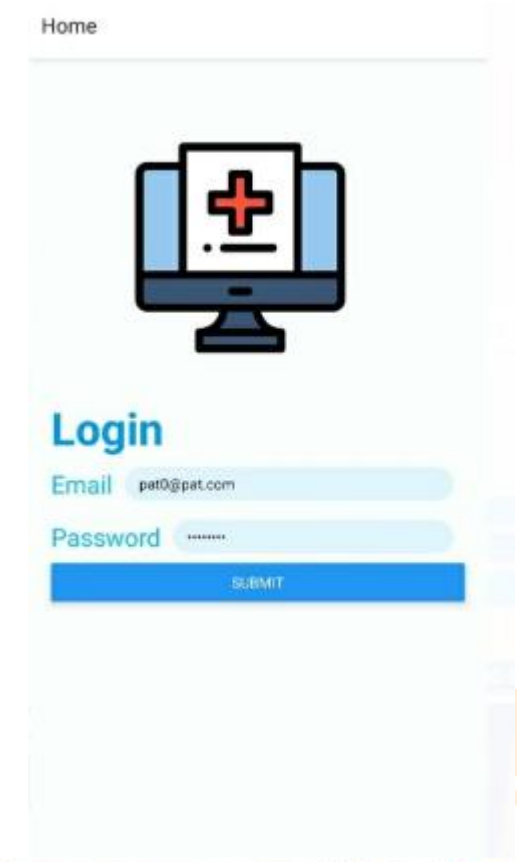
Step8: If user sends the keywords of ending conversation then stop and go to step1.

V. RESULTS AND OUTPUTS

5.1Report screen shows information about the report available

5.2Registeration and login screen

5.3Sharing documents with doctors by sharing QR code



VI. Conclusion

As an age old saying goes ”Health is Wealth” in the present scenario we can now consider in addition to health, health records are also wealth. So it is more important to keep our health records safe. The world has started moving towards patient-driven interoperability where patients provide the on- demand access to their health records. In this model, the patients is considered as the sole owner to his health records who would decide on sharing what data and with whom. This drift from an institute-driven to patient-driven comes with a bundle of challenges which are effectively addressed by Blockchain by

decentralizing the whole mechanism in contrast to the traditional way of data management. 200 health executives were interviewed by IBM's Institute for Business Value Blockchain, of which 16 percent of people are ready to deploy commercial Blockchain. As discussed above, Blockchain does not just help in decentralizing the data, it also gives the real-time data access, keeps the data confidential handles high volumes of data efficiently, and also authenticate and authorize the data.

The present study provides a preliminary framework to elicit the various complexities and interdependencies in the implementation of an AI-blockchain system for EHR management, specifically in the UAE context. CGM is shown to be a valuable tool in specifying, mapping, expounding, and altering complex system requirements. Five high-level intermediate goals are defined as: Enforcing Blockchain, Providing Tools, Increasing Security, Reducing Transaction Costs, and Increasing Interoperability, to satisfy the mandatory requirement of a successful EHR management system, along with a total of twenty-two tasks. Various non-functional requirements were also captured: New Jobs, Empowering Youth, Improved Public Health, Securing Immediate Family HRs, Reduced Transaction Time, while several others may be become evident with further refinement.

REFERENCES

1. Rifi, Nabil, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher."Toward using blockchain technology for eHealth data access man-agement." In 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME), pp. 1-4. IEEE, 2017.

2.Kotsiuba, Igor, Artem Velvkzhanin, Yury Yanovich, Iuna Skarga Ban-durova, Yuriy Dyachenko, and Viacheslav Zhygulin. "Decentralized e-Health Architecture for Boosting Healthcare Analytics." In 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), pp. 113-118. IEEE, 2018.

3.Kamau, Gabriel, Caroline Boore, Elizaphan Maina, and Stephen Njenga. "Blockchain Technology: Is this the Solution to EMR Interoperability and Security Issues in Developing Countries?." In 2018 IST-Africa Week Conference (IST-Africa), pp. Page-1. IEEE, 2018

4.Alhadhrami, Zainab, Salma Alghfeli, Mariam Alghfeli, Juhar Ahmed Abedlla, and Khaled Shuaib. "Introducing blockchains for healthcare." In 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), pp. 1-4. IEEE, 2017

5.Y. Ge, D. K. Ahn, B. Unde, H. D. Gage, and J. J. Carr, "Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations," Journal of the American Medical Informatics Association, vol. 20, pp. 157-163, 2013.

6. C. Clifton, M. Kantarcioğlu, A. Doan, G. Schadow, J. Vaidya, A. Elmagarmid, et al., "Privacy-preserving data integration and sharing," in Proceedings of the 9th ACM SIGMOD workshop on Research issues in data mining and knowledge discovery, 2004,
pp. 19-26.

7. J. R. Vest and L. D. Gamm, "Health information exchange: persistent challenges and new strategies," Journal of the American Medical Informatics Association, vol. 17, pp. 288-294, 2010.