CONFIDENTIAL HEALTH RECORD USING BLOCKCHAIN

Aishwarya L1, Hariprasad N1, Prathiksha P Desai1, Shashank D2

[1]Dept, of ISE, The National Institute of Engineering, Mysuru
[2]Asst, Professor, Dept., of ISE, The National Institute of Engineering, Mysuru

---***---

Abstract - With the conversion of ancient medical records, medical establishments encounter tough issues, like electronic health record storage and sharing. Patients and doctors pay substantial time querying the specified knowledge once accessing electronic health records, however the obtained knowledge don't seem to be essentially correct, and access is typically restricted. On this basis, this study proposes a medical knowledge sharing theme supported permissioned blockchains that use ciphertext-based attribute encoding to confirm knowledge confidentiality and access management of medical knowledge.

Under premise of guaranteeing patient identity privacy, a polynomial equation is employed to attain associate absolute association of keywords, then blockchain technology is combined. Additionally, the projected theme has keyword-in distinguishability against adaptive chosen keyword attacks beneath the random oracle model. Analysis shows that the theme has high retrieval potency.

Key Words: **Electronic health records, knowledge sharing, searchable attribute-based encoding, blockchain, cryptologic algorithms.**

1. INTRODUCTION

Digital Technology has drastically modified our daily lives and also the method of communication. Drugs is associate information-oriented entity. Maintaining paper-based records of patients within the attention organizations will become strenuous with time. Electronic health record (EHR) systems will fully modify the health care system that utilizes clinical data to assist suppliers deliver higher quality of care to their patients.

These edges were offered by Electronic Health Record (EHR) and Electronic medical history (EMR) systems. However, they still face some problems concerning the protection of medical records, user possession of knowledge, knowledge integrity etc. the answer to those problems may well be the utilization of a unique technology, i.e., Blockchain. This technology offers to produce a secure, temper-proof platform for storing medical records and different attention connected data.

When these records are outsourced on a public platform, then the task to secure these records will increase even a lot of. Therefore for such privacy to be maintained there ought pressing to take the specified measures to shield the health records by permitting solely licensed users to look at these records. Therefore here we have a tendency to are proposing knowledge classification encoding technique that's accustomed defend the records confidential knowledge.

2. BLOCKCHAIN TECHNOLOGY AND ITS DEPENDENCIES

Blockchain may be a chain of blocks that are connected along and are unceasingly growing by storing transactions on the blocks. This platform uses a redistributed approach that enables {the data the knowledge the knowledge} to be distributed which every bit of distributed information or normally called data have shared possession. Blockchains holds batches of transactions that are hashed so providing them security and that they are managed by peer-to-peer networks.

A blockchain has sure edges like security, anonymity, and integrity of knowledge with no third party intervention. These edges build it an inexpensive option to store patients medical records thereon, as a result of the innovation of technology within the attention trade has created the protection of patients medical knowledge a prime priority. Variety of researchers have conjointly known that victimization blockchain technology in attention would be a possible answer.

2.1 MODEL ARCHITECTURE

To understand the blockchain design allow us to use the subsequent figure one that explains the full method of a group action being send from a user on the blockchain network.

1. A brand new group action being sent by a user on the blockchain network suggests that a brand new block is made. A block within the blockchain is employed for keeping transactions within them and these blocks are distributed to all or any of the connected nodes in the network. That group action placed within a block is broadcasted to all or any of the nodes within the network.

2. This validation is performed by the connected nodes using some famous algorithms to verify the dealing associated to confirm that sender is a genuine a part of the network. Once a node succeeds in performing arts the validation that node is rewarded with crypto-currency.

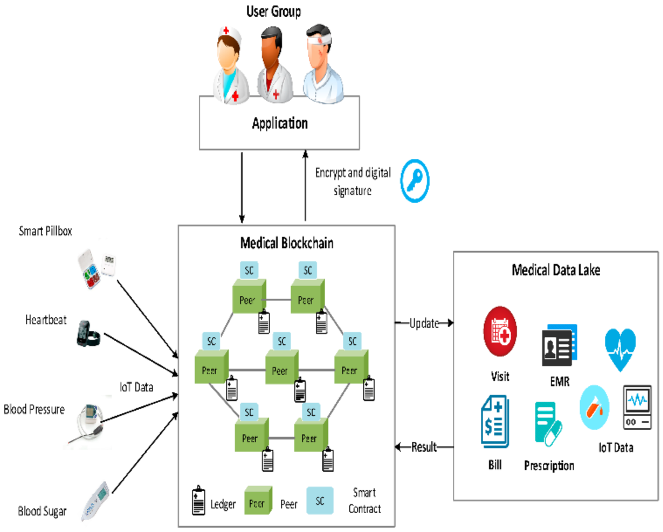


Fig 2.1: An over of blockchain Architecture

3. Once validation is finished that block is side to the blockchain.

4. Once the full method of validation is performed the dealing is completed.

3. PROPOSED SYSTEM

The objective of proposing a system for maintaining EHRs is to secure them before deploying them for sharing among health care suppliers. The projected system is predicated on the following:

1. A web-based system with secure login and registration.

2. Cloud storage for versatile retrieval and could be a possible various.

3. Information Classification and secret writing.

1. Web-based system with secure login and registration:

A web-based system is accessed anyplace, anytime with the assistance of fine net property. The system are designed in such some way that solely approved users to access the relevant data. Patients and doctors ought to 1st register. Once registration, they'll be a given a singular Key which will be employed by them to avail the knowledge.

2. Cloud Storage For Flexible Retrieval And Is A Feasible Alternative:

Cloud storage provides fast readying. It's bigger accessibility and responsible, conjointly information backup and disaster recovery is feasible. The storage prices square measure low as a result of there's no would like of buying, managing and maintaining big-ticket hardware that creates Cloud storage economically possible.

3. Data Classification and Encryption:

Classification are done on the premise of sensitivity levels of confidential medical data.

This will be done mistreatment numerous cryptologic techniques like (SHA) algorithmic program, Advanced secret writing (AES) algorithmic program to produce security to the information in step with their associated sensitivity level.

- AES, SHA for providing confidentiality.
- Hashing techniques like SHA-1, MD5 for integrity, e.g. passwords.
- For believability we have a tendency to propose digital signatures.
- Security for databases.
- Attainable elimination of various attacks like SQL Injection, Cross Side-Scripting, etc.

There square measure numerous crypto logical techniques obtainable and ever varies with relation to cryptography. Its optimum to cypher higher sensitive details with higher level of secret writing wherever concealment such data could be a major focus. Lower sensitive details of associate electronic like report time and date that become vital at some specific times is encrypted with the lower level of secret writing.

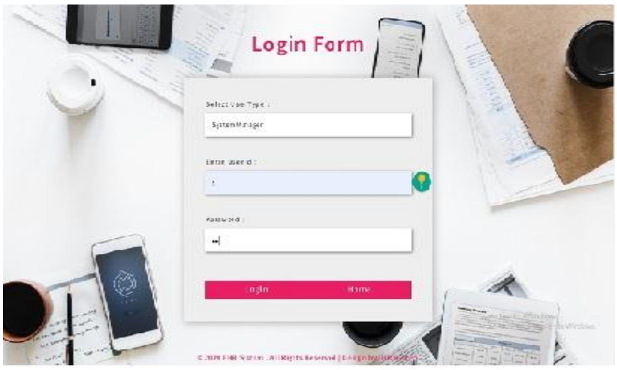
The system conjointly maintains privileges permission in step with the authority level of the user. To elucidate it merely a patient isn't allowed to update or produce records however a doctor will.

4. IMPLEMENTATION

The system permits the doctor to transfer the document so doctor is asked his secret key wherever the system uses this key beside the doctor and patient info to make a system generated key to write the document.

4.1. SYSTEM DESIGN

In the level one, the system manager can login and adds the hospital employees, doctors and checks for the authentication and access the data like manage department, manage hospitals manage, data user and patients details and once they retrieve they logout.



Login Form

Select User Type :
SystemManager

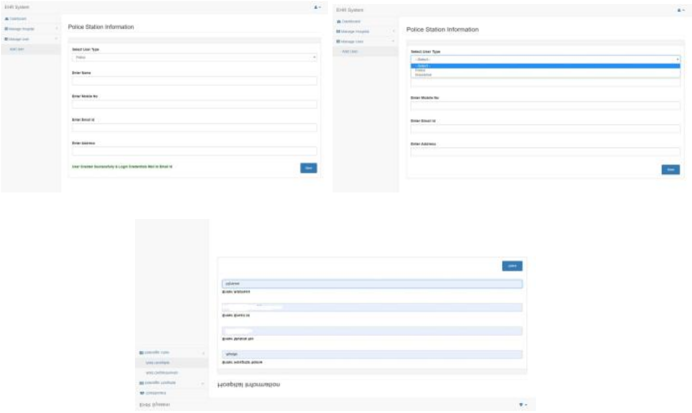
Enter User Id :

Password :

Login Home

Fig-2: login page of System manager

In the below fig the system manager, doctors, information user like police, insurance hospital employees will access the EHR system and manage concerning and look at and examine the patients details about their health record.



EHR System

Police Station Information

Select User Type

Enter Name

Enter Mobile No

Enter Email Id

Enter Address

Fig-3: system manager Dashboard

The EHRs to be keep on cloud, a cloud framework wants to be enforced for the projected system. The framework ought to give Platform as a Service (PaaS) so the complete system is deployed within the cloud itself. Cloud provides with multiple advantages that best suit the system to be enforced like straightforward sharing, reduces capital prices and provides flexibility. The cloud framework should give network resources, computing capabilities and a dashboard that helps the users to navigate through the system. The complete system is deployed on the cloud platform wherever the EHRs are often shared with ease and decode it likewise.

4.2. SYSTEM ARCHITECTURE

System style is that the very important most significant and vital a part of any framework because it is employed for the event of the system from its theory. This section includes the modules, design and varied parts that are combined.

Together to create the complete to create framework. As outlined earlier the aim behind this projected framework is to make such a decentralized system that's temper-proof, secure a confidential blockchain-based system for electronic health records.

The projected framework or system has 3 entities or modules. These modules once combined along would keep our system operating. These entities or modules have any ideas that require to be understood they're explained as follows.

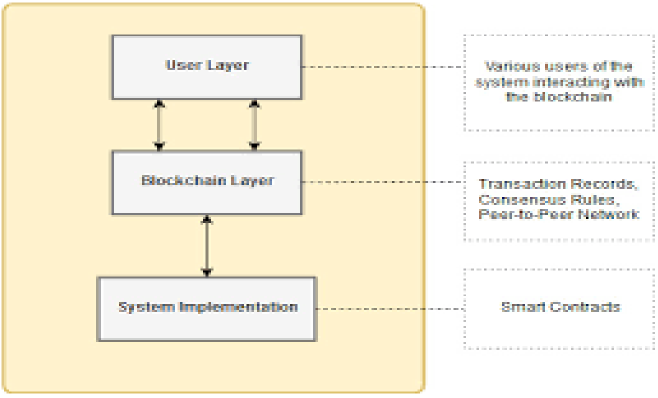

User Layer
Blockchain Layer
System Implementation
Various users of the system interacting with the blockchain
Transaction Records, Consensus Rules, Peer-to-Peer Network
Smart Contracts

Fig-4: System Style of Proposed Framework

In order to secure the patient's info from hacker's doctor id and patient's id are going to be hashed and that we generate a QR-code image and store this within the information. By victimization blockchain for every have received and if the generated QR-code is same then they will access the data concerning the patients. The dynamic table can contains patients name, age, gender, date of treatment .Each treatment outline is encrypted exploitation AES algorithmic rule and is keep as block within the info.

IF the patient's details has to be view by police insurance company then they create a hash value with the ids they have received and if the generated QR-code is same then they can access the information about the patients. The dynamic table will contains patients name, age, gender, date of treatment .Each treatment summary is encrypted using AES algorithm and is stored as block in the database.

5. CONCLUSION

Blockchain technology holds high promise of being a wide adopted mechanism within the tending system for partitioning problems that have long involved the trade. At an equivalent time, there square measure several square measures of blockchain that are comparatively untested in a very tending surroundings, like the requirement for a service level agreement, viability of privacy, quantify ability of a system to handle massive numbers of participants, management and restrictions around access to patient knowledge, and problems with patient record possession.

Despite its tremendous potential, tending systems ought to be cautiously optimistic relating to blockchain technology and maintain a healthy skepticism toward the plug close it these days. As tending systems commence securing and digitizing their infrastructure, they ought to concentrate on introducing novel clinical call support systems exploitation analytics and AI.

REFERENCE

[1] Fernández-Alemán, José Luis et al. ,"Security and privacy in electronic health records: A systematic literature review" in Journal of Biomedical Informatics , Volume 46 , Issue 3 , 541 – 562.

[2] R. Wu , G.-J. Ahn and H. Hu , "Secure sharing of electronic health records in clouds" , Proc. 8th IEEE Int. Conf. Collaborative Comput., Netw., Appl. Work-sharing , pp.711 - 718 , October 2012.

[3] JPC Rodrigues J, de la Torre I, Fernández G, López-Coronado M,, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," Journal of medical Internet research, vol. 15, no. 8, 2013.

[4] R. Zhang and L. Liu, "Security Models and Requirements for Healthcare Application Clouds," in Proc of CLOUD '10. IEEE, 2010, pp. 268-275.

[5] T. D. Gunter and N. P. Terry, “The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions,” J. Med. Internet Res., vol. 7, no. 1, pp. e3–e3, Mar. 2005.

[6] C. Pirtle and J. Ehrenfeld, “Blockchain for Healthcare: The Next Generation of Medical Records?,” J. Med. Syst., vol. 42, no. 9, p. 172, Aug. 2018.

[7] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, “Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Pers.

[8] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” J. Am. Med. Informatics Assoc., vol. 24, no. 6, pp. 1211– 1220, 2017.

[9] A. Boonstra, A. Versluis, and J. F. J. Vos, “Implementing electronic health records in hospitals: a systematic literature review,” BMC Health Serv. Res., vol. 14, no. 1, p. 370, Sep. 2014.