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

BLOCKCHAIN FOR MEDICAL DATA ACCESS AND PERMISSION MANAGEMENT

Dhananjayan D[1*], Abhilash L[2], Ajay V[3], Thenmozhi R[4]

[1,2,3]UG Students, Department of Information Technology, SRM Valliammai Engineering College, Kancheepuram, Tamil Nadu, India
[4]Assistant Professor, Department of Information Technology, SRM Valliammai Engineering College, Kancheepuram, Tamil Nadu, India

---

Abstract - *The repeated administrations are a data concentrated space where a great deal of data is made, dissipated, set away, and got to step by step. For example, data is made when a patient encounters a couple of tests (for instance mechanized tomography or modernized center point tomography checks), and the data will require to be scattered to the radiographer and after that a specialist. The outcomes of the visit will be set away at the recuperating office, which ought to be gotten to at a later time by a specialist in another recuperating office inside the framework. Indisputably development can expect a basic occupation in enhancing the idea of thought for patients (for instance using data examination to settle on taught restorative decisions) and possibly decline costs by more capably assigning resources in regards to workforce, equip, etc. For example, data captured fit as a fiddle is hard to get in structures (for instance extravagant and data segment goofs), costly to account, and being available when required. These troubles may incite helpful decisions not made with complete information, the prerequisite for repeated tests in view of missing information or data being secured in another recuperating focus at a substitute state or country (at the expenses of growing costs and weight for the patients, etc. On account of the possibility of the business, ensuring the security, security, and trustworthiness of human administrations data is crucial. This highlights the necessity for a sound moreover, secure data the board system.*

Key Words*: *Tomography, Radiographer, Recurperating Office, Specialist, data segment, prerequisites

1. INTRODUCTION

Generally, Electronic Medical Records (EMRs) contain helpful and clinical data related to a given patient and away by the careful social protection supplier. They support the recuperation and examination of social protection data. To all the more promptly reinforce the organization of EMRs, early periods of Wellbeing Information Systems are arranged with the ability to make new EMR models, store them, and request and recoup set away EMRs of intrigue. They can be respectably fundamental game plans, which can be schematically depicted as a graphical UI or a web advantage. These are ordinarily the front-end with a database at the back-end, in a joined or scattered utilization. With patient transportability (both inside and remotely to a given country) being continuously the standard in the present society, it ended up obvious that various free EMR courses of action must be made interoperable to energize sharing of social protection data among different providers, even over national edges, as required. For example, in helpful, the movement business focus focuses, for instance, Singapore, the requirement for continuous social protection data sharing between different providers and across over nation's advances toward winding up logically explained.

To empower data sharing or even patient data adaptability, there is a fundamental for EMRs to formalize their data structure and the approach of HIS. Electronic Health Records (EHRs), for example, are proposed to empower understanding recuperating history to move with the patient or be made open to different human associations providers (for instance from a trademark helpful concentration to a crisis office in the capital city of the country, before the patient outputs for medicinal thought at another restorative concentration in a substitute country).3 EHRs have a more uncommon data structure than EMRs. There have in like way been exercises to develop HIS and structures that can scale and brace future needs, as authenticated by the contrasting national what's progressive, by and large exercises, for instance, the Fascicule Sanitaria Electronica (FSE) involvement in Italy, the epos involvement in Europe, and a reliable assignment to oversee sharing of EHRs.4,5,6 Starting late, the conviction of great contraptions (for instance Android and is devices and wearable devices) has other than comprehended an adjustment in perspective inside the government disability industry.7 Such contraptions can be customer had or presented by the social affirmation provider to survey the succeeding of the customers (for instance patients) and train/enable medicinal treatment and seeing of patients. For example, there is a wide level of adaptable (applications) in progress, flourishing, weight decay, and other government managed savings related classes. These applications generally fill in as the following instrument; for instance, choosing the customer works out/works out, keeping the check of ate up calories, and grouped bits of learning (for instance number of steps taken, and so forth.

There are in like way contraptions with installed sensors for further made solid errands, for example, wrist knickknacks to assess heartbeat amidst exercises, or contraptions for self-testing of glucose. For instance, Leo and accessories proposed a telephone-based remote body sensor system to store client physiological information utilizing body sensors

inserted in a watchful shirt.8 The information (for example client's major signs) can be dependably gathered and sent dependably to a sharp contraption, before being sent to a remote human affiliations cloud for further examination. Another model is Ambient Assisted Living philosophies for human affiliations expected to see creative telehealth and telemedicine affiliations, all together to give remote individual flourishing checking.

1.1 OBJECTIVE

Social insurance is an information serious area where a lot of information is made, scattered, put away, and got to day by day. For instance, information is made when a patient experiences a few tests (for example electronic tomography or automated hub tomography examines), and the information will require to be dispersed to the radiographer and afterward a doctor. The aftereffects of the visit will at that point be put away at the emergency clinic, maybe which ought to be gotten to at a later time by a doctor in another medical clinic inside the system. Innovation can assume a huge job in upgrading the nature of consideration for patients (for example utilizing information investigation to settle on educated therapeutic choices) and conceivably diminish costs by more productively apportioning assets as far as a workforce, gear, and so on.

1.2 BENEFITS

The System has been designed from a user-friendly perspective where the data can be shared everywhere. The patient should not worry about their medical data which can be securely stored in the cloud. Data can't be accessed without prior health care's permission. If any patient is away from their health care, their data can be accessed through the cloud.

1.3 CHALLENGES

Problems imposed by patient mobility are the availability of medical data related to the patient at a secondary care hospital-based physician for clinical analysis, specialist referrals and/or surgeries. Typically, healthcare providers are interconnected by means of the so, called Health Information Systems (HIS) allowing them to exchange medical data. However, the size of current HIS is limited to a set of the hospital or a given region, and the common practice is that patient-related medical data are not available at the healthcare provider gets contacted by the patient to receive secondary care allowing them to exchange medical data.

2. LITRATURE SURVEY

The Systems have encountered many reference papers, this work enabled to understand the process of sharing a medical data in an efficient way.

[1] Raija Halogen, "Wishes for wearables from patients with migraine Research full-length paper", September 2018

Migraine Association and was aimed at identifying migraine patients with pre-symptoms and whether they would be willing to use wearable sensors to detect pre-symptoms. The survey received responses from 565 persons, 90% of whom were willing to use wearable sensors to measure pre-symptoms and support treatment.

[2] Mehmet Saliva, "Functionality of hospital information systems: Results from a survey of quality directors at Turkish hospitals.", December 2018

We surveyed quality directors (QDs) at civilian hospitals in the nation of Turkey. Data were collected via web survey using an instrument with 50 items describing core functionality of HIS. We calculated mean availability of each function, mean and median values of perceived impact on quality, and we investigated the relationship between availability and perceived importance.

[3] Mehrdad Farzandipour, "Usability Evaluation of Three Admission and Medical Records Subsystems Integrated into Nationwide Hospital Information Systems: Heuristic Evaluation", June 2018

Introduction Usability is one of the quality criteria for information systems and its weakness is one of the main barriers to the adoption of these systems. The purpose of this study was to evaluate the usability of admission and medical records module of three widely used hospital information systems (HISs).

[4] Kabiru Dalai Garb, "Significance and challenges of medical records: a systematic literature review", June 2018

They support clinical decision-making, provide evidence of policies and support the hospitals in cases of litigation but despite the above importance of medical records, the challenges affecting the medicals records such as storage, access, safety and security are keenly identified and enumerated.

3. MODULE DESCRIPTION

(i) USER INTERFACE MODULE

In this Module, new user can register and existing user can login to the application. The user need to enter the following details to register the hospital, Hospital Name, E-Mail, Password & Confirm Password.

(ii) CLOUD MODULE

In this module, the list of medical data which has been uploaded by the health care has been displayed. The Required data can be searched from the list.

(iii) FILE REQUEST MODULE

As per the name, the request has been given for the required medical data. The Request will be stored in provider's Inbox.

(iv) UPLOAD MODULE

In this module, medical data has been encrypted using AES – 128 algorithm and then securely uploaded iin the cloud.

(v) DOWNLOAD MODULE

In this module, the requested file has been sent with the file key. By using the key, we can decrypt the data and download the file.

4. SYSTEM DESIGN

The User Interface is created using JSP, HTML, Bootstrap and java language is used. The Backend process is done by using MySQL.

4.1 ARCHITECTURAL DESIGN

The Proposed system consist of five modules, in which the user interface module can be used to authenticate into the system. For Register purpose, initially A CSP Key (Customer Service Provider) has been generated. Followed by their credentials (Hospital Name, E-Mail, Password & Confirm Password). Login can be done by entering Hospital Name & password to authenticate into the application. After authentication, home page has been displayed in which upload module is present where we can upload the medical data into the cloud. By Clicking inbox tab, the list of requests given to the hospital has been displayed. In Download Module, if the request has been accepted by the provider health care, that particular data will be displayed along with it's file key.

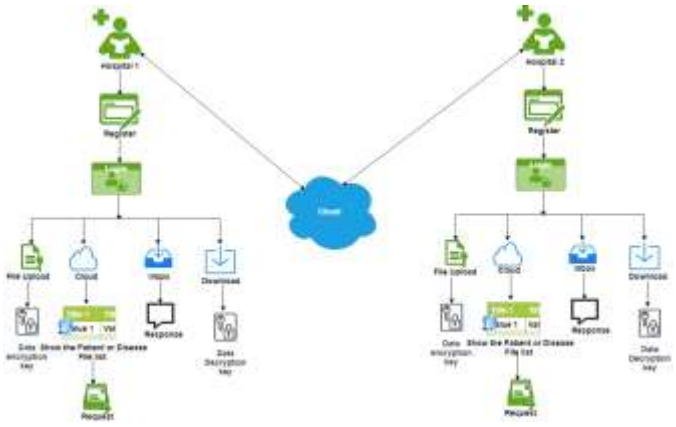

Fig -1: Architecture Diagram

4.2 PROPOSED METHOD

In the existing structure to beat that issue server will be kept up a normal database. So as a facility the officials first have to select with the customer singular nuances while enrolling time for each and every customer while enrolling time they can get CSP key for each and every customer normally while enrolling time they can get CSP key. After that, they can log in with user credentials and they can exchange that all data related to treatment and ailment and how to deal with that issue everything will be exchanged while exchanging time server will give a security to that archive by using of AES figuring so the record is secured in the database. So, a comparative substance will see each and every customer if the individual is related to that account server. So in case, they require the course of action about that disease they can pick that disease and send the interest adversary that illumination archive then that related to that record request will go to the stress crisis center in case the restorative facility recognize that request, only that customer can get that record and report key. If that facility required the passageway that records, they have to enter that customer CSP key it will confirm in case it was correct or not if it was certified, they will ask regarding whether two keys were comfortable point archives as a customer they can download.

AES ALOGRITHM

In Upload Module, file uploading into the cloud has been encrypted. In this system, AES – 128bit key Encryption has been used. While uploading the file key will be generated in order to decrypt the data.

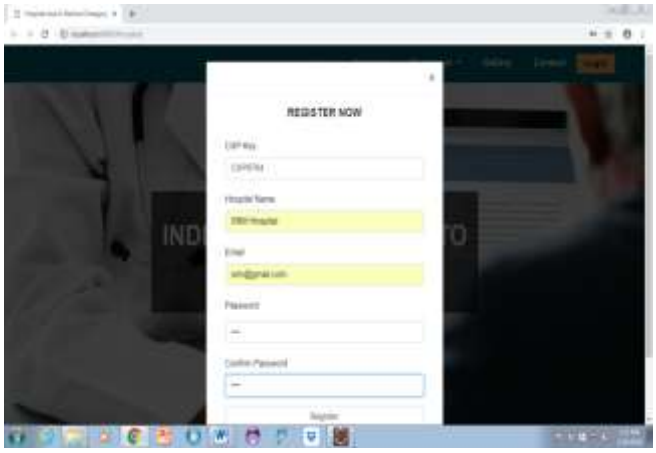

Fig – 2: User Interface Module – Register

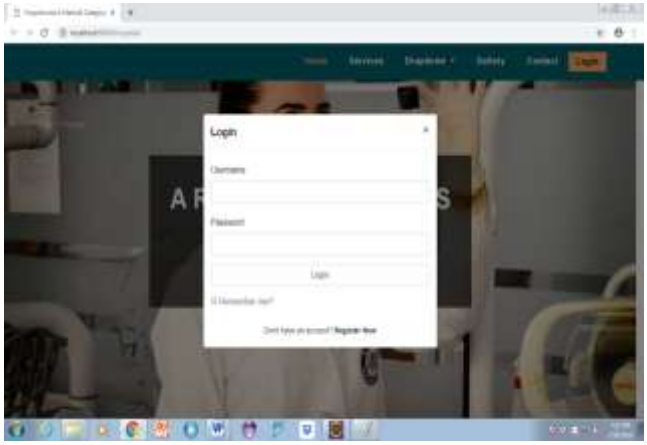

Fig – 3: User Interface Module – Login

Fig – 4: Upload Module

Fig – 5: Cloud Module and File Request Module

Fig – 6: File Request Module

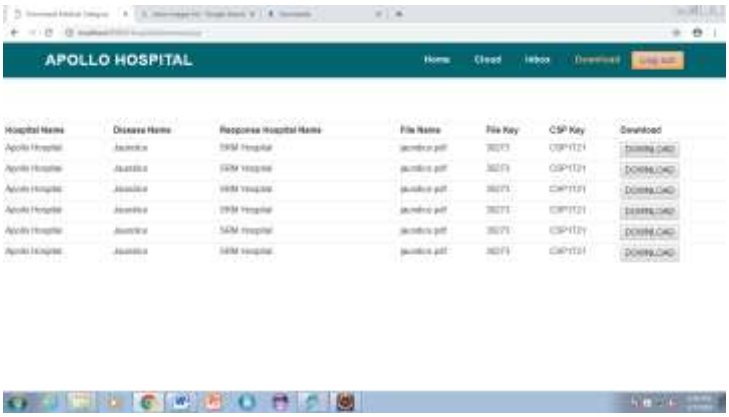

Fig – 7: Download Module

5. CONCLUSION

While data integrity and distributed storage/access of blockchain offer opportunities for healthcare data management, these same features also pose challenges that need further study. The strong data integrity feature of blockchain results in immutability that any data, once stored in the blockchain, cannot be altered or deleted. However, if the record is healthcare data, then such personal data would come under the protection of privacy laws, many of them would not allow personal data to be kept perpetually—Article 17 of the soon-enforceable General Data Protection Regulation in the EU has strengthened the rights of individuals to request personal data to be erased. One of the principles of the Organization for Economic Cooperation and Development privacy guideline, on which many data protection laws are based, provides the right-to-erasure to individuals. Given the sensitivity of healthcare data, anyone getting to use blockchain to store them cannot ignore this legal obligation to erase personal data if warranted. Another practical issue is how to fit it is for blockchain to store healthcare data. Blockchain was originally designed to record transaction data, which is relatively small in size and linear. In other words, one only concerns itself about whether the current transaction can be traced back to the original "deal". Healthcare data, such as imaging and treatment plans, however, can be large and relational that

require searching. How well blockchain storage can deal with both requirements is currently unclear. In order to affect these challenges, many have suggested the notion of off-chain storage of knowledge, where data is kept outside of blockchain during a conventional or a distributed database, but the hashes of the data are stored in the blockchain. This is said to be the simplest of both worlds, as healthcare data is stored off-chain and should be secured, corrected, and erased as appropriate. At the same time, immutable hashes of the healthcare data are stored on-chain for checking the authenticity and accuracy of the off-chain medical records. This idea, however, is not without potential challenges. With the tightening of data protection laws around the world and the attempts by privacy commissioners to regard metadata of personal data as personal data, it may not be very long that hashes of personal data are considered as personal data; then the whole debate of whether blockchain is fit to store personal data may start all over again.

5.1 Future Enhancement

My future work depend upon my traditional approach is to implement real time blockchain. For that, Hyperledger Sawtooth has been used in order to make a permission blockchain for medical data sharing. Virtual Machine has to be created for every hospital, which can be achieved by using cloud service either Amazon Web Service (AWS) or Microsoft's Azure or other cloud platforms. A blockchain network has been created using Hyperledger Sawtooth. Docker has to be used to pack the application and run in the container (for example., In a cloud based Virtual Machine), can be achieved using Kubernetes. Each Node has been developed using node.js and each block has been configured using either java or Go. The Major advantages of the Hyperledger sawtooth blockchain is immutable, decentralized and permissioned access of data.

REFERENCES

[1]. S.H. Han et al., —Implementation of Medical Information Exchange System Based on EHR Standard,‖ Healthcare Informatics Research, vol. 16, no. 4, 2010, pp. 281–289

[2]. Q.Alam et al., —A Cross Tenant Access Control (CTAC) Model for Cloud Computing: Formal Specification and Verification,‖ IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, 2017, pp. 1259–1268

[3]. J. Zhang, N. Xue, and X. Huang, — A Secure System for Pervasive Social NetworkBased Healthcare,‖ IEEE Access, vol. 4, 2016, pp. 9239–9250.