International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Securing Electronic Health Records using Blockchain

Pooja B[1], Aishwarya C[1], Divyashree S[1], Srinidhi Kulkarni[2]

[1]*Dept of CSE, Jyothy Institute of Technology, Bangalore, Karnataka, India*
[2]*Assistant Professor, Dept of CSE, Jyothy Institute of Technology, Bangalore, Karnataka, India*

Abstract - *Electronic Health Records (EHRs) are completely constrained by clinics rather than patients, which entangles looking for therapeutic advice from various emergency clinics. Patients face a basic need to concentrate on the subtleties of their own social insurance and re-establish the board of their own medicinal information. The fast advancement of blockchain innovation advances populace social insurance, including therapeutic records just as patient-related information. This innovation gives patients complete, permanent records, and access to EHRs free from specialist organizations and treatment sites. In this paper, to ensure the legitimacy of EHRs embodied in blockchain, we present a characteristic based mark conspire with numerous experts, wherein a patient supports a message as per the property while uncovering no data other than the proof that he has borne witness to it. Besides, there are various experts without a confided in single or focal one to create and circulate open/private keys of the patient, which keeps away from the escrow issue and fits in with the method of disseminated information stockpiling in the blockchain. By sharing the mystery pseudorandom work seeds among specialists, this convention opposes intrigue assault out of N from N −1 adulterated experts*.

***Key Words*: Blockchain, EHRs, Security, ABS**

1. INTRODUCTION

Electronic Health Records (EHRs) give an advantageous wellbeing record stockpiling administration, which advances conventional patient medicinal records on paper to be electronically available on the web. This framework was intended to enable patients to have the control of producing, overseeing and sharing EHRs with family, companions, human services suppliers and other approved information buyers. Also, gave that the human services analyst and suppliers of such administration get to these EHRs over the on board, the progress program of social insurance arrangement is relied upon to be accomplished. However, in the present circumstance, patients disperse their EHRs over the various territories amid life occasions, making the EHRs move starting with one specialist organization database then onto the next. Hence, the patient may lose control of the current medicinal services information, while the specialist organization more often than not keeps up the essential stewardship. Patient access consents to EHRs are restricted, and patients are normally unfit to effectively impart this information to scientists or suppliers. Interoperability challenges between various suppliers, medical clinics, look into foundations, and so forth add additional obstructions to superior information sharing. Without facilitated information the board and trade, the wellbeing records are divided rather than firm.

Already, numerous limitations have been put on sharing enormous EHRs on account of the dangers to information security or spillage of private patient data amid information trade. Moreover, current EHRs are overseen by emergency clinics and suppliers, while patients are denied of the privilege to openly control their own EHRs. Through using blockchain innovation, guidelines for account information and overseeing character are built up, and the blockchain of EHRs is developed. Moreover, this innovation records the examining hints of all exchanges in a permanent dispersed record, which ensures duty and straightforwardness in the parade of information trade. Along these lines, the patient can record social insurance and demonstrative data from specialists in their very own EHRs, consequently diminishing the quantity of therapeutic mishaps and saving patient protection.

2. BLOCKCHAIN

Blockchain is simply growing list of records named blocks which are connected via cryptography

Blockchain innovation was in the past created for the cryptographic money Bitcoin and was first exhibited in the Bit-coin whitepaper by Nakamoto in 2008. Since blockchain innovation showed up, it has been commended as another mechanical upheaval simply like the development of the steam motor or the Internet in view of its tremendous impaction on society

Blockchain innovation empowers conveyed open records that hold changeless information in a protected and scrambled way and guarantee that exchanges can never be adjusted. While Bitcoin and different digital forms of money are the most well-

known instances of blockchain use, this "appropriated record innovation" (DLT) is finding a wide scope of employment. Information stockpiling, money related exchanges, land, resource the board and a lot more users are being investigated.

Each block contains 4 components namely current hash, previous hash, timestamp and nonce.

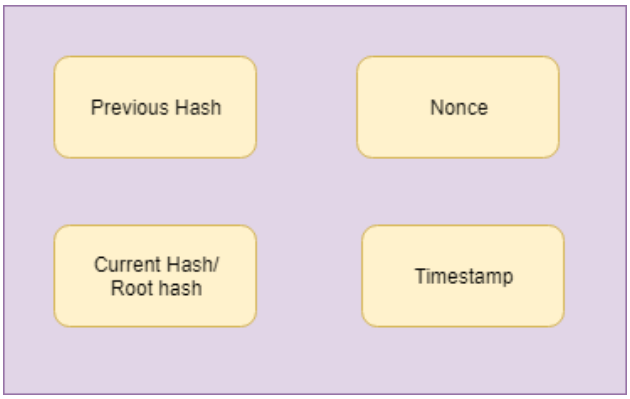

Fig -1: Block

According to Survey, all things considered, each mark has explicit characteristics. Mark is important to meet certain criteria that are journalist to traits. Gathering marks where any individual from a group can be benefit for any another individual from a group. For an occurrence, if Alice needs a mark from a worker of Bob's organization and if the important individual is missing, in some other individual from the sway's organization can sign thusly abgs works. In this plan expulsion of a part from a gathering is empowered or evacuation of a portion of the client's properties is conceivable. Already [1], ABGS appeared however it couldn't disavow. ABGS was acquainted with incorporate traits in a gathering mark plot [2].

3. SYSTEM DESIGN

EHRs has mainly 4 actors

i. Admin
ii. Data Owner
iii. User
iv. Auditor

Each actor has their own preference and functions.

Functionalities of Admin are Login, Profile(View Profile, Edit Profile, Change Password), Auditor List, View Auditor ,Add Auditor, Update Auditor, Data Owner, View data owner, Add data owner, Update Data owner, Key Generation via RSA algorithm, Department(Attribute I),Designation(Attribute II) And Logout.

Functionalities of Data Owner are Login, Profile(View Profile, Edit Profile, Change Password), Add Users, View data owner, Add data owner, Update Data owner, File Upload, View Details, File Access Control, Control File Access Control, View File Access Control, Transaction history, and Logout.

Functionalities of User are Login, Profile Management, File Download, Transaction, Send Request and Logout.

Functionalities of auditor are profile management and verification.

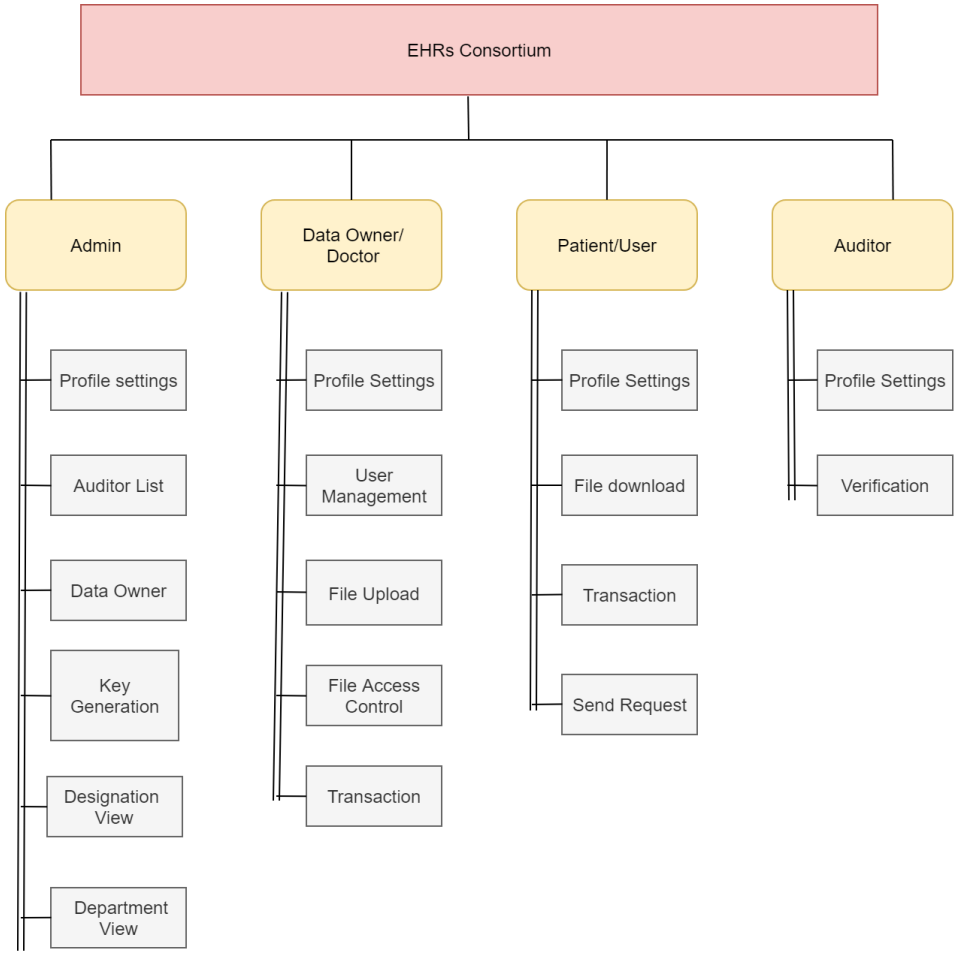

Fig -2: System Design

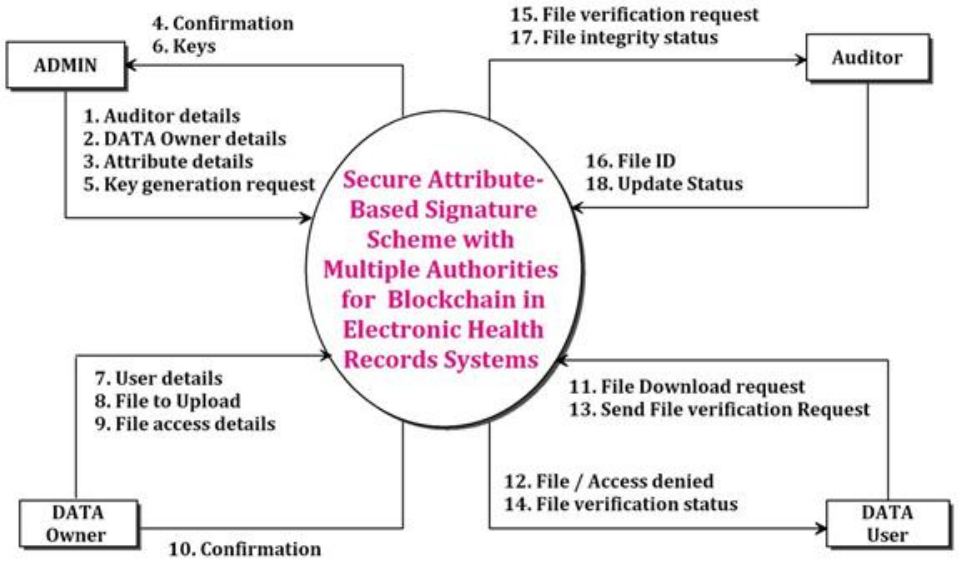

Fig -3: Context Analysis

4. METHODOLOGY

4.1 File Transfer

In this process, select a document and exchange that record to the server. The server gets every one of the subtleties and creates a Message Digest, when MD record is produced it recovers all the open key has a place with the client bunch i.e.(MD+Public key) creates a protected MD, Encrypt secure MD with client Private keys and produces Ring-Signature and send a mail to all clients.

Fig - 4: File Transfer Process

4.2 Block Creation Process

The block contains four elements.

i. Root hash is generated with the help of the SHA-1 algorithm.

ii. The previous Block hashtag is picked from the metadata table.

iii. The timestamp is a time the block is getting created.

iv. The nonce is generated with the help of a random generator.

The above four elements are packed as header and encrypted and later compressed which is stored in the cloud.

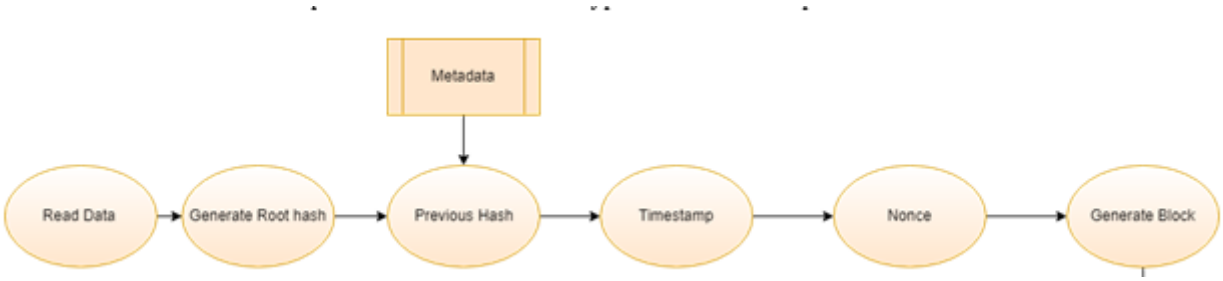

Fig - 5: Block Creation Process

4.3 File Download Process

The client needs to initially choose the record to be downloaded and keys must be inputted to pick up the entrance. On the off chance that keys are legitimate, get to is conceded else informs the client to enter appropriate keys. On the off chance that gets to is picked up, square id and metadata are acquired from the document. At that point, the square is downloaded from the cloud and uncompressed as squares are packed and put away in the cloud. The uncompressed square is unscrambled and the record gets downloaded in the client's framework. Once the download is finished, an affirmation message gets showed.

The Key is sent via mail to user. Each user is sent a private key without which the file cannot be downloaded.

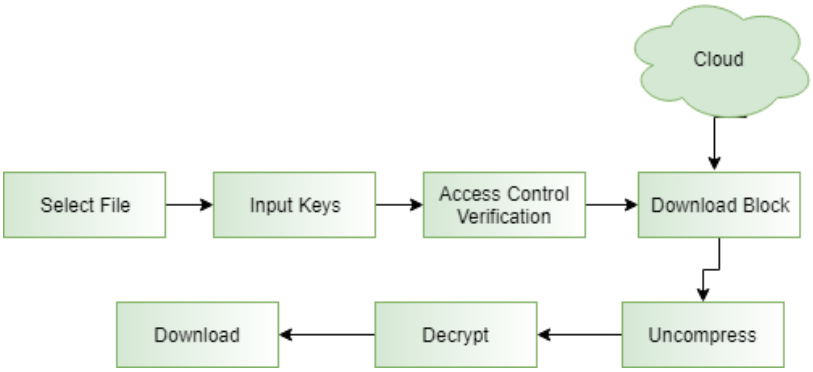

Fig - 6 : File Download Process

5. REQUIREMENT ANALYSIS

5.1 Software Requirements

Operating system : Windows

Coding Language : Java (Jdk 1.7)

Web Technology : Servlet, JSP

Web Server : TomCAT 6.0

IDE : Eclipse Indigo

Database : My-SQL 5.0

UGI for DB :SQLyog

JDBC Connection: Type 4

6. RESULTS AND SNAPSHOTS

Below page shows the admin profile. The details can be edited and password can alo be changed.

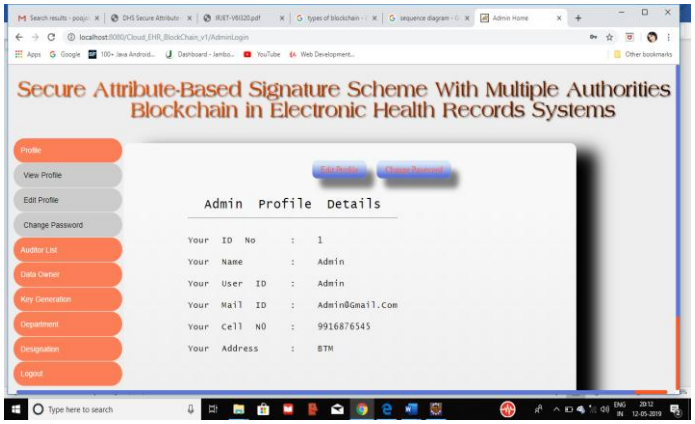

Fig - 7: Admin Profile Details

Below screen is key generation screen, on clicking the update key, key gets updated.RSA mechanism takes place.

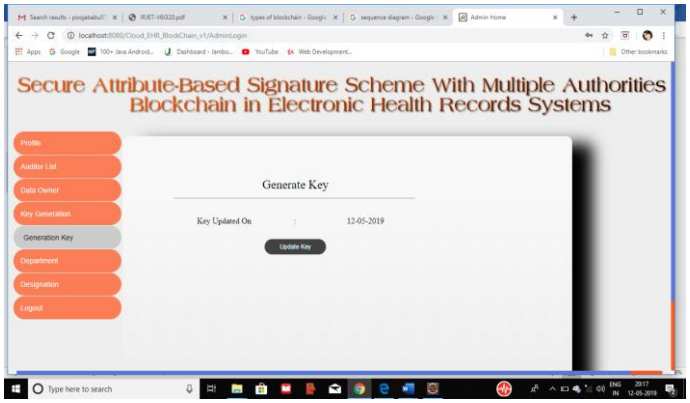

Fig -8: Key Generation Screen

Below screen is a page where file can be uploaded. File must be given name and can be uploaded.

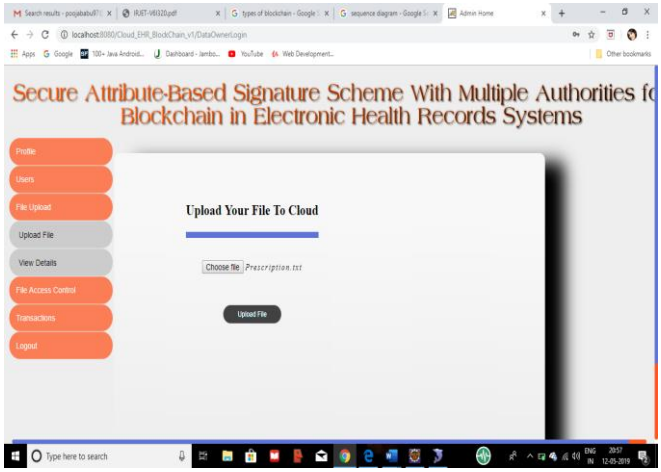

Fig - 9: File Upload Screen

Below Screen shows the acknowledgement as file is uploaded to cloud. Acknowledgment shows the details of file uploaded and cloud details to which file is uploaded.

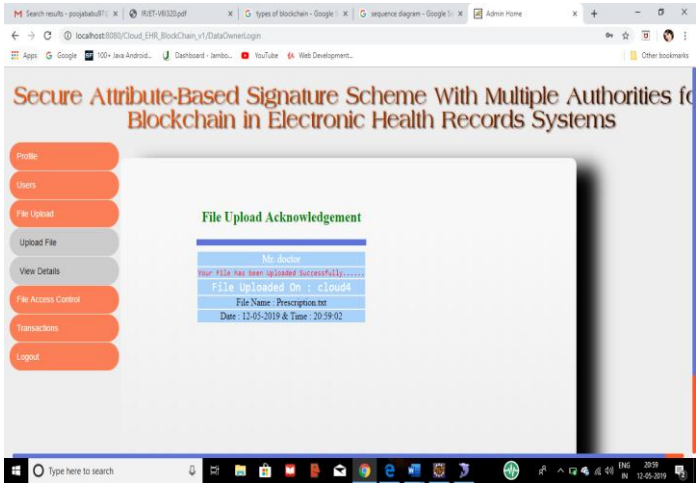

Fig -10: Acknowledgement

Below Screen is file download screen. On selecting the file to be downloaded, private key received via mail must be uploaded to download the file.

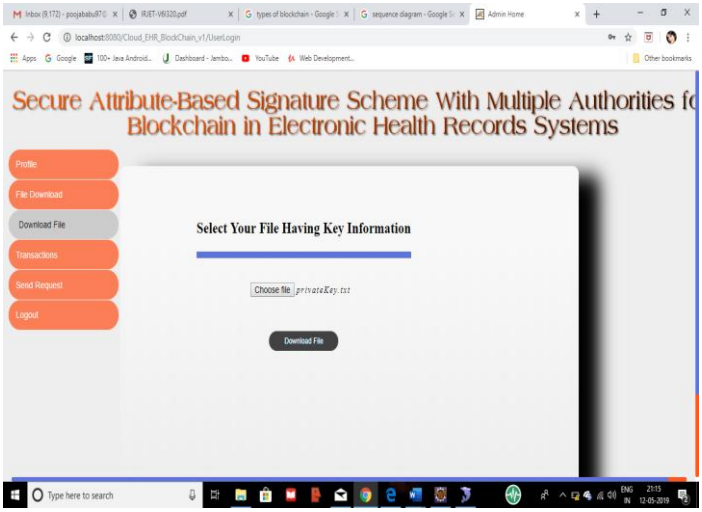

Fig -11: Private Key Upload

6. CONCLUSION

Blockchain enables the organization of check, characterization and data sharing while in the meantime giving information related to assurance, helpful resource saving and empowering for the patient and making masses social protection more intelligent. Taking the favored outlook of this technique, it achieves perfect security putting something aside for the patient.

REFERENCES

[1] D. Khader. Attribute based group signature scheme. Cryptology eprint archive, report 2007/159, 2007. Http://eprint.iacr.org/.

[2] D. Khader, ‘‘attribute based group signature with revocation,’’ in proc. Iacr cryptol. Eprint arch., jun. 2007, pp. 1–19. [online]. Available: https://eprint.iacr.org/2007/241.pdf