Blockchain Usage in the Electronic Health Record System using Attribute-Based Signature

B. Suma, G Murali

Abstract: ***Block-chain is a list of records which are stored in its blocks that are linked through cryptography. It is used previously for bitcoin transactions only. Now the government and also other organizations are going to use this block-chain in different fields. Electronic Health Records (EHRs) are used for storing the information about the patients. In EHR the information is stored in the paper through web which has some disadvantages. Here we use block-chain and Attribute- Based Signatures (ABS) to store the information about the patient's in the blocks of block-chain which is stored in cloud. By this we can provide security to the patient data and also there are no storage problems and also through ABS we provide some attributes to the users who are going to access the data of patient.***

Keywords: Cloud, Block-chain, Security, Hashing, Attributes, Privacy.

I. INTRODUCTION

Electronic Health Records (EHRs) are using for storing the patient records in an electronically accessible way. This system was mainly designed for patients to have the control of producing, sharing and managing their health records within their friends, doctors and some other important persons. It also helps to provide the access permissions if we need it.

Healthcare researcher and providers are used this services by accessing these EHRs across-the aboard. Now-a-days, patients having their EHRs at different areas. This causes the EHRs to change their databases from one service provider to another. By this, patient lose their control over the existing data. Patient having the access permissions on their own EHRs is very limited. Interoperability is also one of the issue in EHR. So we have to design a new system which overcome these EHR issues and prioritize patient mainly[5].

Attribute-Based Signatures (ABS) is used for people who are the sign makers. Sahai and Waters are the one who first introduced Attribute-Based Encryption [8]. By using a message with sign makes the receiver to identify information easily. In ABS, the signer has some set of attributes given by the above authority. With this they can sign on the message by satisfying their attributes. The signature only reveals about the signer with some attributes and also satisfying about the predicates which was attached to the message.

The signature hides the attributes and also the information which is used to identify the signer. Multiple signatures of the same signer may collide to avoid this the information about the signer is also hidden. We make standard assumptions using the bilinear paring operations which helps us to create the framework for the ABS. We keep the patient's data more securely by this framework of attributes of ABS. By this hacker's cannot theft the data of the patient easily. Data confidentiality is not the only one reason for security requirement, we should also consider Flexiblility and fine-grained access control[1]. Here we describe several problems that are raised in EHR and solve those problems by using block-chain with ABS help.

II. RELATED WORK

2.1 Block-chain:

Block-chain supports secure transactions directly between the sender and receiver. It is an end-to-end distributed ledger technology which helps in recording the transactions. Block-chain mainly works on secure data storage. Block-chain makes our data more secure and it allows more data when compared to other databases. Now block-chain is using in all data storage organizations mostly.

2.2 Electronic Healthcare Record(EHR) Issues:

EHR is a storage record which stores the patient records on web which is previously stored on the paper. In EHR there are some issues for storing the patient records. The storage space, security and the data access permissions to the patients and some other. In EHR the records which are stored is placed in the database. The space issues will arise as the database has storage space limit. Security is another issues of EHR the records of patients which are stored in the database can be hacked. Through this hacking patient's health details is taken by the hacker and this may lead to harm the patient.

Data access permissions has not been given to the patients only the data is managed by the hospital management. If the patient wants any urgent information regarding healthcare it will be difficult. If the patient wants to share the information, then it is also not possible. EHR should be useful for the cost reduction but in-order to provide security for the data stored in it we are investing more[4]. These type of issues are the drawbacks in the EHR.

Revised Version Manuscript Received on 16 September, 2019.

B. Suma, M.Tech Student, Dept Of Computer Science And Engineering, Jntua College Of Engineering, Pulivendula, Andhra Pradesh, India
(Email: sumabupathi@gmail.com)
Dr. G Murali, Assistant Professor, Dept Of Computer Science And Engineering, Jntua College Of Engineering, Pulivendula, Andhra Pradesh, India

2.2.1Security issues of EHR:

Years	Number of reported breaches	Breaches	Information hacked
2009	19	Hacked/ industrial Incident	Health Records
2010	190	Hacked	Health Planning data
2011	199	Loss	Business data, Healthcare data
2012	215	Hacked/Industrial Incident	Health Records
2013	280	Loss	Healthcare Records
2014	316	Hacked/Industrial Incident	Business Data, Health Records
2015	275	Hacked/Industrial Incident	Business Data, Healthcare Data, Health Records
2016	329	Unauthorized Access/Disclosure	Business Data, Healthcare Data, Health Records
2017	360	Unknown	Healthcare Data
2018	367	Theft	Business Data

Table 1. details of reported breaches in the corresponding years[3]

This Table 1 explains about the incidents occurred in particular years. These number of breaches are the complaints registered due to the security issues of EHR in the mentioned years.

Hacking is very common now with the increase in the latest technology. Hackers are mainly focusing on the healthcare as it has less security than the other. While using EHR there are some hacking incidents.

Figure 1 below shows the number of breaches reported on those years. Due to those incidents we can say that EHR has security issues.

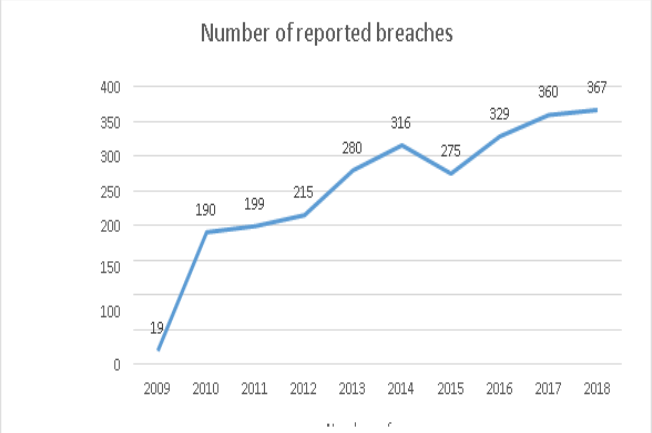

Figure 1. Hacking incidents of EHR

To avoid these security issues we use the block-chain for the storage purpose to provide more security for the patient's data. By using the block-chain hacker cannot theft the data because hacker should hack each and every block. So it makes difficult to hack each and every block.

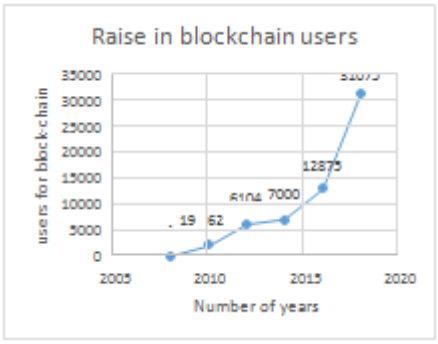

Figure 2. Raising of users for block-chain due to disadvantages of EHR

Figure 2 explains the users increase of block-chain due to the disadvantages of the EHR. By using block-chain we can make the patients data more secure than EHR. Increase in number of hacking incidents made increase of users for block-chain.

III. PROPOSED WORK

In this Proposed work the issues in EHR is resolved. In this proposed work block-chain is used to store the data/information about the patient by using hashing techniques. In this proposed work we are using keys to provide security for the information which is stored. We are using two keys here. These keys are used for the verification purpose whether authorized users or other users using it

The storage problem also resolved as we are storing it in the blocks of block-chain which is placed in cloud which we are using. Patient can also access the data immediately whenever he wants by using the keys. Here we are giving the attributes to the people who are using this information through ABS. While transferring file sender makes a

signature on the file. This signature is going to be verified to know whether it was send by the single sender or by multiple senders [7]. The algorithms used in this are RSA, DES and MD5.

3.1 Advantages:

- Accurate and up-to-date information of patient is provided.
- It provides quick access to the patients.
- Information is shared securely between the patients and the hospital.
- It helps the hospital people to know more accurately about the patient and identify the patient's condition and make patients more safe.
- It improves communication between the doctor and patient by knowing the information of patient more clearly.

3.2 System Architecture:

Figure3 is the System Architecture of the proposed work. In this we have Data Owner, Auditor, User, Admin.

3.2.1Data Owner:

Data owner encrypt the files and upload it to the block-chain by using a key which was generated by DES algorithm.

3.2.2Auditor:

Auditor verify the user details whether the user has the permissions or not. Auditor also verify the attributes and also the signature.

3.2.3User:

User decrypts the file which was uploaded by the data owner with the help of key generated by RSA algorithm.

3.2.4Admin:

Admin maintains the records which was stored in the block-chain.

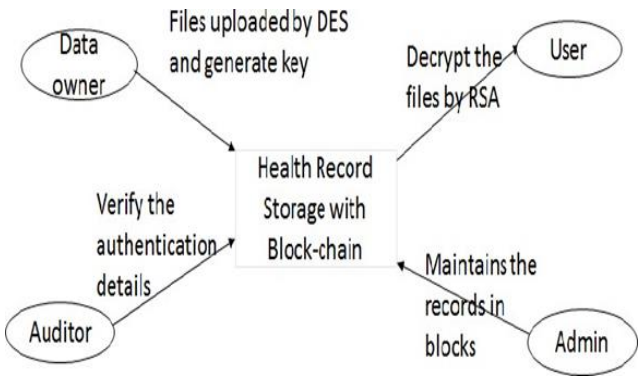

Figure 3. System architectre

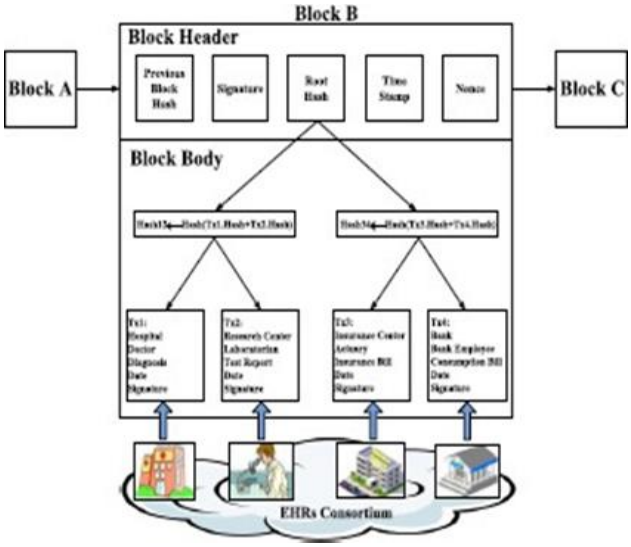

Figure 4. Block-chain Architecture

Figure 4 explains the storage details of blocks in block-chain. Block-chain Architecture helps us to know the internal block storage parts. It has header, body parts. In header we have previous block details and also the signature and its hash value. In the block body it stores the records of patients.

3.3 DataEncryption Standard(DES) algorithm:

The Data Encryption Standard belongs to symmetric-key algorithm which can be used for encrypting electronic data. DES uses cryptographic algorithm to protect the electronic data[2]. Here DES algorithm is used to generate the key for the file which is uploaded in the cloud. Attributes are given to those who are going to access the patient information auditor and data owner and admin gives the permissions when they add any new user to the list. By verifying the key and checking the attributes user can access the file which contains the patient's data.

3.4 Rivest Shamir Adleman(RSA) algorithm:

Rivest–Shamir–Adleman belongs to public-key cryptosystems. RSA implements digital signatures which are digital and public key cryptosystem[6]. It is used for data transmission securely. As it is a asymmetric algorithm we have two keys here which are used for the encryption and decryption purpose. One key is a private used for decryption and another key is private key used for encryption purpose. Here we use this algorithm for the file encryption purpose. After the encryption the file which contains patient's data is uploaded to cloud. The file then stored in the cloud and through the key verification it can be downloaded and used by the authorized users as per their given attributes.

3.5 Message-Digest (MD5) algorithm:

Initially MD5 algorithm is used as a cryptographic hash function. There is insecurity for storing the passwords in plain text database. So MD5 algorithm is used for hashing the real password and values of hash rather than content stored in the database[3]. Later it was suffered from extensive

vulnerabilities. Here MD5 algorithm is used while placing the information in blocks of block-chain. Through this algorithm it places the previous hash value, data and the hash value of that data which will be stored in the next block.

3.6 Symmetric Encryption and Asymmetric Encryption:

In symmetric encryption there is only one key. In asymmetric we have two keys. Private key belongs to the one who uploads the information or data. Public key is given to all the users who are going to access the file. Public is known to all while private key is confidential.

IV. RESULT AND ANALYSIS

Storing and Securing the data are the most important tasks. In-order to store data more securely without any storage problems we are using block-chain.

Months of stored records	Records stored per block
Jan-Mar'18	3953
Apr-Jun'18	4386
Jul-Sep'18	4269
Oct-Dec'18	4159
Jan-Mar'19	2730
Apr-Jun'19	4426

Table2.Number of records stored per block

Table 2 explains about the storage of number of records per block. The records are stored in each block securely with the date and time of the storage.

Usage of Block-chain instead of EHR has solved a lot of issues like the storage and security. So in Organizations, Hospitals, Government and other are using the block- chain.

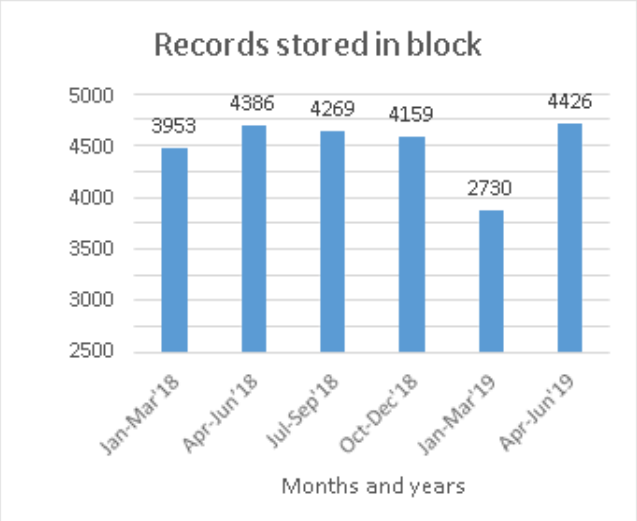

Figure 5. Number of records per block

Figure 5 explains the storage details of the patient's records in the blocks of block- chain. By storing these records in the block- chain we provide more security for the patient's health records.

Table 3 shows the number of records stored in the blocks on july 2 2019 at particular time. This storage of records is taken from the rinkeyby simulator.

Records storage time on 2 july'19	Number of records stored in blocks
9:08:00PM	3.366
9:15:00PM	3.516
9:22:00PM	3.551
9:29:00PM	4.533
9:36:00PM	4.251
9:43:00PM	4.433
9:50:00PM	3.916
9:57:00PM	4.051
10:04:00PM	4.933
10:11:00PM	7.0833

Table 3. Number of records stored in blocks at a particular time

Figure 6 shows the storage rate of the records in blocks in particular time. This records which are stored can be accessed by the authenticated users only.

The authenticated users have the predefined attributes which was given to them by using ABS. The user should match with that attributes then only user can access these records.

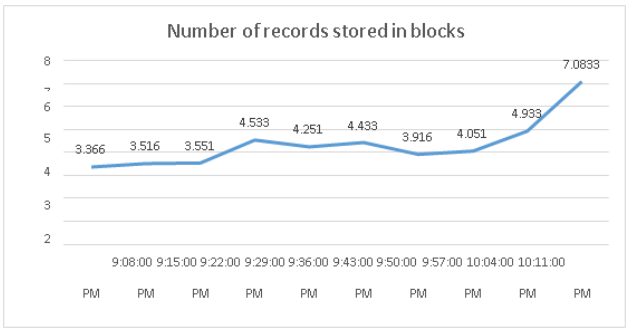

Figure 6. Number of records stored in blocks on particular time

V. CONCLUSION AND FUTURE WORK

Mainly focusing on the privacy of the patient's health information we introduced MB-ABS and also the block-chain. They made patients information more secure by providing authorized access. The private keys are generated by using the algorithms which makes the users use data authorized without any corruption. At present here we are using single attribute. In future system, we can add more number of attribute's. In future work, we can create hybrid cloud setup. At present system, we are using Diffie-Hellman encryption technique. In future, we can use RNS crypto system (RNS- Residual Number System).

REFERENCES

1. June Lin, Zhigio Wan, Robert H. Deng, Senior Member, IEEE, April- 2012, HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing
2. Indumathi Saikumar, March-2017, DES- Data Encryption Standard
3. Zhao Shun Wang , Mary Cindy Ah Kioon and Shubra Deb Das, 2013, Security Analysis of MD5 Algorithm in Password Storage.
4. https://www.americanactionforum.org/weekly-checkup/electronic-health-records-become-valuable-pone-hackers/
5. Ariel Ekblaw, Asaph Azaria, Thiago Vieira and Andrew Lippman Media Lab, 2016, MedRec:Using Blockchain for Medical Data Access and Permission Management.
6. Eygeny Milanov, 3-june-2009, The RSA Algorithm
7. Manoj Prabhakaran, Hemank Maji and Mike Rosulek, 15-April-2008, Attribute- Based Signatures:Achieving Attribute-Privacy and Collusion
8. Brent Waters, Amit Sahai, 2005, Fuzzy Identity Based Encryption.