A Patient Centric Healthcare System using BlockchainTechnology in Cloud

Mrs. M. Prabha[1], Aswini A[2], Bhavani T[3], Chithara J[4]

[1]*Assistant Professor, Dept. of Information Technology, Velammal College of Engineering andTechnology, Madurai, Tamilnadu, India*
[2-4]*UG Student, Dept. of Information Technology, Velammal College of Engineering and Technology,Madurai, Tamilnadu, India*

Abstract: - *Cloud* computing *Technology is a shared network information delivery model. Cloud is an infinite resource pool which is a virtualization concept. Hence users can easily access their data from anywhere. At an equivalent time there exist privacy and security issues. This paper addresses different data security and privacy protection issues during a cloud computing environment. The information is encrypted and secured using blockchain before outsourcing to the cloud. 128 bit Advanced Encryption Standard (AES) is employed to extend data security and confidentiality. The unique features of blockchain, a distributed ledger technology which is considered as "unhackable" is also used to secure the information. Health Information Exchange (HIE) provides an interesting benefits for patient care like improving healthcare quality and expediting coordinated care. This paper provides a solution for the multiple barriers to patient-centric HIE within the current system, like security and privacy concerns, timely access to the proper records across multiple healthcare facilities.*

***Keyword* :- Cloud computing, Encryption, AES, Blockchain, HIE.**

1. INTRODUCTION

Cloud computing offers a chance for people and corporations to upload to powerful servers the burden of managing large amounts of knowledge and performing computationally demanding operations. The increasing popularity of cloud computing, more Data owners are encouraged to outsource their data to cloud servers for convenience and reduced cost in data management. Data owners offer services to an outsized number of companies and corporations , they stick with high security standards to enhance data security by following a layered approach that has encoding , key management, strong access controls, and counterintelligence .

Cryptography secures our personal data or information from the unauthorized users. Cryptography means "secret writing" which suggests is that the science and art of remodeling messages to form them secure and resistant to attacks by unauthorized users. In cryptography two sorts of operation are often performed. The Encryption and Decryption operation can treat using key management. An encryption is that the process of converting the first data into another format is understood as cipher text, which isn't easy to know and unreadable.

Generally, Electronic Medical Records (EMRs) Contain medical and clinical data associated with a given patient and stored by the responsible Healthcare provider.

To raise support the management of EMRs, early generations of Health Information Systems (HIS) are designed with the potential to make new EMR instances, store them, and query and retrieve stored EMRs of interest. HIS are often relatively simple solutions, which may be schematically described as a graphical interface or an internet service. These are generally the front-end with a database at the back-end, during a centralized or distributed implementation. As the patient mobility is increasingly the norm in today's society, it became evident that multiple stands- alone EMR solutions must be made interoperable to facilitate sharing of healthcare data.

To facilitate data sharing or maybe patient data portability, there's a requirement for EMRs to formalize their arrangement and therefore the design of HIS. Electronic Health Records (EHRs), for instance, are designed to permit patient medical record to maneuver with the patient or be made available to multiple healthcare providers

.There have also been initiatives to develop HIS and infrastructures that are ready to scale and support future needs, as evidenced by the varied national and international initiatives. These developments have paved the way for private Health Records (PHR), where patients are more involved in their data collection, monitoring of their health conditions, etc.

Healthcare may be a data-intensive domain where an outsized amount of knowledge is made, disseminated, stored, and accessed daily. It's clear that technology can play a big role in enhancing the standard of look after patients.

The following contents are arranged as follows. Section 2 contains literature survey. Then section 3 contains the methodology .Section 4 contains the detailed description of the system model. Section 5 contains result and future enhancement.

2. LITERATURE REVIEW

The paper [1] studies about the performance analysis of AES encryption algorithm, DES encryption algorithm and blowfish encryption algorithm.

DES is the most widely used encryption scheme, especially in financial application. AES is one of the ideal for encrypting messages. Blowfish consumes less memory in compared with AES and DES. [2] Two fish encryption algorithm is similarly same space consists of Blowfish because the Two fish algorithm is derived from the Blowfish algorithm. The paper [3] studied existing security issues in cloud computing. Environment and proposed a new method for securing cloud data in real environment. AES encryption provides confidentiality, authenticity and access control. Then performance of proposed approach was analyzed based on delay. The paper [4] illustrates the specific problems and highlights the benefits of the blockchain technology for the deployment of a secure and a scalable solution for medical data exchange in order to have the best performance possible. The paper [5] Studies different security issues in service delivery models of cloud computing. They also suggest an integrated security model for providing different levels of security to data in cloud infrastructure. The threats and attacks that are possible to launching cloud computing data storage are studied in and then proposed a new security mechanism. [6] Potential opportunities for improving EHR adoption, health care services, and research are provided. It provides useful strategic planning for potential users to start cloud projects. [7] Security SLA models provide standard security controls and have innovative security metrics that enable cloud service providers to realistically measure and guarantee security. The paper [8] architecture provides privacy-preserving, user-self-controlled data sharing and decentralization by using blockchain and several attribute-based cryptosystems and a novel blockchain-based architecture for data sharing with attribute-based cryptosystem (BaDS) in this paper. [9] Propose a reputation-based data sharing scheme to ensure high- quality data sharing among hospitals. This paper illustrates the problems and highlights the benefits of the blockchain technology for the deployment of a secure and a scalable solution for medical data exchange in order to have the best performance possible.

3. METHODOLOGY

The proposed system undergoes encryption and secured using blockchain technology before outsourcing to the cloud.

3.1 ENCRYPTION ALGORITHMS

Cloud encryption encodes or transforms the data before it's transferred to cloud storage. Encryption uses mathematical algorithms to transform data (may it be a text, file, code or image, to an unreadable form that can conceal it from unauthorized and hackers. It is the simplest and most important way to make sure that cloud data can't be abused, stolen and read by someone with an anomalous motive. Some of the effective encryption algorithms are AES, DES, Blowfish, Twofish , IDEA.

3.1.1 AES ENCRYPTION:

AES may be a block cipher algorithm, it supports 128 bit block and key size is 128, 192, 256 bits. Maximum there's 14 processing round is processed within the AES and therefore the number of round is depends upon the key size. It uses higher length key sizes like 128, 192 and
256 bits for encryption. Hence it makes AES algorithm sturdier against hacking. It uses too simple algebraic structure considered as a drawback of AES.

3.1.2 DES ENCRYPTION

DES is a block cipher; it takes plain text as a input of given size and output as a cipher text with given size. This algorithm transforms 64 bit input into a 64 bit output with a series of steps. So there are 2^56 possibilities of keys which might take a decade to seek out the right key using brute-force attack. DES algorithm is computationally very complex.

3.1.3 RSA ENCRYPTION

RSA is an algorithm used by modern computers to encrypt and decrypt messages, and it uses different keys. RSA has its authenticity and confidentiality. It is used for specific security purposes. It is very slow in some cases.

3.1.4 BLOWFISH ENCRYPTION

Blowfish may be a symmetric block cipher algorithm for encryption and decryption. It is 64- bit block cipher. It optimized for 32-bit processors with large data caches. It's benefit is especially the password- hashing method. It also has weakness in decryption process over other algorithms in terms of your time consumption and serially inthroughput.

3.1.5 TWOFISH ENCRYPTION

Two fish may be a symmetric block cipher encryption algorithm, derived from Blowfish. It uses 128 bit block size and key size is 128, 192, 256 bits. It is one of the five finalists of Advanced Encryption Standard consent, but it was not selected. It is considered as the fastest encryption standard

3.1.6 IDEA ENCRYPTION

The International encoding Algorithm (IDEA), it uses a block cipher and it is considered to be secure. The process of key generation begins by dividing 128-bit keys into eight pieces of the 16- bit sub key. These are the first eight sub keys for the algorithm with details of the first six subkeys for round 1 and the last two sub keys for round 2. These are some of the efficient algorithm used for information Security .Comparative analysis of the algorithm (AES, DES, RSA, Blowfish, Two fish and IDEA encryption) are given below.

Features	AES	DES	RSA	Blowfish	Two fish	IDEA
Developed	2000	1977	1977	1993	1993	1991
Key Length	128 bits 192 bits 256 bits	56 bits	More than 1024 bits	32-448 bits	128-256 bits	128 bits
Cipher Type	Symmetric block Cipher	Symmetric block Cipher	Asymmetric block Cipher	Symmetric block Cipher	Symmetric block Cipher	Symmetric block Cipher
Block Size	128 bits	64 bits	Minimum 512 bits	64 bits	128 bits	64 bits
Number of Rounds	10,12,14	48	1	16	16	8.5
Speed(Encryption And Decryption)	Faster	Moderate	Slower	Fast	Slow	Fast
Memory	High	High	High	Low	Moderate	Moderate
Security	Excellent Security	Not enough Security	Least Security	Good Security	Not enough Security	Least Security

Table 1: Comparative Analysis of AES, DES, RSA, Blowfish, Two fish, IDEA

3.2 WHY AES?

Table I shows the comparative analysis of encryption algorithms - AES, DES , RSA, blowfish, twofish, IDEA based on key length, cipher type, block size, security, encryption/decryption speed, Memory etc. A comparative study between different encryption methods based on stimulated time for encryption and decryption has done in. [3] Based onthese experiments they concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. Based on their results they reached in a conclusion that AES algorithm is much better than other algorithms. From table I show that RSA is least secure and AES is most secure and faster one. Now a day an important problem faced by all organization and providers is that fastest and secure delivery of services to the customers. Security of any system also depends on user satisfaction level. Hence the proposed system provided security to user data through encryption before uploading on the cloud. AES algorithm is used for data encryption and decryption, since it is faster and secure.

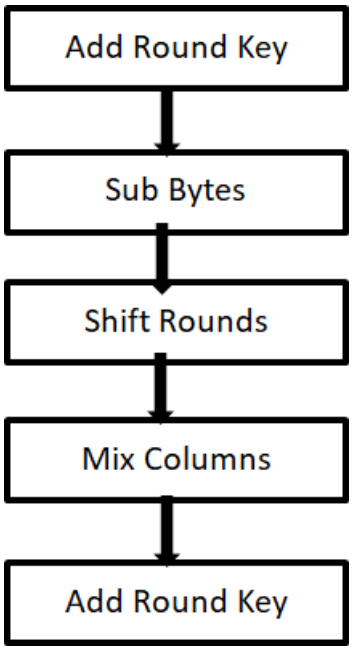

Fig 1: Steps in Advanced Encryption Standard Algorithm

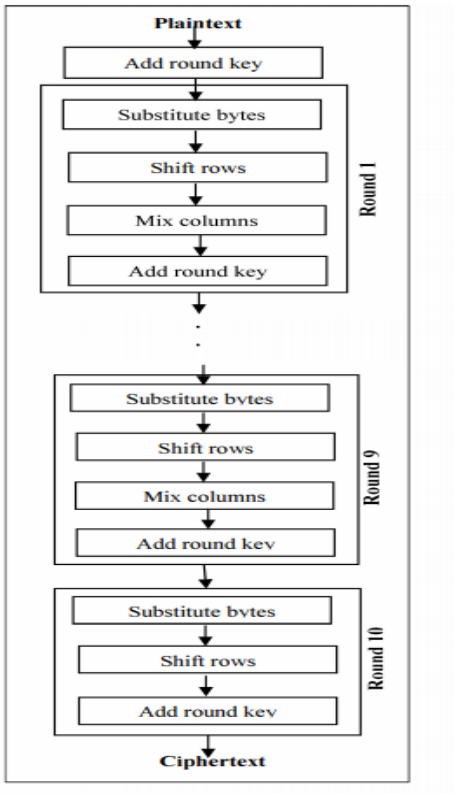

Fig 2: General Structure of AES

3.3 BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed public ledger database that is maintained by a network of verified participants or nodes and stores immutable blocks of data that can be shared securely without third- party intervention. Data are protected and recorded with time stamp and hash values of the previous blocks. This ability for data preservation provides significant reason that has driven the utilization of blockchain in healthcare, wherein a big amount of knowledge is subject to extensive exchange and distribution. Blockchain can create a single system for stored, constantly updated, heath records for secure and rapid retrieval by authorized users. By avoiding miscommunication between different healthcare professionals involved in caring for the same patient.

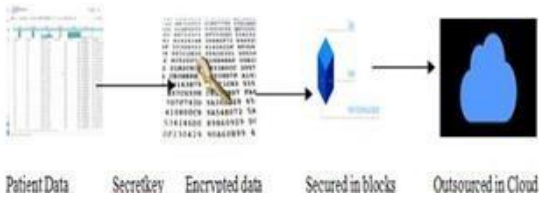

Fig 3: Architecture of Data Security in HIE.

4. SYSTEM MODEL

4.1 REGISTRATION MODULE

The user can login with their username and password. If a fresh user must login, the user got to be register their before login. It is a process of enrolling or being enrolled into the cloud .Both user (patients) and thus the healthcare provider must enroll so as to access patient's records.

During this process your basic information are collected and stored within the Cloud. The cloud id for a selected user will get automatically generated during the registration.

4.2 HEALTHCARE PROVIDER MODULE

4.2.1 Loading Patients Records

In this process, the health provider chooses patient healthcare records for uploading and maintaining the dataset within the cloud.

4.2.2 Key Generation

The secret key's generated using cryptographic algorithm. This key will be used for encrypting the dataset. The 128 bit AES algorithm is used to encrypt the records.

4.2.3 Encrypt Patient Records

The data is encrypted for secure maintenance. so as that the unauthorized person cannot be able to access the data that are presented within the cloud.

4.2.4 Block Creation

After creating the block, the healthcare provider will outsource the records into the cloud. In case, if they have to retrieve a record from cloud, first the healthcare provider searches the records.After getting an approval and key from the cloud service provider the healthcare provider can download the info.

4.3 PATIENT MODULE

4.3.1 Request Record

To download the record patient must sent requestto the cloud.

4.3.2 Decrypt and Download Patient Records

After getting an approval and key from the cloud service provider the healthcare provider can download the info.

4.4 CLOUD MODULE

The cloud service provider maintains all the patient records and also they're going to provide permission to the user to access the info. The Cloud Service Provider receives the document request from the info User, verifies the authentication before granting permission. Then the Cloud Service Provider executes the query and returns the encrypted document according to the search token.

4.4.1 Public Verification Key

Public verification key's a security measure designed to make sure that your document outsourced in cloud doesn't get hacked. By verifying public key, the info Owner and thus the info User adding another layer of protection to thedocuments or files within the cloud by conforming each other's identity.

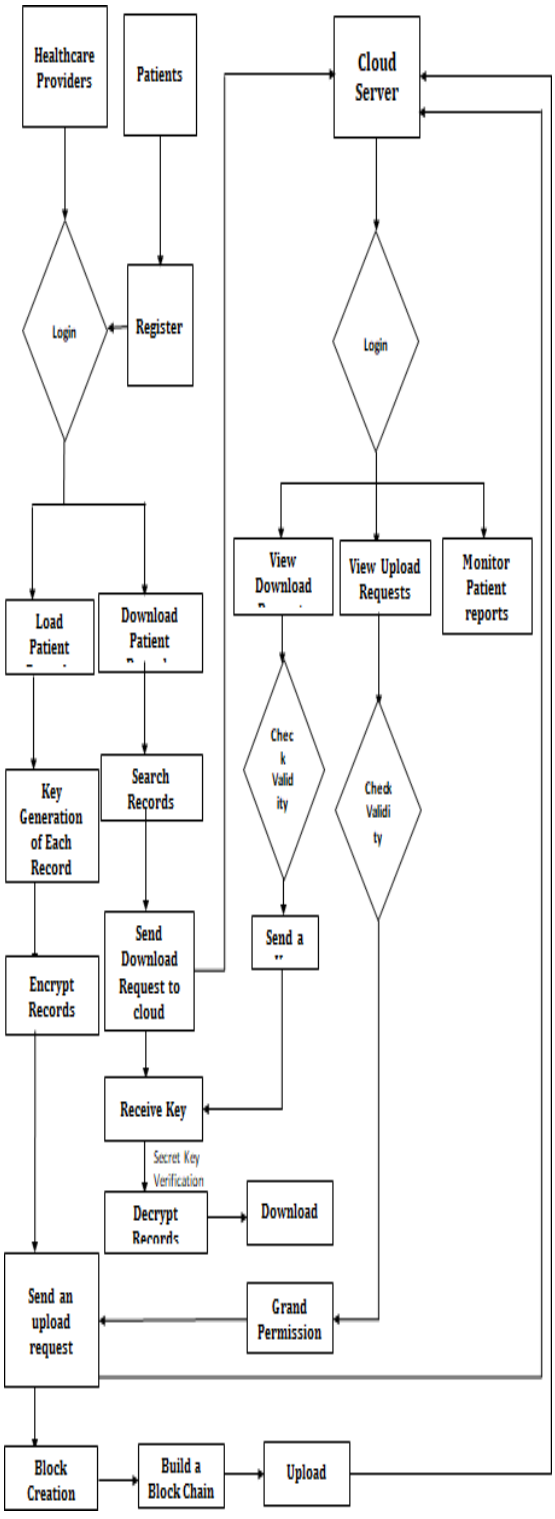

Fig 4: Flow Diagram of Patient Centric HIE

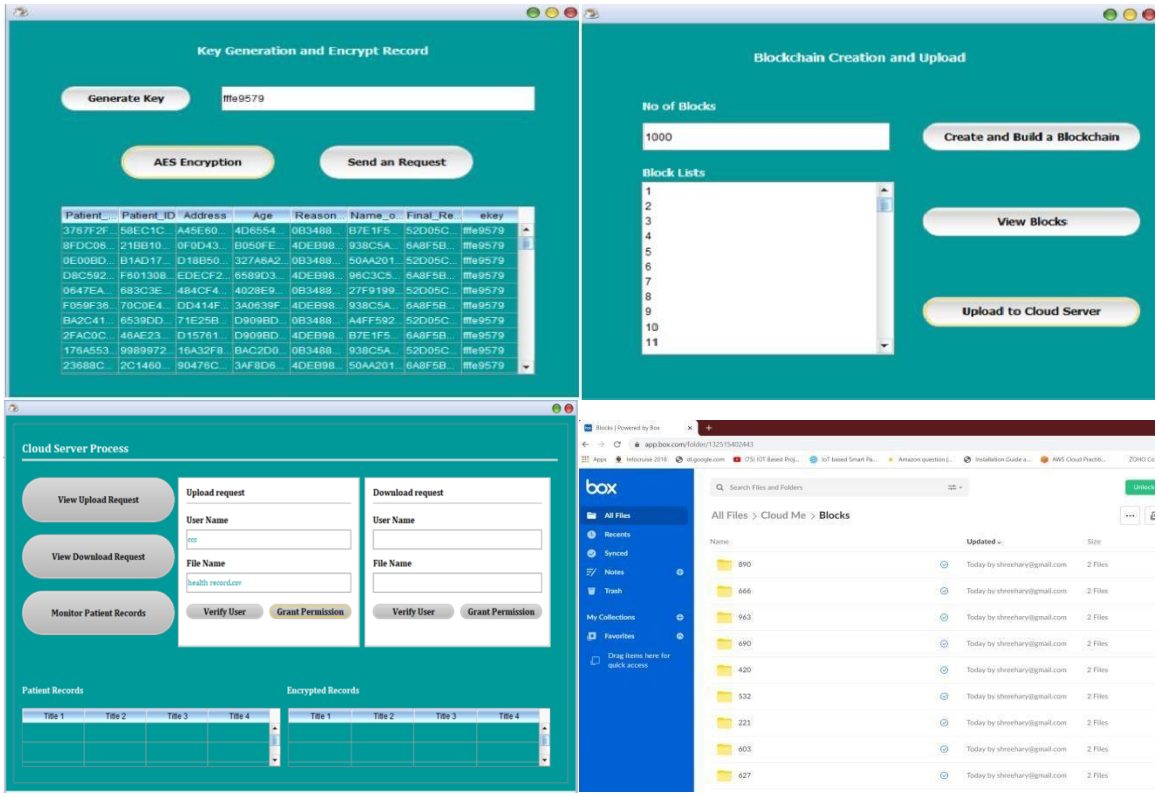

Fig 5: Implementation of Patient Centric HIE

5. RESULT AND FUTURE ENHANCEMENT

This paper proposes a patient centric Health Information Exchange system which provides a coordinated care among the hospitals .The patient data is much secured using encryption algorithms,blockchain before outsourcing the patient's data into the cloud. The longer term enhancement is the classification based on Security. Classification of data is done. This classification scheme takes various aspects such as access frequency, update frequency and access by various entities etc. supported the sort of knowledge. Once the info is assessed and tagged, then level of security related to this specific tagged data element can be applied.

REFERENCES

[1] A. Ramesh, Dr. A. Suruliandi ME., Ph.D, "Performance Analysis of Encryption Algorithms for Information Security", International Conference on Circuits, Power and Computing Technologies

.[2] A.Jeevalatha, Senthilnathan, "Evolution of AES, Blowfish and Two fish Encryption Algorithm", International Journal of Scientific & Engineering Research.

[3] Babitha. M. P, K.R. Ramesh Babu, "Secure Cloud Storage Using AES Encryption", 6 International Conferences on Automatic Control and Dynamic Optimization Techniques (ICACDOT) International Institute of Information Technology.

[4] A. Mu-Hsing Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services" Journal of Medical Internet Research, 2011.

[5] A. Mu-Hsing Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services" Journal of Medical Internet Research, 2011.

[6] V. Casola et al., "Healthcare-Related Data in the Cloud: Challenges and Opportunities" IEEE Cloud Computing, 2016.

[7] P.C. Tang et al., "Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption" 2006.

[8] Yunru Zhang, Debiao He, and Kim-Kwang Raymond Choo, "BaDS: Blockchain-Based Architecture for Data Sharing with ABS and CP- ABE in IoT," Wireless Communication. and Mobile Computing., 2018.

[9] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine, and Nada Chendeb Taher, "Towards Using Blockchain Technology for eHealth Data Access Management," in Proc. IEEE on Advances in Bio. Engineering. Oct. 2017.