Securing Personal Health Records In Cloud Using Dual Key Encryption

Arockia Panimalar.S [1], Subhashri.K[2], Karthika.S[3], Kavya.G[4]

[1,2] Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, India
[3,4] IV M.Sc SS, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Coimbatore, India

---***---

Abstract - *The Personal Health Record(PHR) is a collection of information about patient's health. Here data will be stored in the centralized manner, where the user can access the data from anywhere. To improve the security level of data, Dual-key encryption method is used along with Attribute Based Encryption (ABE). The data stored in database is in the encrypted form and only during the time of retrieval the data will be decrypted. In this paper, a secured third party storage method using attribute based encryption is proposed for personal health records. Using third party storage system tremendous number of data can be stored and can be accessed easily using query distribution methods. In order to implement attribute based encryption, data from front end is stored in the back end as a symbol based format. Moreover Dual system encryption method is used which is an advanced encryption method that will work on both front end and back end thus making the data more secured. In addition, implementation of this architecture in cloud makes the data centralized, and the patients can continue their treatment anywhere at any time. This helps the patients to maintain their Personal Health Record (PHR) and get quality treatment.*

***Key Words*: Dual Key Encryption, Attribute Based Encryption (ABE), Personal Health Record (PHR), Electronic Health Record (EHR).**

1. INTRODUCTION

A personal health record is essentially a gathering of data about patient's health. On the off chance that the patients have a shot record or a container of therapeutic papers, they as of now have a fundamental personal health record. And they have probably encountered the big drawback of paper records. The hospital may rarely have their details with them. The Electronic personal health record systems remedy that problem by making patient's personal health record accessible to you anytime via a web enabled device, such as computer, phone or tablet. Personal health records are not the same as electronic health records or electronic medical records, which are owned and operated by doctors' offices, hospitals or health insurance plans. There are a growing number of doctor's offices using these systems, but those that do often limit the access to and control of the medical record.

A secured third party storage method using attributes based encryption for personal health records is proposed. This web based storage system is developed using web based applications. Using third party storage system tremendous number of data can be stored and can be accessed easily using query distribution methods. The given details will be clustered and updated in the third party storages through web.

Dual system encryption method is an advanced encryption method which will works on both front end and back end. So that data will be much secured. This is because in case of any celebrities, politician or any public personality may undergo for any crucial treatments, at that time the treatment data should not be get leaked. This became a prestigious issue for that public personality. So this method provides a dual system encryption. This is an advanced encryption method which encrypts the data into symbols while storing in the database. So that even low level working in the hospital or the organization will not able to find out the treatment history for any patients.

In added with in case of implementing the data architecture in cloud architecture, all the data will be getting centralized. So that the patients can continues their treatment anywhere at any time. This helps the patient to maintain their PHR and can able to get quality treatment. Here search complexity is increased due to higher data storage. So that patients can be searched with any criteria like their figure print, iris, patient name, father name, DOB, last treatment place and etc.

The third party actor will be the insurance company, so that the centralized data can be accessed by the subscribed insurance company server. This method will not produce any fake data for insurance claim. By using this method insurance can be properly utilized by the patients after their treatments. The insurance company can look over the treatment location, treatment type, nature of the treatment, bill generated for the treatment and etc in order to provide the proper claim for the patient.

2. RELATED WORK

Several application scenarios are used in electronic healthcare (e-health), eg. Electronic health records, accounting and billing, medical research, and trading intellectual property. E-health systems like Electronic Health

Records (EHRs) are used to decrease costs in health care and to improve personal health management.

A.R.Sadeghi et al.(2010) proposed a security engineering for building up protection areas in e-health foundation, this gave the client stage security and joins this with arrange security ideas.

M.Li et al.(2011) proposed to conquer the issue of approved private catchphrase seeks on encoded PHR in cloud computing conditions.

Akshita et al. (2016) proposed to implement the security in cloud server using attribute based encryption which is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon attributes.

Susan Hohenberger and Brent Waters (2013) proposed the design of ABE schemes with faster decryption algorithms.
C. Wang et al.(2010) proposed to address the challenge of defining and enforcing access policies based on data attributes, and, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to entrusted cloud servers without disclosing the underlying data contents.

3. PROPOSED SYSTEM

In the proposed system, all the details that are currently maintained manually are computerized. Due to computerization, the data entered are very much secured, and cannot be accessed or changed by unscrupulous persons. The proposed system is totally user friendly and menu driven thus helping a person to use this with ease and accuracy. The record can be easily updated at any time.
The dual encryption algorithms which use the same key for both encryption and decryption are known as symmetric key algorithms. These asymmetric key algorithms allow one key to be made public while retaining the private key in only one location. They are outlined with the goal that discovering the private key is amazingly troublesome, regardless of the possibility that the comparing public key is known. A client of public key innovation can distribute their public key, while keeping their private key mystery, enabling anybody to send them a encrypted message.

A. Configuring Organization and Dataset

Medical domain is the initial module and contains a hospital environmental based application. An admin is available for controlling the whole application. Admin can create doctor, patient and actors those who can access this application. Admin can customize the whole application and provide rights and customization to the actors.

B. Centralized the Mining Server

In order to access all the data, we need a centralized server. This server contains all the information about the organization like doctor details, patient details, patient's treatment information, treatment history, medical reports, and insurance details. This centralized server is for the entire hospitals county wide. Actors will be separated according to their roles and responsibilities. A unique code will be generated for all doctors and patients. So that fake doctors will be identified easily.

C. Dual Key Encryption

The decentralized server's data will be encrypted dual times before reaching the server. The entire data will be decrypted twice except the ID. The ID will represent the field for data access. Hybrid cryptography will be implementing for the encryption process. AES has a fixed block size of 128 bit and a key size of 128, 192, or 256 bit, has specified with block and key sizes in multiples of 32 bit, with a minimum of 128 bit. The block size has a maximum of 256 bit but the key size has no theoretical maximum AES operates on a 4×4 column-major order matrix of bytes, termed the state.

D. Processing the actor with ABE

ABE (Attribute Based Encryption)-The main process in this module is, only actors can access the data with data access control. The encrypted data will be decrypted during the time of retrieval only. Remaining time the data will be remains encrypted in the server's database. While retrieving the data only permitted data of the particular actor will be visible to the actor. Other data and fields will be in encrypted format. To actors cannot able to access the unwanted or sensitive information of the organization.

E. Data Log and Access History

Data log and access history will be deals with the data patterns like permissions, actors involved, accessed data by the actors, accessed fields, latest updates in the server, last accessed data and time of the server and server restrictions. This module gives the overall data access and security issues in the server. This module can be accessed by both admin and actors.

4. ENCRYPTION PROCESS

A colossal measure of information is being put away in the cloud, and quite a bit of this is delicate information. Care ought to be taken to guarantee get to control of this sensitive information which can regularly be identified with health, critical reports or even individual data. There are extensively three sorts of access control: User Based Access Control (UBAC), Role Based Access Control (RBAC), and Attribute

Based Access Control (ABAC). In UBAC, the Access Control List (ACL) contains the rundown of clients who are approved to get to information. This is not plausible in cloud where there are numerous clients. In RBAC, users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have access to data but not the junior secretaries. ABAC is more reached out in scope, in which clients are given attributes and the information has connected get to access policy. Just clients with valid set of attributes, fulfilling the access policy, can get to the information. An area where access control is broadly being utilized is healthcare. Clouds are being utilized to store sensitive information about patients to empower access to restorative experts, doctor's facility staff, analysts, and strategy producers. It is vital to control the access of data so that only authorized users can access the data. Utilizing ABE, the records are encoded under some access policy and put away in the cloud. Clients are sets of attributes and corresponding keys. Just when the clients have matching set of attributes, would they be able to decode the data put away in the cloud.

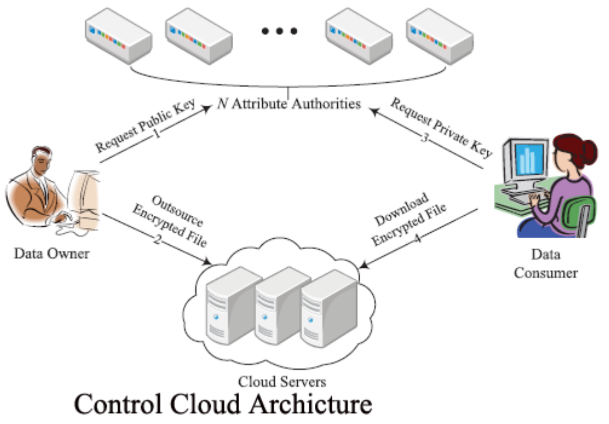

Fig: Process of Encryption and Decryption

A. Encryption

When the first party wants to send a message M to the second party, he/she determines the key 2*L*K and every character from the message is replaced by a binary value. An eight-bit octet is generated randomly and set in a temporary vector V. the bits in the vector V from position K [1,1] to position K[1,2] are replaced by bits from the secret message. Then the resulting vector V is stored in a file. As long as the message file has not reached its end yet, we move to the next row of the key matrix and another octet is generated randomly and the replacement is performed repeatedly and the resulting vector is stored in the file. The previous procedure is repeated over and over again pending the end the message. The resulting file is sent to the receiver who beforehand has the key matrix. In the event that the key length is insufficient to cover the entire message amid the encryption procedure, the key will be reapplied again and again until the point when the encryption of the entire message is finished.

B. Decryption

The encrypted file is decrypted by using the following steps. An octet is perused from the encrypted binary plain text message EBPM file, at that point it is set in an impermanent vector V, from this vector, bits are removed from position K(1,1) to position K(1,2) and set in a BPM record. Since the EBPM document is regardless not void, the following octet is read from the EBPM record and afterward it is set in a transitory vector V. From this vector, bits are removed from position K (2, 1) to position K (2, 2) and added to the parallel plain instant message BPM document. The above steps are repeated over and over again until the EBPM file becomes empty. Every octet form the BPM file is transformed to the corresponding character, and then is put in the plaintext file. At the point when the EPBM is unfilled the plaintext record turns into the message. On the off chance that that the key length is insufficient to cover the entire message amid the decryption process, the key will be reapplied again and again till the decoding of the entire message is finished.

C. Attribute Based Encryption (ABE)

ABE (Attribute Based Encryption) the main process in this module is, only actors can access the data with data access control. The encrypted data will be decrypted during the time of retrieval only. Remaining time the data will be remains encrypted in the server's database. While retrieving the data only permitted data of the particular actor will be visible to the actor. Other data and fields will be in encrypted format. To actors cannot able to access the unwanted or sensitive information of the organization.

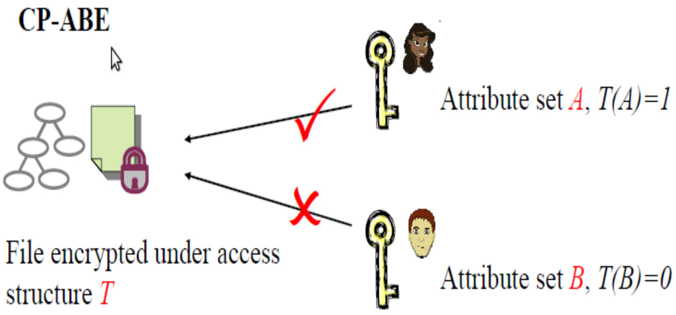

Fig: Process of ABE

5. Conclusion and Future Enhancement

We proposed a secure Personal Health Record system framework using dual key encryption along with Attribute Based Encryption (ABE) to realize fine-grained, patientcentric access control. We use different ABE scheme to share PHR data with users from different domains. The information's flow should be developed. Help messenger, alert, list of values. Database should be structured with minimum redundancy. This helps the patient to maintain their PHR and can able to get quality treatment. Here search complexity is increased due to higher data storage. So that patients can be searched with any criteria like their finger print, iris, patient name, father name, DOB, last treatment place and etc. Here the third party actor will be the insurance company, so that the centralized data can be accessed by the subscribed insurance company server. This method will not produce any fake data for the insurance claim. We can also use client server architecture for more security purposes. Here we used single cloud architecture but in future multiple clouds can be used.

6. REFERENCES

[1] http://www.irjaet.com/Volume3-Issue-2/paper49.pdf

[2] https://www.ijarbest.com/journal/v2i3/519

[3] http://ijitech.org/uploads/652143IJIT9427-129.pdf

[4]https://www.oneidentity.com/products/cloud-access-manager

[5]https://www.slideshare.net/SafiUllah2/hospital-management-system-25384877

[6]Akshitasaxena ,NitinChaudhary, "Decimal attribute based encryption in cloud server",vol 5,issue 12,dec 2016.

[7]Danan Thilakanathana, Shiping Chenb, Surya Nepal B, Rafael Calvoa, Leila Alemb," A platform for secure monitoring and sharing of generic health data in the Cloud".

[8]Gurupreet Singh, Supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for information Security", Volume 67- No 19, April 2013.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89– 98