ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Attribute Based Encryption for Securing Personal Health Record on Cloud

[1] Deepali A.Gondkar, [2] Nisha.A.Auti, [3] Nilofer U.Sayyed
Department of Computer Engineering.
TSSM'S Bhivarabai Sawant College Of Engineering & Research,Narhe,Pune.

Abstract: - **Personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. The main aim of this research work is to propose a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access.**

I. INTRODUCTION

As we know personal health record are very sensitive information which we share with doctor that time it has to securely share and get used by authorized user. For that purpose our system is working which share the attribute of personal health record based on principal of attribute based encryption. Due to this technique the required fields are get assign to authorized party without giving whole information. Advantage of this is the information get secure and second the authorized user concentrate on required data rather than other things. For data we using encryption techniques which are changed based on attribute type .In our system we storing the personal health record on the cloud while it is in encrypted format so it is more secure from outside unauthorized user. Here while taking the input of personal health record it cover almost all field so that this database of personal health is more complete. All field are encrypted based on the type for example frequently used field get encrypted using RSA e.g. name, age. The image format data like x-ray report are get encrypted using DES. And remaining field are get encrypted using AES .e.g. address, pin code no etc. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patient's control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing.

Yet, issues such as risks of privacy exposure, flexible access and efficient user revocation have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi- trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Personal health record (PHR) is very sensitive information which get share. So to secure from unauthorized user the information stored in encrypted format on cloud. Due to cloud you can use your information from anywhere and on anytime. The data store on cloud database is up to date and easily scalable. In case of medical field the history of the patient health is play major role while deciding current treatment. That's why PHR helps in keeping record at high efficiency. At backend record are stored in encrypted format so it is highly secure. For encrypting the major encryption technique are used which are change based on field demand.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

II. OUR APPROACH

System provides the interface for taking personal health record field store it in encrypted format. It provide interface for storing the Doctor database, other authorities database. When admin and central authority decides the patient assigned to which doctor based requirement. Then only the doctor can access the patient data. When the patient ,and doctor database get created at that time the auto generated password get send to particular via mail so valid email address should be there further the that password change is depend on that user. Due this system user securely get login to the system. The doctor get patient data only when the central authority and admin approve it. If doctor need more attribute of patient he can make request of that attribute.

Cryptography is method by which we protect sensitive information. Due to this the storage and transmission get secure.
The process of encryption and decryption include few important terms

1. Plane text=the normal English words convening the sensitive information. Which we want to hide.
2. Cipher text=conversion of plain text to some unreadable text which is combination of symbol, character, number. In this we achieve that hide part. No one can get actual meaning of original data.
3. Encryption=In this by using encryption algorithm, key we can convert the plane text to cipher text.
4. Decryption=It's a reverse process in which we can convert cipher text to plain text using decryption algorithm and key.
5. Key=Is combination of symbol, number, character. Plays very important role at process of encryption and decryption.

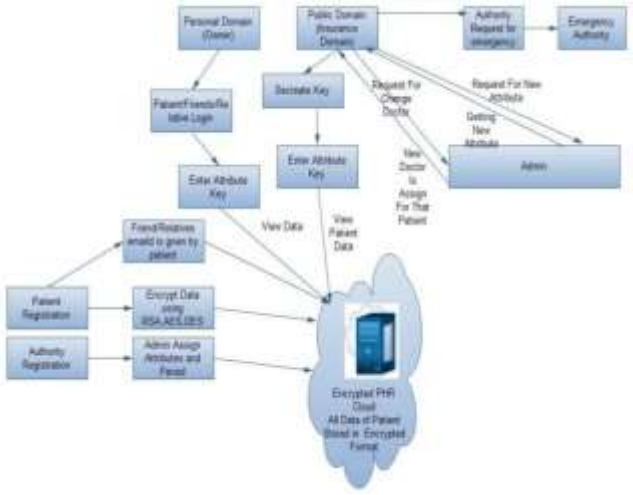
In the proposed work going to concentrate on tree technique of cryptography 1.RSA, 2.DES, 3.AES.

Following Processes will be involved in Project
• Data Encryption Before Insert Into Cloud
A PHR service allows a patient to create, manage and control her personal health data in one place through the web, which has made the storage, re- trivial and sharing of the medical information more efficient.
A feasible and promising approach would be to en- crypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary.

• Grouping of personal and Public Users (Personal and Public Domains) Each patient is owner of his/her PHR. During registration he/she can gives his/her friend or relative email id that can access his/her data. Patient and email id of friends or relative are present in personal domain while during registration we are assign doctor, nurse to that patient that authorities are present in public domain.

• Deal with Break-glass Access
For certain parts of the PHR data, medical staffs need to have temporary access complete data of patients. The medical staffs will need some temporary authorization (e.g., emergency key) to decrypt those all data. Under our framework, this can be naturally achieved by letting each patient delegate her emergency key to an emergency department (ED).

SYSTEM OVERVIEW



DETAIL SPECIFICATION

Personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. PHR system is deal patient information .It update the information based on updates. For deciding new treatment this previous information play very important role .

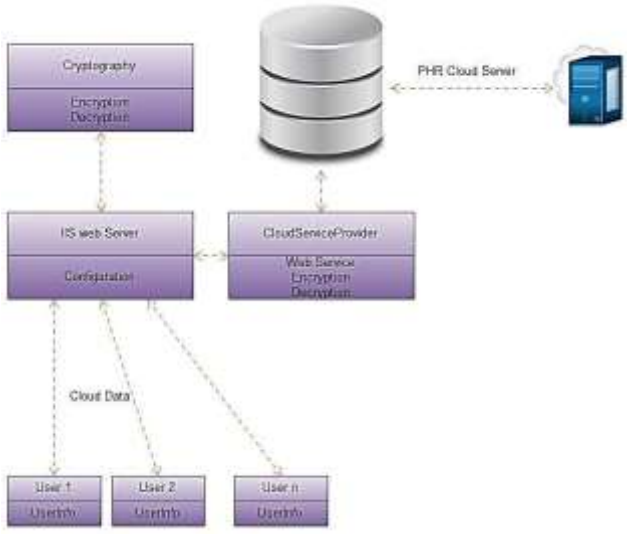
ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

First is login page where we can perform four operations 1>create new user account for doctor, nurse, health care providers
2>create patient account 3> forgot password
Once the account for new user get created it get approved by two authority 1.central authority 2.admin
After this approval only that new user can login to system to view the required data such login have to choose role as general
There are three category in role 1>General 2>Central authority 3>Admin
We have to select the role and give the appropriate user name, and password to enter into the system .While creating new user account that user decides the username and system generated password get mail to that user email address given while creating the account.
New user account creation form having following fields

User name, First name, last name, email address, phone number, age, address ,country here our system give two option India, America ,Hospital name according to country the list of hospital get change. Our system cover few hospital in each country in given list , This new user while creating account have to decide the role there few option as Doctor, Nurse, researcher, visitor, therapist, medical lab technologist, dietitian, accountant, emergency authority, police

III. DETAIL WORKING



MATHEMATICAL MODEL

Encryption

1. Input: Attribute Value (Attr).
2. Get Byte [](B1) of that Attr.
3. Generate Public Key (Pk).
4. Perform Encryption on B1.
5. Convert B1 into string (EAttr).

Decryption

1. Input: Encrypted attribute value (EAttr)
2. Convert EAttr into byte [](B2).
3. Generate Private Key.
4. Perform Decryption on B2.
5. Convert B2 into string (DAttr).

Secrete Key

1. Input : Private Key (see Decryption-3) and No. of Authority (NAuth) =10.
2. Get Length of private key Length = Private Key. Length.
3. To become private key multiple of NAuth(i.e. 10) padd it by zero (0).
4. M = Length / NAuth
Each authority having 'M' no. of bytes.

For Each Byte value from 'M'.
For (int I = 0 ; I <M.Length ; i++)
{
Square = M[i] * M[i]; Hexvalue = Hex (Square); Hexvalue = Hexvalue+"&" Fullhexvalue = Fullhexvalue +
Hexvalue;
}
5. Add this Hex value into database as a secret key.
Attribute Key Generation

1. List = List of Attribute assign to the user (Authorities).
2. For each (string Attribute in List)
{
For each (char in Attribute)
{
Value = Value + ch;
}
}
3. In the Value we get ASCII value of that character.
4. ASCII values save into database

IV. RESULT

1) Client Application with Login System:-
Here User of system Enter The user name and password and see the record in the account. The password is highly secure. While creation of new account the password get mail to particular user.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

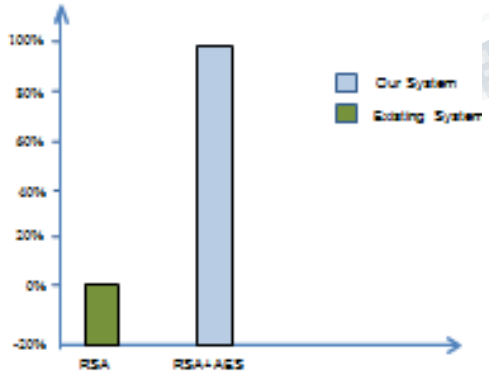
2) Patient Registration with encryption in PHR Cloud Server:-
When the patient information get imported in system database it is in encrypted format. So that it is more secure. Based on attribute type the encryption techniques get change. Encryption techniques used are 1.RSA, 2.DES,3.AES.

3) Revoke Attributes:-
When any new user registration is done. At that time it get approved from admin and central authority. Then the user can access the attribute which are assign to them .If they require more attribute he can put request.

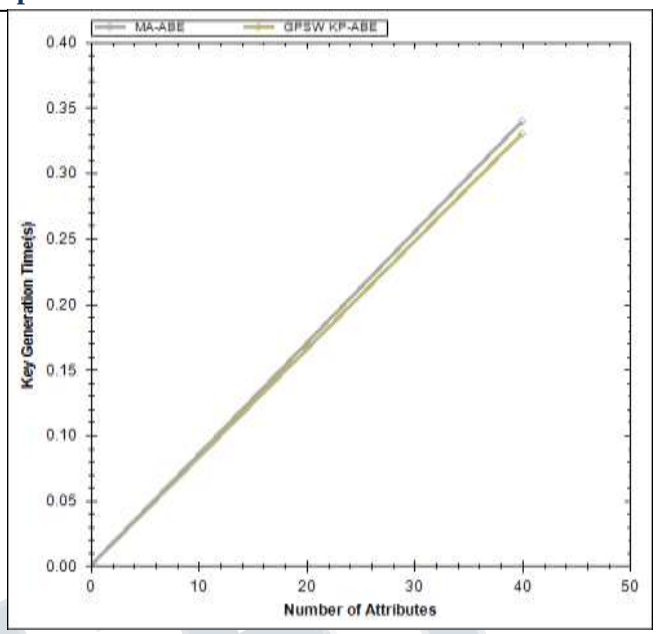
4) Break Glass System:-
In case of emergency the all attribute get to the doctor based on condition which are get assigned by emergency authority.

Comparative Study
RSA+AES:-RSA algorithm is inefficient for searching due to encryption of same input produces different output. So when we search, it does not produce exact result. It just prompts "Match not found". Although there is a record in database. So the best solution is AES algorithm which has good searching efficiency. It creates same result for same input. Apart from this there are more innovative changes in other module than existing system

Performance Graph



each time encryption result different. That's why though patient's record present in database then also it gives 'not available' as a result. So our system uses AES (Advanced Encryption Standard) algorithm for searching which is very efficient and give exact result. So searching is fast and accurate

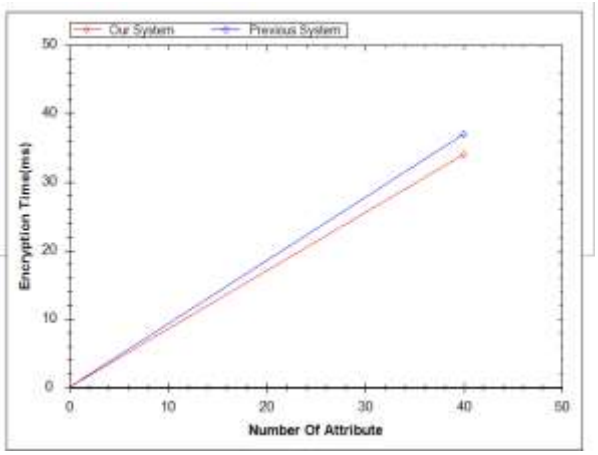


Key Generation Time

In the encryption and decryption key generation is playing very important role. The security of algorithm is based on key generation factor. While generating key, the key generation time and number of attribute play role to decide efficiency. In KP-ABE(Key Policy –Attribute based encryption), during registration of each authorities key is generated and that is too long so it takes more time. While in MA-ABE(Multi authority attribute based encryption) for each authority having different key and it is shorter than KP-ABE so it takes less time than KP-ABE. In KP-ABE key is generated by considering all authorities while in MA-ABE key is generated by considering only registering authority not all authorities.

Algorithm	Key length
RSA(Rivest Shamir Aldeman)	>1024 bits
AES(Advanced Encryption Standard)	56 bit
DES(Data Encryption Standard)	138, 192, 256 bits

Encryption Time:
In encryption time there is consideration of only RSA. RSA generate key which is too long and after generating key, it will encrypt requested data. But when we use RSA+AES+DES, AES and DES use symmetric key cryptography so it will take less time for encryption than RSA Asymmetric Key.



Decryption Time:
In decryption time, RSA needs both keys public and private. Therefore for each request it need to generate both keys so it takes times for decryption but when we use RSA+AES+DES algorithm AES and DES are symmetric key cryptography algorithm then need only one key for encryption and decryption so it takes less time than only using RSA.

V. CONCLUSION

In this way research is helpful for efficient and secure access of sensitive Personal Health Record(PHR). In database the personal information get store using encryption techniques that is why it is more secure and other advantage is based on attribute type the encryption technique get change so that it get more secure and efficient. The break glass is other more powerful feature of this system. The system a provide the simple interface which cover all the important attributes of Personal Health Record (PHR). This system is helpful for all the user which are in different role

REFERENCES

[1] Ming Li Member,IEEE,Shucheng Yu, IEEE, Yao Zheng, Student Member ,IEEE,KuiRen Senior Member,IEEE,andWenjing Lou,Senior Member,IEEE,",Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption ,"IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEMS VOL. XX,NO. XX,XX 2012.

[2] M.Li,S.Yu,K.Ren, and W. Lou," Securing personal health records in cloud computing patient-centric and fine- grained dataaccess control in multi-owner settings," in SecureComm'10,Sept 2010,pp.89-106.

[3] S.Yu.C.Wang, K.Ren and W. Lou, "Achieving secure scalable and fine grained data access control in cloud computing , " in IEEE INFOCOM'10,2010.

[4]A.Boldyreva, V.Goyal, and V.Kumar,"Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08,2008,pp.417-426.

[5]M. Pirretti, P. Traynor, P.McDaniel, and B. Waters, "Secure attribute-based systems" Journal of Computer Security, vol. 18, no 5,pp 799-837,2010.

[6]B.Lynn, "The pbc library,"http://crypto.stanford.edu /pbc/.

[7]Y.Zheng, "Key-policy attribute based encryption scheme implementation,"http://www.cnsr.ictas.vt.edu /resources.html.