Securing Personal Health Records By Utilizing Multi-Authority Attribute Based Encryption

Mitali Katkar, Priya Keshri,Akash Ekunde,Namrata More

Engineer, computer Engineering, Indira college of engineering and management ,Maharashtra, India
Engineer, computer Engineering, Indira college of engineering and management ,Maharashtra, India
Engineer, computer Engineering, Indira college of engineering and management ,Maharashtra, India
Engineer ,computer Engineering, Indira college of engineering and management ,Maharashtra, India

ABSTRACT

*Personal health records (PHR) is an emerging patient-centric model of health information exchange which is often outsourced to be stored at third party such as cloud providers. There have been wide privacy concern as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients control over access to their own records ,it is one of the method to encrypt the PHRS before outsourcing. Yet issues such as risk of privacy exposure, scalability in key management , flexible access and efficient user revocation have remained the most challenges towards achieving fine-grained cryptographically enforced data access control. We propose a novel of patient-centric framework and a suite of mechanisms for data access control for records, we leverage attribute based encryption (ABE) techniques to encrypt each patients PHR file. Different in securing data outsourcing, we focus on the multiple data owner scenarios and divide the users in the records system into multiple security domains that greatly reduces the key management complexities for owners and users. A high degree of patient privacy is guaranteed by exploiting multi-authority.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. Extensive analytical and experimental results are presented which show the security, scalability and efficiency. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. Our security analysis is secure under the decisional bilinear Diffie-hellman assumption***.***

Keyword: - ***attribute based Encryption*** *, multi-authority, fine grained, and revocation*

1. INTRODUCTION

We work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability one to many encryption methods such as Attribute based encryption can be used. In Attribute based encryption data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient. In addition, the encrypter is not required to know the ACL. Using Encryption, access policies are expressed based on the attributes of users or data which enables a patient to selectively share her/his records among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption , key generation and decryption are only linear with the number of attributes involved.

1.1 OBJECTIVE AND GOALS

1. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed .
2. Input design is the process of converting a user-oriented description of the input into a computer based system. This design is to avoid errors in the data input process and show the correct direction
3. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors.

1.2 SCOPE

To provide high security and privacy for personal health records, existing multi-authority attribute based encryption could be further enhanced to proactive multi authority attribute based encryption.

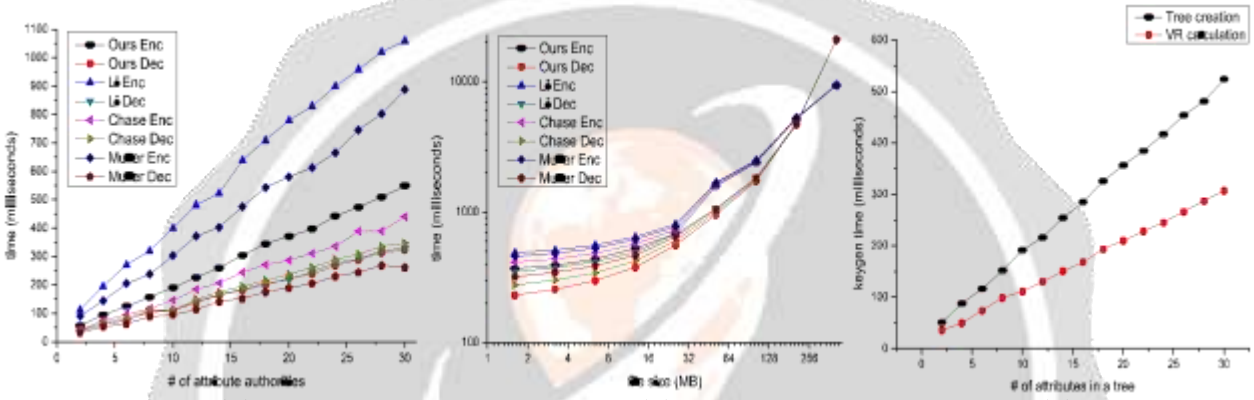
2. LITERATURE SURVEY

Attribute based encryption for fine-grained data access control:

A generalization of identity-based encryption that corporate attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that multiple users who possess can decrypt properly. Attribute based encryption not only deals with fine-grained access control but also prevents against collusion

Key policy attribute based encryption:

It is the modified form of the classical model of encryption. Exploring key policy attribute based encryption scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that can decrypt the data. It is the public key encryption technique that is designed for one to many communications.



(A) (B) (C)

. (A) Encryption and decryption time with different attributes number. File size is 100KB.
(B) Encryption and decryption time with different file size. 20 attributes in T_0.
(C) Time to create a privilege tree and decrypt a verification parameter from

SYSTEM ARCHITECTURE:

The encryption schemes has various process each as key generation, encryption, decryption, evaluation. This scheme is becomes homo-morphic which means it does not grow too large regardless of the complexities of its functions. The multi-authority attribute based encryption is the advanced attribute based encryption in which it will have many attribute authorities for handling the different data sets of users from various domains.

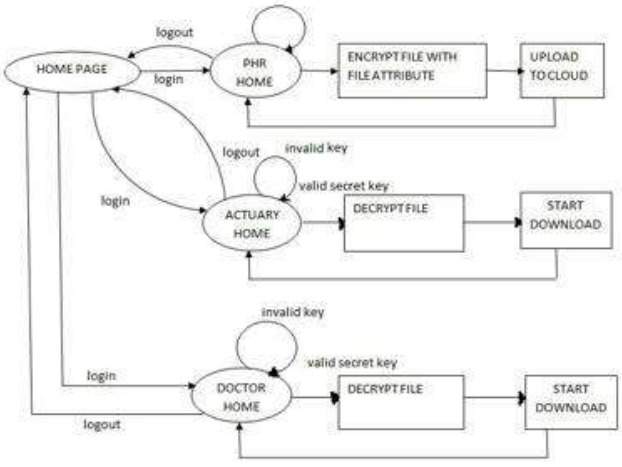


Fig -1: **SYSTEM ARCHITECTURE DIAGRAM**

2.1 Risk Management

For risk identification, scope document, requirements specifications and scheduling is done. The risks for the project can be analyzed within the constraint of time and quality

Table -1: Risk Table

ID	description	schedule	quality	overall
1.	algorithm	low	high	high
2.	implementation	low	high	high

2.2 Homo-morphic Encryption

An encryption scheme has algorithm consist of steps:

- Key generation – create two keys that is the private key prk and the public key puk.
- Encryption – encrypts the plaintext P with the public key puk to yield cipher-text
- Decryption –encrypts the cipher-text C with the privacy key prk to retrieve the plaintext P.
- Evaluation – outputs a cipher-text C of f(P)such that Decrypt (prk,P)=f(P).

3. Algorithm1: 1-Out-of-2 Oblivious Transfer

1: Bob randomly picks a secret *s* and publishes *gs* to Alice.
2: Alice creates an encryption/decryption key pair:{*gr* , *r* }
3: Alice chooses *i* and calculates *EKi* = *gr* , *EKi*−1 = *gs gr*and sends *EK*0 to Bob.
4: Bob calculates *EK*1 = *gsEK*0and encrypts *M*0 using*EK*0 and *M*1 using *EK*1 and sends two cipher texts *EEK*0 *(M*0*), EEK*1 *(M*1*)* to Alice.
5: Alice can use *r* to decrypt the desired cipher text *EEKi (Mi)*, but she cannot decrypt the other one. Meanwhile, Bob does not know which cipher text is decrypted.

Algorithm 2 1-Out-of-*n* Oblivious Transfer

1: Bob randomly picks *n* secrets *s*1, . . . , *sn* and calculates *ti* as follows:
$\forall i \in \{1, \ldots, n\} : ti = s1 \oplus \cdots \oplus si-1 \oplus Mi$
2: For each $i \in \{1, \ldots, n\}$, Bob and Alice are engaged in a 1-out-of-2 OT where Bob's first message is *ti* and the second message is *si* . Alice picks *ti* to receive if she wants *Mi* and *si* otherwise.
3: After Alice receives *n* components, she has $ti = s1 \oplus \cdots \oplus si-1 \oplus Mi$ for the *i* she wants and *sk* for $k \_= i$, she can recover the *Mi* by $Mi = ti \oplus si-1 \oplus si-2 \oplus \cdots \oplus s1$

In an 1-out-of-*n* OT, the sender Bob has n messages $M_1, \ldots, M_n$, and the receiver Alice wants to pick one M_i from those $M_1, \ldots, M_n$. Alice successfully achieves M_i without knowing any useful information about other messages, and Bob does not know which M_i is picked by Alice.

We use the 1-out-of-2 OT (Algorithm 1), in which Alice picks M_i from Bob's M_0, M_1, to introduce the 1-out-of-*n* OT described in Algorithm 2.

In Algorithm 2, Alice can achieve M_i if and only if she picks t_i for the i she wants the message and s_k for any $k = i$. If she picks several t_k's, some s_k's are missing and she is not able to recover any message

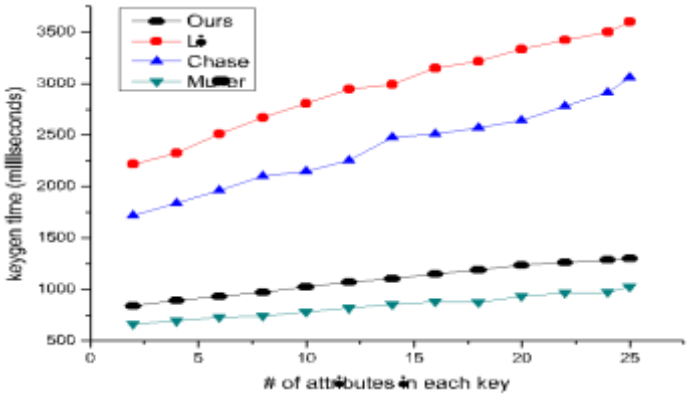


Chart -2:Key generation time with different attributes.

3.1 Related work

A multi-authority system is presented in which each user has an ID and they can interact with each key generator (authority) using different pseudonyms. One user's different pseudonyms are tied to his private key, but key generators never know about the private keys, and thus they are not able to link multiple pseudonyms belonging to the same user. Also, the whole attributes set is divided into *N* disjoint sets and managed by *N* attributes authorities.

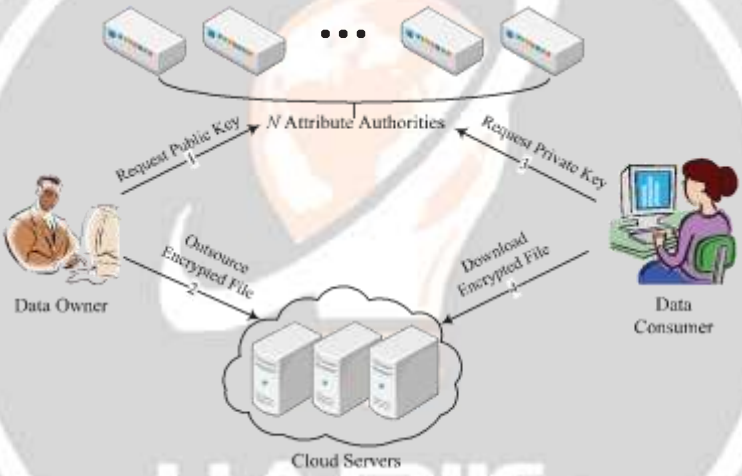


Fig -2: General flow

A ciphertext is associated with a set of attributes, and a private key is associated with a monotonic access structure like a tree, which describes this user's identity. A user can decrypt the ciphertext if and only if the access tree in his private key is satisfied by the attributes in the ciphertext. However, the encryption policy is described in the keys, so the encryptor does not have entire control over the encryption policy. He has to trust that the key generators issue keys with correct structures to correct users. Furthermore, when a re-encryption occurs, all of the users in the same system must have their private keys re-issued so as to gain access to the re-encrypted files, and this process causes considerable problems in implementation.

4. CONCLUSIONS

We have implemented a framework of secure sharing of personal health records, we argue that to fully realize the patient-centric concept, patient should have complete control of their own privacy through encrypting their record file to allow fine-grained access. The framework addresses the unique challenges brought by multiple record owners and users in which it greatly reduce the complexity of key management. We utilize Attribute based encryption to encrypt the personal health record data so that patients can allow access to not only by personal users but also various users from public domains with different professional roles, qualifications and affiliations.

5. REFERENCES

[1]. Masahiro Yagisawa resident in yokohama shi sakae ku. Yokohama shi.japan " Key distribution system and attribute based encryption on non communicative ring".
[2].Soumya parvatikar, puja prakash,richa prakash,pragati dhawale,s.b jadhav" Secure sharing of personal health records using multi authority attribute based encryption in cloud computing".
[3]. Taeho Jung, Xiang-Yang Li, *Senior Member, IEEE*, Zhiguo Wan, and Meng Wan, *Member, IEEE "* Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption".
[4]. W.-G. Tzeng, "Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters," IEEE Trans. Computer., vol. 53, no. 2, Feb. 2004.