International Journal of Computer and Internet Security.
ISSN 0974-2247 Volume 7, Number 1 (2015), pp. 7-12

http://www.irphouse.com

Privacy Confined Personal Health Records Using Attribute Based Encryption

Aravind. B[1] and Arun Kumar. A[2]

Final year, B.Tech Information Technology,
Sri Ramakrishna Engineering College, Coimbatore-641022.

ABSTRACT

The Personal Health Records (PHR) storage over internet is a spiking trend of health information interchange, which is mostly stored in third-party's cloud server. The vital concern over that personal health information is the privacy which is prone to exposure to those third party servers and unauthorized parties. So, there is a need for a mechanism with fine-grained access control and encryption methods for the PHRs stored in semi trusted servers. The main counterpart of this system is an Encryption mechanism known as Attribute Based Encryption(ABE) that is put into work in a multi-user environment with efficient reduced key-management policies and dynamicity of the access policies which is put together with on-demand attribute revocation and break glass policy in case of emergency situations.

Keywords—Personal health records, data privacy, access control, attribute based encryption.

1. INTRODUCTION

The PHR is an online based service that allows a patient to create, manage and take over control over the whole medical record that is previously stored in a semi trusted server. The web enables a user to share, store, retrieve data and edit a data in a very efficient way, especially in environments where many number of users are being involved with the system access. Many of the third party storage servers are outsourced to provide efficient PHR services [1,2].

Attribute based Encryption (ABE) is a more satisfying approach[3] in securing the health information data and it achieves a fine-grained data control and provides a way different access policies based on attributes of the particular user, or an object. The vital point of this system is to prove the patients whether their sensitive health information is secure when being stored in a third-party server.

2. BACKGROUND

The objective is to provide feasible and promising data encryption methods over PHRs before they are getting outsourced. So, the decryption key provided to a particular user is available with the details which remain confidential to the rest of the users. We propose a patient centric model over two different domain such as Public and Private domains where Public domains contain multiauthority-ABE (MA-ABE) since it involves a varied set of users. And personal domains use a minimal key-management overhead for both users and also the owners of the system. Multiple ownerships may be doctors, lab technicians, pharmacists, etc. So the personalized and the professionalized system is a necessary in order to protect the health information stored elsewhere.

The integration of ABE into this system is to reduce the up-to-date issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation which are nonfatal to solve.

3. PATIENT CENTRIC FRAMEWORK

a. Problem Description

The PHR system[2,4] is where a variety of users get involved for data access. The owners are the patients who have overall access to the data and the users are the ones who are given some control of access over the data. There is a centralized storage for storing the PHR of the owner and the users have rights to access over few parts of the original information. The access rights are being provided by the corresponding PHRs itself where it can be handled by multiple users.

So there is a need for Attribute Based Encryption for this environment which provides and efficient data access policies [3] and secure form of health information sharing. Due to nature of web storage structure, the health information is stored in a hierarchical manner.

b. Proposed Work

In the proposed system, there are multiple user situations involved: for each PSD, the key policy ABE is implemented, and for PUD, the previously reported multiple authority ABE is adopted. In the uploaded personal health record, only certain users are allowed to access over selected attributes of owner. The revocation of users is being done by the PHR owner's client web application in a similar way the user's access privileges are revoked.

When a situation of emergency arrives, the regular access policies are open up temporarily to access the identity of the owner, obtain temporary read keys and can be performed only by the Emergency Department (ED) in order to prevent the false usage of break-glass option. After the situation is under control the Emergency access is revoked again by owner, via ED.

4. ARCHITECTURE

The PHRs are stored on a semi trusted servers[2]. The health report is based on the

Attribute Based Encryption Algorithm that enhances the way of encryption of attributes and user revocation along with dynamic access control policies. The secret keys are provided to the users of the system by the multi authority ABE and the temporary keys are retrieved by the Emergency department which has a name known as Break-glass option.

The owners have the ability to distribute the secret keys with read or write access according to the privileges given for each user of the system[5]. The system is clearly illustrated in Fig 1.

Fig 1: System Architecture

5. WORK OF ATTRIBUTE BASED ENCRYPTION

a. Algorithm

ABE Algorithm (along with Advanced Encryption Standard Algorithm)

```
Cipher(byte in[16], byte out[16], key_array r_key[N+1])
begin
byte state[16];
state = in;
AddRKey(state, r_key[0]);
for i = 1 to N-1 stepsize 1 do
SubBytes(state);
ShiftRows(state);
MixColumns(state);
AddRKey(state, r_key[i]);
end for
SubBytes(state);
ShiftRows(state);
AddRKey(state, r_key[N]);
```

End

b. Algorithm for Attribute Key Setup

Step 1: It outputs the master keys and public keys for A as a set of Attributes [5,6].
Step 2: Associate every attribute in A with universe of attribute as U= {1, 2, 3, …, n}.
Step 3: Associate each attributes i U with a number ti and also chose y uniformly at random in public parameter (Zp*) and y.
Step 4: The public key will be:
PK = (T1= gt1,…, T1 = gt | U | , Y = e (g, g) y).
Step 5: The master key will be:
MK = (t1,…, t | U | y).

c. KP-ABE Encryption

- M message in G_T has a set of attributes γ PK is considered as a Public key. Output of the Cipher Text will be E.
- Choose a random value in Zp as s. Encrypt any secret message M in G_T with a set of attributes γ .
- Now the cipher text will be: E=(γ,E'=MY s, {Ei=Ti s} where iϵγ)

d. KP-ABE Key Generation

This algorithm will give out a secret key D along with an access T. So, the access A is realized by the following steps:

- For root node r, set secret_value= y. mark all node un-assigned and mark root node assigned
- Recursively, for each assigned non-leaf node the procedure is as follows,
- If the AND operator and its child nodes are un-assigned, let n be the number of child nodes, set the value of each, except the last child node, to be Si Zp, and the value of the last node to be sn = s -Σ si.
- If the operator V is set as s then mark the node as assigned.
- For each leaf attribute aj,i ∈ T, compute D_j;
  i=Tj^si
  Output: Secret Key Sk= {D_j, i}

e. KP-ABE Decryption

The KP-ABE algorithm[5] takes as input the cipher text E encrypted under the attribute set U, the user's Secret Key (K) for access tree T, and the public key PK. Finally it output the message M if and only if U satisfies T.

6. RESULTS

The main goal of the proposed framework is to realize the patient centric concept for controlling their privacy over PHRs and thus allowing a fine grained access. The system allows the owner to contain dynamicity in policies[6], reduced key management complexity, efficient and secure health record maintenance even though the information is stored in semi trusted servers.

7. BREAK GLASS ACCESS

It is generally sharing a single privilege among all the users of the system at a particular point of time. The use of Break-glass option should be ease-of-use as well as preserving the security of the existing system[7]. The option will be active for a certain amount of time and will be revoked by the owner after the emergency situation gets into control.

It provides greater data confidentiality despite it has an open access but on-demand user revocation and other such techniques are not applicable as in the normally functioning system. The owner actually embeds the 'emergency' function into the PHR where few users are involved as in personal domains. It is built into the PSD section of the cipher text of every health record so that the system is allowing for Break glass policy.

8. CONCLUSION

In this system, the arguments over semi trusted servers storing PHR files are concluded with a system design containing end-to-end privacy for owners to encrypt their files allowing a fine grained access. The ABE is an algorithm well utilized to suit the needs of the users providing secret keys of its kind and sharing only certain content of the whole information to save the PHR from false accessions. The enhanced privacy part of the system guarantees with the previous works. For further works, the MA-ABE is to be enhanced more for the betterment of the efficiency, on-demand revocation and also to improve the security in a wide range.

9. REFERENCES

[1] Ming Li and Shucheng Yu,"Scalable and Secure Sharing of PersonalHealth Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, January 2013

[2] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006

[4] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int' ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89- 106, Sept. 2010

[5] D. Boneh, G.D. Crescenzo, R. Ostrovsky, and G. Persiano. Public-Key Encryption with Keyword Search. In Advances in Cryptology – Eurocrypt, volume 3027 of LNCS, pages 506–522. Springer, 2004.

[6] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Patient Self-Controllable Access Policy on Phi in Ehealthcare Systems," Proc. Advances in Health Informatics Conf. (AHIC 10), 2010.

[7] Cheng Kang Chu, Sheman S.M,Chow, Wen Guey Tzdeng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 468-477, Feb. 2014