Patient Centric Health Model using Attribute Based Encryption

Mr. A.Arokiaraj Jovith, Ms. P. V Sai Vaishnavi

Abstract— The terms Internet and Cloud play a major role in this era of innovations. They provide a new way of optimizing resources and cost. Due to its 'pay as you use' policy most of the industries are moving towards this cloud based model, with this the Health care industry also drifted towards the cloud model. In cloud model the data is out sourced to a third party for maintenance. Even though the adoption of cloud model is a futuristic move, there are lot of concerns with privacy and confidentiality being the major one. This paper discusses about a health care model that can provide security to data stored at a third party site. This model is basically a web based application that provides access to health information. The control of access is completely owned by the patient. Attribute Based Encryption is used for encrypting the medical records and to a large extent provides fine grained level of access control.

Index Terms— Attribute Based Encryption, Cloud, confidentiality, Health care, pay as you use,Access Control,Patient Health Records

1 INTRODUCTION

1. Introduction

Cloud computing in general is referred to as an On demand, self-service internet Infrastructure that enables access of resource anytime and from anywhere [1].Cloud computing is not only changing the business models but also the way in which the Information Technology infrastructure is constructed and consumed.

1.1 Why should health care industry drift towards cloud model [2]

Most of the industries have data stored in the form of electronic records. In health care the medical records are stored on the Centralized Server in the form of electronic records. A patient typically might have multiple health care providers. Currently each provider have their own medical information database. There are scenarios where the electronic medical records [EMR] should be shared across different entities, In this case there is a problem of interoperability which is extremely slow, and apart from it cost and usability are also cause of concerns. Adoption of cloud model will solve the stated concerns for both owners and providers.

1.2 Confidentiality and Privacy of Medical Health Records as an important concern [3]

To reap the promise of the digital health information and to achieve smart spending on health, It is important that the user of the service have complete trust that their information is in safe hands, if this level of trust is not achieved then it is possible that they may not reveal accurate information, which may lead to life threatening consequences

From the service providers' point of view, if the privacy of data is compromised it will cause damage to reputation of the organization, financial harm and harm to their users.

1.3 Encryption [4]

With Health Records being out sourced, the privacy and confidentiality is at stake. This leads to the requirement of encrypting the data before the data is being out sourced .In this project Attribute Based Encryption mechanism was adopted for the same

1.4 ATTRIBUTE BASED ENCRYPTION [ABE]

In ABE user's private key and cipher text are labelled with set of descriptive attributes and access policies respectively. A particular key can decrypt a particular cipher text only if the corresponding attributes and access policies match
There are three types of ABE techniques

1.4.1 Key-Policy Based ABE [5]

In a key-policy attribute-based encryption (KP-ABE) system, cipher texts are labeled by the sender with a set of descriptive attributes, while user's private key issued by the trusted attribute authority captures a policy (also called the access structure) that specifies which type of cipher texts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast

1.4.2 Cipher text-Policy Based ABE

In a cipher text policy attribute-based encryption (CP-ABE) system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the cipher text, stating what kind of receivers will be able to decrypt the cipher text. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority. Such a user can decrypt a cipher text if his/her attributes satisfy the access policy associated with the cipher text. Thus, CP-ABE mechanism is conceptually closer to traditional role-based access control method**.**

1.4.3 Multi Authority Based ABE [6]

In a multi-authority ABE system, we have many attribute authorities, and many users. There are also a set of system wide public parameters available to everyone (either created by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the cipher text. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

2 RELATED WORK

Some of the cryptographic solutions before Attribute Based Encryption came into effect are as follows

Symmetric key cryptographic solutions

In this technique, same key is used for encrypting the plain text as well as to decrypt the cipher text. In other words there exists a shared secret between two parties, for protecting the information. This method became less prevalent later due to reduced scalability that can be achieved.

Public key cryptographic solutions

In this technique, a key pair is used namely public key and private key. One key is used for encryption, while the other can be used for decryption i.e., if public key is used for encryption, the secret key or private key is used for decryption and vice-versa. The main disadvantage of this method is key management becomes an overhead

3 Patient Centric Model

We endeavor to study the patient centric, secure sharing of Medical records stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive.

Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR 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.

3.1 Modules

1.Registration

2 .Upload files

3. ABE for Fine-grained Data Access Control

4.Setup and Key Distribution

5.Break-glass

Registration

This is a simple module, where multiple users of the health model be it patients, physician, pharmacist or any other third party user register themselves in order to start using the health care e-service. The registration involves, providing basic details and other role specific details as required

Upload Files

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted files to the server. Each owner's file is encrypted under a certain fine grained model.

ABE for Fine-grained Data Access Control

In this module ABE is used to realize fine grained access control for outsourced data , where each patient's electronic health record files are encrypted using a broadcast variant of Cipher text-Policy Based Encryption

Setup and key distribution

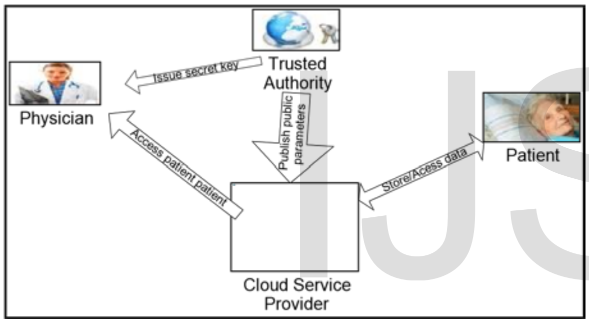
There are two ways for distributing secret keys.

First, a health record owner can specify the access privilege of a data reader in her access policy, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in Google Doc

Second, a reader could obtain the secret key by sending a request (indicating which types of files she wants to access) to the owner via portal, and the owner will grant her a subset of requested data
Types. Based on that, the policy engine of the application automatically derives an access structure, and runs key generation algorithm to generate the user secret key that embeds her access structure.

BREAK-GLASS

In this module when an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break glass access is needed to access the victim's Health Records (HR). In our framework, each owner's HR's access right is also delegated to an emergency department (ED) to prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.



4

Fig 1. Architecture

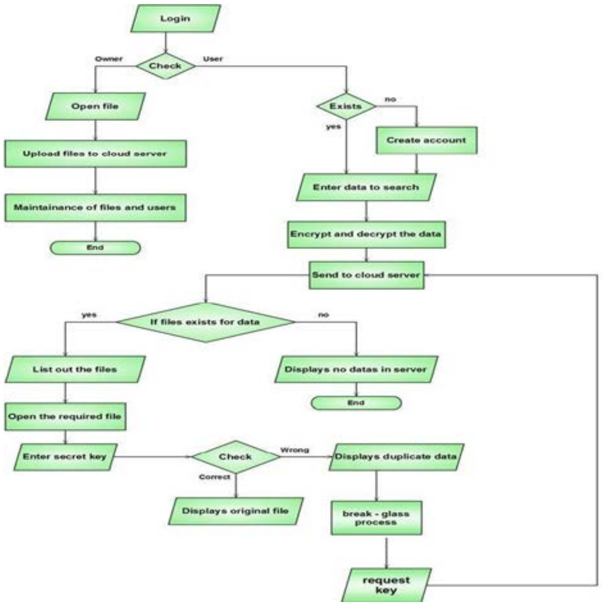


FIG 2. FLOW DIAGRAM

Setup This algorithm takes as input a security parameter κ. and returns the public key *PK* as well as a system master secret key *MK*. *PK* is used by message senders for encryption. *MK* is used to generate user secret keys and is known only to the authority.

Encrypt This algorithm takes as input the public parameter *PK*, a message *M*, and an access structure *T*. It outputs the cipher text *CT*.

KeyGen This algorithm takes as input a set of attributes γ associated with the user and the master secret key *MK*. It outputs a secret key *SK* that enables the user to decrypt a message encrypted under an access structure *T* if and only if γ matches *T*.

Decrypt This algorithm takes as input the cipher text *CT* and a secret key *SK* for an attributes set γ. It returns the message *M* if and only if γ satisfies the access structure associated with the cipher text *CT*

Algorithm Definition

Setup(1^λ) It takes as input the security parameter 1^λ and outputs the system master key *MK* and public parameters *PK*. *ver* is initialized as 1.
Enc(*M,AS,PK*) It takes as input a message *M*, an access structure *AS*, and current public parameters *PK*, and outputs a cipher text *CT*.

KeyGen(*MK,S*) It takes as input current system master key *MK* and a set of attributes *S* that describes the key. It outputs a user secret key *SK* in the form of
$(ver, S, D, \bar{D} = \{D_i, F_i\}_{i \in S})$.

Dec(*CT,PK,SK*) It takes as input a cipher text *CT*, public parameters *PK*, and the user secret key *SK* having the same version with *CT*. It outputs the message *M* if the attribute set of *SK* satisfies the cipher text access structure.

Otherwise, it returns ⊥ with an overwhelming probability

Advantages of Patient Centric Model

- Accurate Storage of information
- Maximum control given to data owners
- Privacy is preserved to a large extent
- Well defined procedure to handle emergency
- Less overhead in key management

4. Conclusion

The Health Information Records needed protection from hackers and crackers. The proposed method can provide basic security to the health care system, using Attribute Based Encryption [ABE]. Since this system is unique based on access conditions, it is not easily hack able also reduced key management and better privacy were observed.

The Future work may try to increase the level security compared to the existing one.

5. Acknowledgement

This research paper was done by me as part of 2 years master's degree in Information Security and cyber forensics. I have tried my level best to present this information as clearly as possible using basic terms that I hope will be

I have completed this paper under the able guidance and supervision of my professor Mr. A.ArokiaRaj Jovith .I will be failed in my duty if I do not acknowledge the esteemed scholarly guidance, assistance and knowledge I have received for timely and fruitful completion of this work

Mere acknowledgment may not redeem the debt I owe to my parents for their support during the entire course of this project

Last but not the least, I am thankful to all the faculties of my department and my friends for their co-operation and support.

5. References

[1] Mell P, Grance T. The NIST definition of cloud computing. Communication ACM. 2010; 53(6):50.

[2] Security models and requirements for health care application clouds;Rui Zang and Ling Liu

[3] Guidelines as per office of the national coordinator for health information technology

[4] Bharti Ratan Madnani1, Sreedevi N2, Attribute Based Encryption for Scalable and Secure sharing of Health Records in cloud computing design and implementation. International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013

[5] 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

[6] M. Chase and S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp. 121–130.

About the authors:

Mr.Arokia Raj Jovith: Works as an Assistant Professor(Senior Grade)
in Department of Information Technology at SRM University, Chennai

Ms. P V Sai Vaishnavi: is a student purusing Master of Technology in Information Security and Cyber Forensics at SRM University, Chennai