

Data Security on Cloud Network using Key Policy Attribute Based Encryption

Lavanya Natarajan¹, Sujata Kulkarni²

Electronics and Telecommunication, Thakur College of Engineering and Technology, Mumbai, India ^{1,2}

Abstract: The advent of technology in healthcare ensures medical services to be provided more efficiently. Medical services are now provided through online assistance as well and the patients can maintain their health-related data in the cloud network. Personal health record (PHR) is deployed on the public cloud network. So, the data has to be stored on a central server which is guarded by the access control mechanism. But the data owners lose control on the data from the moment the data is stored in the server. Therefore, these systems do not fulfil the requirements of data outsourcing scheme. It is essential to ensure that the third party storing the data does not gain access to the plain data. In order to enhance security to the personal health records, attribute based encryption is used to encrypt the data before outsourcing it to the cloud. Personal health record users are divided into public and private domains. This will reduce the key management problem for owners and users. The proposed scheme will give personal health record owners full control of his/her data using Attribute based Encryption (ABE). In the proposed Key Policy Attribute Based Encryption (KP-ABE) scheme, the keys are only associated with the policy which have to be satisfied by the attributes to decrypt the data. Immense security and performance analysis based on computation time and key generation speed shows that the proposed scheme is highly efficient.

Keywords: Personal Health record, Attribute based Encryption, Key Policy Attribute Based Encryption.

I. INTRODUCTION

In cloud network, various services are provided via internet with greater flexibility and availability at lower cost. Personal Health Record (PHR) is a tool used to collect, track and share past and current information about the health of someone in your care. Due to the high cost of building and maintaining data centres, third-party service providers provide PHR service. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A convenient and reliable approach is encrypting the data before outsourcing it to the cloud network. Basically, the PHR owner themselves should decide how to encrypt their files and to allow which set of users to obtain access to each file.

A PHR file should be accessible to users who are provided with the decryption key (Secret Key), while remain inaccessible to the rest. And the patient shall retain the right to revoke the access privileges whenever they feel it is necessary. The authenticated users can access the PHR for personal use or professional purposes depending on their requirement. We divide types of users into two domains, personal domain and public domain. To protect personal health data stored on semi-trusted servers, we adopt attribute-based encryption as main encryption primitive. Using ABE, access policies are expressed based on attributes of users or data.

In this paper, we propose a scheme that allows health organizations to store encrypted health data in the cloud. The proposed framework works as follows. First the central database where health data are stored in encrypted format is shared with authorized users only. The data owner decides who can access their health information. Thus, a secure access policy is enforced in the system.

II. RELATED WORK

PHR (Personal Health Record) is used to store health-related data in a documented format and maintained by the individual it concerns with. According to the U.S. Department of Health and Human Services, a personal health record (PHR) is similar document maintained by the owner of the record. But the access can be given to limited people like doctor. In an electronic health record system [1], patients, healthcare providers, and medical devices can upload health records and retrieve and view them at a later time. In addition to this, the patients may assign access rights to allow family, friends, and restrict the healthcare providers to edit parts of their record. Patients and their delegates may wish to efficiently perform searches in an efficient manner over part or all of the record. Figure1 represents the model of E-Health system. The PHR is managed by the third-party service provider i.e cloud data storage provider.



Google Health, launched in May 21, 2008 as a personal health information service by google. The launch followed a two-month trial at the Cleveland Clinic in which estimated 1,500-10,000 patients participated. Google describes its product as a PHR “but also a bit of a different model” which in addition to offering a place to store, manage and share one’s health information also provides a directory of online services to act on this information on a daily basis. Such platform strategy means patients will be able to automatically import their records, prescription history and test results, interact with services and tools such as appointment scheduling, prescription refills and wellness tools by the third-party providers as they are added to the directory.

Google Health is based on open standards (Continuity of Care Record for data exchange, SOAP for the web-services interoperability), provides a development API, programming libraries and test infrastructure. It was discontinued in 2011 as it lacked other communication and convenience features that the users look for while dealing with their health-related data[3].

Microsoft HealthVault is a web-based personal health record created by Microsoft, in October 2007, to store and maintain health and fitness information. This website addresses both individuals and healthcare professionals, and in June 2010 expanded its services beyond the United States to include the United Kingdom. Generally, the HealthVault consists of two parts – an electronic repository for storing health related details and a specialized search engine for health information on the World Wide Web. HealthVault is addressed as a Pay and use health vault to store and to share medical information at the risk of its owner outsourcing it to the cloud network. HealthVault stands out from the other providers by an extensive partner network particularly in the area of medical and fitness devices. Microsoft plans to make money by placing ads next to the HealthVault search results. Similarly, to Google Health, Microsoft offers an open API and a SDK including libraries for .NET, Java and Ruby.

III. OVERVIEW OF PROPOSED SYSTEM

The proposed system is to enable secure patient-centric PHR access to the users and to provide efficient key management simultaneously. This system divides the architecture into multiple security domains namely, public domains and personal domains based on the users’ access requirements. The PUDs consist of users who provide access based on their designation, such as doctors, nurses, and medical researchers. To be precise, a PUD can be mapped to any independent sector in the society, such as the health care, government, or insurance sector.

1. Initialization of PHR

The purpose of maintaining a central repository of PHR is to facilitate user with robust and reliable access of their data 24/7. Besides, the data collected in the PHR deployed on the cloud. The data owners will interact with it without worrying about data format inconsistencies. While storing the data, the plain data is converted into encrypted data. The other communication and convenience features that the users look for is enabled in the PHR.

2. Sensitive data outsourcing

After acquiring data from users in the PHR, certain and limited number of anonymization techniques are employed on it. The sensitive attribute of name and identifying attributes are removed from the data and encryption is applied on it. This data is then uploaded on the cloud so that it can be shared with the health organizations after authorization. The purpose of removing unique identifying attributes from the outsourced data is to secure against unauthorized access over outsourced data in the untrusted domain of public cloud along with the encryption. Although encryption itself can withstand against the unauthorized possession of data storage facility but removing unique identifiers from the central repository adds another layer of protection within the encrypted data.

3. User request for data access

The authorized users after getting valid credentials forward their request to the cloud server provider. As the storage of data is in the encrypted format, the secret key is required for decryption. The user after getting encrypted data will decrypt the data using the secret key and will acquire the desired information.

IV. IMPLEMENTATION

Initially the system is divided into multiple user domains based on the security like personal domain (PSD) and public domain (PUD). Each domain provides access to only a subset of its users. For each security domain, one or more authorities are assigned to govern the access of data. In case of personal domain, the data owner in the PHR manages the record and performs key management themselves. They can decide to whom the access is to be granted and whom to be denied.

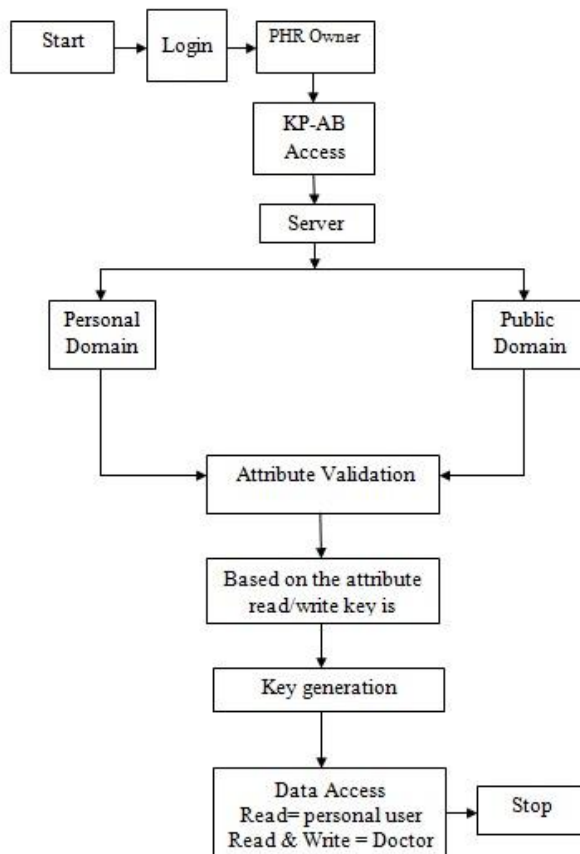


Figure 1 System flow chart

ABE system is comprised of k attribute authorities and one central authority. In this system, every attribute authority is assigned a value, dk. The system uses the following algorithms:

Set up:

In this phase, a random algorithm is executed by the central authority or another trusted authority. It takes the security parameter as the input and outputs a public key, secret key pair for each of the attribute authorities. It also gives a system public key and master secret key as output which is required used for decryption.

Attribute Key Generation:

In this phase, a random algorithm is used by an attribute authority to generate a secret key based on the attributes. It takes the authority’s secret key, the authority’s valued k, a user’s GID and a set of attributes in the authority’s domain as input. The output given is the secret key for the user.

A. KP-AB Access Control:

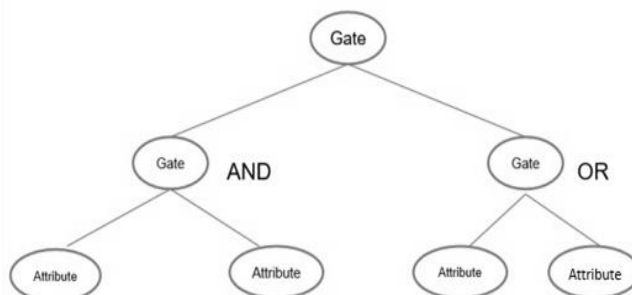


Figure 1 Access control mechanism

This technique is used to encrypt each user’s record file for providing fine-grained and scalable data access in the PHRs. KP-ABE scheme consists of the following four algorithms: [9]



1. Setup: In this phase, the initialization of parameters is done as per the requirement of the basic setup. A security parameter κ is taken as the input and then returns the public key PK and 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.

2. Encryption: This is the process of ciphering which changes the plain text into a cipher text to safeguard the data. The input in this algorithm is a message M, the Public key PK, and a set of attributes. The output obtained is the cipher text E.

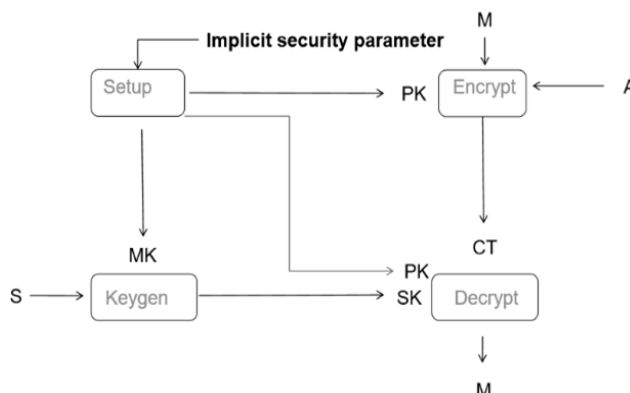


Figure 2 KP-ABE Algorithm

3. Key Generation: This algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that permits the user to decrypt a message encrypted under a set of attributes if and only if the value equals to the value of T.

4. Decryption: It takes as input the user’s secret key SK for Access structure T and the ciphertext E, which was encrypted under the attribute set. The output message M is retrieved only when the attribute set fulfils the criteria of the user’s access structure T[9].

Table 1 Performance of KP-ABE

Parameters	KP-ABE
Fine grained access control	Low, High if there is re-encryption technique
Efficiency	Average, High for broadcast type system
Computational Overhead	Most of computational Overhead
Collision resistant	Good

V. RESULT

The multiple owners may encrypt according to own ways, using different sets of keys. An alternative to this is to employ a central authority (CA) to do the key management on behalf of all record owners, but it requires too much trust on a single authority. Attribute based encryption (ABE) technique is used to encrypt each user’s record file for providing fine-grained and scalable data access in the PHRs[9]. Considering the drawbacks of the single authority system like load bottleneck, key escrow problem and multiple attribute management tasks by Single Central Authority, different entities (owners) responsible for monitoring different attributes is suggested[3]. The system comes under MAABE. The system allows selective sharing of records. It allows on-demand, efficient user attribute revocation. The implementation of multiple security domains for the users reduces the key management complexity immensely for owners and users. Thus the key escrow problem is also managed[6]. The ABE allows each user to select the pairs of attributes to encrypt the records. As each record of user is encrypted as per their own attributes, the keys are non-hack able as well as unpredictable.

The multiple owners may encrypt according to own ways, using different sets of keys. An alternative to this is to employ a central authority (CA) to do the key management on behalf of all record owners, but it requires too much trust on a single authority. Attribute based encryption (ABE) technique is used to encrypt each user’s record file for providing fine-grained and scalable data access in the PHRs[9]. Considering the drawbacks of the single authority system like load bottleneck, key escrow problem and multiple attribute management tasks by Single Central Authority, different entities (owners) responsible for monitoring different attributes is suggested[3]. The system comes under MAABE. The system allows selective sharing of records. It allows on-demand, efficient user attribute revocation. The implementation of multiple security domains for the users reduces the key management complexity immensely for



owners and users. Thus the key escrow problem is also managed[6]. The ABE allows each user to select the pairs of attributes to encrypt the records. As each record of user is encrypted as per their own attributes, the keys are non-hack able as well as unpredictable.



Figure 3 PHR login

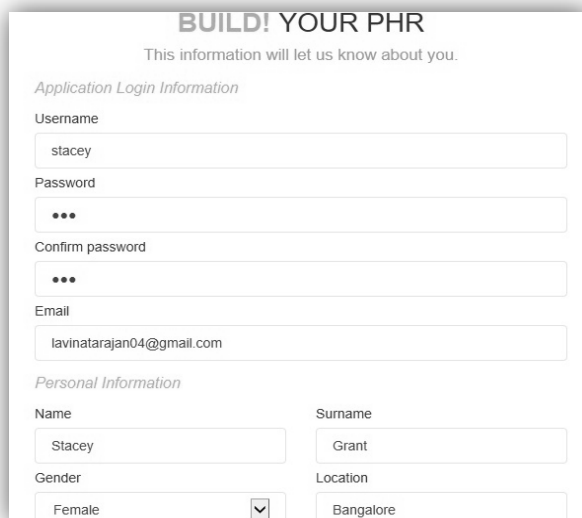


Figure 4 Patient registration page

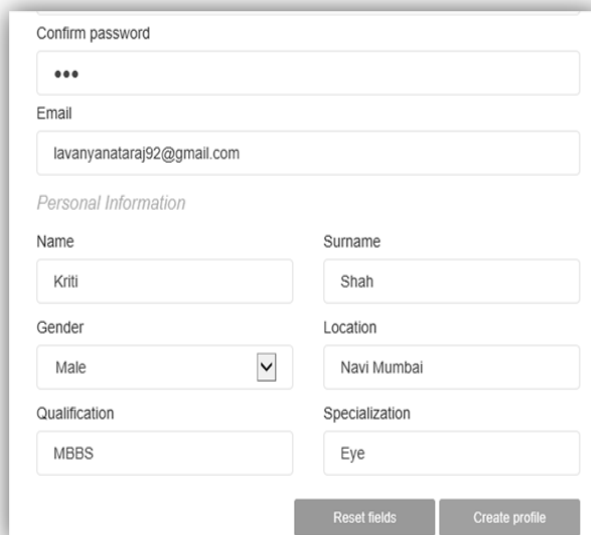


Figure 5 Doctor registration page

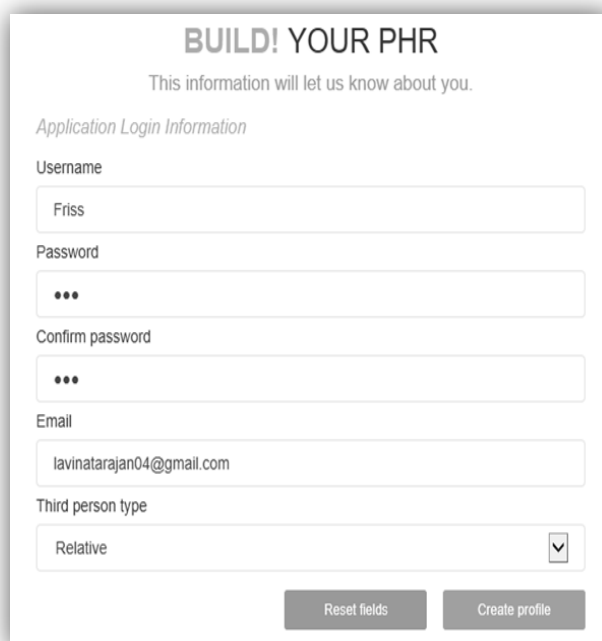


Figure 6 Third person registration page

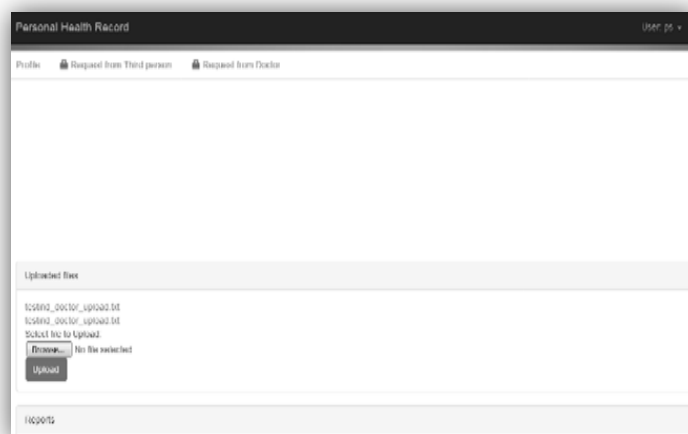


Figure 7 Patient account login

VI. CONCLUSION

A PHR file should be accessible to the authenticated users, while remain inaccessible to the rest. To protect personal health data stored on semi-trusted servers, we adopt attribute-based encryption as main encryption primitive. Using ABE, access policies are expressed based on attributes of users or data. The key-policy Attribute Based Encryption scheme used in the PHR will allow only the authorized users to access the data. Two important issues pertaining to this sharing of data have to be addressed: one is the privacy protection for individuals and second one is its oblivious processing within the untrusted domain of cloud computing. The personal health record system provide security against collusion attacks, Brute force, Mathematical attacks, Timing attacks and Chosen Cipher-text attacks. The proposed system is not easily hackable. The key management problem is also reduced enhancing the guarantee of privacy.

FUTURE WORK

As future study, it will be interesting to enhance the fine-grained access control in cloud computing with a third-party auditor to verify the server that stores and process the records. In KP-ABE scheme, delegation of private keys means converting the original access structure A into a stricter access structure A' . Also, Future work can include further —



comprising of more than only two domains reserved for special users. Also, Future work can include further comprising of more than only two domains reserved for special users. Along with attribute-based encryption, other cryptographical algorithms coupled with several access control mechanisms can be thought to be implemented.

REFERENCES

- [1] 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'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.
- [2] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp.417-426.
- [3] <http://www.informationweek.com/healthcare/electronic-health-records/5-reasons-why-google-health-failed/d/d-id/1098623>
- [4] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.
- [5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
- [6] 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," in SecureComm'10, Sept.2010, pp. 89-106.
- [7] 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.
- [8] 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.
- [9] S.Yu, C.Wang, K.Ren, and W.Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.
- [10] G. Mariammal, N. Uma Maheswari, R. Venkatesh, P. Lakshmanan, "Implementation of Secret Delegation for Secured Attribute Based Access Control in Cloud Computing," in IJECS Vol 2 Issue 4 April, 2013 pp 986-990.