ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Controlled Access and Management of Personal Health Records using Key-Policy Attribute Based Encryption

Sanjaykumar. B. Vhotkar, Prof. R. V. Argiddi

P.G. Student (M.E. CSE), Dept. of Comp. Sc. & Engg, W I T, Solapur University, Solapur, Maharashtra, India.

Associate Professor, Dept of Comp. Sc. & Engg, W I T, Solapur University, Solapur, Maharashtra, India.

ABSTRACT: Controlled access and management of Personal Health Records(PHR) in shared environment like Cloud Computing is very challenging task. This paper deals with models and techniques which enhance data security in Cloud Computing. We explore how key-policy attribute-based encryption (KP-ABE) scheme can be used to provide security by encrypting the vital medical information stored in PHR. Using this scheme, patients can encrypt their PHRs and store them on a honest-but-curious cloud server such that the server do not have access to sensitive data. Meanwhile, patients maintain full access of their own data, by assigning fine-grained, attribute-based access privileges to selected data users or third parties. Different users or parties can have access to different parts of the data.

KEYWORDS: Attribute-based Encryption, Cloud Computing, fine-grained access control.

I. INTRODUCTION

The medical information stored at the remote server will be shared among different users (e.g. doctors, nurses, pharmacies, patient etc.). Thus, privacy, confidentiality and security issues for the medical information should be a major concern in this topic. Therefore, it is important for the medical information to be encrypted before sending it to the third party remote server. Public key cryptosystem is one of the potent approaches to secure medical information.

Attribute-based encryption (ABE) [4-7], is a fine-grained access control system, which enables a set of users to have differential access rights. On the other hand, ABE is also flexible in defining the access rights of each user. There are two major types of ABE; key-policy attribute-based encryption (KP-ABE)[8-9], and cipher-text-policy attribute-based encryption (CP-ABE) [10-12]. In this paper, we propose an implementation of KP-ABE scheme to apply the encryption to patient’s medical information. KP-ABE encryption time is shorter than CP-ABE. Besides that, KP-ABE has less restriction and limitation on the authorized users who are able to apply decryption to the encrypted medical information. Authorized user (e.g. medical operator) is able to perform decryption if his/her access policy matches the attributes assigned to the encrypted vital signs. In hardware implementation, KP-ABE is also advantageous. KP-ABE scheme is able to realize the lightweight encryption and producing smaller cipher-text size than CP-ABE in a resource constraint device.

II. RELATED WORK

In 1984, Adi Shamir introduced the concept of identity-based cryptography[1]. It used user identity attributes, such as email addresses or phone numbers, instead of digital certificates, for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing users' certificates. It also makes it much easier to provide cryptography to unprepared users, since messages may be encrypted for users before they interact with any system components. This remained an open problem until 2001, when two independent lines of research (Boneh and Franklin [4], as well as Cocks [6]) arrived at solutions to the problem. Since this time, identity-based cryptography has been a heavily-researched topic in the field of cryptography [2].

In 2005, Sahai and Waters introduced a new type of IBE scheme called Fuzzy Identity-Based Encryption (FIBE). In IBE, identities are viewed as arbitrary strings. While in FIBE, identities are being viewed as a set of descriptive attributes. The authors also mentioned on the application of FIBE termed as Attribute-Based Encryption (ABE). In an ABE system, a user's private key and cipher-text are labeled with a set of attributes. A particular private key can decrypt a particular cipher-text only if there is a match between the attributes of the user's private key and cipher-text.

In year 2006, Goyal et al. proposed the Key-Policy Attribute Based Encryption (KP-ABE) for fine-grained sharing of encrypted data [9]. The encrypted data can only be selectively shared at a coarse-grained level. For example, in order to perform data decryption, user needs to give his/her private key to another party. This somehow allows another party to have all the access of the user's data. Another alternative, user can act as an intermediary to perform decryption on the relevant data but this method is arduous. Both approaches are not appealing as they are impractical and inefficient. In KP-ABE, as shown in Fig. 1, a file encrypted(cipher-text) is labeled with a set of descriptive attributes, while the access structure is embedded in the user's private key. User is able to decrypt a cipher-text if the access structure embedded in the private key matches the descriptive attributes labeled in the cipher-text. Fine-grained sharing of encrypted data enables different authorized users to retrieve and decrypt cipher-text based on their access structure. KP-ABE scheme is able to grant different access rights to different users.

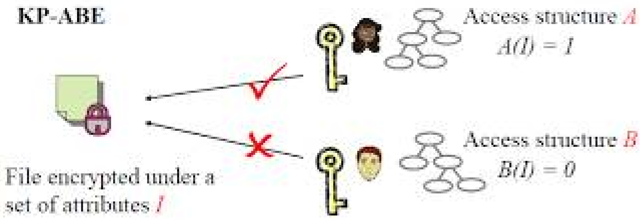

Fig. 1: Schematic of Key-Policy Attribute-Based Encryption

In year 2007, Bethencourt et al. provides the first construction of a cipher-text-policy attribute-based encryption (CP-ABE) scheme [10]. In CP-ABE scheme, as shown in Fig. 2, access structure is use in File data encryption while the descriptive attributes are embedded in the user's private key. A user is able to decrypt the cipher-text if his descriptive attributes satisfy the access structure associated to the cipher-text.

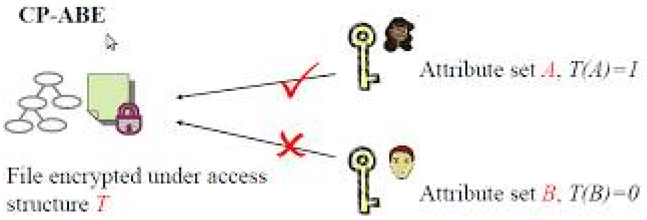

Fig. 2 : Schematic of Ciphertext Policy Attribute Based Encryption

Table 1 summarizes the terminology definition in this section.

TABLE 1: Terminology List

Terminology	Definition	Example
Attributes	Identities of a person	Name, home address, e-mail address, identity number, phone number
Access Structure	A policy/structure to define an authorized person	{("Dept of Medical Services" **AND** "Specialist") **AND** ("Solapur" OR "Pune") **OR** "Name: Dr. SanjayKumar"}
Private Key Generator	A trusted third party that handles the issuance of private keys	

III. PROPOSED ALGORITHM

A. Attribute-Based Encryption Scheme (ABE):

Comparisons between KP-ABE and CP-ABE schemes are studied and analysed to determine their propriety in BSN [11]. Comparisons were conducted in terms of encryption efficiency/time, attribute and access structure's assignment, access control and hardware implementation. In our work, we have intended to achieve a lightweight and secure encryption. In KP-ABE, encryption is performed by using descriptive attributes. Access structure is embedded in the private key which is issued by private key generator (PKG). In CP-ABE, encryption is performed by using the access structure. Descriptive attributes are embedded in the private key issued by PKG. Encryption performs by using descriptive attributes has lower encryption complexity and shorter computation time than encryption to be performed by using access structure. Moreover, medical information is being encrypted at a continuous basis, while key generation for each authorized users is being generated once. Therefore, KP-ABE encryption scheme is more appropriate to be implemented in our work. Patients are involved in the assignment of descriptive attributes or access structure with the assistance from medical agents. Assignment of descriptive attributes in KP-ABE for encryption purpose is much simpler and less time consuming than assignment of access structure in CP-ABE encryption. This is because a slight update mistake in the access structure would cause a complication in the entire encryption and decryption system.

Furthermore, in terms of access control, KP-ABE allows higher flexibility and efficiency in the modification of access control towards any authorized personnel compared to CP-ABE. This is because the updates made on the descriptive attributes are much simpler than updates made on access structure.

In KP-ABE, the encryption time is shorter and cipher-text size is smaller than CP-ABE. This is because the high complexity and processing work to embed the access structure in private keys are done by the PKG. However, for CP-ABE, the encryption computation time is longer and the cipher-text size is larger. Therefore, in terms of hardware implementation, KP-ABE is advantageous. For our prototype, we have implemented the KP-ABE scheme as this scheme is more suitable than CP-ABE in terms of light weight and less power consumption [11]. In KP-ABE scheme as shown in Figure 2, attributes are labeled in the encrypted medical information (vital signs and patient's personal data). Access structure is embedded in the private key.

The private key is issued by a trusted private key generator (PKG). This is an advantage of KP-ABE scheme where attributes label in the encrypted medical information can be easily created and altered. The tedious task of access structure creation and alteration is handled by professional PKG creator.

The KP-ABE scheme consists of four algorithms [15].

- Setup (1^k): The setup algorithm takes as input a security parameter, 1^k and outputs the public parameters, PK and a master key, msk which is known only to the private key generator (PKG).
- Encrypt (m, PK, γ): The encryption algorithm takes as input a message, m, a set of attributes, γ and the public parameters, PK. It outputs the cipher-text, c.
- Key Generation (PK, msk, *p*): The key generation algorithm takes as input the public parameters, PK, the master key, msk and an access policy, *p*. It outputs the private key, D.
- Decrypt (c, PK, D): The decryption algorithm takes as input the cipher-text, c which was encrypted under the set of attributes, public key parameter, structure, . It outputs the message m if γ∈

B. KP-ABE ENCRYPTION IN PC

Once the vital signs are sent to the PC, the PC will perform the KP-ABE encryption on the vital signs. In our implementation, we used the key-policy attribute-based encryption library (libcelia). It is a subroutine library implementing KP-ABE scheme and kpa is a toolkit created by Yao Zheng. Figure 3 illustrates the process flow of the encryption and decryption.

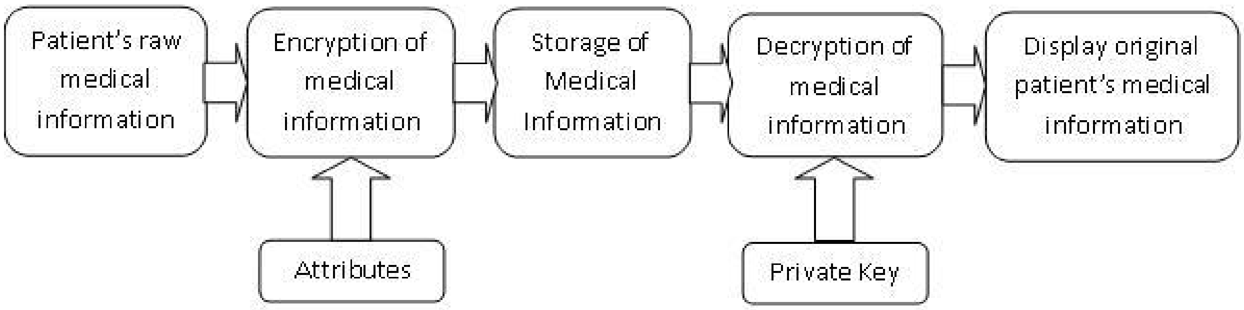
Patient's raw medical information
Encryption of medical information
Storage of Medical Information
Decryption of medical information
Display original patient's medical information
Attributes
Private Key

Fig. 3: Diagram of Process Flow of Encryption and Decryption

- kpabe-setup : The setup algorithm generates system parameters, a public key, and a master secret key under set of attributes.
- kpabe-enc: Encryption algorithm encrypt medical information of patient under a set of attributes.
- kpabe-keygen: The key generation algorithm generates a private key and sends to the authorized medical operators.
- kpabe-dec: The decryption algorithm takes as input the encrypted medical information under a set of attributes, the public key parameters and the private key generated by kpabe-keygen. It then outputs the message original file if access structure embedded in the private key matched the attributes.

IV. SIMULATION RESULTS

A. SYSTEM IMPLEMENTATION.

The basic function of this framework is to upload medical files to PHR server and download the encrypted medical files from the server. The security mechanism is enforced by encrypting the files before uploading to the cloud and decrypting ciphertext after downloading from the cloud. Additionally, in order to support KP-ABE operations, we create a Java application implementing KP-ABE primitive using the Java Pairing-Based Cryptography Library. The Key-Policy Attribute-based Encryption application (gpswabe) is a subroutine application implementing KP-ABE scheme. The source code is divided into two parts, gpswabe.java (construction routine) and SerializationUtils.java (Utility routines). In this gpswabe java application, it implements Setup, Key generation, Encryption, decryption. The kpabe.java application is a set of programs implementing the high level functions of KP-ABE scheme. Since pairing is computationally expensive, we use KP-ABE to encrypt one single element. Then this single element is used to encrypt the plaintext as key in AES symmetric key encryption.

B. KP-ABE PERFORMANCE EVALUATION

In order to evaluate the performance of security framework, we measure the computation time of Key-policy attribute-based encryption and decryption using gpswabe.java. All measurements are taken a workstation running Windows 8.1 with a 64-bit, 2.20GHz Intel Core i7-3632QM CPU. We adopt the type A elliptic curve parameter, where the group order q is 160-bits, which provides 1024-bit discrete log security strength equivalently.

For encryption, shown in Fig. 4, KP-ABE encryption time is linear with the number of attributes.

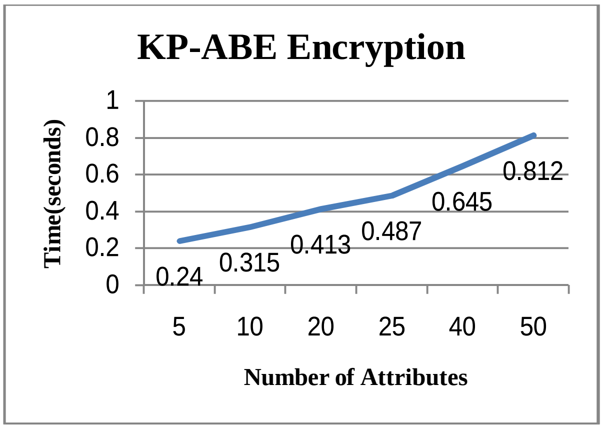

Fig. 4: KP-ABE Encryption Time

In our test, we generate private keys with access structure with simple AND gate. Figure 5 shows decryption time.

DOI: 10.15680/IJIRCCE.2017. 0502164

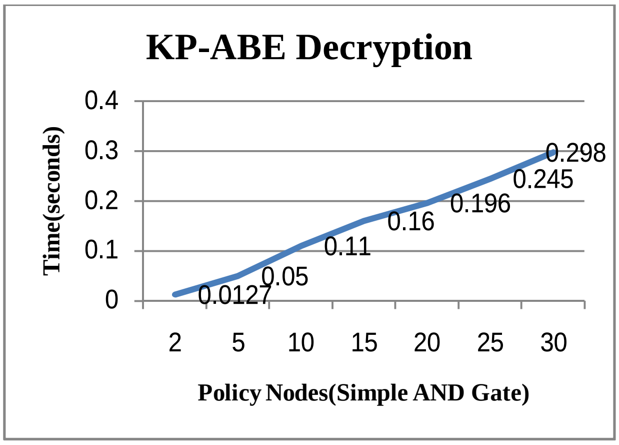

Fig. 5: KP-ABE Decryption Time

V. CONCLUSION

We present the encryption/decryption prototype system to protect the captured vital signs and personal information of patients. This enables patients' medical data to be remotely monitored from the hospital in secured manner. Body sensor nodes are used in the system to capture vital signs from the human body. We demonstrate that, by using key-policy attribute-based encryption (KP-ABE), patients' medical information can be protected and be shared among different medical operators. Our work is a non-real time application. However, we are going to extend our system to real-time application for ubiquitous healthcare purposes. It provides flexibility for patients to collect their vital signs and perform encrypt at any time of the day and at any places according to their preferences.

REFERENCES

[1] Shamir "Identity-based cryptosystems and signature schemes." Advances in Cryptology - Crypto '84, LNCS 0196, pp. 47-53. 1984.

[2] D. Boneh and M. Franklin. "Identity-based Encryption from the Weil pairing." Advances in Cryptology- CRYPTO'01, LNCS 2139, pp. 213–229. 2001

[3] Cheng-Chi Lee, Pei-Shan Chung, Min-Shiang Hwang, "A survey on Attribute-based Encryption Schemes of access control in cloud environments", International Journal of Network Security, Vol.15, No.4, pp.231-240, July 2013

[4] Sahai and B. Waters. Fuzzy Identity Based Encryption. In Advances of cryptology – Eurocrypt 2005, LNCS 3494, pp.457- 473. 2005.

[5] Ostrovsky, R., Sahai, A., & Waters, B.. "Attribute-based encryption with non-monotonic access structures". In Proceedings of the 14th ACM conference on Computer and communications security, pp. 195-203, ACM, 2007.

[6] Chase, M.. "Multi-authority attribute based encryption." Theory of Cryptography, pp. 515-534, 2007.

[7] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. "Fully secure functional encryption : Attribute-based encryption and (hierarchical) inner product encryption." Advances in Cryptology–EUROCRYPT 2010, pp.62-91, 2010.

[8] V. Goyal, O. Pandey, A. Sahai and B. Waters. "Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data." ACM conference on Computer and Communications Security, pp. 89–98, 2006.

[9] Attrapadung, N., Libert, B., & De Panafieu, E. "Expressive keypolicy attribute-based encryption with constant-size ciphertexts." Public Key Cryptography–PKC 2011, pp. 90-108, 2011.

[10] J. Bethencourt, A. Sahai and B. Waters. "Ciphertext-policy attribute-based encryption." IEEE Symposium on Security & Privacy, pp.321-334, 2007.

[11] Goyal, V., Jain, A., Pandey, O., and Sahai, A. "Bounded ciphertext policy attribute based encryption." Automata, Languages and Programming, pp. 579-591, 2008.

[12] Waters, B. "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization." Public Key Cryptography–PKC 2011, pp.53-70, 2011.