IISRC International Industrial Scientific Research Corporation
International Conference on Industrial Scientific Research Engineering
www.worldconferences.org

Scalable and Secure Personal Health Records in Cloud using Attribute Based Encryption with Checkability

P.VANI[1], S.G.NAWAZ[2]
[1]PG Scholar, Dept of CSE, Sri Krishna Devaraya Engineering College, Gooty, AP, India,
E-mail: vani.potlapati@gmail.com.
[2]HOD, Dept of CSE, Sri Krishna Devaraya Engineering College, Gooty, AP, India.

Abstract: This paper presents the design and implementation of Personal Health Records and providing security to them while they are stored at third party such as cloud. Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing and decryption are getting prohibitively high. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, the verifiability of results returned from the third party has yet to be addressed. Aiming at tackling the challenge above, we propose a new Secure Outsourced ABE system, which supports both secure outsourced key-issuing and decryption. Our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the attribute authority and eligible users to perform locally. In addition, for the first time, we propose an outsourced ABE construction which provides checkability of the outsourced computation results in an efficient way. Extensive security and performance analysis show that the proposed schemes are proven secure and practical.

Keywords: Attribute-Based Encryption, Access Control, Outsourcing Computation, Key Issuing, And Checkability.

I. INTRODUCTION

AS a novel public key primitive, attribute-based encryption (ABE) has attracted much attention in the research community. For the first time, ABE enables efficient public key-based fine-grained sharing. In ABE system, users' private keys and ciphertexts are labeled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular ciphertext only if associated attributes and policy are matched. Until now, there are two kinds of ABE having been proposed: key-policy attribute-based encryption (KP-ABE) and ciphertext-policy attribute-based encryption (CP-ABE). In KP-ABE, the access policy is assigned in private key, whereas, in CP-ABE, it is specified in ciphertext. Personal Health Record (PHR) concept has emerged in recent years. We can say that it is a patient centric model as overall control of patient's data is with patient. He can create, delete, modify and share his PHR through the web. Due to the high cost of building and maintaining data centers, third-party service providers provide PHR service. But while using third party service providers there are many security and privacy risks for PHR. The main concern is whether the PHR owner actually gets full control of his data or not, especially when it is stored at third party servers which is not fully trusted. To ensure patient-centric privacy control over their own PHRs, it is essential to provide data access control mechanisms.

Our approach is to encrypt the data before outsourcing. PHR owner will decide which users will get access to which data in his PHR record. A PHR file should available to only those users who are given corresponding decryption key. And the patient shall retain the right to revoke the access privileges whenever they feel it is necessary. The authorized users may either need to access the PHR for personal use or professional purposes. 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.

II. RELATED WORK

A. Key-Policy Attribute-based Encryption (KP-ABE)

KP-ABE is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet.

B. Cipher text Policy Attribute based Encryption (CP-ABE)

CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential.

C. Multi-Authority Attribute-Based Encryption (MA-ABE)

MA-ABE method allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k [10].

III. PROPOSED SYSTEM

Personal Health Record is an internet based application that allows people to access and co-ordinate their lifelong health information and make if appropriate parts of its available to those who need. Personal Health Record's security and protection of its data have been of great concern and a subject of research over the years. There are many different forms of cryptographic mechanisms like AES, MD5 proposed to guarantee data security. In this work we propose a unique authentication and encryption technique using AES algorithm. In PHR data refers to the information that is collected, analyzed and stored. Example Medical history, List of medical problems, Medication history. The PHR owner herself should decide how to encrypt her file and to allow which set of users to obtain access to each file. In PHR infrastructure is the computing platform which processes or exchanges healthcare data such as software package and website.

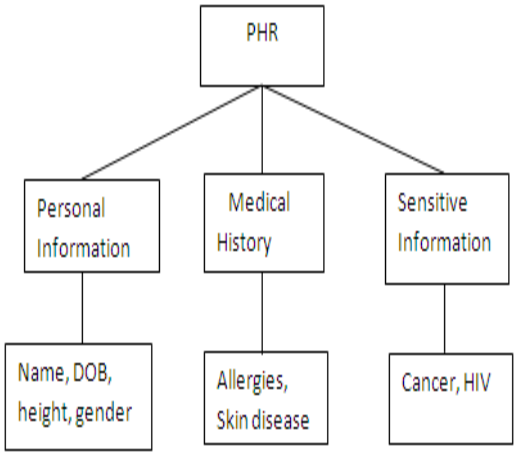

Fig.1. The attribute.

A. Attribute Based Encryption

Using attribute based encryption technique we are providing security to the database. A sensitive data is shared and stored on cloud server, there will be a need to encrypt data stored at third party. In Attribute based encryption cipher text labeled with set of attribute. Private key associated with access structure that control which cipher text a user is able to decrypt. We are using 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 the users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-retrieval to solve, and remain largely open up-to-date.

B. The Attribute Hierarchy

We are using attribute based encryption for providing security. For that we use following distribution of attributes that are mainly important.

C. Security Definition

In this work, we assume that all the entities except AA are ''honest-but-curious''. More precisely, they will follow our proposed protocol but try to find out as much private information as possible based on their possessions. The adversary model described in Fig.1 is considered. More precisely, since KGSP and U respectively owns the knowledge of OKKGSP for KGSP and user's private key, they are considered as active attackers which are allowed to collude with DSP and SSP to launch harmful attack separately. Following this consideration, two types of adversaries are categorized. . Type-I adversary defined as a group of curious users colluding with SSP and DSP, is able to potentially access private keys for all the corrupted users, all the ciphertext stored at SSP, all the blinded transformation keys stored at DSP, etc, and aims to decrypt ciphertext intended for users not in the group. . Type-II adversary defined as KGSP colluding with SSP and DSP, is able to potentially access all the keys for KGSP, all the ciphertext stored at SSP, all the blinded transformation keys stored at DSP, etc, and aims to decrypt any ciphertext.

Analysis: Our second construction has almost the same efficiency with the first one. Specifically, in key-issuing, though another key combination operation is required at attribute authority side, it costs mutiplications for j'j times, which is negligible using the modern devices. Then, we provide the security analysis below. Theorem 2. The second construction is secure against chosen plaintext attack in the sense of the security definition modified under DBDH assumption.

D. Checkability

Beyond outsourced key generation and decryption, the checkability on KGSP is supported in our second construction. Specifically, since KGSP[1] (or KGSP[2]) cannot distinguish the outsourced private key generation from the two outsourced tasks. If KGSP[1] (KGSP[2])

fails during any execution of KeyGen(out), it will be detected with probability $\frac{d-1+|\omega|}{2|\omega|}$ which is not less than 1/2. In addition, through appending redundancy, the dishonest action of DSP can be easily detected in our construction.

Advantages of Proposed System:

- Quickly find out information of patient details.
- In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.
- If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.
- To provide easy and faster access information.
- To provide user friendly environment.
- To provide data confidentiality and write access control.

IV. CONCLUSION

We provide a new outsourced ABE scheme simultaneously supporting outsourced key-issuing and decryption. With the aid of KGSP and DSP, our scheme achieves constant efficiency at both authority and user sides. In addition, we provide a trust-reduced construction with two KGSPs which is secure under recently formulized RDoC model. Unlike the state-of-the-art outsourced ABE, checkability is supported by this construction. The security of proposed schemes have been analyzed and given in this paper. Experimental results demonstrate that our constructions are efficient and practical.

V. REFERENCES

[1] A. Sahai and B. Waters, ‘‘Fuzzy Identity-Based Encryption,’’ in Proc. Adv. Cryptol.-EUROCRYPT, LNCS 3494, R. Cramer, Ed., Berlin, Germany, 2005, pp. 457-473, Springer Verlag.

[2] D. Zeng, S. Guo, and J. Hu, ‘‘Reliable Bulk-Data Dissemination in Delay Tolerant Networks,’’ IEEE Trans. Parallel Distrib.Syst. http://doi.ieeecomputer society.org/ 10.1109/TPDS.2013.221.

[3] M. Green, S. Hohenberger, and B. Waters, ‘‘Outsourcing the Decryption of ABE Ciphertexts,’’ in Proc. 20th USENIX Conf. SEC, 2011, p. 34.

[4] Z. Zhou and D. Huang, ‘‘Efficient and Secure Data Storage Operations for Mobile Cloud Computing,’’ in Cryptology ePrint Archive, Report 2011/185, 2011.