International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
SKRGC Since 2012

http://www.ijcsjournal.com Volume 4, Issue 2, No 4, 2016. ISSN: 2348-6600
Reference ID: IJCS-134 PAGE NO: 789-794

A Survey on Personal Health Records Using Multi Authority Attribute-based Encryption

[1]Dr.V.Jayaraj , [2]V.Ankayarkanni

[1]Assistant Professor, School of CSE & Applications, Bharathidasan University ,Trichy

[2]Research Scholar , Bharathidasan University ,Trichy

Abstract— A PHR service allows a patient to create, manage, and control her Personal health data storage, retrieval and sharing of the medical information in web. The patient could actually control the sharing of their sensitive Personal health information's are stored on a third party server which people may not fully trusted. To ensure patient centric privacy control over their own PHR have fine-grained access control mechanisms that work in the semi trusted servers and the PHR owner encrypt her file should only be available decrypt it. Each attribute authority (AA) in it governs disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt PHR file under its data attributes MA-ABE by putting forward an efficient on demand user/attribute revocation scheme, and prove its security under standard security assumptions

Keywords- PHR, Attribute Based Encryption (ABE), Multi Authority Attribute Based Encryption (MAABE).

1. INTRODUCTION

Personal Health Record (PHR) is emerged as a patient- centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data center. Due to the high cost of building of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist health care regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive Personal Health Information (PHI), the third -party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI In security based ensure privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. Hence we move to a new encryption pattern namely Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, which enables a patient to selectively share their 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.

As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The multi authority attribute based encryption (maabe) scheme is used to provide multiple authority based access control mechanism. The phr owner them self should decide how to encrypt their files and to allow which set of users to obtain access to each file. A phr file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary.

The goal of patient-centric privacy is often in conflict with scalability in a phr system. The authorized users may either need to access the phr for personal use or professional purposes. Delineation and implementation of accepted standards for health-care data, accurate patient identification and record matching, and the definition of incentives for accelerated deployment of health information technology. In response to these challenges, we present in this paper an alternative option, the health record banking (hrb) system. Emulating commercial banking, this approach uses health-record banks to serve the need for immediately accessible and secure data for diverse stakeholders.

2. RELATED WORK

This paper is mostly related to work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used [1]. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the ACL

✓ Trusted authority

A number of works used ABE to realize finegrained access control for outsourced data [3] [4]. Recently, Narayan et al. proposed an attributebased infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE [5] that allows direct revocation. There are several common drawbacks of the above works. First, they usually assume the use of a single Trusted Authority (TA) in the system. This not only may create a load bottleneck but also suffers from the key escrow problem. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys [1].

✓ Multi-Authority ABE

A Multi-Authority ABE system is comprised of k attribute authorities and one central authority. Each attribute authority is also assigned a value, dk. The system uses the following algorithms: Set up: A random algorithm that is run by the central authority or some other trusted authority. It takes as input the security parameter and outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

✓ Attribute Key Generation:

A random algorithm run by an attribute authority. It takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain and output secret key for the user. Central Key Generation: A randomized algorithm that is run by the central authority. It takes as input the master secret key and a user's GID and outputs secret key for the user. Encryption:

A randomized algorithm runs by a sender. It takes as input a set of attributes for each authority, a message, and the system public key and outputs the cipher text. Decryption: A deterministic algorithm runs by a user. It takes input a cipher-text, which was encrypted under attribute set and decryption keys for that attribute set. This algorithm outputs a message m.

Using ABE and MA-ABE which enhances the system scalability, there are some limitations in the practicality of using them in building PHR systems. For example, in workflow based access control scenarios, the data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently. In those scenarios one may consider the use of attribute-based broadcast encryption [9]. In addition, the expressibility of our encryptor's access policy is somewhat limited by that of MAABE's, since it only supports conjunctive policy across multiple AAs.

Problem Survey:

Personal Health Record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing

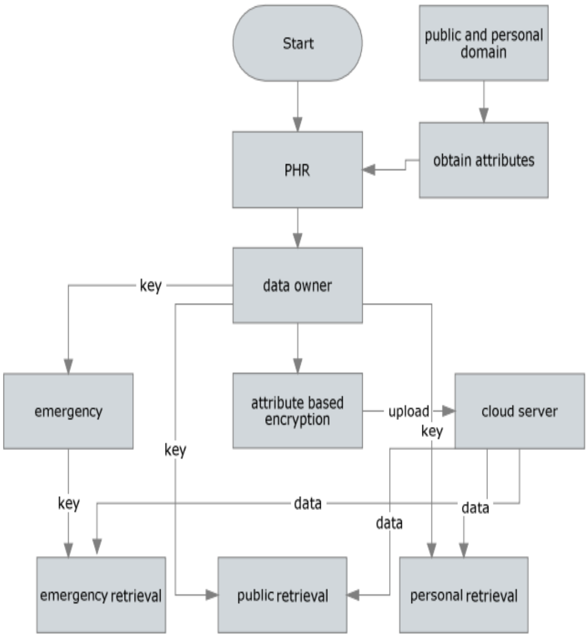
1) Securing Personal Health Records M. Li, S. Yu, K. Ren, and W. Lou [1] proposes a novel and practical framework for fine-grained data access control to PHR data in cloud computing environments, under multi owner settings. To ensure that each owner has full control over her PHR data, they leverage Attribute-Based Encryption (ABE) as the encryption primitive, and each owner generates her own set of ABE keys. his way, a patient can selectively shaIn tre her PHR among a set of users by encrypting the file according to a set of attributes, and her encryption and user management. complexity is linear to the number of attributes rather than the number of authorized users in the system

2) Securing Personal Health Records M. Li, S. Yu, K. Ren, and W. Lou [1] proposes a novel and practical framework for fine-grained data access control to PHR data in cloud computing environments, under multi owner settings. To ensure that each owner has full control over her PHR data, they leverage Attribute-Based Encryption (ABE) as the encryption primitive, and each owner generates her own set of ABE keys. his way, a patient can selectively shaIn tre her PHR among a set of users by encrypting the file according to a set of attributes, and her encryption and user management complexity is linear to the number of attributes rather than the number of authorized users in the system. To avoid from high key management complexity for each owner and user, they divide the system into multiple Security Domains (SDs), where each of them is associated with a subset of all the users. Each owner and the users having personal connections to her belong to a personal domain, while for each public domain they rely on multiple auxiliary Attribute Authorities (AA) to manage its users and attributes. Each AA distributive governs a disjoint subset of attributes, while none of them alone is able to control the security of the whole system. In addition, they discuss methods for enabling efficient and on-demand revocation of users or attributes, and break-glass access under emergence scenarios.

3) Authorized Private Keyword Search M. Li, S. Yu, N. Cao, and W. Lou [3] proposes the systematic study the problem of authorized private keyword searches (APKS) over encrypted PHRs in cloud computing. They make the following main contributions. First, they propose a finegrained authorization framework in which every user obtain search capabilities under the authorization of local trusted Authorities (LTAs), based on checking for user's attributes. The central TA's task is reduced to minimum, and can remain semi-offline after initialization. Using an obtained capability, a user can let the cloud server search through all owners' encrypted PHRs to find the records that match with the query conditions. Their framework enjoys a high level of system scalability for PHR applications in the public domain. To realize such a framework, they make novel use of a recent cryptographic primitive, hierarchical predicate encryption (HPE), which features delegation of search capabilities. Based on HPE they propose two solutions for searching on encrypted PHR documents, APKS and APKS+. The first solution enhances search efficiency, especially for subset and a class of simple range queries, while the second enhances query privacy with the help of proxy servers. Both schemes support multi-dimensional multi-keyword searches and allow delegation and revocation of search capabilities. Finally, they implement their scheme on a modern workstation and carry out extensive performance evaluation. Through experimental results they demonstrate that their scheme is suitable for a wide range of delay-tolerant PHR applications. To the best of their knowledge, their work is the first to address the authorized private search over encrypted PHRs within the public domain.

4) Privacy of Electronic Medical Records J. Benaloh, m. Chase, e. Horvitz, and k. Lauter [3] proposes the encryption schemes with strong security properties will guarantee that the patient's privacy is protected. However, adherence to a simple encryption scheme can interfere with the desired functionality of health record systems. In particular, they would like to employ encryption, yet support such desirable functions as allowing users to share partial access rights with others and to perform various searches over their records. In what follows, they consider encryption schemes that enable patients to delegate partial decryption rights, and that allow patients (and their delegates) to search over their health data. They shall propose a design that refers to as Patient Controlled Encryption (PCE) as a solution to secure and private storage of patients' medical records. PCE allows the patient to selectively share records among doctors and healthcare providers. The design of the system is based on a hierarchical encryption system. The patient's record is partitioned into a hierarchical structure, each portion of which is encrypted with a corresponding key. The patient is required to store a root secret key, from which a tree of sub keys is derived. The patient can selectively distribute sub keys for decryption of various portions of the record. The patient can also generate and distribute trapdoors for selectively searching portions of the record. Their design prevents unauthorized access to patients' medical data by data storage providers, healthcare providers, pharmaceutical companies, insurance companies, or others who have not been given the appropriate decryption keys.

Flow Chart



MATHEMATICAL MODEL

1. Encryption

i. Input: Attribute Value (Attr).
ii. Get Byte [](B1) of that Attr.
iii. Generate Public Key(Pk).
iv. Perform Encryption on B1.
v. Convert B1 into string(EAttr).

2. Decryption

i. Input: Encrypted attribute value(EAttr)
ii. Convert EAttr into byte [](B2).
iii. Generate Private Key.
iv. Perform Decryption on B2.
v. Convert B2 into string(DAttr).

3. Secret Key

i. Input : Private Key (see Decryption-3) and No. of Authority (NAuth) =10.
ii. Get Length of private key : Length = PrivateKey.Length.
iii. To become private key multiple of NAuth (i.e. 10) pad it by zero (0). M = Length / NAuth
vi. Each authority having 'M' no. of bytes. For Each Byte value from 'M'.
vii. For (int I = 0 ; I < M.Length ; i++)
viii. {
ix. Square = M[i] * M[i] ; Hexvalue = Hex (Square) ; Hexvalue = Hexvalue + "&" Fullhexvalue = Fullhexvalue + Hexvalue;
x. }
xi. Add this Hex value into database as a secret key.

4. Attribute Key Generation

List = List of Attribute assign to the user(Authorities). Foreach (string Attribute in List){ Foreach (char ch in Attribute) { Value = Value + ch; } } In the Value we get ASCII value of that character. ASCII values save into database

CONCLUSION AND FUTURE WORK

The Personal Health Records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy.

In future, to provide high security and privacy for Personal Health Record (PHR), the existing Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption

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 multiowner settings," in SecureComm'10, Sept. 2010, pp. 89–106. [2] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011 [3] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114. [4] 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 [5] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010. [6] 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. [7] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010. [8] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp.417–426. [9] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009. [10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

AUTHORS PROFILE

Authors Profile with photo's …

Author 1:

Dr.V.Jayaraj, 1 Assistant Professor, School of CSE & Applications, Bharathidasan University ,Trichy

Authors Profile with photo's …

Author 2:

v.Ankayarkanni, M. Phil Scholar, School of Computer Science Engineering and Applications, Bharathidasan University, Tiruchirappalli, Tamil Nadu, India, kannimsc92@gmail.com