OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

SECURE PERSONAL HEALTH RECORD SYSTEM THROUGH SHARABLE AND TRACEABLE IN CLOUD

SYED ABED ALI
PG Student, EES Computer Science and Engineering, Aurangabad

Abstract: **A Personal Health Record service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can hare her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centres, many Personal Health Record services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing Personal Health Record in cloud computing have been proposed in. While it is exciting to have convenient Personal Health Record services for everyone, there are many security and privacy risks the value of home-based health monitoring has been recognized lately Studies 24-hour ambulatory monitoring System which Perform home-based health monitoring tasks. In our framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, The attribute hierarchy of files – leaf nodes are atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to. two ABE systems re involved: for each PSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, our proposed revocable MA-ABE scheme is used. The framework is illustrated in We term the users having read and write access as data readers and contributors, respectively, System Setup and Key Distribution. The system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access. Each Personal Health Record owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN). There are two ways for distributing secret keys**

----------∴∴∴----------

I INTRODUCTION

In field of communication, communication is fastest growing area. Using advantage of it allow user to achieve "any time, anything and anywhere" access to required medical information. The traditional paper-based health records generate an extensive paper waste. So there is great interest of moving from paper-based health records to electronic health records (EHRs). With the growth of information and medical technology, health records are transformed from traditional paper records to electronic medical records which are widely used. It leads to the development of a new exchange system of medical information which was named PHRs[1]. PHRs is a new patient-centric health information system. For storing information conveniently and efficiently, medical information is outsourced the third-party semi trusted servers over the internet. So PHR systems are widely deployed and hence improve people's daily life compared with traditional paper-based systems for its interesting advantages like high efficiency, better accuracy, and broader availability. According to a recent report [4], there are more than 77% patients and 70% physicians who want to get involved with PHR systems. The Health Insurance Portability and Accountability Act (HIPAA) has been established for years to regulate PHR related operations [5]. In patients' sensitive Personal Health Information (PHI) contains highly-private information like social security number, address, and date of birth, all of which can be easily used by attackers for malpractice [6], [7]. Several medical records theft and stolen incidents [8] have been reported recently where attackers steal and publish patient health information to a third party

over the Internet. According to a recent survey [9], researchers estimate the economic impact of medical identity theft in the United States at 41.3 billion dollars per annum. More than 78% of participants in [10] worry about the leakage and misuse of their personal information and health condition, so that they fear to use of PHR systems. For providing privacy and security to the health information, information is encrypted before outsourcing it over internet. Basically, the PHR owner i.e. patient herself should decide how to encrypt her PHR and to allow which set of users will access the information. A PHR will 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 [11]. Traditional public key encryption PKE[1] is not useful here as it has disadvantages like key management complexity, finegrained access, and scalability. To overcome these problems Attribute Based Encryption (ABE)[2] is good solution. Chase and Chow[3] proposed a MA-ABE solution referred to as CC MA-ABE program. Generally, PHR service allows a user to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. As PHR is multi owner system that encrypts their PHR according to their own way. Here each user obtains keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to use a central authority (CA) to do the key management on behalf of all PHR owners.

II LITERATURE SURVEY

Traditional Access Control for EHRs:

Traditionally, research on access control in electronic health records (EHRs) often places full trust on the health care providers where the EHR data are often resided in, and the access policies are implemented and enforced by the health providers. Various access control models have been proposed and applied, including role-based (RBAC) and attribute-based access control (ABAC). In RBAC, each user's access right is determined based on his/her roles and the role-specific privileges associated with them. The ABAC extends the role concept in RBAC to attributes, such as properties of the resource, entities, and the environment. Compared with RBAC, the ABAC is more favorable in the context of health care due to its potential flexibility in policy descriptions. A line of research aims at improving the expressiveness and flexibility of the access control policies.

However, for personal health records (PHRs) in cloud computing environments, the PHR service providers may not be in the same trust domains with the patients'. Thus patient-centric privacy is hard to guarantee when full trust is placed on the cloud servers, since the patients lose physical control to their sensitive data. Therefore, the PHR needs to be encrypted in a way that enforces each patient's personalized privacy policy, which is the focus of this paper.

Cryptographically Enforced Access Control for Outsourced Data

For access control of outsourced data, partially trusted servers are often assumed. With cryptographic techniques, the goal is trying to enforce that who has (read) access to which parts of a patient's PHR documents in a fine-grained way. Symmetric key cryptography (SKC) based solutions. Vimercati et.al. proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods, which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable. In [4], files in a PHR are organized by hierarchical categories in order to make key distribution more efficient. However, user revocation is not supported. In [6], an owner's data is encrypted block-by-block, and a binary key tree is constructed over the block keys to reduce the number of keys given to each user. The SKC-based solutions have several key limitations. First, the key management overhead is high when there are a large number of users and owners, which is the case in a PHR system. The key distribution can be very inconvenient when there are multiple owners, since it requires each owner to always be online. Second, user revocation is inefficient, since upon revocation of one user, all the remaining users will be affected and the data need to be re-encrypted.Furthermore, users' write and read rights are not separable. Public key cryptography (PKC) based solutions. PKC based solutions were proposed due to its ability to separate write and read privileges. Benaloh et. al. Securing Personal Health Records in Cloud Computing [4] proposed a scheme based on hierarchical identity based encryption (HIBE), where each category label is regarded as an identity. However, it still has potentially high key management overhead. In order to deal with the multi-user scenarios in encrypted search, Dong et.al. proposed a solution based on proxy encryption [5]. Access control can be enforced if every write and read operation involve a proxy server. However, it does not support fine-grained access control, and is also not collusion-safe. Attribute-based encryption (ABE). The SKC and traditional PKC based solutions all suffer from low scalability in a large PHR system, since file encryption is done in an one-to-one manner, while each PHR may have an unpredictable large number of users. To avoid such inconveniences, novel one-to-many encryption methods such as attribute-based encryption can be used [7]. In the seminar paper on ABE [8], data is encrypted to a group of uses characterized by a set of

attributes, which potentially makes the key management more efficient. Since then, several works used ABE to realize fine-grained access control for outsourced data [6,7,8]. However, they have not addressed the multiple data owner settings, and there lacks a framework for patient-centric access control in multi-owner PHR systems. Note that, in [2] a single authority for all users and patients is adopted. However, this suffers from the key escrow problem, and patients' privacy still cannot be guaranteed since the authority has keys for all owners. Recently Ibraimi et.al. [8] applied ciphertext policy ABE (CP-ABE) [9] to manage the sharing of PHRs. However, they still assume a single public authority, while the challenging key-management issues remain largely unsolved.

III METHODOLOGIES OF PROBLEM SOLVING AND EFFICIENCY IS- SUES

Since the cloud server is no longer assumed to be fully trusted, data encryption should be adopted which should enforce patient-specified privacy policies. Securing Personal Health Records in Cloud Computing. To this end, each owner shall act as an authority that independently generates and distributes cryptographic keys to authorized users. However, as mentioned before, the management complexities may increase linearly with the number of users and owners. Our proposed framework can solve this problem well. The key idea is twofold. First, in order to lower the complexity of encryption and user management for each owner, we adopt attribute-based encryption (ABE) as the encryption primitive. Users/data are classified according to their attributes, such as professional roles/data types. Owners encrypt their PHR data under a certain access policy (or, a selected set of attributes), and only users that possess proper sets of attributes (decryption keys) are allowed to gain read access to those data. Second, we divide the users in the whole PHR system into multiple security domains (SDs), and for each SD we introduce one or more authorities which govern attribute-based credentials for users within that SD. There are two categories of SDs: public domains (PUDs) and personal domains (PSDs). Each owner is in charge of her PSD consisting of users personally connected to her. A PUD usually contains a large number of professional users, and multiple public attribute authorities (PAA) that distributively governs a disjoint subset of attributes to remove key escrow. An owner encrypts her PHR data so that authorized users from both her PSD and PUDs may read it. In reality, each PUD can be mapped to an independent sector in the society, such as the health care, education, government or insurance sector. Users belonging to a PUD only need to obtain credentials from the corresponding public authorities, without the need to interact with any PHR owner, which greatly reduces the key management overhead of owners and users.

User revocation- There are two types of user revocation. The first one is revocation of a user's attribute, which is done by the AA that the user belongs to, where the actual computations can be delegated to the cloud server to improve efficiency. The second one is update of an owner's access policy for a specific PHR document, based on information passed from the owner to the server. Break-glass. 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 PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department. 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.

IV ARCHITECTURAL DESIGN

We endeavor to study the patient centric, secure sharing of PHRs 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.

Main Functions of System:

Registration

In this function normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader have access to.

Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

- PUD - public domains
- PSD - personal domains
- AA - attribute authority
- MA-ABE - multi-authority ABE
- KP-ABE - key policy ABE

Upload files

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

ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

Setup and Key Distribution

In this module the system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access.

Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN)

There are two ways for distributing secret keys.

First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.

Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, 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 keygen of KP-ABE to generate the user secret key that embeds her access structure.

Break-glass Method:

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 PHR. In our framework, each owner's PHR'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.

V CONCLUSION

In this project, we have proposed a novel framework of access control to realize patient-centric privacy for personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that patients shall have full control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management when the number of owners and users in the system is large. We utilize multi-authority attribute-based encryption to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from different public domains with different professional roles, qualifications and affiliations. An important future work will be enhancing the MA-ABE scheme to support more expressive owner-defined access policies.

REFERENCES

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee,G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A Berkeley view of cloud computing (February 2009)

[2] At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded (2006), http://articles.latimes.com/2006/jun/26/health/he-privacy26

[3] The health insurance portability and accountability act of 1996 (1996), http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp

[4] Benaloh, J., Chase, M., Horvitz, E., Lauter, K.: Patient controlled encryption:

ensuring privacy of electronic medical records. In: CCSW 2009: Proceedings o the 2009 ACM workshop on Cloud computing security, pp. 103–114 (2009)

[5] Mandl, K.D., Szolovits, P., Kohane, I.S.: Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 322(7281), 283 (2001)

[6] Wang,W., Li, Z., Owens, R., Bhargava, B.: Secure and efficient access to outsourced data. In: CCSW 2009, pp. 55–66 (2009)

[7] Damiani, E., di Vimercati, S.D.C., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Key management for multi-user encrypted databases. In: StorageSS 2005, pp. 74–83 (2005)

[8] Atallah, M.J., Frikken, K.B., Blanton, M.: Dynamic and efficient key management for access hierarchies. In: CCS 2005, pp. 190–202 (2005)
[9] Blundo, C., Cimato, S., De Capitani di Vimercati, S., De Santis, A., Foresti, S., Paraboschi, S., Samarati, P.: Managing key hierarchies for access control enforcement: Heuristic approaches. In: Computers & Security (2010) (to appear)
[10] Scholl, M., Stine, K., Lin, K., Steinberg, D.: Draft security architecture design process for health information exchanges (HIEs). Report, NIST (2009)
[11] Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM TISSEC 4(3), 224–274 (2001).