SAFE ALLOCATION OF INDIVIDUAL HEALTH RECORDS IN CLOUD COMPUTING

N.Koteswar Rao*1, Dr.R.V.Krishnaiah2

1MCA Student, Dept of MCA, DRK Institute of Science and Technology, Hyderabad (AP), India.
2PG Coordinator, Dept of CSE, DRK Group of Institutions, Hyderabad (AP), India.

ABSTRACT
A physical condition record where health data and information associated to the concern of a patient is maintained by the patient is a personal health record. To provide a complete and accurate summary of an individual's medical history which is accessible online is the intension of a personal health record (PHR). However, to illegal parties, there have been an extensive confidentiality concerns as personal health information could be exposed to those third party servers. To encrypt the PHRs before outsourcing and to guarantee the patients’ control over access to their own PHRs is a capable method. In this paper, for data access control to PHRs stored in semi-trusted servers we propose a novel patient-centric framework and a suite of mechanisms. To encrypt each patient's PHR file, we control attribute based encryption (ABE) techniques in order to achieve fine-grained and scalable data access control for PHRs. We mainly focus on the various data owner scenario, and separate the users in the PHR system into various security domains which greatly reduces the key organization difficulty for owners and users which are unlike from previous works in secure data outsourcing. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Under emergency, our scheme enables a dynamic modification of access policies which supports efficient on-demand user and break-glass access. In this paper, wide-ranging systematic and experimental results are shown in our proposed scheme.

Keywords: Physical Health Record, Attribute Based Encryption, Third Party Servers, Patient Record.

1. INTRODUCTION
Many PHR services are outsourced to or provided by third-party service providers, due to the high cost of building and maintaining specialized data centers. Personal health record (PHR) in recent years, has emerged as a patient-centric model of health information exchange [1,2]. There are many security and privacy risks which could impede its wide adoption while it is exciting to have convenient PHR services for everyone which is shown in fig.1. On the other hand, due to the high value of the vulnerable personal health information (PHI) [3], the third-party storage space servers are often the targets of various hateful behaviors which may lead to disclosure of the PHI [4,5]. It is essential to have fine-grained data access control mechanisms that work with semi-trusted servers and to guarantee patient-centric privacy control over their own PHRs [6]. A feasible and capable approach would be to encrypt the data before outsourcing. Basically, to allow which set of users to obtain access to each file, the PHR owner herself should decide how to encrypt her files [7].

2. SECURE ALLOCATION OF PERSONAL HEALTH RECORDS
A PHR file should be available to the users who are given the related decryption key, while remain secret to the rest of users [8,9]. However, in a PHR system, the goal of patient-centric privacy is often in conflict with scalability. The authorized users may either need to access the PHR for personal or professional purposes. There are two categories of users as personal and specialized users, respectively [10]. In addition, since it is difficult for an owner to determine a list of them and those users’ access requests are generally unpredictable. On the other hand, there are multiple owners who may encrypt according to their own ways, and are different from the single data owner scenario considered in most of the existing works in a PHR system, possibly by using different sets of cryptographic keys [11,12].
Since patients are not always online, by letting each user obtain keys from every owner whose PHR she wants to read would limit the accessibility. To employ a central authority (CA) an alternative is to do the key management on behalf of all PHR owners, but this requires too much faith on a particular authority [13]. We adopt attribute-based encryption (ABE) as the main encryption primitive in order to protect the personal health data stored on a semi-trusted server. By encrypting the file using ABE, under a set of attributes access policies are expressed based on the attributes of users which enables a patient to selectively share her PHR among a set of users, without the need to know a complete list of users [14]. The complexities per encryption, number of attributes involved are the key generation and decryption which are only linear [15,16].

3. ABE FOR INFORMATION ACCESS ORGANIZATION

For outsourced data a number of works used ABE to realize fine-grained access control especially, to secure electronic health records (EHRs) there has been an increasing interest in applying ABE [17]. Recently, for EHR systems an attribute-based infrastructure is proposed where each patient’s EHR files are encrypted using a broadcast variation of cipher text policy attribute-based encryption (CP-ABE) that allows direct revocation [18]. To generate self-protecting Electronic medical records (EMRs) using ABE are investigated, which can either be stored on cloud servers so that EMR could be accessed when the health provider is offline [19,20]. However, there are numerous frequent limitations of the above works. First, the use of a single trusted authority (TA) in the system is usually assumed. In addition, generating secure keys to assign all attribute organization responsibilities to one TA is not feasible, including certifying all users’ attributes or roles. In fact, to define and certify different sets of attributes belonging to their (sub) domains become appropriate authorities as dissimilar organizations usually form their own (sub) domains. For example, for certifying medical specialties a professional association would be responsible, while a regional health provider would certify the job ranks of its staffs. Second, for dynamic policy updates/changes there still lack an efficient and on-demand user revocation mechanism for ABE with the support, which are essential parts of safe PHR distribution. Finally, most of the previous works have dissimilar attribute definitions as they do not distinguish between the individual and public domains key organization necessities and scalability issues. Our thought of conceptually separating the system into two types of domains is similar, however a key difference is in a single TA is still implicit to manage the entire specialized domain.

4. GENERAL IDEA OF OUR FRAMEWORK

To provide safe patient-centric PHR access and well-organized key organization at the same time is the main goal of our framework. According to the different users’ data access requirements the key idea is to divide the system into multiple security domains and personal domains. Based on their professional roles the public domains (PUDs) consist of users who make access. In practice, a PUD can be mapped to an self-governing
sector in the society, such as the health care, administration or assurance sector. For each personal domains (PSD), based on access rights assigned by the owner the users are personally associated with a data owner and they make accesses to PHRs. We exploit ABE to recognize cryptographically imposed, patient-centric PHR access in both types of safety domains. Especially, for each leading a displace subset of attributes there are numerous “attribute authorities” (AAs) in a PUD multi-authority ABE is used. Without directly interacting with the owners, the users in PUDs obtain their attribute-based secret keys from the AAs. To specify role-based fine-grained access policies for her PHR files and to control access from PUD users, owners are free, while do not need to know the list of authorized users when doing encryption.

5. RESULTS

We have proposed a new framework of protected sharing of personal health records in cloud computing. We have estimated the scalability and effectiveness of our solution in terms of storage space, communication and computation costs. We replicate the server’s computation cost spent in user revocation to estimate the system performance of user revocation. We show that our solution is both scalable and efficient through implementation and simulation.

6. CONCLUSION

A novel frame of safe distribution of personal health records in cloud computing has been proposed in this paper. Considering partially trustworthy cloud servers, to allow fine-grained access, we dispute to fully realize that the patient-centric concept shall have complete control of their own privacy through encrypting their PHR files. The frame addresses the exclusive challenges brought by multiple PHR owners and users, in which the complexity of key management is greatly reduced by improving the privacy and guarantees the compared with previous works. To encrypt the PHR data we utilize ABE, so that patients can allow access not only by personal users but also with various users from public domains. Moreover, to handle efficient and on-demand user revocation we improve an existing MA-ABE scheme and prove its security.

REFERENCES


