Mobile Health Information Security in the eHealth Cloud

Hongmei Chi
hchi@cis.famu.edu

Florida A&M University
1333 Wahnish Way, Tallahassee, FL

Abstract - With the healthcare industry facing a new reality, healthcare applications are steadily impacting the mobility and security of how caregivers and hospitals are authorized to access vital information. In this Chapter, a proposed privacy-preserving EHR system using ciphertext-multi authority attribute-based encryption (CPMA-ABE) will be built. In this system, patients can encrypt their EHRs and store them on semi-trusted cloud servers such that servers do not have access to sensitive EHR contexts. Meanwhile patients maintain full control over access to their EHR files, by assigning fine-grained, attribute-based access privileges to selected data users, while different users can have access to different parts of their EHR. In addition, security issues for mobile health are discussed as well.

Categories and Subject Descriptors

K.6.5 [Management of Computing and Information Systems]: *Security and Protection, Authentication, Unauthorized access*

General Terms

Security

Keywords

Cloud computing, electronic health records, security, privacy, role based access control, mobile health, encryption

1. INTRODUCTION

Describe Electronic Health Records (EHRs) are further driving the volume of data as patients' files, x-rays, lab results, and other sensitive medical records are transmitted across the network. Today, nearly one-third of healthcare providers use mobile devices to access EHRs. With the healthcare industry facing a new reality, healthcare applications are steadily impacting the mobility and security of how caregivers and hospitals are authorized to access vital information. However, mobile services are still not generally allowed to operate with highly sensitive and personal data, mainly due to the lack of a defined security standard, low protection of data transferred through the mobile and wireless network and no standard and widely accepted user authentication method that ensure confidentiality.

Recent developments in mobile and communication technologies enable implementation and deployment of various services that can be accessed over mobile devices, as voice, multimedia and data services. Utilizing mobile devices in the healthcare sector can significantly improve efficiency and quality of health care delivered to patients.

The benefits of electronic health records (EHR) have been widely adopted to enable healthcare providers, insurance companies and patients to create, manage and access patients' healthcare information from anywhere, and at any time. With EHRs being supported by individual hospitals and providers, it makes it difficult for a patient to visit one doctor and have his/her medical record available from another. An EHR is a patient-centered, longitudinal, comprehensive and prospective container of a patient's medical data [6], aiming at increasing the quality and efficiency of integrated healthcare. EHR can be maintained in a centralized environment at one healthcare provider or be decentralized and spread across different sites.

To help eliminate this problem more health care providers and hospital are moving vital and sensitive medical data to the clouds. However, moving to the clouds can lead to many security challenges associated with authentication, identity management, access control, policy integration, trust management, data-centric security and privacy and compliance management (Takabi H., 2010) when it comes to using the cloud to store EHRs.

Mobile access to EHR in the cloud can provide a great advantage to various stakeholders, such as patients, healthcare personnel, and healthcare institutions. For example, patients can monitor their condition on their own, be more involved in their medical treatment and decision making process, and stay connected with the healthcare provider at all times. By introducing mobile and wireless technologies, healthcare organizations can cut communication and treatment costs by reducing the number of patient hospital visits and hospital stays while increasing availability and productivity (Raju, 2004). Healthcare providers can be offered universal, timely access to patients' health records, medical knowledge databases, and consultation with other experts in specific fields at the point of necessity. Before mobile services in healthcare can live up to their full potential, many issues and challenges must be addressed and resolved, which are: privacy, security, and protection of highly private and sensitive data.

Security and privacy being the biggest concerns for cloud computing, healthcare organizations have to take into consideration that when data is moved to the clouds, patients' data is open to potential abuse and security threats. Cloud computing has become a promising computing paradigm drawing extensive attention from academia and industry (Mell P., 2011). With this paradigm the location is shifted to a third party service provider, which handles the management of hardware and software resources. Cloud computing can not only increase the efficiency of data management and sharing, but allows healthcare providers to access patients' healthcare data from anywhere at any time. In the article (Wu R., 2012) it is stated that managing healthcare applications in the clouds would make revolutionary changes in the way healthcare providers deal with healthcare information.

Sharing EHRs is one of the key requirements in healthcare domain for delivering quality healthcare services. However, the sharing process could be very complex and involved several entities in such a dynamic environment. Each EHR system in clouds is associated with multiple healthcare practitioners with different duties and objectives. Access control solutions must be in place to guarantee that access to sensitive information is limited only to those entities that have a legitimate need-to-know privilege allowed by patients. For example, a patient may not be willing to share his medical information regarding a HIV/AIDS diagnosis with a dentist unless a specific treatment is required. Therefore, the access control mechanism must support selective sharing that allow patients to quickly and easily authorize a variety of medical associates to access their sensitive records in whole or partially and access control policies from distributed EHR sources must be accurately reflected and enforced accordingly in the integrated EHRs.

This research presents work towards a potential solution to the problem of cloud privacy and security in public, private, and hybrid cloud environments including protection for transmission and storage of documents in situations where access to online services may be limited or impossible. Additionally, methods for adapting Distributed EHR cloud system for cloud based environments are detailed and a secure cloud framework for accessing, storing and sharing health records is presented.

2. EHEALTH CLOUD

In this scenario, a trusted third party was needed to serve as the group manager, who is trusted by all group members and responsible for choosing the practitioners who were allowed to attend the consultation of Sue. In addition, the providers of EHRs for the patient in this scenario are diverse, given Sue may have other health problems such as diabetic, heart disease, etc. Finally, Sue may have some historical health information in her EHR, to which the group of specialists and practitioners do not have the access.

The security and privacy issues involved in this usage scenario were from a patient's view and also a practitioner's view as well. For practitioners, the security and privacy issues can be characterized in the following two statements:

1. How to securely obtain the EHRs of patient Sue, which is relevant to her breast cancer treatment, while staying in compliance of HIPAA minimal disclosure. This concerns the problem of secure EHR collection and integration.

2. How to certify the authenticity of EHRs obtained from different CDOs or information from Sue's EHR upon authorization by Sue. This relates to the problem of secure storage and management of EHR.

Similarly for the patient, Sue needs to be ensured that the diagnosis from the group of practitioners can be trusted with a true medical certificate. This is one of the problems of secure EHR usage models.

2.1 Approach

Clearly EHRs can store and process very sensitive data and should have the proper security and privacy framework and mechanisms since the disclosure of health data may have severe consequences especially for patients. E-health cloud systems must accommodate various workflows, not only related to the patients' medical data but also accounting and billing of treatments, and medication. In particular, the current e-health solutions and standards mainly focus on network security and access control policies; however, they do not address the mobile aspect in dealing with security, i.e., the security of the software, application and hardware being used by health professionals.

The aim of this research is to present a novel approach to the secure transfer medical information from Electronic Health Record (EHR) to a patient or healthcare provider at the point of need. Additionally, during development both security and usability requirements have to be taken into consideration. EHR data needs to be managed with customizable access control in both spatial and temporal dimensions. Presented is a ciphertext policy multi authority (CPMA) that provides more flexibility in both roles (spatial capability) and time (temporal capability) dimensions to control the access of sensitive data.

For the secured sharing of personal health records, the data is stored in cloud servers and key management is provided by a single trusted authority (Warren and Chi, 2014). It not only leads to load bottleneck, but also creates the key escrow problem. As it is a single trusted authority there may be user collision due to the confusion in key distribution. It is not secured to delegate the key management for all attributes to the single trusted authority. There is a need to divide the users into public and professional users based on the divide and rule, for the secure sharing of PHR. Both the user and owner can manage the minimal keys under a set of attributes.

The CPMA security model will be based on algorithmic combination of role-based access control and time-bound hierarchical key management, with such that a valid user of the EHR system is authorized a time interval to access EHR data based on his/her role. Figure 1 shows the proposed cloud architecture security model, which uses five logical components: user input, ABE Encryption, system logging, authentication, and application access of data.

Problem: A multi-authority environment with users associated with multiple authorities.

I. To enforce secure Role Based Access Control (RBAC) of shared data in such a multi-authority environment.

II. To design an approach that supports key revocation in such a multi-authority environment.

An example of such a scenario is an organization that involves multiple departments or users wherein RBAC of shared data is desired. Only authorized users' based on their role assigned in an organization should be able to access sensitive data. A user could be associated with one or more roles and with multiple clinics/hospital. The main goal is to propose an approach to enforce RBAC in such an organization along with a user revocation feature. The main objective is to enable role based access control in an organization. Focusing on one variants of ABE CP-ABE, CP-ABE is a promising cryptographic technique that ensures access control of shared data.

The main goal of the framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. The PUDs consist of users based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be hospital, government or insurance sector. In case of PSD, its users are personally associated with a data owner (such as family members or close friends), and they access the PHRs based on access rights assigned by the owner.

In order to prove the approach, a prototype system will be built for an EHR system that uses CP-ABE to encrypt and secure medical data over the cloud with fine-grained access control. The proposed system will utilize al features of cloud computing combining them with EHR system features to gain one unified central system.

This section aims to provide researchers and developers with knowledge on how to protect personal health data stored on cloud servers. In this Chapter, a proposed privacy-preserving EHR system using ciphertext-multi authority attribute-based encryption (CPMA-ABE) will be built. In this system, patients can encrypt their EHRs and store them on semi-trusted cloud servers such that servers do not have access to sensitive EHR contexts. Meanwhile patients maintain full control over access to their EHR files, by assigning fine-grained, attribute-based access privileges to selected data users, while different users can have access to different parts of their EHR. The system also provides extra features such as populating EHR from different EHR cloud systems using ABE.

The contributions of this research are as follows:

1. The main aim of the proposed system is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements.

2. A unified EHR cloud environment will be defined to represent hierarchical structures of EHRs from multiple domains (i.e. public and personal).

3. This system will provide a web interface for both healthcare providers and patients to manage EHRs, and third-party applications to leverage the cloud system for retrieval and collection of EHRs.

4. This security model, which will use multiple forms of ABE encryption and be based on using ciphertext policy multi authority attribute-based encryption (CPMA), to encrypt and decrypt patients' personal health data stored in the cloud.

3. EHR CLOUD SYSTEM

There are many notable EHR standards for storing, processing and transmitting patient healthcare records such as HL7 CDA, Continuity of Care Record (CCR), HL7 Continuity of Care Document (CCD). The CCR and CCD standards have gained wide acceptance in the healthcare community due in part to the support provided by major EHR vendors including Google Health, and Microsoft HealthVault. With the growing number of EHR platforms, interoperability is becoming a major issue which the CCR and CCD standards seek to solve through a patient health summary which contains the most commonly used and required information used and stored by EHR systems.

The **Access Portal** service provides a patient, both the form of a web service and web based cloud application. The Access Portal service would allow patients to securely access their own personal health records over the internet as well as enabling some level of immediate interaction with their health care providers (e.g. messaging their family doctor, correcting their patient history, filling in forms, etc.). The Access Portal service exposes the patient to both a web based application and web service that allows greater flexibility including mobile applications. Patients are granted access to the portal via their health care provider (the institution or person considered to be the owner of their health record in the 1EHR system). Access Portal services obtain patient records by consuming Provider services on the same cloud. This enables the Access Portal service to provide portals for not just the patients who have records stored within the 1EHR system but any external system with middleware available as well.

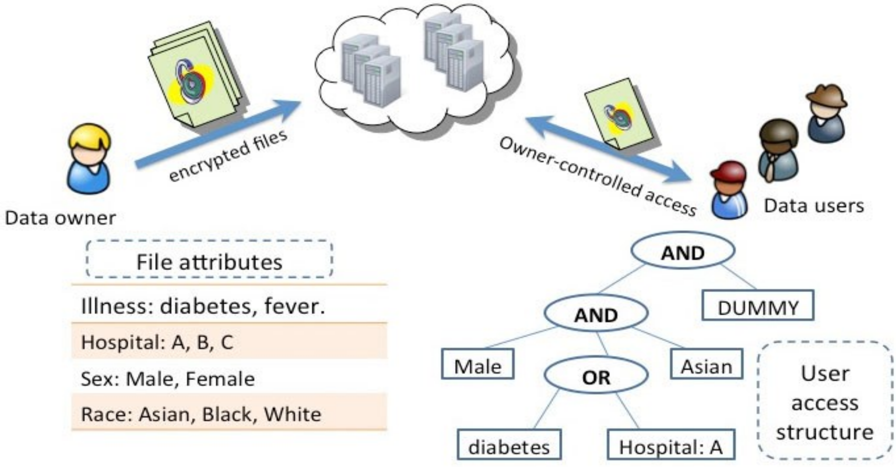

Figure 1: EHR Cloud architecture.

CPMA Security model: While much work has been done in the area of role based access control, little has been done in terms of adapting this type of model to cloud computing paradigm. In (Abbas & Khan 2014) RBTBAC model offers more flexibility of both roles (spatial capability) and temporal capability to control the access of sensitive data from time dimension. The reference security model mainly has three entities cooperatively to manage and control the usage of EHR data in security as shown in Figure 2.

The trusted authority (TA) contains two parts, one is encryptor, which is responsible for encrypting various EHR data from different EHR providers into a uniform cipher text format, and the other is an access control enforcer, which is used to enforce predefined access control policies. The remote EHR database is a necessary component to store the encoded composite EHR data. The original medical data of a patient is collected from repositories of different EHR providers. Then they are encrypted and uploaded to the remote EHR database by the encryptor. To request access to medical data of a patient, a user is required to have two types of credentials: system identity credential and access credential. System credential is exclusive to each user and only used to log into EHR system, but cannot access any medical data. While an access credential associates with an access for a set of EHR data. In RBTBAC, the key technical issue is generation of access key, so that users can access different pieces of EHR data in different time intervals (Abbas & Khan 2014).

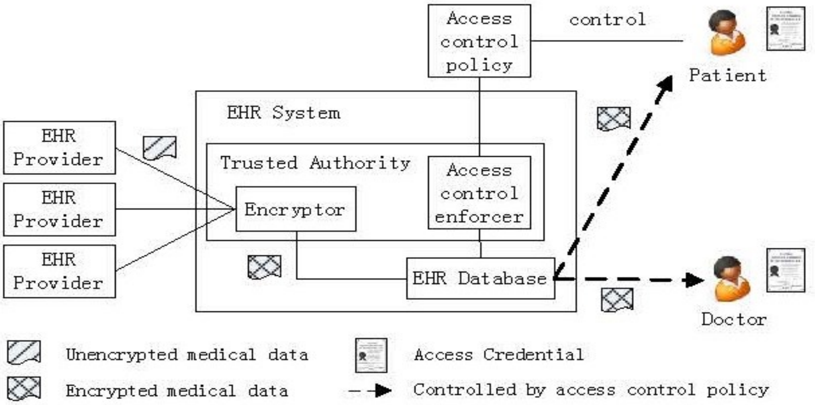

Figure 2: RBTBAC Model

The scope of access depends on the access control policy, the role of user (spatial constraint), and temporal constraint of the access. Consequently, with both valid system identity credential and access credential, users can legally obtain corresponding encrypted data from EHR databases and decrypt them in the legitimate time interval (time bound).

Standard encryption is inefficient when selectively sharing data with many people, since the data needs to be re-encrypted using every user's public key. The main approach is to build upon access model by incorporating the use of Attribute-based Encryption. In an ABE system, the plaintext is encrypted with a set of attributes. With the proposed system combining both CP-ABE and MA-ABE, will allow patients to share their individual medical records more securely. With adding CP-ABE and MA-ABE methods, the goal is to enforce who has (read) access to certain parts of patients' EHRs. In securing an individual's EHR, each EHR would be labeled with ciphertext with a set of descriptive attributes {administrator, physician, nurse, MD, PhD, etc.}, and then provide decryptor with a (key, policy) pair. If and only if the attribute of an individual satisfies the access policy of the ciphertext, the individual can decrypt the ciphertext. The proposed system consists of four algorithms (*setup*, *encrypt, key-gen, and decrypt*), along with using role-base.

EHR Case Studies: This section discusses case studies and shows the approach to support selective sharing and securing of EHRs

Emergency Access to a Patient Health Records: In many cases of medical emergencies a patient will arrive in critical condition and be unable to provide a necessary history. EHR Provider based services would allow for EHR clients (including mobile clients) to be created that may request a read only limited health record containing the most pertinent patient information (e.g., allergies, next of kin, blood type, etc.) to emergency room workers and paramedics (possibly while still en-route through the use of mobile EHR clients). Such clients can connect to a EHR based Cloud system as well as external EHR systems through third party services, creating a network of emergency EHR sharing between medial institutions, hospitals, doctors offices and clinics. A limited read-only record reduces the chance of abuse and privacy while still providing emergency access to emergency workers.

Temporary and Limited Patient Records: In many cases, segments of a patient's health record are required to complete some action. For example, a receptionist in a doctor's office may be required to view a patient's insurance information to process a claim but it would be undesired for them to have full access to a patient's health record. Provider based services are ideal in such a case as the receptionist could be authorized to use only the Provider service and access only the insurance segment of a resulting CCR or CCD document. The read-only nature of the Provider service would also limit potential abuse resulting from unauthorized changes to health records.

Sharing Records between Health Institutions: Suppose Bob is a veteran who had a bullet wound in his abdomen during a battle before. He had a primary surgery in a VA hospital at that time. However, he did not be fully recovered due to severity of the wound. The bullet wound badly affects his pancreas system. Since then, he has suffered from diabetes and needs to periodically take prescribed medicines from a pharmacy. And he has inherited allergies to certain kinds of medicine. Hence, he has to take a special prescription from his primary doctor. Every three months, his homecare doctor needs to monitor the status of his pancreas system. One day, he had a heart attack at home and was sent to a nearby VA hospital where he usually obtains care services by an ambulance. On the way to the VA hospital, the emergency medical technician (EMT) tried to access Bob's medical related information and carried out some emergency actions. The EMT also reported the information to the hospital. When Bob arrives, the VA hospital, his primary doctor, Dr. Lee, had already collected all related medical information of Bob and prepared a preliminary plan.

This scenario involved four healthcare providers from different healthcare domains: primary care hospital, pharmacy, clinic lab and emergency. Each domain manages their EHR systems in the clouds, which store Bob's EHRs since Bob has obtained healthcare related services from them before. And their EHRs are organized and stored based on EHR data schemas. Two healthcare practitioners including Dr. Lee from the VA hospital and the EMT are also involved in the workflow. Depending on their roles, each would have different access privileges to Bob's EHR.

EHR Cloud Setup: Security is always a top priority issue when a cloud computing healthcare system is developed. In order to eliminate this issue, the suggested solution consists of a two domain (*personal and health*) cloud system that acts as a means of data exchange, and the storage of electronic medical records. Healthcare providers will be able to exchange data with other hospitals, healthcare providers, health insurance providers, healthcare practitioners, pharmacies, and other third parties. In addition, patients will also be able to access their medical records, give access to healthcare providers, and create their own personal health records.

To ensure that each owner has full control over their EHR data, the leverage of ciphertext policy attribute-based encryption (ABE) as the encryption primitive, as each owner generates their own set of ABE keys. In this way, a patient can selectively share their EHR among a set of users by encrypting the file according to a set of attributes, and their encryption and user management complexity is linear to the number of attributes rather than the number of authorized users in the system.

The health domain will consist of users who will need access based on their professional roles (*physicians, nurses, researchers, insurance billers*), whereas the personal domain will consist of users associated with the patient (*family*). Each domain will be built on an infrastructure layer, which provides computing, and storage capabilities to host various EHR systems. This type of layer in the cloud can be achieved through computing software solutions such as XenServer, Amazon, Microsoft Azure and Eucalyptus. The middle layer will be the management layer, which includes the User Interface, the Security Service module, the EHR Manager module, and the Policy Manager module. The User Interface will have different views according to users' identities: healthcare professionals, patients and administrators, which will display data according to their role and rights and determine amount of time.

To demonstrate this approach the consideration of either Amazon or Windows Azure to build and manage the proposed cloud. The following is also need the use of a database server (MySQL or SQL Server), the use of JavaServer pages that will allow access to mobile and web pages.

For testing, the following two open source programs: OpenEMR (OpenEMR) and OpenMRS (OpenMRS) were used. OpenEMR is a free and open source electronic health records and medical practice management application that can run on Windows, Linux, Mac OS X, and many other platforms. OpenEMR is ONC Complete Ambulatory EHR Certified and it features fully integrated electronic health records, practice management, scheduling, electronic billing, internationalization, and free support. OpenEMR is a web based software application that uses a web server such as Apache, MySQL as the database and PHP as its programming language. OpenMRS is a software platform and a reference application, which enables design of a customized medical records system with no programming knowledge. OpenMRS is based on a conceptual database structure, which is not dependent on actual types of medical information or on particular data collection so the EHRs can be customized for different uses. OpenMRS has the following features: Central concept dictionary, Security, Privilege-based access, Patient repository, Data entry, Data export and Standards support.

The challenge to testing the cloud setup is to find an efficient and scalable approach to integrate role-based access control and time bound key management under a dependable access control framework, which delivers both security and scalability required for role-based and time bound access to EHRs. As mentioned before a user can have several different roles, so they may need to have multiple keys to access different pieces of EHR data. The testing of possible attacks will consist of using attacks from outside users, and attacks from users with unauthorized roles and permissions.

With testing, CPMA security model, privacy will be better provided for patients from the following aspects:

1. When users access EHR data, access will be limited to a time period based on the user's role and permission type.
2. Patients will control access to better protect their privacy, this can help patients better understand and control their EHR data more tightly and know who is accessing their data.
3. Lastly, once an access credential has expired it will automatically become invalid and access to the EHR will be revoked.

4. MOBILE HEALTH APPS

Mobile health has potential to improve healthcare quality, improve efficiency, and reduce cost, security and privacy are areas that require legal and policy attention to ensure that mHealth patients' data are properly protected. Those services in mHealth are possible not only patients own mobile devices, but also doctors and other medical service providers may access patient electronic health records (EHR) easily. In Fig. 3, one basic system architecture of mobile health system is provided (Li et al., 2014). The system architecture includes three components: wearable sensors, smartphone, ad web services. For example, when the patient takes a temperature, the sensor will get the number, then it will transfer the test result to the smart phone. The smart phone will store this test result into the patient's electronic health records, and it will further push the test result to the web service. The patient's doctor will get a notification to look at the test result and give the immediate feedback to the patient.

5. IMPLEMENTING AND TESTING

The use of ABE, is a building block in the proposed privacy-preserving EHR system. That is because ABE not only offers fine-grained access control similar to RBAC or ABAC, but also enforces data protection. To test and fully evaluate the CPMA encryption scheme, a Linux based implementation was created, to add extended functions, features and distributed authority setup. As the implementation is based on CP-ABE implementation it uses the same PBC library (https://crypto.stanford.edu/pbc/) for the algebraic operations and only supports Linux based systems. For CPMA, a role-based attribute set using the role information such as {john.doe.family, john.doe.friend and john.doe.physician}. CP-ABE is divided into two libraries, libbswabe (a library implementing the core crypto operations) and cpabe (higher level functions and user interface), also had to install a Linux library (libcelia) for implementing a CP-ABE.

The prototype system for the following test application and have implemented CPMA algorithm using the CP-ABE toolkit. To build the library and toolbox, the following is needed GNU multi-precision (GMP) library, pairing-based crypto (PBC) library. The pairing based crypto (PBC) library can be downloaded from http://crypto.stanford.edu/pbc/download.html. Also implemented the cpabe package a convenient set of tools that are available from (Advanced Crypto Software Collection, 2013). The build process generates the static library libcelia.a which is being installed in /usr/local/lib directory. After building and installing libcelia, users can build and install cpabe with the same commands. There should be four executable generated: cpabe-setup, cpabe-keygen, cpabe-enc and cpabe-dec and corresponding manual files. The executable files were installed in /usr/local/bin directory.

Testing of CPMA: the data owner uploads their data into the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The data owner can change the policy over data files by updating the expiration time. The Data owner can have capable of manipulating the encrypted data file. The data owner can set the access privilege to the encrypted data file. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner consumer is administrated by a domain authority.

The user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, the Domain authority gives all the privileges and the Attribute Authority controls the Data users only. Users may try to access data files either within or outside the scope of their access privileges; so malicious users may collude with each other to get sensitive files beyond their privileges. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Its parent domain authority or the trusted authority manages an attribute authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner. The cloud service provider, the trusted authority, and attribute authorities are always online. And the cloud is assumed to have abundant storage capacity and computation power. Two types of keys handle key management in the system. The first one is related to the CP-ABE key and its day-to-day use. While, the other one is related to AES encryption scheme and its use in emergency access. Also each type can be analyzed from both patients and providers point of view. There are three types of keys in CP-ABE master (key, public key, and private key):

- Master Key: A private key is used to generate user's private keys. This key is only stored in the secure webserver which acts as a key authority in the system. This key is kept private and it will not be shared with any user, provider, or third party that may have access to the system.

- Public Key: A public key that is needed to encrypt or decrypt data in CP-ABE systems. This key will be shared with all users, providers, and systems that may have access to the system.
- Private Key: A unique key that will be generated for each entity, when it joins the system. This key uniquely describes each entity with the associated attributes. The users will use their keys to gain access to data that was authorized for them. This key should be accessible only by its owner.

Emergency Access: Sometimes medical staffs need to have temporary access to certain parts of the PHR data when an emergency occurs to a patient, who may be unconscious and unable to modify the access policies beforehand. The medical staffs require a temporary authorization (e.g., emergency key) to decrypt those parts of data. This can be easily achieved in this system by allowing each patient delegate his or her emergency key to an emergency department (ED). At the beginning, each owner defines an "emergency" attribute and includes it into the Personal domain part of the ciphertext of each PHR document to allow emergency access. The patient then generates an emergency key and delegates it to the ED who stores it in a database of patient directory. During emergency, the medical staff requests and obtains the corresponding patient's emergency key from the ED and then access the decrypted PHR documents using that key. After recovering from the emergency, the patient can revoke the emergency access by changing the access policy.

Evaluations and Performance: to measure the computation time of ABE using cpabe toolkit, and the cpabe toolkit created by John Bethencourt. CP-ABE toolkit use a 160-bit A type elliptic curve group based on the super singular curve $y^2 = x^3 + x$ over a 512-bit finite field without preprocessing. Since the most time-consuming computation in ABE operations is computing bilinear map, which is define as a simple AND gate. Therefore, there is no internal node within the access structure. As expected, the Key generation time of ABE, is precisely linear in the number of attributes in CPABE. For CP-ABE, the key generation process needs to select one random element in Zp (a finite field) and perform three exponentiations in G (an elliptic curve group) for each attribute. For KP-ABE, the process only needs to select one random element in Zp (during the construction of polynomial p) and perform one exponentiation in G for each leaf node. Therefore, the key generation time of KP-ABE is roughly three times faster than the key generation time of CP-ABE.

Using symmetrical encryption schemes in securing EHRs is the simplest and fastest form of encryption. Figure 4 shows the difference in speed between AES and CP-ABE when used to encrypt different magnitudes of files. CP-ABE is slower than AES, because of the need to apply it more than once slows the system as compared to AES which use only one operation to access a file. The size of the EHR needing to be encrypted and decrypted plays a key role in how the speed is affected, the number of operations needed to access the data.

Access policy complexity also plays major role in the speed of CP-ABE. Figure 4 measures the encryption speed of CP-ABE algorithm when encrypting a 10 MB file using several diverse access policies. The speed of CP-ABE decreases, while the size of the access policy increases.

6. CONCLUSION

This paper proposes a novel framework of secure sharing of personal health records in cloud computing and discusses the relevant issues for design mHealth apps. The framework addresses the unique challenges brought by multiple EHR owners and users, in that greatly reduces the complexity of key management while enhancing the privacy guarantees compared with previous works. Attribute-based encryption was utilized to encrypt the EHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations. Furthermore, the enhancement of existing CP-ABE schemes which handles efficient and on-demand user revocation, and provide its security. This service was provided to a third-party server which reduce the controlling risk of the EHR owner. CP-ABE provides encryption and extra access control function of each attribute for the purpose of securing data access control. As the users grow in number the use of CP-ABE fine-grained data access control, means different types of users can access EHRs using many forms of attributes.

However, issues of trust, privacy, and security, in addition to several technical issues that must be addressed before healthcare providers can fully adopt and trust the e-Health Cloud, offset the benefits gained, by putting forward an attribute-based encryption control model for EHR systems. Differing from the traditional MA-ABE models, CPMA is more flexible of attribute roles and has the capability to control the access of sensitive data according to the use of time dimension.

REFERENCES

[1] Abbas, A., & Khan, S. U. (2014). A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds. Biomedical and Health Informatics, IEEE Journal of, 18(4), 1431-1441.

[2] AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health cloud: opportunities and challenges. Future Internet, 4(3), 621-645.

[3] Alam, M. G. R., Cho, E. J., Huh, E. N., & Hong, C. S. (2014, January). Cloud based mental state monitoring system for suicide risk reconnaissance using wearable bio-sensors. In Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication (p. 56). ACM.

[4] Bethencourt, J., Sahai, A., & Waters, B. (2007, May). Ciphertext-policy attribute-based encryption. In Security and Privacy, 2007. SP'07. IEEE Symposium on (pp. 321-334). IEEE.

[5] Gao, X., Xu, J., Sorwar, G., & Croll, P. (2013). Implementation of E-Health record systems and E-Medical record systems in China. The International Technology Management Review, 3(2), 127-139.

[6] Garkoti, G., Peddoju, S. K., & Balasubramanian, R. (2014, December). Detection of Insider Attacks in Cloud Based e-Healthcare Environment. In Information Technology (ICIT), 2014 International Conference on (pp. 195-200). IEEE.

[7] González-Martínez, J. A., Bote-Lorenzo, M. L., Gómez-Sánchez, E., & Cano-Parra, R. (2015). Cloud computing and education: A state-of-the-art survey. Computers & Education, 80, 132-151.

[8] Kay, M., Santos, J., & Takane, M. (2011). mHealth: New horizons for health through mobile technologies. World Health Organization, 66-71.

[9] Karlen, W., Dumont, G. A., & Scheffer, C. (2014, August). Sharing Vital Signs between mobile phone applications. In Engineering in Medicine and Biology Society (EMBC), 2014 36th Annual International Conference of the IEEE (pp. 3646-3649). IEEE.

[10] Lee, N., & Kwon, O. (2015). A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services. Expert Systems with Applications, 42(5), 2764-2771.

[11] Li, H., Zhang, T., Chi, H., Chen, Y., Li, Y., & Wang, J. (2014). Mobile health in China: Current status and future development. Asian journal of psychiatry, 10, 101-104.

[12] Lu, S., Ranjan, R., & Strazdins, P. (2014). Reporting an experience on design and implementation of e - Health systems on Azure cloud. Concurrency and Computation: Practice and Experience.

[13] Luxton, D. D., Kayl, R. A., & Mishkind, M. C. (2012). mHealth data security: the need for HIPAA-compliant standardization. Telemedicine and e-Health, 18(4), 284-288.

[14] Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. Journal of medical systems, 39(1), 1-8.

[15] Murad, A., Schooley, B., & Abed, Y. (2013, November). A secure mHealth application for EMS: design and implementation. In Proceedings of the 4th Conference on Wireless Health (p. 15). ACM.

[16] Rahim, F. A., Ismail, Z., & Samy, G. N. (2014). Information Privacy Concerns in Electronic Medical Records: A Preliminary Investigation. In Knowledge Management in Organizations (pp. 177-185). Springer International Publishing

[17] Warren, L., & Chi, H. (2014, March). Securing EHRs via CPMA attribute-based encryption on cloud systems. In Proceedings of the 2014 ACM Southeast Regional Conference (p. 20). ACM.

[18] WHO (2011). mHealth: New horizons for health through mobile technologies. Retrieved on Feb.16th 2015 from http://www.who.int/goe/publications/goe_mhealth_web.pdf