IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 5, Ver. VII (Sep – Oct. 2014), PP 33-40
www.iosrjournals.org

Secure Sharing of Personal Health Record in Server with On-track ECG Monitoring

Dona Mary Thomas
(Dept. of Computer Science and Engineering, Mahatma Gandhi University, Kerala, India)

***Abstract*:** *Personal Health Record (PHR) paved the way to the patient centric model of health information exchange. This 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. But there have been wide privacy concerns about whether the patients could actually control the sharing of their sensitive Personal Health Information (PHI). This paper proposes a new patient centric framework and mechanisms for data access control to PHRs stored in semi-trusted servers using Attribute Based Encryption (ABE) technique. It focuses on the multiple data owner scenario, and divides the users in the PHR system into multiple security domain that greatly reduces the key management complexity for owners and users. It also proposes a new application for the on-track monitoring of patient's health data with the help of ECG device where communication between client and server is achieved through the GPRS network. The utilization of electrocardiogram transmission will improve efficiency of medical care and service for patients if they could be monitored constantly by health care providers. AES and ABE encryption techniques are used in my work.*
Keywords: *Attribute based encryption (ABE), ECG, GPRS, Personal health record (PHR), secure sharing.*

I. Introduction

Personal Health Record (PHR) concept has emerged in recent years. PHR is a collection of information pertinent to a patient's health. This service allows a patient to make, handle, and organize his/her personal health data in one place through the web. Patients can control the health information in PHR and can get it anywhere at any time with Internet access. Each patient has assured the full control of his/her personal health records. It is shared with wide range of users, such as healthcare providers, researchers, relatives or friends. Due to the high cost of building and maintaining specialized data centres, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault. But while using third party service providers there are many security and privacy risks for the PHR. The main concern is whether the PHR owner or the patients actually gets full control of his/her data or not, especially when it is stored at third party servers which is not fully trusted. On the one hand, Health care regulations are there such as HIPAA, which incorporates business associates [2]. On the other hand, the third party storage servers become the targets of various malicious behaviours that lead to hacking of PHI. The incident happened at Department of Veterans affairs database is an example of this. The database information, which contains many important data including their ssn and health problems, was stolen by an unauthorised employee [3]. To ensure patient centric privacy control over their own PHRs, it is essential to provide data access control mechanisms. This can be achieved by encrypting the data before outsourcing. PHR owner will decide which users will get access to which data in his PHR record and can decide the encryption pattern. Any user with the corresponding decryption key can view the PHR files. Furthermore, the patient shall always retain the grant and revoke privileges when they feel it is necessary [4]. However, there arises a conflict with the goal of patient centric privacy and PHR system's scalability.

The authorized users may need to access the PHR for different purposes, either for public or professional purposes or for personal users. Medical doctors, pharmacists, and researchers comes under professional users and family members, friends comes under personal users. The former has potentially large scale and the owner will easily be overwhelmed by the overhead of key management. Users are divided into two domains, personal domain and public domain. In addition, since those users access requests are generally unpredicted-able; it is difficult for an owner to determine a list of them. On the other hand, different from the single data owner scenario considered, there are multiple owners who may encrypt according to their own ways, by using different sets of crypto-graphic keys. An alternative method is employing a single trusted authority for doing the key management functions. But it causes the key escrow problem.

This paper proposes a patient centric secure sharing of PHR [1] and protects the personal health data stored on semi-trusted servers by using attribute-based encryption as main encryption primitive. ABE technique provides security to the database. In this, cipher text labeled with set of attributes. Private key associated with access structure controls which cipher text a user is able to decrypt. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share their PHR among a set of

users by encrypting the file under a set of attributes. There is no need to know the 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. 'N' number of users can be added into this application and thus achieves scalability. For security purpose, ABE is used. The data is encrypted using AES. The system is enhanced with an application for the on-track monitoring of patient's health data.

II. Related Works

This thesis is mostly related to the cryptographically based access control for the outsourcing data and attribute based encryption. Vimercati et.al. proposed a Symmetric key Cryptography[5] based solution for securing outsourced data on semi-trusted servers , which can achieve fine-grained access control. Unfortunately, the file creation complexity and user grant/revocation operations are linear to the number of authorized users, which is less scalable. For efficient key distribution, files in a PHR are classified by hierarchical categories [6]. But it does not support user revocation. There are many key limitations for the SKC-based solutions. First, if there are large numbers of users and owners, the key management overhead is high. The key distribution can be very difficult when there are multiple owners, since it requires each owner to always be online. Second, user revocation is inefficient because all the remaining users will be affected during the revocation of one user and the data need to be re-encrypted.

Public Key Cryptography based solutions were proposed due to the separate write and read privileges ability. Benaloh et. al. proposed a scheme based on hierarchical identity[6] based encryption (HIBE), where each category label is represented as an identity. But it has high key management overhead. To deal with the multiuser scenarios, Dong et.al. proposed a solution based on proxy encryption. For every write and read operations which involves a proxy server, access control can be enforced. But it does not support fine-grained access control, and does not compromise collusion-safe Attribute based encryption (ABE). In SKC and traditional PKC based solutions file encryption is done in a one-to-one manner and they suffer from low scalability in a large PHR system. In order to avoid such difficulties, one-to-many encryption methods such as attribute-based encryption can be used. In ABE technique, key management becomes more efficient and data is encrypted to a group of uses characterized by a set of attributes. Since then, several works uses ABE to achieve fine-grained access control for outsourced encrypted data However; the multiple data owner settings are not addressed here, and it lacks a framework for patient-centric access control in multi-owner PHR systems. It results to the key escrow problem, and privacy of the patient cannot be guaranteed since the authority has keys for all owners. CP-ABE is another encryption technique to acquire complex control on encrypted data. This technique assures the confidentiality of the encrypted data. However, this also assumes a single public authority, while the key-management issues remain unsolved. However, there are several common drawbacks of the above works. First is that it uses a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since all the encrypted files can be accessed by the TA, and leads to the potential privacy exposure. In addition, delegation of all the attribute management tasks to one TA is not applicable, including authenticating all users' attributes or roles and generating secret keys.

Cipher Text Policy Attribute based Encryption (CP-ABE) is an encryption technique for acquiring complex control on encrypted data. In this, access structures are built within cipher texts. This technique is used to keep encrypted data confidential. However, this also assumes a single public authority, and key-management issues remain largely unsolved. However, there are several common drawbacks of the above works. This not only may create a bottleneck problem, but also suffers from the key escrow problem since the TA can access all the encrypted files, creating privacy exposure.

Key-Policy Attribute-based Encryption (KP-ABE) is another crypto system for fine grained sharing of encrypted data. In this, cipher texts are labelled with sets of attributes. The key-policy ABE outsourced data in to the cloud, where a single data owner can encrypt the data and share with multiple authorized users, and attribute-based access privileges contained keys are distributed. They also propose a method for the data owner for efficient revocation of users by delegating the changes of affected cipher texts and user secret keys to the server. Since the key update operations can be aggregated over time, their scheme achieves low amortized overhead. To revoke users/attributes effectively is a well known challenging problem in ABE. Traditionally, this is done by the authority by broadcasting periodic key updates to unrevoked users frequently. But this does not achieve complete backward/forward secrecy and it is less efficient. In addition, Ruj et.al proposed an alternative for the above problem using decentralised ABE scheme [7]. This scheme enjoys better policy expressiveness. The communication overhead of revocation is high, because it requires the data owner to transmit the updated cipher text components to every non-revoked user. There is no differentiation between personal and public domain.

The novel system bridges the above gap by proposing a unified security framework for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHRs, and distributes users' trust to multiple authorities that better reflects reality. 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/she 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. This also proposes a suite of access control mechanisms by combining the strengths of both CC MA-ABE [8] and the YWRL ABE scheme. Using this scheme, patients can choose and enforce their own access policy for each PHR file, and the user revocation does not involve any high overhead.

III. System Architecture

This section describes the novel patient-centric secure data sharing framework for server based PHR systems.

3.1 Problem Definition

Consider a PHR system where there are multiple PHR owners and PHR users. The problem occurs when a number of PHR owners and users are involved. The owners refer to the patients. Owners have the full control over their own PHR data. They have the permission to create, manage and delete it. All the PHR files are stored in a central server. The users can be a friend, a caregiver, or a researcher. Only authorised users can access the PHR documents through the server in order to read or write to someone's PHR. Multiple owner's data can be simultaneously accessed by a user. This leads to the need of Multi-Authority Attribute Based Encryption (MA-ABE)[8].

1) Prevention of Unauthorized Users: Patient should have the ultimate control over their personal health record. They have the power to determine which users shall have access to their medical record. The two main security objectives for any electronic health record system are user controlled read/write access and revocation. Users controlled the write access control in PHR context prevents the unauthorized access of users to gain access to the record and modifying it.
2) Fine Grained Access Control: Fine grained access control means that different users are authorized to read different sets of documents. The main goal of the framework is to provide secure patient-centric PHR access and efficient key management simultaneously. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute.
3) Attribute Revocation: The PHR system should support users from two main domains such as personal domain and public domain. The public domain users may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. The management of users and keys should be minimized to enjoy the usability of the system.

3.2 Security Model

The server is considered to be semi-trusted. The server will honestly follow the protocol and it will try to find out as much as secret information in the PHR files. In addition, it is assumed that each party in the system is preloaded with a pair of public/private key. The entity authentication can be done by challenge response protocols.

3.3 System Architecture

Fig.1 depicts the proposed system architecture for secure sharing of personal health record. In this proposed scheme, the system is divided into two main security domains, such as personal domain (PSDs) and public domain (PUDs) according to the user's data access requirements. The PUDs includes users who make access based on their professional roles, such as doctors, nurses and insurance agents. Personal domain users have personal relationships with the patient such as family members or friends. Here, the data owner refers to those who possess the PHR and data reader who can access the encrypted PHR.

In the PSD, the owner makes use of key-policy attribute based encryption (KP-ABE). For the PSD users, the owner generates the secret keys. The multi-authority attribute based encryption (MA-ABE) is used in the PUD. Secret keys for PUD users are generated by the attribute authorities (AA) depending on their profession. There are multiple AAs, each governing a disjoint subset of attributes. Users in the PUD obtain their secret key not from the owners, but from the AAs. The multi-domain approach models different user types and access policies in a PHR system. The utilization of ECG transmission improves the efficiency of the system.

3.4 Details of the Proposed Framework

In the proposed framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users and ECG transmission. In addition, two ABE systems are involved: for each PSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, revocable MA-ABE scheme is used.

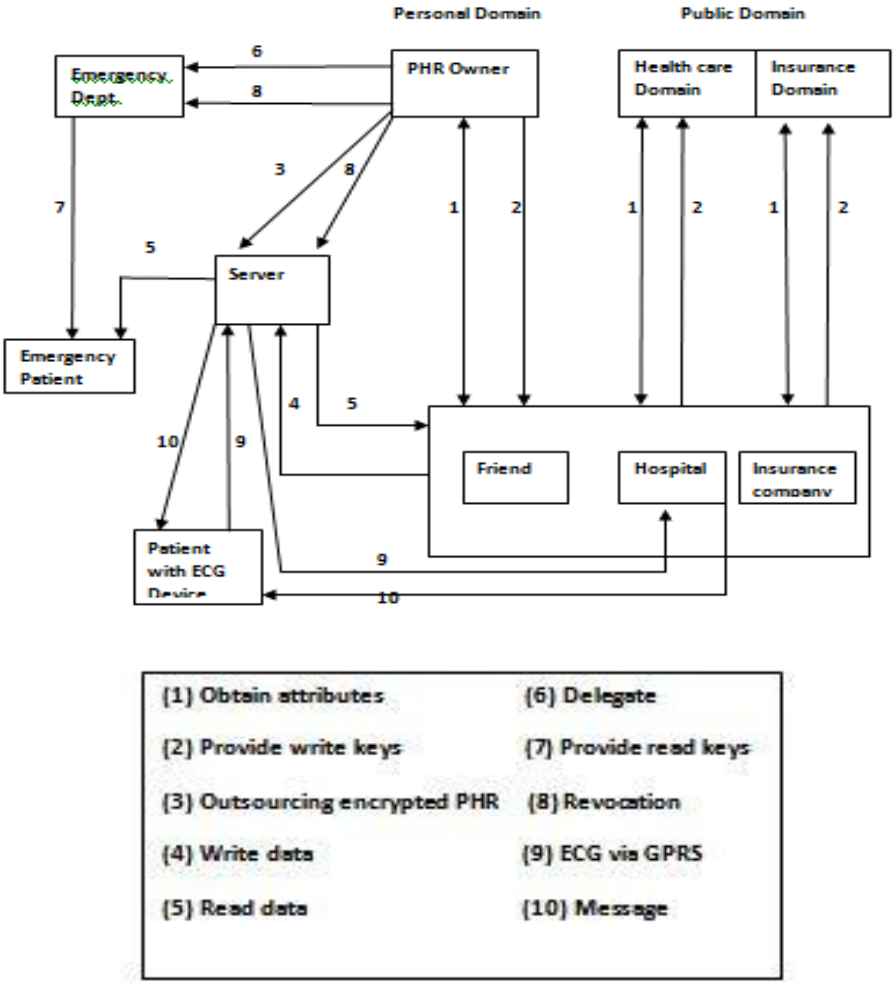

Fig.1.The proposed framework for patient-centric, secure and scalable PHR sharing on semi trusted storage under multi owner settings.

3.4.1 System Setup and Key Distribution

The system defines a common set of data attributes shared by every PSD, such as "personal information", "medical history", "sensitive information" see Fig.2. Distribution of the attributes is important.

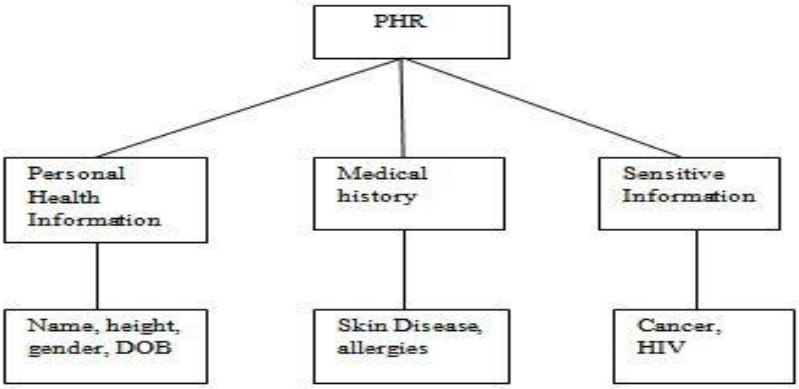

Fig.2. The Attribute Hierarchy

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 mail. For distributing secret keys, a PHR owner can specify the access privilege of a data reader in her PSD, when first using the PHR service and let her application generate and distribute corresponding key to the latter. Second, a reader in PSD could obtain the secret key by sending a request to the PHR owner via mail, and the owner will grant her a subset of requested data types. The policy engine of the application automatically derives an access structure, and runs key generation of KP-ABE to generate the user secret key. When the user is granted all the file types under a category, her access privilege will be represented by that category instead. Obtaining attributes is reflected by (1) in Fig.1. Write keys are distributed by AAs that permit data contributors to write to some patient's PHR ((2)).

3.4.2 PHR Encryption and Access

The owners upload ABE encrypted PHR files to the server ((3)). Each owner's PHR file is encrypted by using ABE and AES. Only authorized users can decrypt the PHR files, excluding the server. The data contributors will be granted write permission to someone's PHR, if they have correct write keys ((4)). The data readers decrypt the files by appropriate attribute based keys ((5)).

3.4.3 User Revocation

Revocation of a data reader ((8)) or their attributes/access privileges are considered here. There are several possible cases. Revocation of one or more role attributes of a public domain user, revocation of a public domain user which is equivalent to revoking that entire user's attributes, revocation of a personal domain user's access privileges, and revocation of a personal domain user.

3.4.4 Policy Updates

The sharing policy for an existing PHR document by updating the attributes in the cipher text can be done effectively by the PHR owner. Various operations such as add/delete/modify can be done by the server on behalf of the user.

3.4.5 Break-glass

During an emergency situation, the regular access policies may no longer be applicable. In order to handle this situation, break-glass access is needed to access the victim's PHR. In this framework, each owner's PHR's access right is also delegated to an emergency department ((6)). To prevent from abuse of break-glass option, the emergency staffs needs to contact the emergency department to authenticate his/her identity, and obtain temporary read keys ((7)). After the emergency is over, the patient can revoke the emergent access via the ED.

3.4.6 ECG Transmission

ECG signal [9] is analyzed and heart rate information is computed. Electrocardiogram is transmitted to the server via GPRS ((9))and the server contains already some readings. The transmitted reading is then compared with the existing readings in the server. If it is a normal reading, then just a warning message((10)) is send to the patient. If it is above a threshold value, then the reading is send to the concerned doctor and first aid can be taken by the patient. Also a severe warning message is send to the patient. In heart rate computation, distance between the R peaks is determined and frequency of the R peaks for each minute is computed.

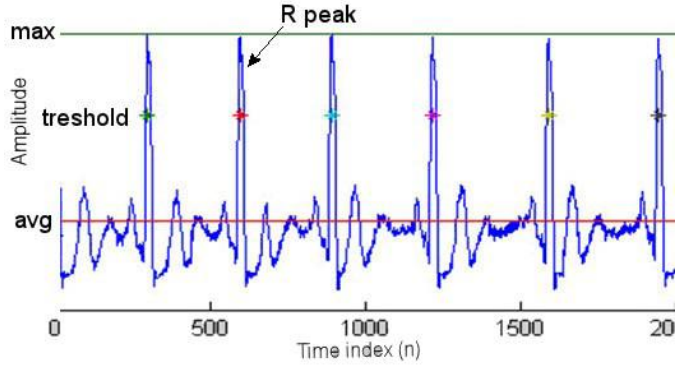

Fig.3. Heart Rate Detection

The proposed heart detection algorithm steps are as the following:

- Compute the average value of the 1 second duration of the ECG data. Calculate the maximum value of the 1 second duration of the ECG data. Determine the adaptive threshold level. (Threshold = (average + maximum)/2).
- Find the peak locations that exceed the threshold level for the rest 5 second duration of ECG data.
- Measure the heart rate by using the distances between the peaks. If the calculated heart rate is not between 40 and 130, ignore that value.
- Compute the average value of obtained heart rates.
- Repeat these operations in every 6 second.

Fig.3 shows the R peaks on an ECG data and adaptive threshold level which is shown.

IV. Key Design Issues

In this section, several key design issues in secure sharing of PHR in server are addressed.

4.1 Using MA-ABE in public domain

This framework delegates the key management functions to multiple attribute authorities for the public domain. The Chase-Chow (CC) MA-ABE scheme [8] is used to achieve stronger privacy for data owners. It is common to associate the cipher text of a PHR document with an owner-specified access policy for users from PUD. One technical challenge is that CC MAABE is essentially a KP-ABE scheme. The access policies are enforced in user's secret keys and the key-policies do not directly translate to document access policies from the owner's points of view. This design show the CC MA-ABE can actually support the owner-specified document access policies. It agrees upon the formats of the key-polices and specifies which attributes are required in the cipher text. It functions similar to CP-ABE.

4.2. Expressive File Access Policies

A more expressive encryption's access polices can be achieved by key –policy generation rule. The user's attributes/roles belonging to different types assigned by the same Attribute Authority are correlated with respect to primary attribute type. The enhance key-policy generation rule states that there should be no intersection with the attribute tuples which are assigned by the same Attribute Authority for different users. The basic encryption rule states that, as long as there are multiple attributes of the same primary type, corresponding non intersected attribute tuples are included in the cipher text attribute set. The primary type based attribute association is shown in Fig.4. There is a "horizontal association" between two attributes belonging to different types assigned to each other.

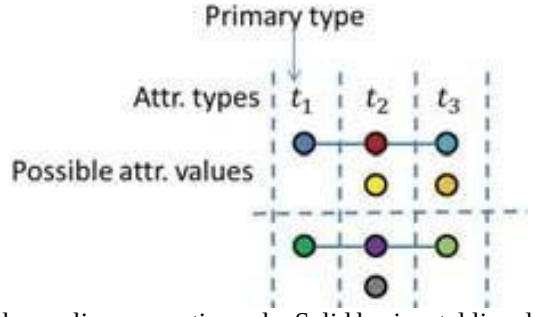

Fig.4. Illustration of enhanced key policy generation rule. Solid horizontal line denotes possible association of attributes for two users.

For example, if an attribute type is associated with another attribute type and the latter is a primary type, then a user's possible set of that attribute type should not intersect with that of another user. Since in reality, the PUDs number is small, this scheme is efficient than CP-ABE [8], in which as per the number of organizations the length of cipher text grows linearly. Each file is encrypted using a randomly generated file encryption key (FEK), and it is then encrypted using ABE.

4.3 Impose Write Access Control

An undesirable thing is that if there are no limitations or restrictions on write access, any user can able to write to someone's PHR with the use of public keys only. By granting write access, a data contributor should obtain proper authentication from the server and the verification is done by the server itself who grants/rejects write access.

4.4 Handle Dynamic Policy Updates

This scheme also supports the dynamic operations such as add, modify, delete of part of the document access policies or the data attributes by the PHR owner. A patient has the authority to simply delete the cipher text components corresponding to an attribute in their PHR files. For example, if a PHR owner does not want some doctors to view their file after he/she finishes a visit to a hospital, he/she can simply delete the cipher text parts corresponding to attribute "doctor" in his/her PHR files. By using proxy revocation techniques, addition and modification of attributes/access policies can be done easily, but they are expensive. So to make this computation more efficient a random number s is stored by each owner in encrypting the FEK of each document. And new cipher text components are constructed corresponding to added/updated attributes based on s. The owner can keep a random seed s` in order to reduce the storage cost and generate the s for each encrypted file from s` by using a pseudorandom generator. Thus one modular exponential operation becomes the main computational overhead.

4.5 Break-glass Access under Emergency

In certain situations, medical staffs need to have a temporary access when a emergency condition happens to a patient, sometimes who may become unconscious and is unable to change their access policies beforehand. In order to decrypt the data, the medical staff will need some temporary authorization such as emergency key to decrypt the patient's file. For this, let each PHR owner delegate their emergency key to an emergency department (ED). Each owner should define an "emergency" attribute and builds it into the personal domain part of the cipher text of the PHR document that allows break-glass access. By using the single node key policy "emergency", the owner can generates an emergency key and delegates it to the emergency department who keeps it in a database of patient directory. When an emergency situation arises, medical staffs authenticate themselves to the emergency department, requests and obtain the corresponding patient's, and then decrypt the PHR documents using. When the patient recovers from the emergency, he/she can revoke the break glass access. This can be done by computing a re-key and submit it to the emergency department and the server update her and cipher text to their newest versions.

V. Security Analysis

This section analyzes the security of the proposed PHR sharing solution. It prevents the unauthorized read access and thereby achieves data confidentiality. By MA-ABE scheme, the system is secure under attribute based selective set model [8].This scheme provides data confidentiality of the PHR data against unauthorized users and maintaining collusion resistance against users. This framework also achieves secrecy and security of write access control. The security of the proposed scheme is compared with several existing works. Comparison is done in terms of confidentiality guarantee, access control, and supported revocation method. Four representative schemes are chosen for the comparison such as 1) the VFJPS scheme based on ACL (Access Control List); 2) the BCHL scheme based on HIBE [6] in which each PHR owner acts as a key distribution system; 3) the HN revocable CP-ABE scheme [8], where the proposed scheme adapt it by the assumption of one PUD with a centre authority and several PSDs; 4) the NGS scheme in which a privacy preserving EHR system is proposed. It adopts attribute based broadcast encryption encryption (ABBE) to achieve data access control; 5) the RNS scheme in which is an enhancement of Lewko-Waters MA-ABE with revocation ability for the data access control.

Table 1 System Comparison

Scheme	Security	User Domains	Access Policy	Revocation Means
VFJPS	Not against user-server collusion	All	ACL level	ACL level, immediate
BCHL	No collusion risk	All	ACL level	N/A
HN	Not against user-server, single TA	PUD	Any monotonic formula	Attribute level, immediate
NGS	Single TA	PUD	Attribute and ID-based policy	ACL level, immediate

RNS	Against N-1 AA collusion	PUD	Any monotonic Boolean formula	Attribute level, immediate
Proposed Scheme	Against N-2 AA collusion	All (PSD and PUD)	Conjunctive form with wildcard	Attribute level, immediate

The results are shown in Table 1. From the table it is clear that the proposed scheme achieves high privacy guarantee and on demand revocation. In comparison with the RNS scheme, attribute authority are independent in RNS and in the proposed scheme attribute authority issue user secret keys collectively. However, the revocation method in the proposed scheme is more efficient in terms of communication overhead. In addition, the proposed framework addresses the access requirements in health record systems by dividing the system into PUD and PSD, which encompasses both personal and professional PHR users. Also the utilization of electrocardiogram transmission improves the efficiency of the system. With the use of developed system, not only people can be monitored from outside of hospitals, but also an early treatment is possible. Location data of the patient obtained from GPRS sent to the related units. Thus, the proposed system makes human's daily life more comfortable.

VI. Conclusion

This paper proposes a novel framework of secure sharing of personal health records in server. In order to fully realize the patient centric concept, patients achieve the complete control of their own privacy through encrypting their PHR files to allow fine grained access. Encryption is done by using ABE method, so that patients can allow access not only by personal users, but also various users from public domains with different roles. Furthermore, MA-ABE scheme is used to manage efficient and on demand user revocation, dynamic policy updates and security. It also addresses the key design issues brought by multiple owners and users and greatly reduces the complexity of key management. The system is enhanced with on track ECG monitoring of out-of-hospital patients through GPRS and thus improves its efficiency.

References

[1]. M. Li, S. Yu, K. Ren, and W. Lou, "Scalable and secure sharing of Personal Health Records in Cloud computing using Attribute based encryption, " in secure comm',2012.
[2]. "The health insurance portability and accountability act." [Online] Availablehttp://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp
[3]. "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.
[4]. K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001.
[5]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Overencryption: management of access control evolution on outsourced data," in VLDB '07, 2007, pp. 123–13
[6]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09: Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp. 103–114.
[7]. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT, pp. 568–588, 2011.
[8]. M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121–130.
[9]. FANG Zu-xiang and LAI Da-kun "Uninterrupted ECG Mobile Monitoring" IEEE 2007 Vol no.9 p.p33-34.