A novel personal health record system for handling emergency situations

P. Thummavet[1], S. Vasupongayya[2]
Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University,
Hat Yai, Songkhla 90112, Thailand
E-mail: 5310120127@email.psu.ac.th[1], vsangsur@coe.psu.ac.th[2]

Abstract—**Personal health record (PHR) becomes a popular research topic nowadays. Many research works have proposed several concepts in managing and organizing a PHR. However, there are several uncertain issues left such as the role of a PHR in emergency situations. In this paper, a solution to handle a PHR information management in emergency situations is proposed. Because a PHR is controlled by its owner, the critical challenge in handling the PHR in emergency situations is how emergency staffs can access PHR information, even when the PHR owner is unable to give his/her consent. The proposed scheme allows each PHR to be classified into several categories. Each category presents a different restriction. And, the emergency staffs can access each category according to the policy defined by the PHR owner. The threshold cryptosystem is adapted in this work to allow the selected set of PHR-owner-delegates to grant permission to the emergency staffs when the PHR owner is unconscious.**

Keywords-personal health record; privacy; security; emergency situation; threshold cryptosystem

I. Introduction

Recently, a personal health record (PHR) becomes a hot issue in researches and adoptions. PHR presents the concept of individual health information sharing that is controlled by its owner [1]. In other words, the owner can selectively share his/her health information to selected users through a PHR system. Typical PHR information includes congenital diseases, medical history, allergy, disease risks, lab results, physicians' recommendations, exercise patterns and results. Thus, information stored in a PHR is usually considered to be highly sensitive [1], [2]. Therefore, a PHR management system must protect the data and allow only authorized users to access the data. Usually, a PHR is protected by encrypting before sharing.

There are a lot of research works regarding the security of PHR [2], [3], [4], [5], [6] and [7]. Many research works propose important and useful concepts of the PHR security. However, there are several uncertain issues still. One of those missing issues is how to manage PHR information in emergency situations. Typically, emergency units do not directly involve with the PHR owner. Thus, these personals are not in the PHR system. Therefore, there is no access right for these groups of people. Thus, the emergency staffs are not able to access a PHR of the patients even in emergency situations, even though these staffs are the first responders who will reach the patients. Therefore, allowing an emergency staff to access information stored in PHRs in emergency situations is essential. Information stored in the patient's PHR may help an emergency staff make better decisions.

In this paper, we propose a novel scheme for handling accesses to PHR information in emergency situations. A critical part of our work is how emergency staffs can access PHR information, even when an owner stays unconscious or inconvenient to give his/her consent. The proposed system allow external units (i.e., the emergency staffs) to access an individual PHR according to the PHR owner's policy. Three levels of confidentiality of PHR information including secure, restricted and exclusive levels are proposed. A PHR owner can define any of the three levels to each PHR. The secure level is defined for freely accessing by the emergency staffs without any consent in emergency situations. The restricted level is considered to be sensitive and the emergency staffs must have an access right to access it. However, the PHR owner may not be able to give his/her consent. Thus, the consent can be granted by at least t out of n trusted users, who are defined by the PHR owner. Novelty, we adopt a threshold cryptosystem [8] to originate an access granting mechanism for the restricted-level information. The threshold cryptosystem is an important key to create the access granting mechanism to emergency staffs, in which an owner can specify pre-determined threshold value (t) to the restricted-level information. Consequently, the threshold cryptosystem allows emergency staffs to access the restricted-level information only if they are granted the permission by at least t (pre-determined threshold) out of n trusted users. The exclusive level is considered to be top secret. That is, the emergency staffs cannot access it even in emergency situations. With our proposed scheme, an owner can share PHR information to emergency staffs but still be able to control privacy and confidentiality of highly sensitive information.

The proposed scheme can be implemented as an add-on to any existing PHR management system in order to support emergency staffs under emergency situations. The remaining of this document is organized as follows. Section 2 describes related work. The traditional personal health record management system is discussed in Section 3. Section 4 presents the proposed scheme. Finally, conclusions are given in Section 5.

This work is supported in part by the National Research University Funding no. MED540548S

II. RELATED WORK

There are a few interesting PHR management systems that have features to handle emergency situations [3], [4], [9], [11], [12].

Weerasinghe and Muttukrishnan [9] proposed a PHR system that can exchange medical information in emergency situations. Medical information is protected by the database-level encryption concept [10]. Therefore, a PHR service provider can be defined to serve medical information to an emergency staff during emergency situations. In their work, a trusted granting server (third party) is used to establish the connection between two unknown parties (i.e., emergency staff and PHR service provider). Therefore, each party can assure that the peer party is genuine. The main drawback of their work is that medical information is encrypted by the database key. The database key may introduce privacy risks of PHR owners because the key can allow multiple accesses without any need to request for an authorization from the PHR owners. Furthermore, the access right is binary. That is, the whole database can be accessed, thus an emergency staff can access any information on the database once he/she has the key.

Huda, Yamada and Sonehara [11] proposed a PHR system that has strong authentication using health smart cards. A PHR owner's smart card keeps a digital pseudonym that is indexing the PHRs stored on a database. In emergency situations, after authentication, an emergency staff can decrypt the digital pseudonym and use it to retrieve the PHR information. They claim that an owner's name (field in a database) is replaced with a pseudonym in order to protect privacy of an owner. Therefore, even if records are exposed to unauthorized parities, the owner's privacy is still preserved from those unauthorized parties. However, the same problem occurs that is the access is still binary. Thus, an emergency staff can access any information even though that information is highly sensitive.

The HCPP (Healthcare system for Patient Privacy) [12] introduced a solution for handling emergency situations with backup mechanisms. The backup mechanisms work by letting an owner defines his/her emergency information. The emergency information is stored at a trusted server controlled by the government offices. In emergency situations, an emergency staff can access the emergency information without compromising the secret information. HCPP allows the owner to control which information can be accessed or cannot be accessed in emergency situations. However, HCPP does not support any information in the case when the physicians need more information other than the defined emergency information. In contrast, the proposed scheme in this work defines three levels of protections. In emergency situations, an emergency staff can access secure-level information immediately but if an emergency staff needs further information beyond the secure level. An emergency staff can request to access the restricted-level information but he must be granted the permission by at least t out of n trusted users, who are defined by the PHR owner.

The break-glass access was proposed by Li, Yu, Zheng, Ren and Lou [3], [4]. Typically, a PHR is encrypted by the key-policy attribute-based encryption (KP-ABE) [13]. KP-ABE enables an owner to specify a set of attributes embedded into an encrypted PHR file. For information selected by an owner to be emergency information, it will be encrypted with a set of desired attributes plus the attribute "emergency". Then, an owner generates the emergency key containing the attribute "emergency" as an access policy. The emergency key is delegated to an emergency department (ED). In emergency situations, an emergency staff authenticates himself to ED, then requests and obtains the emergency key for decrypting the emergency PHR files. Similar to the HCPP, the break-glass access mechanism does not satisfy an emergency staff if he needs further information other than the selected emergency information. Unlike our work, the proposed scheme can satisfy that requirement by the access granting mechanism for the restricted-level information.

III. TRADITIONAL PERSONAL HEALTH RECORD SYSTEM

The most widely used PHR model [2], [5], [6], [7] due to its simplicity, is illustrating in Figure 1. The model consists of three entities: user authority (UA), PHR server and users. According to the model, UA manages all tasks concerning a user in the PHR system, such as certifying users, generating keys and certificates, authenticating users, distributing keys and certificates, and revoking users. The PHR server acts as a warehouse of the PHR in which the owners can share their PHRs to selected users securely. To protect the PHR information, a PHR must be encrypted at a client before uploading to the PHR server. Typically, a PHR contains health information related to an individual but is often accessed by multiple users, such as the owner, family members, physicians, and caregivers. Therefore, the one-to-many encryption scheme is employed by several PHR management systems [2], [3], [4], [5], [6] and [7]. The most common encryption scheme used to protect PHRs [5], [6], [7] is Ciphertext-policy attribute-based encryption (CP-ABE) [14]. According to the CP-ABE, the owner can specify an access policy and embed the policy into the encrypted PHR file. Only the user who has the CP-ABE private key satisfying the required access policy can decrypt the protected PHR file.

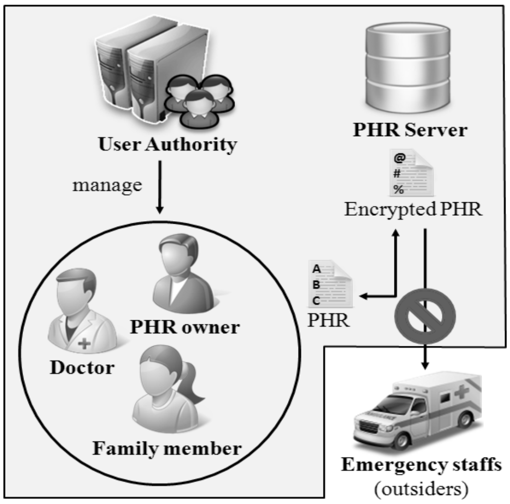

Figure 1. Traditional personal health record system.

Thus, only the users selected by an owner can access information stored in the PHRs. During emergency situations, however, the owner may be unconscious or inconvenient to grant any access right to the emergency staffs, who are typically not in the PHR system [3], [4], [9], [11], [12]. Therefore, in this paper we will improve the PHR system to support emergency staffs in order to access the PHR information under emergency situations. The proposed scheme can improve the missing important requirement of traditional PHR systems.

IV. Proposed Scheme

In this section, the proposed improvement scheme to the referred traditional PHR system in order to support accessing information stored in PHRs during emergency situations is described. The primary concern of our work is similar to the traditional system that is the privacy and confidentiality of individual information must be protected. Therefore, the emergency staffs referred in this paper are assumed to be trustworthy. In addition, the emergency units, who will certify the emergency staffs, are assumed to be trusted by the PHR system.

In order to protect the privacy and confidentiality of the PHR information, the proposed scheme defines three levels of confidentiality of PHR information including **secure**, **restricted** and **exclusive** levels. The secure level refers to the information that must be protected during normal situations. However, the emergency staffs can access the secure-level information immediately during emergency situations. The restricted level also refers to the information that must be protected in normal situations. However, the emergency staffs can access it only if they are granted the permission by at least t out of n trusted users, who are defined by the PHR owner. The exclusive level refers to the information that cannot be accessed by emergency staffs even in emergency situations. In the proposed scheme, an owner can define the confidentiality level to his/her PHR. Thus, the PHR owner has a solution to define a fine-grained access control on his/her PHR.

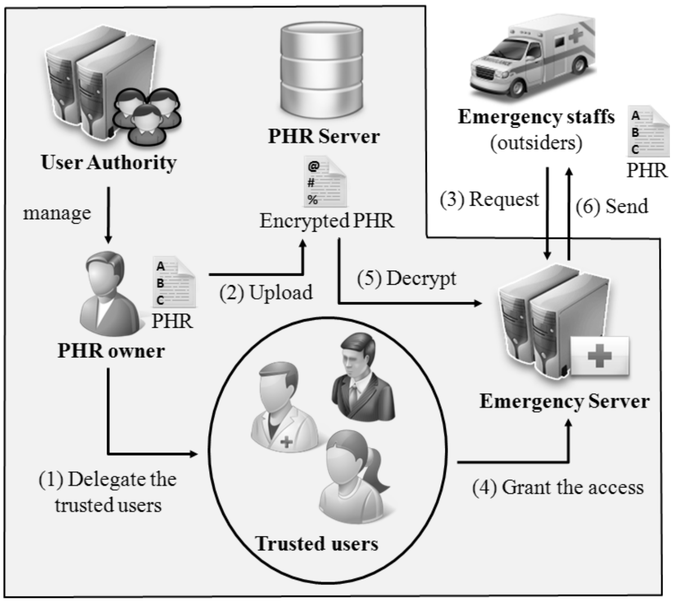

Figure 2. The proposed personal health record system.

The proposed scheme is presented in Figure 2. An emergency server (EmS) is added to the original model (Figure 1) to handle an emergency situation. EmS acts as a service provider that serves emergency staffs (the outsiders) if emergency situations occur. In other words, emergency staffs can request an access to the information stored in the PHR system through the EmS. EmS will strictly perform actions on PHRs according to their confidentiality level defined by the PHR owner. That is, emergency staffs can access information only if they have an access right on that information. Note that, EmS should be a high computational processing unit and have a large network bandwidth in order to support any disaster situation in which a huge number of requests are generated, such as during tsunami, earth quake or great flood.

A. Delegating Trusted Users

In the proposed scheme, an owner can define a set of trusted users (denoted as 1 in Figure 2) to make a decision on granting access rights on the restricted-level information on behalf of the PHR owner during emergency situations. A contact list of trusted users is securely recorded into an EmS database and will be used if emergency staffs request to access any restricted-level information stored in the PHR system. When the emergency staffs request to access the restricted-level information (denoted as 3 in Figure 2), EmS will broadcast the request message to all selected trusted users. If any trusted user approves the request, he/she sends an approval message to EmS (denoted as 4 in Figure 2). If approval messages collected by the EmS are more than or equal to the pre-determined threshold (t) defined by the PHR owner, the EmS can decrypt the protected PHR (denoted as 5 in Figure 2) and the emergency staffs can access the information (denoted as 6 in Figure 2).

B. Preparing PHRs for Emergency Situations

Since information stored in a PHR is considered to be sensitive, a PHR will be encrypted by the CP-ABE at a client before uploading to the PHR server (denoted as 2 in Figure 2). During encryption, the PHR owner can define a confidentiality level (i.e., secure, restricted or exclusive level) to the particular PHR. The following sections describe how the proposed scheme prepares the PHR system for emergency situations.

1) Secure-level information: According to the definition, the information stored in a PHR defined at this level must be protected during normal situations. However, the emergency staffs can access secure-level PHR information immediately. That is, the EmS can decrypt a secure-level PHR instantly and send the decrypted information to the emergency staffs during emergency situations. In other words, a secure-level PHR must be decrypted by the EmS key, namely the emergency key. To do so, an access policy specified by the owner must be modified to support the decryption using the EmS key. The sequence of transactions is shown below.

a) An owner specifies the access policy for encrypting his/her PHR.

b) The PHR client module adds the identity attribute of the EmS key to the access policy.

c) The PHR client module encrypts the PHR using the CP-ABE with the access policy as a parameter.

d) The PHR client module uploads the resulting encrypted PHR to the PHR server through a secure channel.

e) The PHR client module inserts a metadata for this PHR into the EmS database and sets the PHR to the secure-level information.

2) Restricted-level information: According to the definition, the information stored in a PHR defined at this level must be protected during normal situations. The emergency staffs can access the restricted-level PHR information if and only if they are granted the permission by at least t out of n trusted users, pre-selected by the PHR owner. That is, when the emergency staffs request to access a PHR, the EmS will broadcast the request message to all trusted users pre-defined by the PHR owner. If there are at least t approvals, the EmS can derypt the PHR and send the decrypted information to the emergency staffs. The pre-determined threshold (t) is also pre-defined by the PHR owner during the PHR encryption. Thus, the threshold cryptosystem idea is adapted in this work in order to handle such situations.

Typically, a PHR is encrypted using the CP-ABE before uploading to the PHR server. However, the access policy, which is embedded into the resulting encrypted PHR file, must be modified. By adding the identity attribute of the unique emergency key, which is generated to be a key for this particular PHR, the resulting encrypted PHR file can be decrypted by the unique emergency key as well. However, this unique emergency key is also encrypted using the threshold cryptosystem. Once the PHR owner selects a set of trusted users, the PHR system will assign a secret key for each of these trusted users. The secret key is a random string. Each secret key is encrypted with the associated trusted user's public key. Thus, only the pre-defined users can decrypt the secret keys. The encrypted unique emergency key and the encrypted secret key of each trusted user are then uploaded to the EmS database. The encrypted restricted-level PHR is however uploaded to the PHR server. The sequence of transactions is shown below.

a) An owner specifies the access policy for encrypting his/her PHR.

b) The PHR client module contacts the user authority (UA) in order to generate the secret keys and the unique emergency key.

c) The UA encrypts the unique emergency key by the threshold cryptosystem with a list of secret keys and the pre-determined threshold as parameters. Then, the UA maps each secret key to each trusted user and encrypts each secret key with the corresponding trusted user's public key.

d) The UA sends the encrypted unique emergency key and the encrypted secret keys to the PHR client module through a secure channel.

e) The PHR client module adds the identity attribute of the unique emergency key to the access policy.

f) The PHR client module encrypts the PHR using the CP-ABE with the access policy as a parameter.

g) The PHR client module uploads the resulting encrypted PHR to the PHR server through a secure channel.

h) The PHR client module uploads the encrypted unique emergency key and a set of encrypted secret keys to the EmS database through a secure channel.

i) The PHR client module inserts a metadata for this PHR into the EmS database and sets the PHR to the restricted-level information.

3) Exclusive-level information: According to the definition, the information stored in a PHR defined at this level is not accessible by emergency staffs even in emergency situations. Therefore, the EmS cannot decrypt this kind of PHR. Thus, the PHR client module will encrypt a PHR without the need to add any identity attribute of the emergency keys. The sequence of transactions is shown below.

a) An owner specifies the access policy for encrypting his/her PHR.

b) The PHR client module encrypts the PHR using the CP-ABE with the access policy as a parameter.

c) The PHR client module uploads the resulting encrypted PHR to the PHR server through a secure channel.

C. Accessing PHR Information by Emergency Staffs

Under the proposed scheme, the emergency staffs can access information stored in the PHR system through the EmS. Two levels of PHR confidentiality are defined for emergency staffs including secure and restricted levels. If the secure-level information is requested, the emergency staffs can access it instantly. However, if the restricted-level information is requested, the emergency staffs must be granted an access by a set of trusted users pre-selected by the PHR owner. At least t out of n pre-selected trusted users must approve the access right.

The tasks of authenticating the emergency staffs, however, are left for the emergency units that are trusted by the PHR system. Typically, an emergency unit issues some identity information (such as certificate or token) to its emergency staffs. When an emergency staff requests to access PHR information, the EmS will verify the requestor by using such information. Thus, the proposed system does not restrict any authentication protocol for verifying the users. That is, the authentication protocol of the proposed scheme can be applied with any protocol, such as the secure socket layer protocol [15], the challenge and response protocol [11], or the token-based protocol [9]. In addition, the EmS should have a transaction log that records all transactions. This way, the PHR owners can trace all accesses to their PHR information. The following paragraphs describe how emergency staffs can access the PHR information during emergency situations.

1) Secure-level information: To access the secure-level information stored in a requested PHR, an emergency staff sends a request message to the EmS (denoted as 3 in Figure 2).

Then, the EmS and an emergency staff authentication process occurs. Once, the authentication process succeeds, the EmS downloads the requested encrypted PHR from the PHR server. Then, the EmS decrypts the encrypted PHR with its emergency key (denoted as 5 in Figure 2). Finally, the EmS sends the requested PHR information to the emergency staff through a secure channel (denoted as 6 in Figure 2). More concretely, Figure 3 illustrates the sequence of actions occuring during the secure-level information accessing process.

2) Restricted-level information: To access the restricted-level information stored in a requested PHR, an emergency staff sends a request message to the EmS (denoted as 3 in Figure 2). Then, the authentication process between the EmS and the emergency staff occurs. Once the authentication succeeds, the EmS broadcasts the request message along with the encrypted secret key to each corresponding pre-selected trusted user. If a trusted user approves the request, he/she decrypts the encrypted secret key with his/her private key and sends the secret key to the EmS through a secure channel (denoted as 4 in Figure 2). If the number of approvals is more than or equal to the pre-determined threshold (variable t), the EmS can decrypt the encrypted unique emergency key, which is encrypted using the threshold cryptosystem. Then, the EmS downloads the requested encrypted PHR from the PHR server and uses the unique emergency key to decrypt the encrypted PHR (denoted as 5 in Figure 2). Finally, the requested PHR information is sent to the emergency staff through a secure channel (denoted as 6 in Figure 2). More concretely, the process of accessing the restricted-level information is shown in Figure 4.

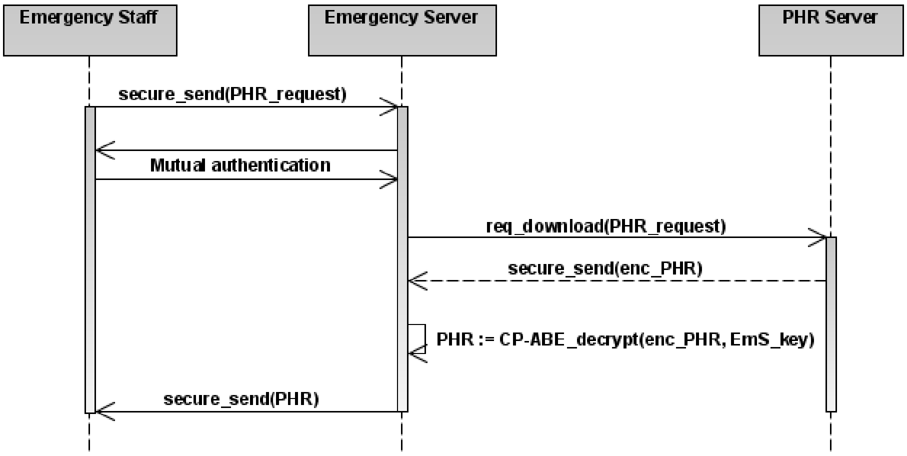

Figure 3. The secure-level PHR information accessing sequence.

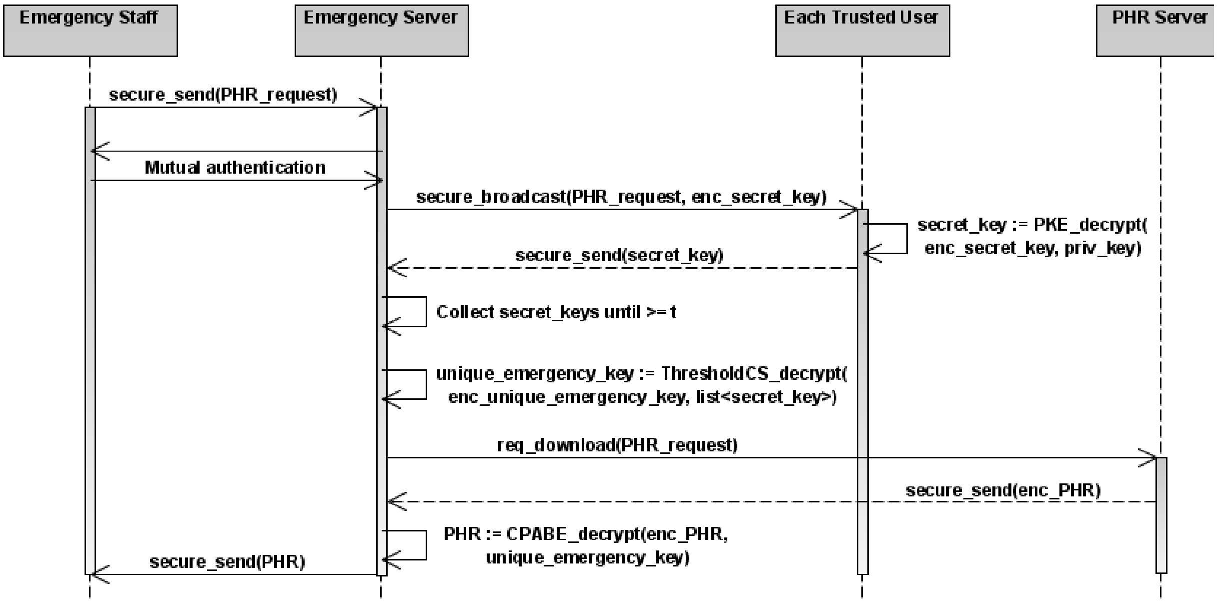
Emergency Staff
Emergency Server
Each Trusted User
PHR Server
secure_send(PHR_request)
Mutual authentication
secure_broadcast(PHR_request, enc_secret_key)
secret_key := PKE_decrypt(
enc_secret_key, priv_key)
secure_send(secret_key)
Collect secret_keys until >= t
unique_emergency_key := ThresholdCS_decrypt(
enc_unique_emergency_key, list<secret_key>)
req_download(PHR_request)
secure_send(enc_PHR)
PHR := CPABE_decrypt(enc_PHR,
unique_emergency_key)
secure_send(PHR)

Figure 4. The restricted-level PHR information accessing sequence.

V. Conclusions

A scheme for managing the PHR information during emergency situations is proposed in this paper. Because the PHR information is usually sensitive, the critical challenge of this work is to manage the PHR access for emergency staffs when the PHR owner is not able to grant his/her consent. Under the proposed scheme, the PHR owner is allowed to define a fine grain access control over his/her PHR information during emergency situations. Three levels of confidentiality including secure, restricted and exclusive are defined. The PHR owner can define one of the three levels to his/her PHR information. The secure-level PHR information is considered open to emergency staffs during the emergency situations. Meanwhile, the restricted-level PHR information can be opened to emergency staffs if and only if there are enough approvals from the pre-selected trusted users. The exclusive-level PHR information, however, is not opened to the emergency staffs.

Thus, the secure-level and restricted-level information enable the owner to specify fine-grained access control on his/her information to emergency staffs. Furthermore, if the owner does not agree to give any access right on any of his/her PHR information, he/she can define the information as exclusive-level PHR information. All access controls are achieved through the use of an additional emergency management server. The emergency management server acts as a connection between the emergency unit staffs and the traditional PHR management system. The emergency units must have a method to authenticate their emergency staffs. Thus, the tasks of authenticating the emergency staffs are done according to the method used by the emergency units. Furthermore, the emergency units in this work are assumed to be trustworthy.

The contribution of this work is to enable the emergency staffs to gain an access to the PHR management system according to the policy defined by the PHR owner. Under the proposed system, the PHR owner can specify a fine grain access control policy during emergency situations. To the best of our knowledge, existing methods still do not allow fine grain access control like what has been proposed in this paper.

References

[1] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, “Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption,” Journal of the American Medical Informatics Association, JAMIA2006., in press.

[2] K. Garson, and C. Adams, “Security and privacy system architecture for an e-hospital environment,” Identity and trust on the Internet, IDtrust2008., in press.

[3] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings,” Security and Privacy in Communication Networks, SecureComm2010., in press.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” Parallel and Distributed Systems, PDS2013., in press.

[5] J. Huang, M. Sharaf, and C. T. Huang, “A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud,” Parallel Processing Workshops, ICPPW2012., in press.

[6] L. Ibraimi, M. Asim, and M. Petkovic, “Secure management of personal health records by applying attribute-based encryption,” Wearable Micro and Nano Technologies for Personalized Health, pHealth2009., in press.

[7] C. Wang, X. Liu, and W. Li, “Implementing a personal health record cloud platform using ciphertext-policy attribute-based encryption,” Intelligent Networking and Collaborative Systems, INCoS2012., in press.

[8] T. P. Pedersen, “A threshold cryptosystem without a trusted party,” Advances in Cryptology. EUROCRYPT1991., in press.

[9] D. Weerasinghe, and M. Rajarajan, “Secure trust delegation for sharing patient medical records in a mobile environment,” Wireless Communications, Networking and Mobile Computing, WiCOM2011., in press.

[10] Y. Ding, and K. Klein, “Model-driven application-level encryption for the privacy of e-health data,” Availability, Reliability, and Security, ARES2010., in press.

[11] M. N. Huda, S. Yamada, and N. Sonehara, “Privacy-aware access to patient-controlled personal health records in emergency situations,” Pervasive Computing Technologies for Healthcare, PervasiveHealth2009., in press.

[12] J. Sun, X. Zhu, C. Zhang, and Y. Fang, “HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare,” Distributed Computing Systems, ICDCS2011., in press.

[13] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” Computer and Communications Security, CCS2006., in press.

[14] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” Security and Privacy, SP2007., in press.

[15] J. Viega, M. Messier, and P. Chandra, Network Security with OpenSSL: Cryptography for Secure Communications, O'Reilly Media, 2002, pp.93-142.