Maejo International Journal of Science and Technology

Technical Note

Privacy-preserving emergency access control for personal health records

Phuwanai Thummavet and Sangsuree Vasupongayya[*]

Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University,
P.O. Box 2 Kohong, Hatyai, Songkhla, 90112, Thailand

* Corresponding author, e-mail: vsangsur@coe.psu.ac.th

Abstract: Recently, a flexible scheme for handling personal health records (PHRs) in emergency situations has been proposed. Under such a scheme, each PHR is classified as secure, restricted, or exclusive information. Secure PHRs are immediately available to the emergency response unit (ERU) staff. Restricted PHRs require additional approvals from a set of authorised people who are pre-selected by the PHR owner. Exclusive PHRs are only accessible by the owner. Previous work assumed that all ERU staff is trustworthy. To be practical, this work eliminates such an assumption. Several mechanisms are applied to ensure the usability and security of the newly proposed scheme. For example, an access-request authentication mechanism is applied to enhance the trustworthiness of the requests that are invoked by the ERU staff. Moreover, a transaction auditing mechanism is applied to provide a non-repudiation feature. This paper discusses the usability and security issues of the proposed scheme in practice and suggests how to classify a PHR considering the above-mentioned privacy levels.

 Keywords: personal health record, privacy, security, ciphertext-policy attribute-based encryption, threshold cryptosystem

INTRODUCTION

Today, people are more aware of information concerning their health because of the rising cost of healthcare. Recently, alternative medicines such as dietary supplements and herbal products have gained popularity [1]. In addition, personal health record (PHR) system is emerging as a preventive healthcare method [2]. The PHR system allows an individual to collect, store, analyse, and share his/her personal health data with a group of trusted people such as family members, family doctors and caretakers [3]. The PHR system usually contains highly sensitive information

[4]; it can include information related to the PHR owner's health such as his/her mental health, disease risks and laboratory test results. Therefore, the PHR system must ensure the security and privacy of the PHR owner's information, and the actual PHRs must be protected from an unauthorised access or modification. Moreover, the PHR owner must be able to manage and control all authorised access to his/her PHRs. To achieve such features, the PHR system should allow the PHR owner to define an access control policy on his/her PHRs, which must be enforced by the PHR system. Thus, an individual can access a PHR if and only if that individual has been granted the authority by the PHR owner via an access control policy. For example, John can grant access to his family doctor, Jason, by defining a policy such as "Jason, who is a doctor, can access my records." Hence the PHR system will allow only Jason, who is a doctor, to access John's PHRs.

An interesting PHR management issue arises during an emergency [5, 6]. Generally, an emergency response unit (ERU) staff member is the first care provider to reach the victim. Providing correct and useful health information (e.g. personal diseases) about the victim in the emergency situation can increase the opportunity to provide proper treatment to save the victim's life or alleviate his/her critical conditions. Therefore, it is vital to allow the ERU staff to access the necessary PHR information of the victim in an emergency situation [7]. According to the above example, John can allow Dr. Jason to access his PHRs because John knows Dr. Jason. In an emergency, John may not know any ERU staff. Thus, John will not be able to define a policy to allow a specific ERU staff member to access his PHRs. During an emergency situation, John may be unconscious and may not be able to grant any permission to the ERU staff at the scene. Moreover, ERU staff should not access John's PHRs unless they are necessary to save his life. Thus, the question is how to allow ERU staff to access the victim's PHRs during an emergency situation.

A scheme to manage and handle PHRs during an emergency situation has been proposed in our previous work [8], which allows different access restrictions. Under such a scheme, each PHR is classified into secure, restricted, and exclusive categories. Different categories provide different access permissions to ERU staff for the victim's PHRs. Secure PHRs are freely available to ERU staff during an emergency situation. Restricted PHRs are accessible to an ERU staff member if and only if he/she was granted access permission by at least t out of n trusted people who are pre-selected by the PHR owner, where t is an acceptable threshold, pre-defined by the PHR owner and n is the total number of trusted people on the PHR owner's list. Exclusive PHRs are not accessible even during an emergency situation. With the proposed scheme, the PHR owners can selectively share their PHRs with the ERU staff while additional data can be requested if needed.

This work extends the previous scheme to cover external ERUs that were not included in the original design [8]. The ERU staff authentication process was not considered in the original design because the ERU staff was assumed to be trustworthy and part of the PHR system. However, in the real world ERU staff can be from various external sources such as public organisations, medical care institutions, private organisations, non-profit organisations or a group of volunteers. Therefore, the ERU staff must be verified by their authorised commander/manager. To guarantee the reliability of the verification process, an access request authentication (ARA) mechanism is proposed in this work as an extension of the previous scheme. Hence the PHR access request from any ERU staff can be performed if and only if the staff member is granted access permission by his/her authorised ERU commander/manager. In addition, a transaction auditing mechanism is used in this study to provide a non-repudiation feature. Furthermore, the security of all connections in the proposed scheme is provided by means of secure sockets layer protocols and secure shell protocols.

RELATED WORK

A database-level encryption was employed by Weerasinghe and Muttukrishnan [9] to provide an information exchange scheme between the ERU staff and the PHR service providers via a trusted third party. Under such a scheme, the actual PHRs are encrypted and stored by a PHR service provider. During emergency situations, the PHR service provider delivers the requested PHR to the ERU staff on behalf of the PHR owner. The authentication of each party should be done by the trusted third party. However, the use of a database key becomes an issue because such a technique can introduce a privacy risk for the PHR owner [10]. To access the information, the ERU staff has access to the key through which multiple access can be performed. Typically, the access permission under such a scheme is binary and the ERU staff can access the entire database. In other words, the ERU staff can access all records stored in a particular database even though some records may not be related to their tasks.

To solve the privacy concern of the database-level encryption technique, a digital pseudonym was introduced by Huda et al [11]. The pseudonym indexes the PHRs for each PHR owner, whose name (i.e. a field in the database) is replaced by a random pseudonym. Then the pseudonym is encrypted and stored on the PHR owner's health smart card. The ERU staff uses the pseudonym to retrieve the victim's PHRs during an emergency situation. Using the pseudonym, even though the database records are exposed to unauthorised users, the PHR owner's privacy is still preserved. However, the scope of the information accessed by the ERU staff cannot be limited because the ERU staff can access all records indexed by a particular pseudonym.

A backup mechanism at a trust centre for the PHR owner was proposed by the healthcare system for patient privacy [12]. Under such a scheme, the PHR owner can define the information that will be available during emergency situations and selects his/her PHRs to be stored at a trusted server. The information stored at the trust centre is freely available to the ERU staff during an emergency situation. Hence the privacy of the PHR owner and the secrecy of the PHR can be preserved. However, only static information pre-selected by the PHR owner is available. In our proposed scheme both static and additional information is available to the ERU staff. The static pre-selected information is the secure PHRs and the additional information is the restricted PHRs, which are available upon request.

A key-policy attribute-based encryption (KP-ABE) [13] was employed in the break-glass access [14, 15] to protect the PHR information. The KP-ABE enables a PHR owner to specify a set of attributes embedded in the encrypted PHR. The PHR owner selects a set of PHRs to be freely available to the ERU staff during emergency situations. Then a special 'emergency' attribute is added during the PHR encryption process. A set of PHRs can only be decrypted by a key that contains the 'emergency' attribute and is distributed to the ERUs during an emergency situation. However, only static pre-selected information is available.

The KP-ABE was also employed by Huang et al. [6] to offer the PHR information according to the severity level of the situation. The PHR owner can assign any of the three severity levels (mild, moderate and severe) to each PHR. Then each PHR is encrypted using the KP-ABE technique with a set of owner-desired attributes and the severity level. The KP-ABE private keys that are based on different severity levels can access the PHR information with different scopes. Under such a scheme, the availability of the pre-defined information is an issue. For example, if the ERU staff is allowed to access mild-level and moderate-level information, then the information is always available even when it is not required.

OUR PROPOSED PRIVACY-PRESERVING EMERGENCY ACCESS CONTROL SCHEME

Our proposed privacy-preserving emergency access control scheme for PHRs is illustrated in Figure 1. The scheme consists of five modules and three players. The modules comprises the user authority (UA), the emergency server (EmS), the PHR server, the audit server and the emergency authority (EA). The players include the PHR owner, the PHR trusted users and the ERU staff.
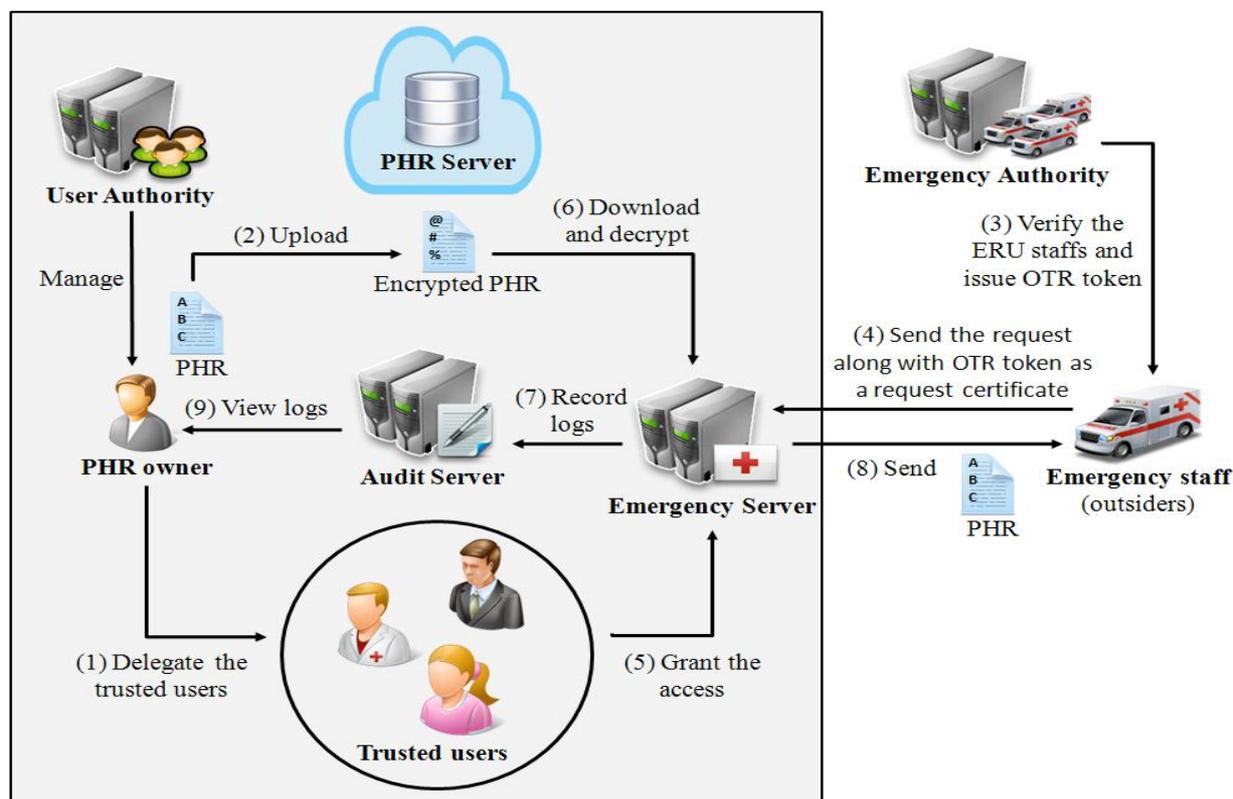

Figure 1. Proposed privacy-preserving emergency access control scheme

The UA is responsible for performing all PHR user management tasks such as creating a user, generating a user key, distributing the user key and revoking the user. The PHR server is an actual PHR storage, which can be internal or public storage. The PHRs are encrypted and uploaded to the storage. The EmS handles all tasks related to an emergency situation. These three modules were presented in the original design [8]. The next two modules are added in this work. The audit server records all activities performed by the ERU staff during emergency situations and produces reports for the PHR owner. The EA is responsible for managing tasks related to the ERU staff, such as verifying ERU staff identity, authorising ERU staff, revoking ERU staff access and generating a one-time request (OTR) token for ERU staff. The EA can be either distributed or centralised as long as it is registered with the proposed scheme.

The PHR owners can manage and track all activities conducted on their PHRs. Trusted users can be partially granted restricted access on behalf of the PHR owner during emergency situations. When the total number of approvals received from the pre-selected trusted users is equal to or greater than the pre-defined threshold, restricted PHR access permission is granted. The ERU staff must be verified and authorised by their corresponding EA.

The ARA mechanism ensures that only authorised ERU staff is allowed to access the PHR system. Each PHR access request invoked by the ERU staff must be verified by its commander/ manager (denoted as EA in Figure 1). Once the ERU staff member is verified, the OTR token, which is a certificate with a specific expiration time, is generated. The request with a valid OTR token is processed by the EmS. The ERU staff cannot reuse the token once it is expired. To expedite this process, the ERU staff can be verified and issued with the OTR token in an emergency vehicle before they arrive at the emergency location. Hence the delay time to access any secure PHR is eliminated because the secure PHRs can be immediately accessed once the valid OTR token is presented. In addition, a transaction auditing mechanism is employed to guarantee a non-repudiation feature of all access conducted by the ERU staff.

Under our proposed scheme, the PHRs are encrypted at the data origin using the ciphertext-policy attribute-based encryption (CP-ABE) technique [16]. Then the encrypted PHR is uploaded to the PHR server (denoted as (2) in Figure 1). Using the CP-ABE scheme, the access policy of each PHR is embedded during the PHR encryption process. The policy is defined by the PHR owner. Only the user who has the CP-ABE private key that satisfies the access policy can decrypt the encrypted PHR. In addition, the secure sockets layer protocol and the secure shell protocol are employed to provide a secure communication among the modules and players under the proposed scheme. The information collected by the network traffic eavesdropping technique remains protected. In the following section the assignment of a privacy level to each PHR is presented. Then the PHR pre-processing and accessing methods are described.

Defining Privacy Level

This section provides a guideline for the PHR owners in order to classify their PHRs into one of the three privacy levels: secure, restricted and exclusive. The guideline is created according to the sensitivity of the PHR information. Typically, health related information of an individual stored in a PHR system has different sensitivity levels. For example, some information such as mental health, domestic abuse/violence, drug abuse, disorders and disabilities is considered to be sensitive for some people. A person usually does not disclose such information to others. Such information can result in disgrace or even unfair job opportunities to its owner [4, 5]. However, other information such as congenital diseases, allergies and disease risks can help the ERU staff make a better decision in treating the victim during emergency situations [7].

The secure PHRs are available to the ERU staff during emergency situations. Therefore, the basic information of a person's health that is necessary to treat the person must be provided. Some people are allergic to simple medicine such as Paracetamol. Such information is important during a life-threatening condition. Thus, a list of information such as congenital diseases, allergies and disease risks is suggested to be under the secure-level category [17]. In addition, a list of emergency contact people for the victim is classified under this category so the people who know the victim can be informed about the situation.

The ERU staff is allowed to access the restricted-level information if an access permission is granted by a certain number of the victim's delegates. Unlike the secure-level information, the restricted-level information will not be available immediately. Thus, the information under this category can only be used by the physicians that are away from the emergency scene, in a fully equipped emergency vehicle or an intensive care unit at a hospital. This set of information should include the person's medical history, laboratory test results, physicians' recommendations, his/her

physicians' contact information, and some relevant health-monitoring data. Such information will help physicians make a better judgment on the next actions.

Finally, the exclusive-level information is considered to be highly sensitive according to the PHR owner judgment. Usually, this set of information includes mental health, domestic abuse/violence, drug abuse, disorders and disabilities [4, 5]. Note that this guideline is provided as a suggestion and the proposed scheme is not limited to it.

PHR Pre-processing

The proposed scheme uses the EmS to perform all PHR retrieving and decrypting tasks during emergency situations. The EmS attribute must be defined in the access policy of the secure and restricted PHRs. The exclusive PHR access policy does not include any attribute of the EmS. As a result, the ERU staff is not allowed to access exclusive PHRs even during emergency situations while the secure PHR is accessible by the authorised ERU staff during emergency situations. To assign a secure PHR, the EmS attribute must be added to the access policy of that particular PHR. Then the PHR is encrypted using the CP-ABE with a defined access policy and the encrypted PHR is securely uploaded to the PHR server. By adding the EmS attribute to the access policy, the EmS is able to decrypt a particular PHR. During an emergency situation, the authorised ERU staff can access the secure PHRs instantly via the EmS.

The restricted PHR is accessible by the authorised ERU staff if and only if they are granted an access permission by at least t (pre-determined threshold) out of n trusted users who are pre-selected by the PHR owner. To assign a restricted PHR, the PHR owner must first select a set of trusted users (denoted as (1) in Figure 1). These trusted users are asked to make a decision to grant access permission on any restricted PHR on behalf of the PHR owner. A restricted emergency key (REK) attribute is added to the access policy of that particular PHR. Then the PHR is encrypted using the CP-ABE with defined access policy. Next, a set of random secret keys associated with the number of trusted users are generated. The REK attribute is encrypted using threshold cryptosystem [18] with a set of random secret keys and a pre-determined threshold (t) as encryption parameters. A random secret key is assigned to each trusted user. Each secret key is encrypted using a corresponding trusted user's public key. The encrypted PHR is securely uploaded to the PHR server while the encrypted REK attribute and the set of encrypted secret keys are securely uploaded to the EmS. Thus, the EmS can decrypt any restricted PHR if and only if at least t trusted users provide their approval. Because each secret key is encrypted with a trusted user's public key, only the trusted user's private key can decrypt the secret key. With the threshold cryptosystem, the REK attribute can be decrypted if at least t secret keys are provided. Using the REK attribute, the EmS can decrypt the restricted PHRs.

PHR Accessing

In this section both secure and restricted PHR accessing sequences are explained. Figure 2 and Figure 3 show sequences of transactions occurring when accessing secure PHRs and restricted PHRs respectively. To enhance the trustworthiness of a request invoked by the ERU staff, the ARA mechanism guarantees that each request must be verified by his/her EA (steps 1–4 in Figure 2 and Figure 3). The OTR token ensures that the ERU staff is verified by his/her EA (step 3 in Figure 2 and Figure 3). The verification process can be expedited by issuing an OTR token to the ERU staff once the emergency case is assigned. Because the OTR token is a certificate with a specific expiration time, the token cannot be reused when its lifetime expires. Therefore, this mechanism

assures that only authorised ERU staff can access the PHRs. All requests and transactions are recorded. Figure 4 shows the transactions collected by the auditing system using our prototype software.
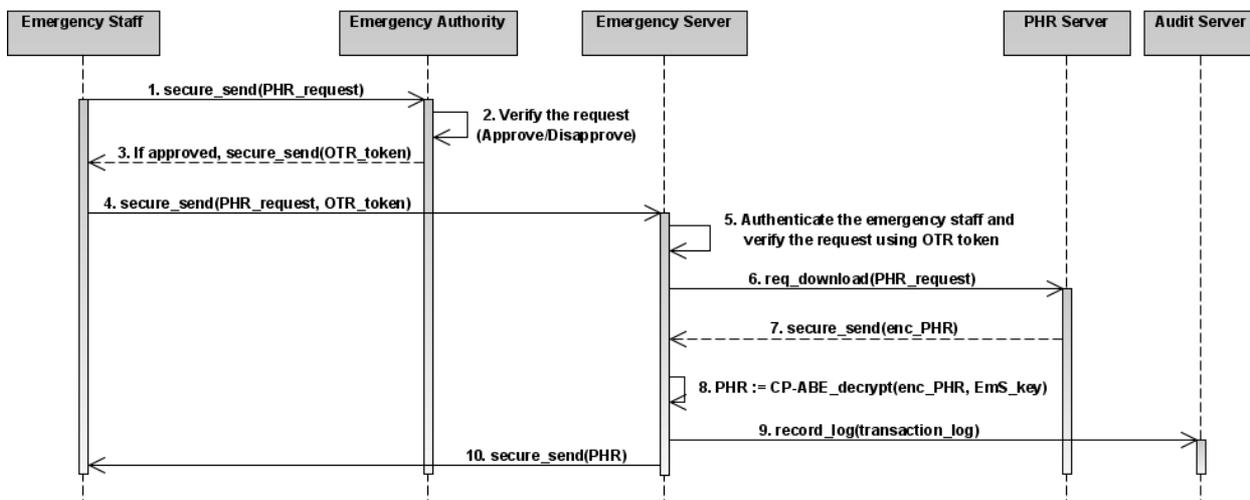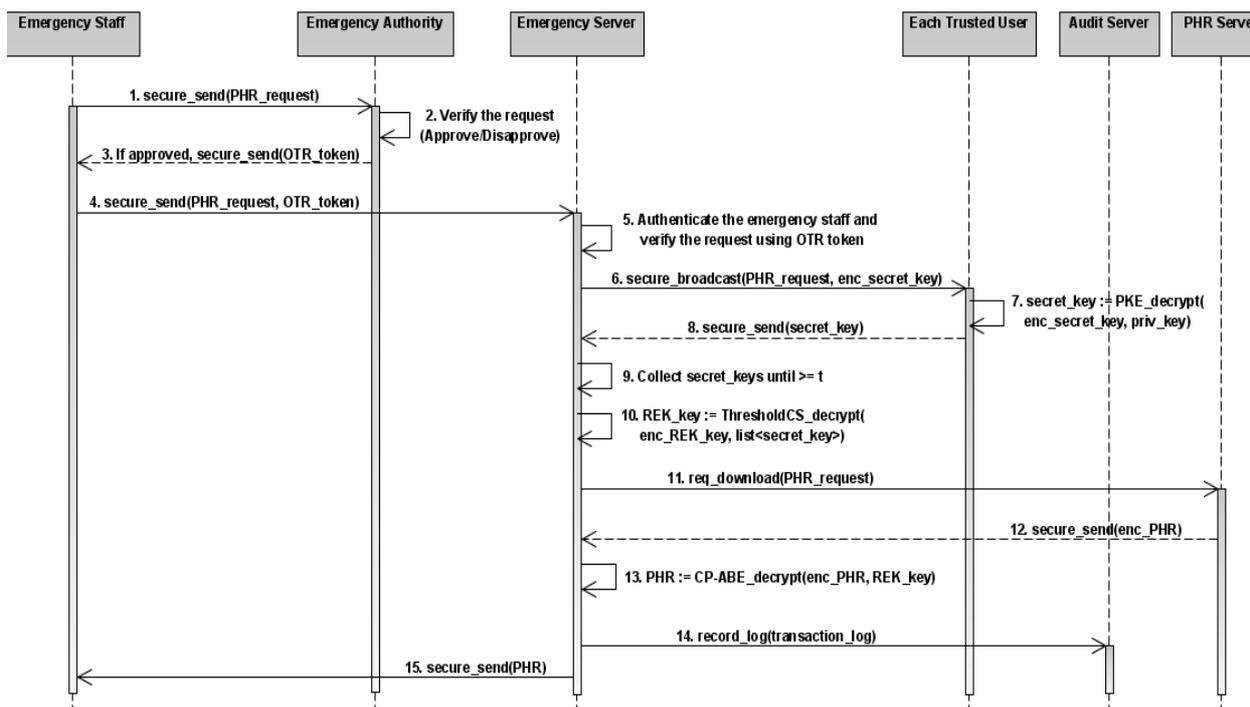

Figure 2. Secure PHR access sequences.

Figure 3. Restricted PHR access sequences

Transaction Auditing

Transaction log type: Event log

☑ Audit all transactions

Event Logs

Date/time	Actor	Event	Object(user)	Object	Actor's IP addr...
2014-01-15 23:54:40	Personal.Alice	Actor uploaded the PHR	Personal.Alice	mental health results an...	127.0.0.1
2014-01-15 23:55:50	Personal.Alice	Actor encrypted the PHR	Personal.Alice	medical history, diagnosi...	127.0.0.1
2014-01-15 23:56:15	Personal.Alice	Actor uploaded the PHR	Personal.Alice	medical history, diagnosi...	127.0.0.1
2014-01-15 23:56:57	Personal.Alice	Actor encrypted the PHR	Personal.Alice	allergies, disease risks a...	127.0.0.1
2014-01-15 23:56:58	Personal.Alice	Actor uploaded the PHR	Personal.Alice	allergies, disease risks a...	127.0.0.1
2014-01-16 00:36:51	Emergency.Mike	Actor downloaded the secure-level ...	Personal.Alice	allergies, disease risks a...	127.0.0.1
2014-01-16 00:41:33	Emergency.Mike	Actor requested an access to the r...	Personal.Alice	medical history, diagnosi...	127.0.0.1
2014-01-16 01:00:08	Personal.John	Actor approved the access request...	Personal.Alice	medical history, diagnosi...	127.0.0.1
2014-01-16 01:02:07	Healthcare.Bob	Actor approved the access request...	Personal.Alice	medical history, diagnosi...	127.0.0.1
2014-01-16 01:14:53	Emergency.Mike	Actor downloaded the restricted-lev...	Personal.Alice	medical history, diagnosi...	127.0.0.1
2014-01-16 01:29:41	Personal.Alice	Actor audited his/her event log	-	-	127.0.0.1

Close

Figure 4. List of transactions collected by the audit server

To access secure PHRs, the ERU staff must send a PHR access request along with the OTR token to the EmS (step 4 in Figure 2). The OTR token is sent to the ERU staff if he/she is verified by his/her corresponding EA. Once the EmS successfully verifies the OTR token, the requested secure PHRs are downloaded and decrypted using the EmS attribute (steps 5–8 in Figure 2). Then the EmS stores the transaction information on the audit server (step 9 in Figure 2) and securely sends the requested secure PHRs to the ERU staff (step 10 in Figure 2).

To access restricted PHRs, the ERU staff must send a PHR access request along with the OTR token to the EmS (step 4 in Figure 3). The OTR token is sent to the ERU staff if he/she is verified by his/her corresponding EA. Once the EmS successfully verifies the OTR token (step 5 in Figure 3), the EmS securely broadcasts the request message to each corresponding trusted user for approval (step 6 in Figure 3). If the trusted user approves the request, the corresponding encrypted random secret key will be decrypted by the trusted user's private key (step 7 in Figure 3). The random secret key is sent to the EmS through a secure channel (step 8 in Figure 3). If the total number of random secret keys collected by the EmS is equal to the pre-determined threshold (t), the EmS decrypts the encrypted REK attribute value using the threshold cryptosystem (steps 9-10 in Figure 3). Next, the EmS downloads the requested PHRs from the PHR server and uses the REK attribute to decrypt the PHRs (steps 11-13 in Figure 3). Finally, the ERU staff receives the requested PHRs from the EmS via a secure channel (step 15 in Figure 3). In addition, the EmS records a transaction log on the audit server (step 14 in Figure 3).

USABILITY AND SECURITY DISCUSSIONS

Usability Issues

Figure 5 shows a typical flow of events during an emergency situation. First, an emergency situation occurs. Second, the call is made to the emergency hotline centre. Third, the emergency location and victim's current conditions are provided to the assigned ERU staff. Fourth, the ERU staff reach the victim. Fifth, the victim is transferred to a hospital or a medical facility. The commonly accepted standard response time from the first call (step 2 in Figure 5) until the ERU staff reach the victim (step 4 in Figure 5) is 8 minutes [19]. This section will cover only secure and restricted PHRs because the proposed scheme allows the ERU staff to access only these types of PHRs.
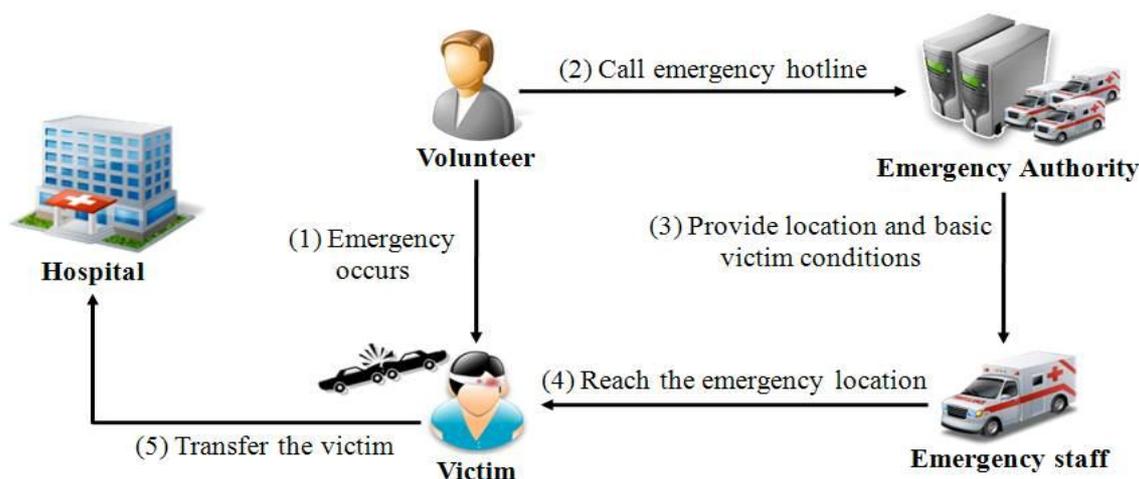
Figure 5. Typical flow of events during an emergency situation

According to the secure PHR access sequences shown in Figure 2, the total processing time to retrieve the secure PHRs includes the required time for: (1) the ERU staff to request an OTR token, (2) the EA to authorise and issue the OTR token, (3) the OTR token to be sent to the ERU staff, (4) the ERU staff to send the PHR request along with their OTR token to the EmS, (5) the EmS to download and decrypt the requested PHRs, and (6) the EmS to send the PHRs to the ERU staff. According to the cellular standard for the third generation [20], the data transmission rate in a moving vehicle is 348 kbps, meaning that 348,000 bits or 43.5 KB of data can be transferred each second. This amount of data can contain a text of approximately 10 novel-size pages. Therefore, the amount of time to transmit a request, an OTR token and a secure PHR is negligible. The EmS processing time depends on the PHR storage and the decryption process. The underlying encryption scheme of the CP-ABE is an advanced encryption standard (AES) [21] in cipher block chaining (CBC) mode [22], which takes less than 3.25 s to encrypt an image with the size of 468 KB [23]. Because the encryption and decryption time for AES-CBC is the same, the decryption processing time can be negligible. Using the current data storage technology, 50,000 records can be searched in 2.5 s [24]. Thus, the PHR storage processing time is not a problem. The only external factor to the total processing time is the EA processing time, which will be discussed later. Using the above supporting evidence, the secure PHR accessing time is reasonable in practical situations.

As described previously, the restricted PHRs are designed for the medical staff at the hospital to treat the victim when he/she is no longer at the emergency location. Therefore, there is a period of time between the call to the hotline and the victim arrival at the hospital during which the medical staff can obtain the necessary approval to access the necessary restricted PHRs. The processing time to retrieve the restricted PHRs includes the required time for: (1) the ERU staff to receive the OTR token, (2) the ERU staff to send the PHR request along with the OTR token, (3) the EmS to send the request to each trusted user, (4) each trusted user to respond to the request, (5) the partial secret key of each trusted user to be sent to the EmS, (6) the EmS to download and decrypt the requested PHRs, and (7) the EmS to send the PHRs to the ERU staff. The above factors discussed for the secure PHRs can also be applied to the restricted PHRs, the only difference being the response time of the trusted user. According to a study [25], the average response time of a person to an incoming text messaging is 431.28 s during simultaneous conversations and 391.88 s during non-simultaneous conversations. Therefore, it can take up to 7 min. for the trusted users to respond to a restricted PHR access approval request. Considering the 8-min. response time standard,

the medical staff at the hospital are able to access the restricted PHRs of the victim before the victim reaches the hospital.

To provide an additional assurance that the trusted users will respond to the request, the PHR owner should include at least one of the trusted users on the emergency contact list. Because the list is classified as a secure PHR, the ERU staff can contact the trusted user directly. The restricted PHRs are designed for the medical staff at the hospital; therefore, the medical staff can be added as an attribute in the access policy during the CP-ABE encryption of the PHRs and can thus access the PHRs. However, they must be a member of an authority that is recognised by the victim's PHR system.

Under the proposed scheme, the EA acts as a trusted agent to verify all of its ERU staff. Because the EA can be from various sources, the process of adding a new EA to the proposed scheme must be done carefully and the new EA must be verified. To ensure the performance of the ERU staff, each EA must be periodically evaluated. The request approval processing time and the OTR token generation time must be used as the key performance indicators to evaluate the EA. In addition, the OTR token lifetime may allow the ERU staff to perform a replay attack on the PHR system. Therefore, the ERU staff misconducts and performances can be used as another key performance indicator to evaluate the EA. The EA with poor performance must be removed.

Security Issues

Four attack models are discussed to account for possible security threats. The first model involves a database intruder. Under the proposed scheme, the actual PHR storage can be a public storage. Therefore, the database intruder or the storage administrator may try to access the information. However, the PHR is encrypted and the decryption keys are securely stored on separate trusted servers (i.e. the UA and the EmS). Hence the encrypted PHR stored on the PHR storage is protected with the assumption that the cryptographic primitives are not broken and the decryption key is not accessible.

The second attack model concerns an unauthorised access. The ERU staff may try to access the PHRs. However, the ARA mechanism prevents such access by allowing only the ERU staff with an approval from their corresponding EA to access the data. The approval is in the form of a valid OTR token. The ERU staff uses the received OTR token as a request certificate to access the requested PHRs through the EmS. An unauthorised access is prevented at the EmS and any attempt from the ERU staff is recorded by the audit server. Because the conduct of each ERU staff is used as a key performance indicator during the EA evaluation process, any misconduct by the ERU staff affects its EA performance. The EA evaluation process and the transaction auditing mechanism can indirectly prevent unauthorised access.

The third attack model is a replay attack. The ERU staff with a valid OTR token may conduct a replay attack. However, the OTR token is a certificate with a specific expiration time. Therefore, the ERU staff will not be able to reuse the OTR token once it is expired. However, this does not cover the period of time that the OTR token remains valid. Therefore, the lifetime of the OTR token must be short. The auditing information can show any misconduct of the ERU staff, which affects the performance of the corresponding EA.

The last attack model is a non-repudiation case. The audit server records all transactions invoked by the ERU staff and all activities can be tracked by the PHR owner. The transaction auditing mechanism is a very important mechanism to provide a non-repudiation feature.

CONCLUSIONS

This work has extended the original design of a PHR system for handling emergency situations to support a more practical scenario. In the original design all players were assumed to be trustworthy. In this work the ERU staff is considered an outsider and unknown to the system. Two mechanisms have been proposed to enhance the trustworthiness of the PHR access requests from an ERU staff member during an emergency situation. First, an ARA mechanism is designed to ensure the verification of the ERU staff by an on-duty emergency unit commander/manager. Any request invoked by an ERU staff member must be approved by his/her corresponding on-duty EA commander. Second, the transaction auditing mechanism is added to allow the PHR owners to track all transactions related to their PHRs. In addition, the auditing mechanism serves as a method for providing a non-repudiation feature for all PHR access performed by the ERU staff. Using the proposed extension, the trustworthiness of the requests invoked by the ERU staff is enhanced and the limitation of the previous work is eliminated.

The current data transmission rate and storage technology allows the proposed scheme to provide the requested PHRs within a commonly acceptable time and there is only one security limitation in the proposed scheme, which is the period of time that the OTR token remains valid. The suggested solution is to keep the lifetime of the OTR token short and to evaluate the EA based on its ERU staff performance and misconduct. Furthermore, a guideline on defining a proper privacy level for each PHR has been presented. The idea of collecting and storing transactions by an audit server is demonstrated using our developed prototype.

ACKNOWLEDGEMENTS

REFERENCES

1. W. Wangcharoen, D. Amornlerdpison and K. Mengumphan, "Factors influencing dietary supplement consumption: A case study in Chiang Mai, Thailand", *Maejo Int. J. Sci. Technol.*, **2013**, *7*, 155-165.

2. A. A. Ozok, H. Wu, M. Garrido, P. J. Pronovost and A. P. Gurses, "Usability and perceived usefulness of personal health records for preventive health care: A case study focusing on patients' and primary care providers' perspectives", *Appl. Ergonom.*, **2014**, *45*, 613-628.

3. 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", *J. Am. Med. Inform. Assoc.*, **2006**, *13*, 121-126.

4. B. A. Malin, K. El Emam and C. M. O'Keefe, "Biomedical data privacy: Problems, perspectives, and recent advances", *J. Am. Med. Inform. Assoc.*, **2013**, *20*, 2-6.

5. K. Caine and R. Hanania, "Patients want granular privacy control over health information in electronic medical records", *J. Am. Med. Inform. Assoc.*, **2013**, *20*, 7-15.

6. J. Huang, M. Sharaf and C. T. Huang, "A hierarchical framework for secure and scalable EHR sharing and access control in multi-cloud", Proceedings of 41st International Conference on Parallel Processing Workshops, **2012**, Pittsburgh, USA, pp. 279-287.

7. J. L. Fernández-Alemán, I. C. Señor, P. Á. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", *J. Biomed. Inform.*, **2013**, *46*, 541-562.

8. P. Thummavet and S. Vasupongayya, "A novel personal health record system for handling emergency situations", Proceedings of 17th International Computer Science and Engineering Conference, **2013**, Nakorn Pathom, Thailand, pp.266-271.

9. D. Weerasinghe and R. Muttukrishnan, "Secure trust delegation for sharing patient medical records in a mobile environment", Proceedings of 7th International Conference on Wireless Communications, Networking and Mobile Computing, **2011**, Wuhan, China, pp.1-4.

10. Y. Ding and K. Klein, "Model-driven application-level encryption for the privacy of e-health data", Proceedings of 5th International Conference on Availability, Reliability and Security, **2010**, Krakow, Poland, pp.341-346.

11. M. N. Huda, S. Yamada and N. Sonehara, "Privacy-aware access to patient-controlled personal health records in emergency situations", Proceedings of 3rd International Conference on Pervasive Computing Technologies for Healthcare, **2009**, London, UK, pp.1-6.

12. J. Sun, X. Zhu, C. Zhang and Y. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare", Proceedings of 31st International Conference on Distributed Computing Systems, **2011**, Minneapolis, USA, pp.373-382.

13. 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", Proceedings of 6th International Conference on Security and Privacy in Communication Networks, **2010**, Singapore, pp.89-106.

14. V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proceedings of 13th ACM Conference on Computer and Communications Security, **2006**, Alexandria, USA, pp.89-98.

15. 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", *IEEE Trans. Parallel Distr. Syst.*, **2013**, *24*, 131-143.

16. J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption", Proceedings of IEEE Symposium on Security and Privacy, **2007**, Berkeley, USA, pp.321-334.

17. S. Aguinaga and C. Poellabauer, "Method for privacy-protecting display and exchange of emergency information on mobile devices", Proceedings of International Conference on Collaboration Technologies and Systems, **2012**, Denver, USA, pp.596-599.

18. T. P. Pedersen, "A threshold cryptosystem without a trusted party", Proceedings of Workshop on Theory and Application of Cryptographic Techniques, **1991**, Brighton, UK, pp. 522-526.

19. P. T. Pons and V. J. Markovchick, "Eight minutes or less: Does the ambulance response time guideline impact trauma patient outcome?", *J. Emerg. Med.*, **2002**, *23*, 43-48.

20. International Telecommunication Union, "About mobile technology and IMT-2000", **2011**, http://www.itu.int/osg/spu/imt-2000/technology.html#Cellular Standards for the Third Generation (Accessed: April 2014).

21. National Institute of Standards and Technology, "Advanced encryption standard (AES)", **2001**, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (Accessed: April 2014).

22. National Institute of Standards and Technology, "Recommendation for block cipher modes of operation", **2001**, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (Accessed: April 2014).

Maejo Int. J. Sci. Technol. **2015**, *9*(01), 108-120

23. R. Doomun, J. Doma and S. Tengur, "AES-CBC software execution optimization", Proceedings of International Symposium on Information Technology, **2008**, Kuala Lumpur, Malaysia, pp. 1-8.

24. K. K. Lee, W. Tang and K. Choi, "Alternatives to relational database: Comparison of NoSQL and XML approaches for clinical data storage", *Comput. Meth. Programs Biomed.*, **2013**, *110*, 99-109.

25. A. Battestini, V. Setlur and T. Sohn, "A large scale study of text-messaging use", Proceeding of 12th International Conference on Human Computer Interaction with Mobile Devices and Services, **2010**, Lisbon, Portugal, pp.229-238.