19th International Computer Science and Engineering Conference (ICSEC)
Chiang Mai, Thailand, 23-26 November, 2015

Using Fingerprints to Identify Personal Health Record Users in an Emergency Situation

Pariwat Choosang[1], Sangsuree Vasupongayya[2]
Department of Computer Engineering, Faculty of Engineering, Prince of Songkla University,
Hat Yai, Songkhla 90112, Thailand
E-mail: 5410120041@email.psu.ac.th[1], vsangsur@coe.psu.ac.th[2]

***Abstract*—Personal Health Records (PHRs) is a system that allows an individual to store and share his/her health related information with others. The PHR owner can control all accesses to his/her data stored on the PHR system. This work aims to propose a privacy-preserved identification scheme to be used in the PHR system during an emergency situation especially when the victim is unconscious. The fingerprint-based scheme under a Protected Biometric Template (PBT) concept is applied to identify the victim without compromising the privacy of the victim. The usability and security discussions show that the proposed scheme is practical under the current existing communication technology and environment.**

Keywords—fingerprint; biometrics; identification; emergency; unconscious; biometric cryptosystems

I. INTRODUCTION

With an advancement of the communication and healthcare technologies and the rising healthcare cost, a concept of Personal Health records (PHR) has emerged [1]. An individual can store any health related information into his/her PHR system, such as mental health, personnel disease, laboratory test result and health checkup results. With the current communication technology, the PHR owner can access his/her PHR system through his/her mobile phone to store or to retrieve his/her data [2]. Such data can be shared among friends, family members, family doctors or caregivers. To protect the PHR owner privacy, however, any access to his/her PHR must be allowed by the PHR owner. Thus, the PHR system must provide an access control method for its users. Recently, the PHR access control method is proposed to allow accesses to the PHR system by the emergency response unit personnel [3]-[4]. Under such system, the PHR owner identity is assumed to be known and easily identified. To be realistic, this work aims to propose a person identification process in order to ensure the correct PHR owner identity during an emergency situation when the victim may be unconscious.

During an emergency situation, identifying a PHR owner, who is the victim, is challenging when he/she is unconscious. Correctly identifying the victim identity is critical in order to retrieve the correct PHR for the emergency response unit personnel to provide a proper first-aid treatment. Moreover, the victim who is unconscious usually requires a fast and proper medical treatment. The lacking of the victim identity may increase unnecessary rescue steps. An identification card is a typical token to identify a person identity. However, the present of such cards is uncertain during an emergency situation such as a car accident or a terrorist attack. Other forms of identification tokens include a smart card [5] or a radio frequency identification (RFID) [6]-[9]. Such forms, however, will usually require a reading or receiving device. Moreover, such tokens can easily be lost or misplaced or swapped during the operation. In contrast to the token, biometrics is an attractive choice for identifying a person [10]-[11]. The fingerprint is outstanding due to its accuracy and low cost in comparison to other biometrics [12]. The emergency response unit personnel can easily collect the victim fingerprint information. Therefore, the fingerprint is selected to identify the victim in this work.

Even though the rescue process is important, the privacy and security of the victim's fingerprint must be kept and protected as well. Fingerprint information can be stolen and facilitated several attacks [13]. To use the fingerprint in a secure manner, the protected biometric template (PBT) [14]-[15] was proposed. Under such scheme, the fingerprint is automatically transformed to a protected form which is irreversible to the original. Thus, the emergency response unit personnel can collect the victim's fingerprint under the PBT concept. As a result, the original fingerprint will not be stored. Since the emergency response unit personnel can belong to either private or public sectors [16], the proposed scheme in this work can allow the emergency response unit personnel to perform their task easily because the privacy of the victim is still preserved. The PBT concept has been used to verify the identity of the emergency hotline caller [17].

In this paper, a privacy-preserved user identification scheme for the PHR system to resolve the victim's identity in an emergency situation is proposed. The PBT concepts called Cancelable Biometrics (CB) and Biometric Cryptosystems (BCS) are utilized to protect the fingerprint information. The proposed system requires two fingerprints of the PHR owner. The first fingerprint will be used to perform a rough filter of the whole database in order to identify a list of possible PHR users. The second fingerprint will be used to perform the final identification from the list produced from the first fingerprint. Once the victim is identified, the PHR allowed during emergency situations will be retrieved.

The rest of this paper is organized as follow. Section II reviews the traditional PHR system and the PBT schemes. The

978-1-4673-7825-3/15/$31.00 ©2015 IEEE

details of the proposed scheme are given in Section III. Section IV discusses some security and usability issues of the proposed scheme. Related works are discussed in Section V. Finally, the conclusion is given in Section VI.

II. BACKGROUND

This section provides information on the traditional PHR system proposed in [3]-[4] for handling emergency situations and the protected biometric template [14],[15],[18]. The details will also include the overview of how to include our proposed scheme into the traditional system and how to construct the protected fingerprints in our proposed system.

A. Traditional PHR system: handling emergency situations

In an emergency situation, the emergency response unit personnel has an important role as the one who conducts an first aid on the victim [16],[19]. The emergency response unit personnel must be from a specific emergency department. Each emergency department is assigned an area to be covered. The emergency response unit personnel must help all victims in their covered area without any hesitation. In order to provide a high quality rescue operation, there exists a standard for the emergency department process [16]. The first step of the process is to identify the victim while the next step is first aid. To identify a victim, sufficient and unique information is required as being suggested in [16] to use at least 2 unique identifiers.

In order to support the emergency response unit personnel in treating the victim, the traditional PHR system provides a way to access the victim's PHRs according to the access control, set by the victim [3]-[4]. Under such scheme, the PHR owner can classify his/her PHRs into three access levels during an emergency, including secure, restricted and exclusive. The secure-level PHRs must contain the information that will be most useful to the emergency response unit personnel such as a personnel disease, blood group/type, allergic reaction and a list of emergency contact people. The secure-level PHRs can be accessed by the emergency response unit personnel if the PHR owner is the victim. The restricted-level PHRs must contain any health related information that will be helpful for the physician at a medical center away from the emergency location. The exclusive-level PHRs contain any information that the PHR owner does not want to share with anyone.

Fig.1 shows the overview of how the emergency response unit personnel requests an access to the victim's PHRs under the traditional PHR system. The emergency response unit personnel must first verifies his identity with his associated emergency department supervisor in order to obtain an access token. Then, the access token will be used to retrieve the victim's PHRs from the Emergency Server (EmS) according to the access control policy set by the victim who is the PHR owner. The EmS acts as the PHR portal for all emergency response unit personnel. However, the victim identity under this scheme is assumed to be correct and known by the emergency response unit personnel. The proposed method in this work will improve the traditional PHR system by providing a scheme to identify the victim's identity.

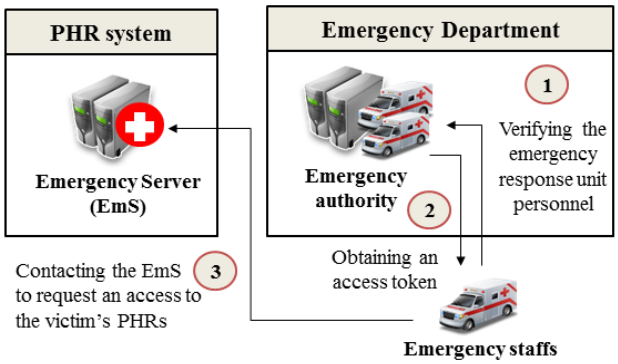

Fig. 1. Overview of how an emergency response unit personnel requests an access to the victim's PHRs under the traditional PHR system.

B. Biometric cryptosystems and Cancelable Biometrics

Privacy is always an issue when biometrics are used for identifying a person. The stolen biometric information can cause a serious concern to its owner. To reduce such a concern, a protected biometric template (PBT) concept was proposed [14],[15]. The PBT has two properties: irreversibility and unlinkability. There are two schemes under the PBT concept: biometric cryptosystems (BCS) and cancelable biometrics (CB). The BCS scheme provides a higher security level than that provided by the CB scheme [14]. A combined approach [18] was also proposed to combine the good sides of the two schemes. The experimental results from [18] also suggested that the combined approach must use at least two fingerprints (each from a different finger) in order to improve the efficiency. This work will apply the combined approach to conceal the PHR owner's fingerprints during the victim's identification process.

The proposed combined approach for fingerprints [18] is not only accurate for an identification process, but also efficient for recovering an individual's identifier [18]. Under such approach, there are two steps. The CB is first used to build a rough filter resulting in a set of candidates. At this step, the original fingerprint template is transformed into a CB. Then, the CB is used for matching with the CBs stored in the databases. The candidates can be constructed from the stored CBs. The candidates must be filtered by a fined-gained manner at the second step using the BCS. The candidates are used as the input of the BCS in order to produce the final decision. This way, the original fingerprint is concealed in such a way that any adversary cannot gain any original information of the fingerprint. Therefore, the fingerprint-based combined approach is an appropriate method to be applied in this work.

III. PROPOSED SCHEME

The proposed secure victim identification scheme for the PHR system during an emergency situation is described in this section. The main focus of this scheme is to correctly identify a victim even when the victim is unconscious. First, the system overview is given. Next, the registration phase is described. Finally, the identification phase is discussed.

A. System overview

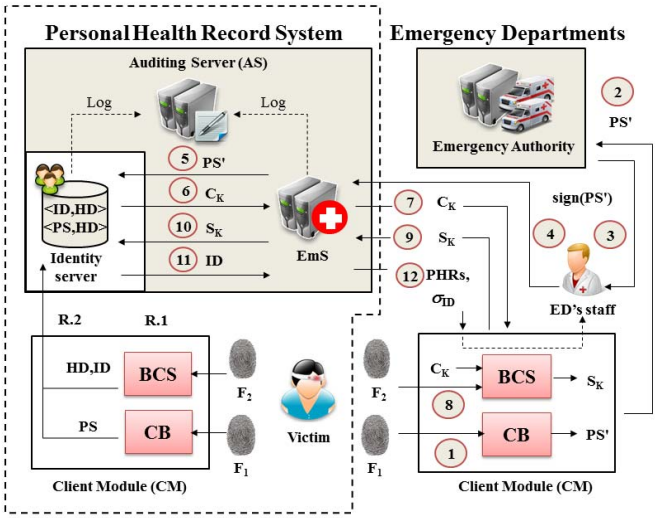

Fig. 2. The overview of the proposed scheme on the PHR system

The traditional PHR system components, including the emergency server (EmS) and the auditing server (AS), will be modified to support the proposed scheme. The AS collects the transaction log of each event. The Emergency Departments (ED) must use their signature key to sign the fingerprint transformed by the PBT in order to provide the authenticity of the request. For the trusted EDs—have already registered with the PHR system—the certificate is already issued to the EDs and the EmS can verify such identity. For the semi-trust EDs, which is new in this work, the certificate can be obtained from a global trusted CA such as VeriSign [20]. Fig. 2 shows the overview of the proposed scheme. The new components are presented in white, while the modified components are presented in gray.

The Identity Server (IdS) and Client Module (CM) is the two newly created module to support the proposed scheme on the server and client side, respectively. The IdS is responsible for managing and resolving the user identity. The user fingerprints transformed thru the CB and BCS schemes will also be stored on the IdS. Meanwhile, the PHR owners or the emergency response unit personnel can interact securely with the PHR system via the CM. The fingerprint template will be modified and concealed at the source. This way, the original fingerprint will not be transferred over the Internet. The CM must be securely connected to the PHR system by means of SSL/TLS [21]. Thus, the security at the network layer will not be discussed in this work. Table 1 shows the list of notations used.

B. Registration phase

The proposed scheme requires a registration phase which consists of two main steps shown as a dotted box in Fig.2. These two steps must be performed by the PHR owner using the proposed CM. Details of the two steps are as follow.

TABLE I. THE LIST OF NOTATIONS

Notation	Description
F_1, F_2	F_1 is the right index fingerprint used in the first stage, while F_2 is the left index fingerprint used in the second stage.
PS	The result from the first stage (generated by the CB) which is called prescreener
HD	HD provides helpful data for the BCS during the ID generating process
ID	The result from the second stage (generated by the BCS) which is called identifier
C_K	A set of k number of HDs in the database which is call a candidate set C
S_K	A set of k number identifiers S with K member
σ_A	Signed data A
$\Delta_{BCS}(F)$	A BCS generated-function with the input fingerprint F The output of this function are ID and HD
$\Phi_{BCS}(F,HD)$	A BCS transformed-function with the input fingerprint F and the input HD The output of this function is ID
$\Phi_{CB}(F)$	A CB function with the input fingerprint F The output of this function is PS
$Sign_B(A)$	A function to sign the input A using the private key B

R.1) The PHR owner must register his/her fingerprints (both index fingers) with the system. The right index fingerprint (F_1) is sent to the CB inside the CM in order to produce the pre-screener (PS) as shown in equation (1) while the left index fingerprint (F_2) is sent to the BCS inside the CM in order to create an identifier (ID) and the helpful data (HD) as shown in equation (2). Then, the PS and <ID, HD> will be sent to be stored in the IdS.

$$\Phi_{CB}(F_1) \rightarrow PS \quad (1)$$

$$\Delta_{BCS}(F_2) \rightarrow <ID,HD> \quad (2)$$

R.2) After receiving the PS and <ID, HD> from step R.1, the IdS will create a new record in two tables: the pre-screener table and the identifier table. The new record to be stored in the pre-screener table is the pair <PS, HD> while the new record to be stored in the identifier table is the pair <ID, HD>. Both tables will be used during the identification process.

C. Identification phase

During the identification phase, the emergency response unit personnel will use the CM to resolve the victim identity as follow.

Step 1. The victim's right index fingerprint is collected to produce the pre-screener PS′ as shown in equation (3).

$$\Phi_{CB}(F_1) \rightarrow PS' \quad (3)$$

Step 2 The PS′ is then sent to the EDs along with the emergency response unit personnel PHR access request.

Step 3. The ED supervisor on duty is then verifying the emergency response unit personnel, signing the PS′ ($\sigma_{PS'}$) as shown in equation (4), and issuing the access token.

$$Sign_{PrvED}(PS') \rightarrow \sigma_{PS'} \quad (4)$$

Step 4. The access token including the access token, the PS′, and the signed PS′ is then sent to the EmS. The EmS can verify the authenticity of the request and the signed PS′.

Step 5. The PS′ is then sent to the IdS in order to get a set of k candidate helpful data called C_K where $C_K = \{HD_i \mid 1 \le i \le k\}$ and k is the parameter set by the PHR owner. One of the k candidate helpful data is the correct HD of the victim. The set of k candidate is selected from the pre-screener table.

Step 6. The C_K is returned to the EmS.

Step 7. The C_K is returned to the emergency response unit personnel.

Step 8. The emergency response unit personnel is then collecting the victim left index fingerprint (F_2) in order to construct a set of k identifiers called S_K where $S_K = \{ID_i \mid 1 \le i \le k\}$. Each ID_i is generated according to equation (5). This way, the emergency response unit personnel will not have the exact ID of the victim nor the original victim fingerprint under the main assumption that the CM is not compromised.

$$\Phi_{BCS}(F_2, HD_i) \rightarrow ID_i \quad for\ 1 \le i \le k \tag{5}$$

Step 9. The S_K is then sent back to the EmS.

Step 10. The S_K is then sent to the IdS by the EmS to retrieve the victim's identifier (ID).

Step 11. Upon receiving the ID, the EmS issues the identity-token T_{ID}, containing the victim's generated identity, the emergency response unit personnel identity and the time stamp. The victim generated identity is a temporary ID generated for the current transaction as long as the access token is valid. The EmS stores the victim's identity, the T_{ID} and the σ_{ID}, which is generated by equation (6).

$$Sign_{EmS}(T_{ID}) \rightarrow \sigma_{ID} \tag{6}$$

Step 12. The σ_{ID} and the PHRs of the victim are then sent back to the emergency response unit personnel to be used in retrieving the data in the future as long as the lifetime of the access token is still valid. Any further requests from the same emergency response unit personnel for the same victim of the same emergency situation can be identified using the signed data σ_{ID}. The EmS can check the authenticity of the signed data and retrieve the correct victim identity. All connections between the emergency response unit personnel and the PHR system are assumed to be secured under SSL/TLS.

IV. Usability and Security Discussions

How the proposed scheme providing usability along with maintaining the security and privacy is discussed in this section. For explanation purpose, the typical flow of events during an emergency situation is shown in Fig. 3. The steps can be as follow: (1) an emergency situation occurs; (2) an witness calls the emergency hotline center; (3) the emergency response unit personnel receives the location and situation information; (4) the emergency response unit personnel reaches the location; (5) the victim is given the first-aid treatment and transferred to a medical facility; and (6) the victim reaches the medical facility for further treatment.

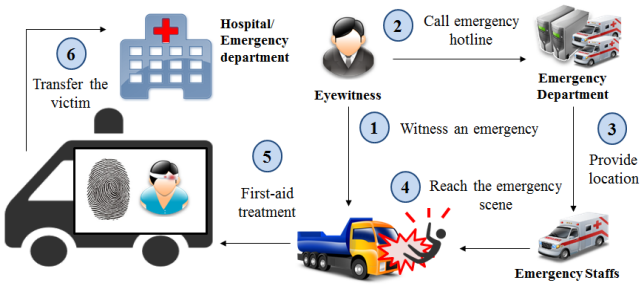

Fig. 3. Typical flow of events during an emergency situation

According to the flow of events shown in Fig. 3, the common acceptable response time from step 2 to step 4 is approximately 8 minutes [22]. Assuming that the emergency department is located at the medical facility, the time from step 4 to step 6 might take up to 8 minutes as well. In order to provide a proper first-aid treatment, the victim's PHRs must be available in less than 8 minutes. In the proposed scheme, the identification phase can only be started after step 4.

A prototype web-based system is developed including the IdS, the EDs, the EmS, and a mobile application (the client module). The secure connection is provided by means of SSL/TLS. The server device is an Intel Core i5 3.1GHz with 4GB of memory. The tested mobile device is the Samsung Galaxy S3 Quad-core 1.4 GHz with 1 GB of RAM. For the BCS, the library in [18] is adopted and modified to be used properly for our proposed scheme. Meanwhile, the CB library is newly designed and implemented specifically in this work. The performance of the newly developed CB is similar to the performance showed in [18].

A. Usability discussion

According to the results presented in the previous work [4], the emergency response unit personnel authentication can be done and finished during step 3 to step 4. Therefore, the actions to be done in less than 8 minutes include the victim identification and the PHRs retrieval. In this work, the focused PHRs are the secure-level PHRs which can be instantly retrieved after all successful authentications. However, the PHR retrieval time (searching, decrypting and transferring) is negligible as reported in [4]. For discussion purposes, there are three pairs of actions including the pair between the emergency department and the emergency response unit personnel, the pair between the emergency response unit personnel and the EmS, and the pair between the EmS and the IdS.

The actions between the emergency department and the emergency response unit personnel start from step 1 to step 3 in Fig. 2. The processing time of all these actions includes the time (1) to collect the victim right index fingerprint, (2) to transform the fingerprint into the PS′, (3) to send the PS′ to the emergency department, (4) to get the signed PS′, and (5) to send the signed PS′ back to the emergency response unit personnel. The argument in the previous work [4] can be used for the transmission time at (3) and (5). The argument is as follow: approximately 43.5KB of data can be transferred in a second under the third generation of cellular standard [23]. The PS′ resulting from the pseudonymous encoded character technique [18] is smaller than 43.5KB. Thus, the transmission

time at (3) and (5) can be negligible. According to [24], the encryption time of RSA with 1024 key size is approximately 0.03 seconds for 1,000 characters. Thus, the processing time at (4) is also negligible. Therefore the processing time at (1) and (2) will dominate the rest. The emergency response unit personnel typically carry a mobile device. Therefore, the tested mobile device is used to measure the processing time. The processing time of collecting and transforming the right index fingerprint into the PS′ on the tested mobile device is approximately 30 seconds. Thus, all actions will take less than 1 minute.

The actions between the emergency response unit personnel and the EmS include step 4, step 7 to 9 and step 12 as shown in Fig. 2. The processing time of all these actions includes the time (1) to send the request and the signed PS′ to the EmS, (2) to send the C_K to the emergency response unit personnel, (3) to collect the right index fingerprint, (4) to construct the S_K, and (5) to send the S_K to the EmS, and to send the PHRs and the $\sigma_{PS'}$ back to the emergency response unit personnel. Similar argument on the transmission time which is negligible can be applied to the time required at (1), (2), and (5). Each candidate size is approximately 160 Bytes. Therefore, the payload will be approximately 4.8KB for 30 candidates (k = 30 which is suggested in [18]). Thus, the only processing time for this communication pair includes the time to collect the right index fingerprint and the time to construct the S_K. According to the results collected from the tested mobile device, Table 2 shows the time to construct the S_K. If k is set to 30, this step will take approximately 140 seconds or 2 minutes and 20 seconds.

The actions between the EmS and the IdS include step 5, step 6, step 10, and step 11 as shown in Fig. 2. The processing time of all these actions includes the time (1) to verify the signed PS′, (2) to construct the C_K, (3) to send the C_K to the EmS, (4) to send the S_K to the IdS, (5) to identify the correct ID of the victim, (6) to send the correct ID back to the EmS, and (7) to retrieve the requested PHRs. The same argument on the processing time of RSA with 1024 key presented in [24] can be used to eliminate the processing time at (1), while the transmission time argument is also applied at (3), (4) and (6). The argument of the previous work on the PHR retrieval time can be applied to the processing time at (7). The processing time at (2) is to select k members of the candidates from the candidate table which is shown to take 10ms on a core i5 2.67 GHz with 2GB of memory [18] which is also negligible. Additionally, the processing time at (5) is only for searching the database of <ID, HD> to find the correct ID of the victim. Thus, the processing time at (5) is also negligible.

TABLE II. PROCEESING TIME TO CONSTRUCT THE S_K FOR EACH VALUE OF K

K	1	5	10	15	20	30
Time	30.76s	47.25s	64.30s	84.38s	101.20s	139.57s

In conclusion, the whole process will take approximately 170 seconds for k = 30. The time is well within the scope because the time is less than 4 minutes which is only half of the time condition. Thus, the proposed scheme still allows the PHRs to be successfully retrieved before the victim is arrived at the medical facility. In the future work, various versions of CB and BCS will be investigated in order to propose a faster CM.

B. Security discussion

Two security aspects are discussed including stealing an identity and performing an illegal access to the PHRs. The fingerprint is considered a sensitive piece of information to identify a person. Therefore, the aim of the first security aspect discussed here is to steal the original fingerprint template. According to our design, the fingerprints F_1 and F_2 are processed at the client side (CM) which has no cache. No data, that is reversible to the original template, is being sent through the Internet. Only the PS and the C_K are being transmitted. Both the PS and the C_K contain only half secret and both of them are irreversible [18]. Therefore, the original fingerprint template will not be exposed to any party except the CM, assuming the CM is not compromised and the adversary cannot break any cryptographic primitive used.

The second security aspect focuses on the attempt to perform an illegal access to the PHRs. For example, the emergency response unit personnel is an adversary by recording all the information such as the set C_K and S_K of a particular person during a real emergency situation. Later, the adversary replays the information to the EmS. In this case, the access token that the adversary obtained from the emergency department will limit the time period when such token can be used. Therefore, if both the emergency department and the emergency response unit personnel are compromised then the PHRs can be retrieved. Thus, the lifetime of the access token must be limited. Furthermore, the emergency department will be evaluated based on its performance. The transaction log can present some suspicious actions taken by the emergency response unit personnel. Therefore, the suspicious actions will raise an investigation on the associated emergency department.

Another example, the adversary obtains the fingerprint of a person and uses such information to retrieve the person's PHRs. This case will be prevented again by the access token. The access token can only be granted by the emergency department supervisor on duty. Thus, the adversary will not be able to gain an access to the required access token. Moreover, the transaction log at various steps such as the emergency department, the identity server, and the EmS can be used for tracking an event or a series of suspicious actions conducted by the adversary.

V. RELATED WORKS

Related works on the victim identification techniques during an emergency situation is provided in this section. The fingerprint-based biometric identification is a technique to resolve the patient identity in various works [10]-[11]. To prevent the risk of identity disclosure, however, the use of biometric is often found in a control and trusted environment. All parties involved will be bounded by a practical work guideline or a career ethical code of conduct. To reduce the risk of identity disclosure issues in a semi-trust environment, the biometric must be used in a protected form instead of its original form. In [17], the fingerprint template is used to identify the reporter in an emergency situation to prevent any

fake call to the emergency hotline number. Moreover, the reporter can request a teleconsultation with an emergency response unit personnel in order to provide a first-aid treatment if necessary. However, only the CB is used in [17] which can cause an accuracy issue when the system is large. In this work, the CB is used as a rough filter in order to screen the whole database for a finite number of candidates. Then, the BCS technique will be applied to make the final identification. This work uses a combined approach in order to preserve the user privacy and to provide a fast result for the emergency response unit personal during operations.

Other than the biometric method, many works in patient identification applications [6]-[9] select RFID as the identity token. However, a specific RFID reader device is needed in order to read and identify the owner of the RFID tag. Similar argument goes with the use of a smart card technique [5]. That is, the victim must always carry it and the risk of lost or stolen does exist. The fingerprint on the other hand is with the victim at all times. Thus, the risk of lost or stolen is reduced.

VI. Conclusion

A fingerprint-based victim identification scheme during an emergency situation is proposed in this work. The scheme is focusing on using the fingerprint in a protected form to provide both security and privacy. The combined approach of PBT namely CB and BCS is used in the proposed scheme. The CB used in this work is newly design and developed. The usability and security discussion shows that the whole scheme can be done within four minutes after the emergency response unit personnel reach the emergency location. Thus, the proposed scheme is practical in the current and existing technology and environment. Future work includes investigating various techniques to be used in the CB, BCS and CM in order to reduce the overall processing time down to two minutes.

Acknowledgment

This work was supported by the Higher Education Research Promotion and National Research University Project of Thailand, Office of the Higher Education Commission (under the funding no. MED540548S at Prince of Songkla University).

References

[1] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," *Journal of the American Medical Informatics Association*, vol. 15, pp. 729-736, 2008.

[2] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys (CSUR)*, vol. 45, p. 3, 2012.

[3] P. Thummavet and S. Vasupongayya, "A novel personal health record system for handling emergency situations," in *Computer Science and Engineering Conference (ICSEC), 2013 International*, 2013, pp. 266-271.

[4] P. Thummavet and S. Vasupongayya, "Privacy-preserving emergency access control for personal health records," *Maejo International Journal of Science and Technology*, vol. 9, pp. 108-120, 2015.

[5] M. N. Huda, S. Yamada, and N. Sonehara, "Privacy-aware access to patient-controlled Personal Health Records in emergency situations," in *Pervasive Computing Technologies for Healthcare, 2009. PervasiveHealth 2009. 3rd International Conference on*, 2009, pp. 1-6.

[6] A. Masters and K. Michael, "Lend me your arms: The use and implications of humancentric RFID," *Electronic Commerce Research and Applications*, vol. 6, pp. 29-39, 2007.

[7] M. W. Raad, "A ubiquitous mobile telemedicine system for the elderly using RFID," *International Journal of Security and Networks*, vol. 5, pp. 156-164, 2010.

[8] P. Rotter, B. Daskala, and R. Compano, "RFID implants: Opportunities and and challenges for identifying people," *Technology and Society Magazine*, IEEE, vol. 27, pp. 24-32, 2008.

[9] W. Yao, C.-H. Chu, and Z. Li, "The adoption and implementation of RFID technologies in healthcare: a literature review," *Journal of medical systems*, vol. 36, pp. 3507-3525, 2012.

[10] D. Marohn, "Biometrics in healthcare," *Biometric Technology Today*, vol. 14, pp. 9-11, 2006.

[11] A. E. F. Zuniga, K. T. Win, and W. Susilo, "Biometrics for electronic health records," *Journal of medical systems*, vol. 34, pp. 975-983, 2010.

[12] E. Okoh and A. I. Awad, "Biometrics Applications in e-Health Security: A Preliminary Survey," in *Health Information Science*, ed: Springer, 2015, pp. 92-103.

[13] P. Campisi, *Security and Privacy in Biometrics*: Springer, 2013.

[14] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, vol. 2011, pp. 1-25, 2011.

[15] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, p. 113, 2008.

[16] S. J. Welch, B. R. Asplin, S. Stone-Griffith, S. J. Davidson, J. Augustine, J. Schuur, et al., "Emergency department operational metrics, measures and definitions: results of the second performance measures and benchmarking summit," *Annals of emergency medicine*, vol. 58, pp. 33-40, 2011.

[17] S. Yun, H. Jung, and S. Yun, "Smart Emergency Rescue System Based on Biometric Authentication," in *Computer Science and its Applications*, ed: Springer, 2015, pp. 1043-1048.

[18] B. Tams and C. Rathgeb, "Towards efficient privacy-preserving two-stage identification for fingerprint-based biometric cryptosystems," in *Biometrics (IJCB), 2014 IEEE International Joint Conference on*, 2014, pp. 1-8.

[19] J. L. Wiler, S. Welch, J. Pines, J. Schuur, N. Jouriles, and S. Stone-Griffith, "Emergency Department Performance Measures Updates: Proceedings of the 2014 Emergency Department Benchmarking Alliance Consensus Summit," *Academic Emergency Medicine*, 2015.

[20] VeriSign SSL/TLS CA. [Online]. Available: http://www.verisign.com/

[21] J. Viega, M. Messier, and P. Chandra, *Network Security with OpenSSL: Cryptography for Secure Communications:* " O'Reilly Media, Inc.", 2002.

[22] P. T. Pons and V. J. Markovchick, "Eight minutes or less: does the ambulance response time guideline impact trauma patient outcome?," *The Journal of emergency medicine*, vol. 23, pp. 43-48, 2002.

[23] International Telecommunication Union. *About mobile technology and IMT-2000*. [Online]. Available: http://www.itu.int/osg/spu/imt-2000/technology.html#Cellular Standards for the Third Generation

[24] S. Saxena and B. Kapoor, "An efficient parallel algorithm for secured data communications using RSA public key cryptography method," in *Advance Computing Conference (IACC)*, 2014 IEEE International, 2014, pp. 850-854.