Based on Electronic Medical Record System with Online Authorization Control and Authentication Scheme

Chin-Ling Chen[1] Ming-Shaw Lu[2] Zong-Min Guo[1] Hsien-Wen Tseng[2]
[1]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan 41349, ROC.
clc@mail.cyut.edu.tw; shawming2001@gmail.com
[2]Department of Information Management, Chaoyang University of Technology, Taichung, Taiwan 41349, ROC.
ckljdstar@gmail.com; hwtseng@cyut.edu.tw

Abstract

Because the roles of anamnesis management are rather susceptible, how to against malicious behavior and protect the patient's privacy becomes an important issue. In recent years, the development of Health-Card is widely adopted as an identification technology, and imposes a large application and provides convenience to the patient at anywhere.

Moreover, there are more and more applications about health care were presented. But this also leads to some problems such as the patient's privacy and how to against illegal access. Unfortunately, there always still existed some disputes and the moral standards of the doctors will be confronted the challenge. The current operations are not suitable for online automatic E-anamnesis management as require in E-Health. To solve this problem, we propose a based on electronic medical record system with online authorization control and authentication scheme. Therefore, not only the patient's privacy could be protected but also raising the medical revenue.

Keywords: E-Health; non-repudiation; verifiable; E-anamnesis; Authentication.

1. Introduction

Due to evolution in communication and management systems, Information Technology is experiencing an era of great improvement. It provides users with new ways to manage and display heterogeneous information. In recent years, healthcare has become a popular issue, and also the use of the techniques for online automatic E-anamnesis management. This may cause some latent problem [8], such as patient's privacy and how to against illegal access. Unfortunately, there always still existed some disputes and the moral standards of the doctors will be confronted the challenge. The current operations are not suitable for online automatic E-anamnesis management as requirement in E-Health.

In other hand, some researchers have pointed out that, electronic medical record exchange among hospitals can provide more information for physician diagnosis and reduce costs from duplicate examinations [4]. In 2007, an E-anamnesis management measure has proposed by Matsunami, K. [9] to solve the cost expensive problem of digitization in the post schemes. He set the medial information system up which can support the patient treatment information to the doctors. However, it is not easy to introduce in ordinary hospital, since it is too much expensive. Moreover, available system on the market is very inconvenient, and often requires customizing for each hospital. Nevertheless, he didn't specify how his scheme can protect the patient's privacy or withstand the illegal access. In spite of lots of scholars had proposed some schemes in anonymity [1-3, 5-6, 11], but there still exists disputes. To solve these problems, we propose a based on electronic medical record system with online authorization control and authentication scheme.

Our scheme used both the timestamp technique and the nonce mechanism. In 1999, Yang and Shieh [10] proposed a timestamp based scheme without maintaining the verification table. They declared their scheme can withstand the impersonation attack. However, in 2008, Liu et al. [7] have pointed out that Yang and Shieh's scheme still can't withstand the impersonation attack. Liu et al. therefore proposed a nonce based improvement scheme and discussed their scheme not only can against the replay attack and impersonation attack but also does not increase the computation cost of the smart card.

In this paper, the crucial issue is to protect the patient's privacy and an adaptive E-anamnesis management mechanism. We integrate both the timestamp and the nonce

techniques in specific phase to achieve the purpose of authenticating the remote user. In additional, to prevent the impersonation attack, the best measure is weighing in the personally fingerprint in our own Health-Card. Therefore, the patient's identity can easily be authenticated and otherwise can reduce the medical consumptions. Also it has contributed to improve in the quality of medical examination, medical safety, and the medical efficiency. Besides, the following requirements and traits must be achieved in our new scheme.

- Prevent of Denial of Service (DoS) attack
- Prevent of device losing attack
- Prevent of forgery attack
- Prevent of parallel session attack
- Prevent of replay attack
- Mutual authentication
- Prevent of illegal access issue
- Non-repudiation

Rest of the paper is organized as follows: session 2 shows our whole system structure and the detail procedures in each phase. In session 3, we elaborate the security analysis and the discussion of requirements of our proposed scheme. Finally, we conclude this paper in session 4.

2. Proposed scheme

There are five roles in our proposed scheme: the patient (P), the doctor (DR), the Healthcare Service Organization (HSO), the remote file server (RS) for accessing and managing E-anamnesis and a tamperproof fingerprint application program interface (FAPI) program which is embedded into an identification machine. The flow chart of our scheme is illustrated as Fig. 1.

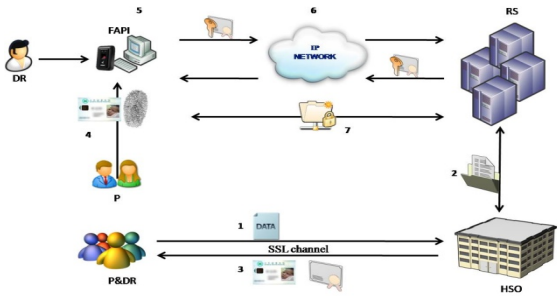

Fig.1. The system flow chart

1. P & DR→HSO：The patient and the doctor send their private fingerprint data to the HSO for registration through secure channel.
2. HSO↔RS：HSO forwards the registration data to the RS for checking and recording it. Then the RS sends back the acknowledgement messages to the HSO.
3. HSO→P & DR：After checking process, the HSO issues the Health-Card to the patient.
4. DR→FAPI：Before the doctor start to diagnose, he or she must put his or her finger on the tamperproof fingerprint identification machine for identification. After passing verification, the FAPI program will be start-up.
5. P→FAPI：P carries the Health-Card to the hospital for examination. First, P sends the authentication message to the FAPI by putting his/her finger on the tamperproof fingerprint identification machine and inserting his Health-Card.
6. FAPI↔RS：The FAPI forwards both the DR and the P's fingerprints to HSO for mutual authentication. If their identities are authorized, then they can start to communicate or access the E-anamnesis; otherwise, the request will be rejected.
7. RS↔FAPI：Only the authorized DR can ask the RS to insert, modify or query the P's E-anamnesis. And all the behaviors of the DR will be recorded into the RS's database for tracing.

2.1 Notation

ID_X : The identity of X.
f_X : Denotes X's biometric fingerprint.
$h(\cdot)$: A one-way hash function.
T_i : The i^{th} timestamp.
α, β : Randomly nonce.
γ : The expected valid time interval for transmission delay.
K : The session key shared between patient and RS.
Sig_X : The signature value of X.
$E_K(\cdot)$: Use session key K to encrypt the message.
$D_K(\cdot)$: Use session key K to decrypt the message.
$S_{SK_X}(\cdot)$: Use X's private key to make the signature.
$V_{PK_X}(\cdot)$: Use X's public key to verify the signature.
C_x : The ciphertext x.
$A \stackrel{?}{=} B$: Compare whether A is equal to B.
$\|$: The concatenation operation.
$\oplus$: Exclusive-or operation.
g : A public primitive element.

Our scheme divides into four phases namely registration phase, login phase, authentication phase and communication phase. We describe the steps of each phase in our scheme as follows.

2.2 Registration phase

Step 1: The patient sends his or her personal information and fingerprint to the HSO for registration, and also the doctor, too.

Step 2: The HSO checks and records the verified data of the patient and doctor into remote file server.

Step 3: After checking procedure, the HSO issues the Health-Card to the patient and the certificate to the doctor, respectively.

2.3 Login phase

Step 1: Before examination, the DR must put his or her finger on the fingerprint identification machine to obtain his or her fingerprint f_{DR} via FAPI program. And FAPI sends f_{DR} to the RS for authentication.

Step 2: Upon receiving the request, the RS does the data comparing. If there found nothing, then reject it; otherwise, the RS sends the " Successful Verification" messages back to the FAPI with the timestamp T_s of the RS.

Step 3: After receiving the response message, the FAPI sends an authentication request message to synchronize with server.

Step 4: The server confirms the synchronization procedure by the above steps.

2.4 Authentication phase

Step 1: The patient carries a Health-Card to the consulting room and puts it into the fingerprint identification machine to obtain his or her biometric fingerprint f_p. The FAPI generates a random number α and current timestamp T_1. Finally, the FAPI generates the verifiable data includes the identities of the patient and the doctor, α and T_1. The FAPI uses patient's private key to generate his or her signature as Sig_P follows.

$$Sig_p = S_{SK_P}(ID_P \| ID_{DR} \| \alpha \| T_1)$$

To avoid the attacks (Ex. man-in-the-middle attack or replay attack), the FAPI also uses the session key K to encrypt the $(ID_P \| ID_{DR} \| \alpha \| T_1)$ into ciphertext C_p.

$$C_P = E_K(ID_P \| ID_{DR} \| \alpha \| T_1)$$

For authentication, the FAPI computes the C_P and the patient's fingerprint f_p as a hash value Y by using a collision-free one-way hash function for authentication.

$$Y = h(C_P \oplus f_P)$$

Continuously, the FAPI sends (Sig_p, C_p, Y) to the RS for verification.

Step 2: After receiving (Sig_p, C_p, Y), the RS decrypts the ciphertext C_p to obtain ($ID_P \| ID_{DR} \| \alpha \| T_1$) and verifies the signature Sig_p with the session key K and the patient's public key, respectively. The RS performs the following computations.

$$D_K(C_P) = (ID_P \| ID_{DR} \| \alpha \| T_1)$$

$$V_{PK_P}(Sig_P) \stackrel{?}{=} (ID_P \| ID_{DR} \| \alpha \| T_1)$$

Check if $T_1' - T_1 \le \gamma$

, where γ is the expected valid time interval for transmission delay.

Check if ID_P is valid or not.

Check if ID_{DR} is valid or not.

Continuously, the RS queries the corresponding fingerprint f_p to check if hash value Y is correct or not.

$$Y \stackrel{?}{=} h(C_P \oplus f_P)$$

After the verification, the RS generates the ciphertext C_{RS}, verifiable data (Sig_{RS}, Z), and sends back to the FAPI as follows.

$$C_{RS} = E_K(ID_{RS} \| \alpha \| \beta \| T_2)$$

$$Sig_{RS} = S_{SK_{RS}}(ID_{RS} \| \alpha \| \beta \| T_2)$$

$$Z = h(C_{RS} \oplus \beta)$$

The RS sends (Sig_{RS}, C_{RS}, Z) to the FAPI for verifying.

Step 3: Upon receiving (Sig_{RS}, C_{RS} , Z), the FAPI decrypts the ciphertext C_{RS} and verifies whether the signature Sig_{RS} is the same as in the step 2 of this phase or not. The equations are as follows.

$$D_K(C_{RS}) = (ID_{RS} \| \alpha \| \beta \| T_2)$$

$$V_{PK_{RS}}(Sig_{RS}) \stackrel{?}{=} (ID_{RD} \| \alpha \| \beta \| T_2)$$

Check if α is valid or not.

Check if $T_2' - T_2 \le \gamma$.

Check $Z \stackrel{?}{=} h(C_{RS} \oplus \beta)$.

Continuously, to avoid the replay attack

and complete the mutual authentication, FAPI sends the mutual authentication request (A, M_{upd}) back to the RS, where the computation of A is as follows.

$$A = h(M_{upd} \oplus \beta)$$

Step 4:After receiving request message A, the RS firstly verifies the correctness of A by nonce β and the received M_{upd}.

$$Check\ A \stackrel{?}{=} h(M_{upd} \oplus \beta)$$

If the above equation holds, the RS sends back the corresponding mutual authentication message (B, M_{upd}) by the computation method as same as the message A.

$$B = h(M_{upd} \oplus \alpha)$$

Step 5: Upon receiving the respond message (B, M_{upd}), the FAPI also verifies its correctness in advance as follows.

$$Check\ B \stackrel{?}{=} h(M_{upd} \oplus \alpha)$$

If the above equation holds, the FAPI and the RS complete the mutual authentication. Continuously, both of the FAPI and RS will update the session K with newly K' after the session of communication phase. We will describe the communication phase as detail in the next phase.

2.5 Communication phase

Step 1:The FAPI encrypts the request message for inserting, updating or retrieving the E-anamnesis with the session K as follows.

$$C_{FAPI}=E_K(ID_P \| ID_{DR} \| f_P \| M_2 \| T_3)$$

Then the FAPI sends the ciphertext C_{FAPI} to the RS, where M_2 is the message for dispatch, update or insertion; T_3 is the current timestamp.

Step 2:Upon receiving C_{FAPI}, the RS firstly decrypts and checks the validity of C_{FAPI}. The RS performs the following computations.

$$D_K(C_{FAPI})=(ID_P \| ID_{DR} \| f_P \| M_2 \| T_3)$$

Check if $T_3'-T_3 \le \gamma$.

Check the validity of ID_p and ID_{DR}.

Continuously, the RS searches the stored fingerprint f_p' and compares if the received fingerprint f_p equals to f_p' or not.

If the identity of FAPI is authorized, the RS confirms what is the request M_2 and renews the nonce β with β'.

Step 2.1:If M_2 is a request for inserting E-anamnesis, the RS inserts the E-anamnesis into its database. At next, the RS uses the session key K to encrypt the response message (M_3, nonce α, β' and the timestamp T_4) into C_1 with the session key K.

$$C_1 = E_K(M_3 \oplus \alpha \| \beta' \| T_4)$$

, where α is another half key received in the past step.

Finally, the RS sends C_1 to the FAPI.

Step 2.2:If M_2 is a request for updating E-anamnesis, the RS updates the E-anamnesis with M_2. At the next, the RS generates and encrypts the response message (M_3, nonce α, β' and the timestamp T_4) into C_1 with the session key K.

$$C_1 = E_K(M_3 \oplus \alpha \| \beta' \| T_4)$$

Finally, the RS sends C_1 to the FAPI.

Step 2.3:If M_2 is a request for retrieving E-anamnesis, the RS uses the ID_P as an index key to query the corresponding E-anamnesis. At next, the RS generates and encrypts the E-anamnesis, nonce α, β' and the timestamp T_4 into C_1 with the session key K.

$$C_1 = E_K(E\text{-}anammesis \oplus \alpha \| \beta' \| T_4)$$

Finally, the RS sends C_1 to the FAPI.

Otherwise the RS rejects this request.

Step 3:After receiving the response message C_1, the FAPI decrypts the ciphertext with the session key K.

$$D_K(C_1) = (E\text{-}anammesis \oplus \alpha^* \| \beta' \| T_4)$$

In order to identify the identity of the RS, the FAPI performs the following computations.

Check if $T_4' - T_4 \le \gamma$

Check $\alpha * \stackrel{?}{=} \alpha$

If it is holds, the FAPI acquires the patient's E-anamnesis by following computation.

$$E\text{-}anammesis = E\text{-}anammesis \oplus \alpha \oplus \alpha^*$$

To avoid the potential attacks, the FAPI renews the nonce α', then uses the α' and the received β' to regenerate the newly session key K' based on the difficulty of DLP (Discrete Logarithm Problem).

$$K' = g^{h(\alpha' \| \beta')}$$

Afterward, the FAPI encrypts the message digest as the mutual authentication message C_2 with the old session key K as follows.

$$C_2 = E_K(\alpha' \| \beta' \| K')$$

Then the FAPI sends C_2 to the RS.

Step 4: Upon receiving the mutual authentication message, the RS firstly decrypts it by using the old session key K. The equation is as follows.

$$D_K(C_2) = (\alpha' \| \beta^* \| K')$$

If the validity of β^* can be confirmed, the RS also uses α' and β' to regenerate the newly session key K' as follows.

$$K' = g^{h(\alpha' \| \beta')}$$

Then the RS sends the succeed in upgrading message M_4 back to the FAPI. Afterward, the RS replaces the session key K with K' immediately.

Step 5: After receiving and verifying the validity of the response message M_4, the FAPI executes the procedure of replacing session key K with K'.

Thus, both of the FAPI and RS not only complete the mutual authentication but also update their session K with newly K' after the session of communication phase.

3. Analysis and Discussion

In this section, we discuss the security and the requirement of our online authorization scheme. It deserves to be mentioned that the biometric fingerprint is unique as their identity. Therefore, both the identities of the patient and the doctor are counterfeited infeasible.

3.1 Resist attacks

3.1.1 Denial of service attack issue

The adversary may want to palsy the services of the server RS by sending some meaning or unmeaning authentication messages. But these illegal requests will be conscious by following equations.

Check if $T_1' - T_1 \le \gamma$.

Check if ID_p is valid or not.

Check if ID_{DR} is valid or not.

Check $Y \stackrel{?}{=} h(C_P \oplus f_P)$

It's very clearly that our scheme is effective to prevent the DoS attack.

3.1.2 Device losing attack issue

If there unfortunately has a device lose, or the Health-Card has been stolen. It's still safely, because of the patient's personal fingerprint is unique. Therefore, the adversary cannot prove his or her identity and pass the examination equation in authentication phase as follows.

$$f_P \stackrel{?}{=} f_P'$$

Meanwhile, the adversary cannot get the E-anamnesis or use the stolen Health-Card to have an examination by any trick.

3.1.3 Forgery attack issue

Since the authentication message Y contains C_P and f_P. It is impossible for an adversary to forge a legal authentication message with C_p and biometric fingerprint f_p such as $Y = h(C_p \oplus f_p)$. Our scheme can withstand of forgery attack.

3.1.4 Parallel session attack issue

If there has a possible our authentication messages are intercepted by the adversary, he or she can do nothing. The certificates are given in below.

$$C_P = E_K(ID_P \| ID_{DR} \| \alpha \| T_1)$$

$$Y = h(C_P \oplus f_P)$$

The authentication message (C_p, Y) is sent to RS from P.

Another authentication message (C_{RS}, Z) is responding to P from RS.

$$C_{RS} = E_K(ID_{RS} \| \alpha \| \beta \| T_2)$$

$$Z = h(C_{RS} \oplus \beta)$$

Without any knowledge of α or β, the adversary cannot modify the authentication proofs Y or Z. Even he or she intends to forge a legal authentication message by falsifying a biometric fingerprint f_p. And the request will be rejected or be terminated because of the biometric fingerprint f_p is unique and the equations are not holds in below.

$$Y \stackrel{?}{=} h(C_P \oplus f_P)$$

$$Z \stackrel{?}{=} h(C_{RS} \oplus \beta)$$

Consequently, the adversary won't achieve his illegal goals.

3.1.5 Replay attack issue

In authentication phase, the RS will verify the validly of timestamp T_1 when he or she has received the authentication message. Also the FAPI will verify the correctness of timestamp T_2 when he or she has received the authentication message. Hence, it will be detected if the adversary replays the illegal authentication message. For this reason, this attack will not happen in our scheme.

In addition, the session key will be renewed during the communication has been done. The operations are as follows. First, the FAPI calculates a new synchronization request message A including the update massage M_{upd} and nonce β.

$$A = h(M_{upd} \oplus \beta)$$

The RS firstly examines the identity of FAPI after receiving. Furthermore, the RS similarly calculates an acknowledge message B and sends back to the FAPI.

$$A \stackrel{?}{=} h(M_{upd} \oplus \beta)$$

$$B = h(M_{upd} \oplus \alpha)$$

Finally, both RS and FAPI renew their session key K after the FAPI successfully verify the acknowledge message B.

3.2 Mutual authentication issue

In our proposed scheme, the verifiable proofs are given to verify the legality of each identity and to exchange their authorization information. Thus the adversary impersonates the legal user or server to cheat another one to get the E-anamnesis impossible. We will discuss it step by step in below.

First of all, the RS can verify P by inspecting the following equations.

$$Y \stackrel{?}{=} h(C_p \oplus f_p)$$

Similarly, P can verify RS by inspecting the following equations.

$$Z \stackrel{?}{=} h(C_{RS} \oplus \beta)$$

Due to the values of C_p, C_{RS}, the nonce α and β are computed by encrypting with the session key as follows:

$$C_p = E_k(ID_P \| ID_{DR} \| \alpha \| T_1)$$

$$C_{RS} = E_k(ID_{RS} \| \alpha \| \beta \| T_2)$$

The verifiable proof of RS can be done as follows:

$$Y \stackrel{?}{=} h(C_P \oplus f_P)$$

$$= h(ID_P \| ID_{DR} \| \alpha \| T \oplus f_P)$$

The verifiable proof of P can be done as follows:

$$Z \stackrel{?}{=} h(C_{RS} \oplus \beta)$$

$$= h(ID_{RS} \| \alpha \| \beta \| T_2 \oplus \beta)$$

Therefore, our scheme satisfies the essential requirement of mutual authentication by checking above equations.

3.3 Prevent illegal access issue

In registration phase of our proposed scheme, the HSO distributes each physician a certificate aim at their limits of authority. Consequently, the HSO also offers each physician the inquire authority of E-anamnesis aim at their limits of authority. As the authority feature, no one can access the E-anamnesis and medicine records without authority's authorization. Even if the adversary can intercept the ciphertext including the E-anamnesis sends from the HSO, but he or she has no competence to decrypt the acknowledge message. Therefore, prevent illegal access issue can be hold.

3.4 Non-Repudiation issue

In such design, as the authentication information or synchronization request are encrypted with sender's signature or contains his or her biometric fingerprint. Consequently, the participants can get the related non-repudiation proof during the communication. In the authentication phase, the server will decrypt the ciphertext and verify the correctness of the patient's signature by using their session key and the patient's public key, respectively. The verification equations of each participator are as follows.

At the FAPI side, the non-repudiation proofs are as follows:

$$Sig_P = S_{SK_P}(ID_P \| ID_{DR} \| \alpha \| T_1)$$
$$C_P = E_K(ID_P \| ID_{DR} \| \alpha \| T_1)$$
$$Y = h(C_P \oplus f_P)$$

At the server side, the non-repudiation proofs are as follows:

$$D_K(C_P) = (ID_P \| ID_{DR} \| \alpha \| T_1)$$
$$V_{PK_P}(Sig_P) \stackrel{?}{=} (ID_P \| ID_{DR} \| \alpha \| T_1)$$
$$Z = h(C_{RS} \oplus \beta)$$

Hence, this issue manifest that our scheme can achieve the requirement of non-repudiation which we have mentioned above.

4. Conclusion

Due to our proposed scheme presents an online authentication protocol and E-anamnesis management system that achieves the following goals.

(1) Against possibly attacks.

(2) Mutual authentication.

(3) Prevent of illegal access.

(4) Non-repudiation.

We proposed a based on electronic medical record system with online authorization control and authentication scheme such that against attacks, mutual authentication, prevent of illegal access, and non-repudiation can be guaranteed.

In the future, we hope this fingerprint and digital signature techniques can be widely adopted in any necessary medical treatment system. Also it has contributed to improve the quality of medical examination, medical security and medical efficiency.

References

[1] Ashrafi, M. Z. and Ng, S. K., "Privacy-preserving e-payments using one-time payment details," *Computer Standards and Interfaces*, Vol. 31, No. 2, pp. 321-328, 2009.

[2] Chien, H. Y., **"**New efficient user authentication scheme with user anonymity facilitating e-commerce applications," *The 9th IEEE International Conference on E-Commerce Technology and the 4th IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC-EEE 2007)*, pp. 461-464, 2007.

[3] Hu, L., Yang, Y. and Niu, X., "Improved Remote User Authentication Scheme Preserving User Anonymity," *Fifth Annual Conference on Communication Networks and Services Research (CNSR '07)*, pp. 323-328, 2007.

[4] Huang, E. W. and Liou, D. M., "Performance Analysis of a Medical Record Exchanges Model," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 11, No. 2, pp. 153-160, 2007.

[5] Hwang, S. Y., Wen, H. A. and Hwang, T., "On the security enhancement for anonymous secure e-voting over computer network," *Computer Standards & Interfaces*, Vol. 27, No. 2, pp. 163-168, 2005.

[6] Liao, Y. P. and Wang, S. S., "A secure dynamic ID based remote user authentication scheme for multi-server environment," *Computer Standards & Interfaces*, Vol. 31, No. 1, pp. 24-29, 2009.

[7] Liu, J. Y., Zhou, A. M. and Gao, M. X., "A new mutual authentication scheme based on nonce and smart cards," *Computer Communications*, Vol. 31, No. 10, pp. 2205-2209, 2008.

[8] Masseroli, M. and Marchente, M., "X-PAT A: Multiplatform Patient Referral Data Management System for Small Healthcare Institution Requirements," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 12, No. 4, pp. 424-432, 2008.

[9] Matsunami, K., "Clinical Supporting System developed with Filemaker Pro -Collaboration of paper medical record with electronic preservation-," *IEEE/ICME International Conference on Complex Medical Engineering, (CME 2007)*, pp. 323–326, 2007.

[10] Yang, W. H. and Shieh, S. P., "Password authentication scheme with smart cards," *Computers & Security*, Vol. 18, No. 8, pp. 727–733, 1999.

[11] Yu, Y., Xu, C., Huang, X. and Mu, Y., "An efficient anonymous proxy signature scheme with provable security," *Computer Standards & Interfaces*, Vol. 31, No. 2, pp. 348-353, 2009.