10

A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security

Ping Wang[1], Chih-Chiang Ku[1] and Tzu Chia Wang[2]
[1]*Department of Information Management, Kun Shan University,*
[2]*Institute of Computer and Communication Engineering,*
National Cheng Kung University,
Taiwan

1. Introduction

The number of commercially-available web-based services is growing rapidly nowadays. In particular, cloud computing provides an efficient and economic means of delivering information technology (IT) resources on demand, and is expected to find extensive applications as network bandwidth and virtualization technologies continue to advance. However, cloud computing presents the IT industry not only with exciting opportunities, but also with significant challenges since consumers are reluctant to adopt cloud computing solutions in the absence of firm guarantees regarding the security of their information.

Two fundamental issues arise when users applying cloud computing to software as a service (SaaS). First, if enterprise data is to be processed in the cloud, it must be encrypted to ensure its privacy. As a result, efficient key management schemes are required to facilitate the encryption (and corresponding decryption) tasks. Second, as the sophistication of the tools used by malicious users continues to increase, the data processed in the cloud is at increasing risk of attack. Consequently, there is an urgent requirement for robust authentication schemes to ensure that the data can be accessed only by legitimate, authorized users.

Network attacks such as phishing or man-in-the-middle (MITM) attacks present a serious obstacle to consumer acceptance of cloud computing services. According to reports released by privacy watchdog groups in the US, more than 148 identity theft incidents, affecting nearly 94 million identities, occurred in 2005 in the US alone (Mark, 2006). Identity theft is therefore one of the most severe threats to the security of online services. As a result, it is imperative that SaaS providers have the means to authenticate the identity of every user attempting to access the system. Due to the non-denial requirements of remote user identity authentication schemes, this is most commonly achieved using some form of biometrics-based method.

The term "biometrics" describes a collection of methods for identifying individuals based upon their unique physiological or behavioral characteristics (Furnell et al. 2008). Generally speaking, the physiological characteristics include the individual's fingerprint, vein pattern, DNA and shape of face, while the behavioral characteristics include the handwriting dynamics, voice and gait. Automated biometric recognition systems are now widely used

throughout the automotive; IT and banking industries (see Figs. 1 and 2). For example, Miura et al. (2005) developed a biometric authentication system based on the individual's finger vein for accomplishing secure online authentication over small devices such as notebook computers, cell phones, and so on.

Fig. 1. Fingerprint scanner and smart card reader

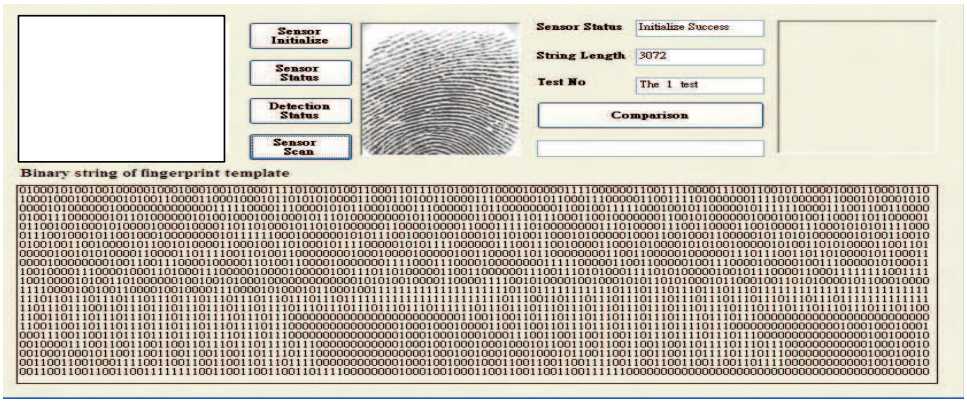


Fig. 2. Sensor-based scanning of user fingerprint template

However, existing biometric authentication systems cannot absolutely guarantee the identity of the individual. For example, biometric features such as the fingerprint may be acquired surreptitiously and then used by a malicious user. Similarly, even in multi-factor authentication methods such as smart cards, in which the biometric information is protected using a password, the password may be cracked by network hackers and the biometric information then copied and counterfeited. These proposals are invariably based on the assumption of employee honesty. Unfortunately, this assumption cannot also be guaranteed in practical applications, and many real cases have been reported in which dishonest interior staff have stolen users' authentication details from the authentication database and have then used these details to acquire the customers' private information for financial gain (see Fig.3).

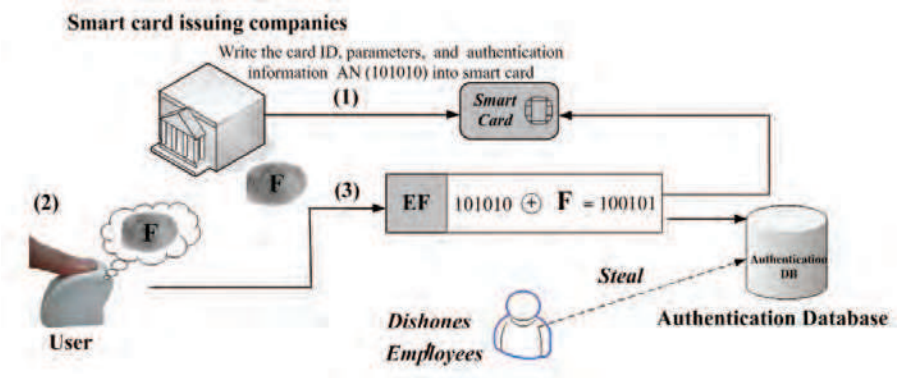


Fig. 3. Theft of biometric features by dishonest staff

To resolve the security issues described above, the present study proposes a new remote authentication scheme based on a secret-splitting concept. In the proposed approach, part of the biometric data is encrypted and stored on a smart card, while part of the data is encrypted and stored on a server (see Fig. 4). This approach not only resolves the problem of data abuse by interior staff, but also helps protect the users' information against malicious attack such as hacking into the Certificate Authority (CA) since to counterfeit the entire biometric information, dishonest staff or hackers must simultaneously decrypt two secret keys rather than just one.

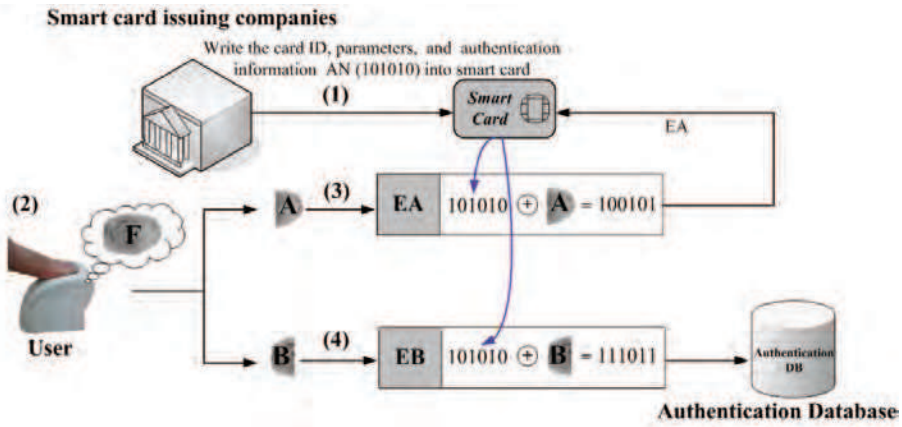


Fig. 4. Proposed authentication scheme based on secret-splitting

In addition to the secret-splitting concept, the proposed authentication scheme utilizes the Diffie-Hellman key exchange / agreement algorithm (Diffie & Hellman, 1976) to guarantee the security of the data transmissions between the terminal and the server. The main differences between the scheme proposed in this study and existing methods can be summarized as follows: (i) the smart card stores only part of the fingerprint template used in the identity authentication process. As a result, the user's identity is protected even if the card is lost or stolen. (ii) the template information stored on the smart card and server,

respectively, is independently encrypted. Consequently, the information obtained by a hacker or dishonest member of staff from a successful attack on the authentication database is insufficient to pass the liveness test.
A remote authentication scheme based on a secret-splitting concept is proposed for resolving the problem of user privacy in cloud-computing applications. In contrast to existing multi-factor authentication schemes, the proposed method minimizes the threat of attacks by dishonest interior employees since only a subset of the information required to pass the liveness test is stored on the user authentication database.
The remainder of this chapter is organized as follows. Section 2 briefly reviews the essential properties of identity authentication schemes and presents the related work in the field. Section 3 introduces the remote identity authentication scheme proposed in this study. Section 4 examines the robustness and computational efficiency of the proposed approach. Finally, Section 5 presents some brief concluding remarks.

2. Existing multi-factor authentication methods

Remote authentication is essential in ensuring that only legitimate individuals are able to access a network and make use of its resources. Typically, remote authentication is achieved using one of the following well-known schemes: (1) user account / password, (2) network address / domain name, (3) shared secret keys, (4) public keys, (5) digital signatures, (6) biometric authentication, (7) digital certificates, or (8) smart cards. Figure 5 shows a typical authentication procedure using a smart card in conjunction with the user's fingerprint.

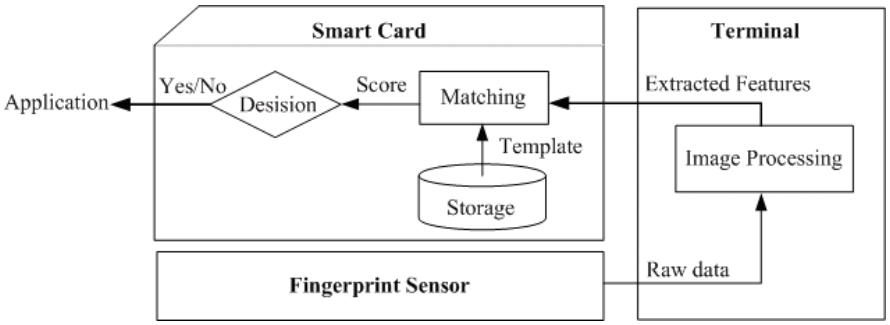


Fig. 5. Remote authentication using smart card and fingerprint

Password-based authentication schemes have the advantage of simplicity, but are reliant upon the user memorizing the password and remembering to modify it periodically in order to maintain the security of their account. Smart cards, in which the user's identity authentication information is encrypted on an embedded chip, have a number of benefits compared to traditional password-based methods, namely (i) the user's information is protected by a simple Personal Identity Number (PIN); (ii) the risk of identity theft is minimized by means of sophisticated on-chip defense measures; and (iii) single smart cards can be programmed for multiple uses, e.g. banking credentials, medical entitlement, loyalty programs, and so forth. Consequently, various multi-factor authentication schemes based upon smart cards and integrated biometric sensors have been proposed.
In a pioneering work of multifactor authentication schemes, For example, J.K. Lee et al. (2002) proposed a remote identity authentication scheme in which a smart card was

integrated with a fingerprint sensor. In the proposed approach, the smart card, a secret password, and the user's fingerprint were taken as inputs in the login process and the fingerprint minutiae, encrypted with the time stamp and the user's authentication template, were then compared with the authentication value stored on the card. To enhance the security of the ElGamal public key system (ElGamal, 1985) used in J.K. Lee et al. (2002), the encryption parameters were randomly generated in accordance with both the user's fingerprint minutiae and the time stamp. However, while the proposed method is therefore robust toward replay attacks, clock synchronization is required at all the hosts, which is a significant challenge in open network environments.

Kim et al. (2003) proposed an integrated smart card / fingerprint authentication scheme in which a password list was not maintained at the server such that the users were able to change their passwords at will. Moreover, protection against replay attacks was provided by means of Nonce technology, thereby avoiding the need for clock synchronization at the hosts. However, Scott (2004) showed that the Nonce-based design rendered the system vulnerable to imitation attacks given the collection by a hacker of a sufficient number of network packets to calculate the authentication value.

Later on, Lin and Lai (2004) showed that under certain circumstances, the method proposed by Lee et al. was unable to resist identity masquerade attacks. Accordingly, the authors proposed a new scheme for enhancing the security of the method presented in J.K. Lee et al. (2002) by allowing the users to choose and change their passwords at will. However, Mitchell and Tang (2005) showed that the method proposed by Lin and Lai also contained a number of serious flaws, most notably (i) hackers may simply copy the fingerprint from the imprint cup; (ii) the time stamp generated during a legal login procedure may be detected by a malicious user and then modified in order to login illegally at some future point in time; and (iii) the system contains no rigorous mechanism for preventing malicious users from using old passwords to perform an illegal login operation when the legitimate users change their passwords.

Recently, Fan et al. (2006) proposed a three-factor remote authentication scheme based on a user password, a smart card and biometric data. Importantly, in the proposed approach, the server only stores an encrypted string representing the user identity. That is, the biometric data is not revealed to any third party; including the remote server. The scheme is implemented using a two-step procedure. In the first step (the registration step), an encrypted user template is constructed by mixing a randomly-chosen string with the biometric characteristics of the user via an exclusive-or operation (XOR). In the second step (the login step), the fingerprint minutiae obtained via a sensor are encrypted using a second randomly-chosen string, and the two strings are then sent to a sensor for matching. The scheme has the advantage that all three security factors (the password, the smart card and the biometric data) are examined at the remote server, i.e., the system is a truly three-factor remote authentication system. Furthermore, the authentication process performed at the remote server does not require the exact value of the user's biometric data to be known. As a result, the security of the user's biometric information is improved. However, when the registration process is performed in a centralized way (e.g., a central Certificate Authority (CA) is used to issue certified users with a certificate), the scheme is vulnerable to the theft of the user's fingerprint minutiae by interior dishonest staff. In other words, while the scheme preserves the privacy of the users in the login and authentication phases, the security of the biometric data is not guaranteed during the registration phase.

3. A secret-splitting remote authentication scheme

This section proposes a novel remote authentication protocol for network services based on the secret-splitting concept. The proposed protocol comprises three phases, namely the initialization phase, the registration phase, and the authentication phase (see Fig. 6).

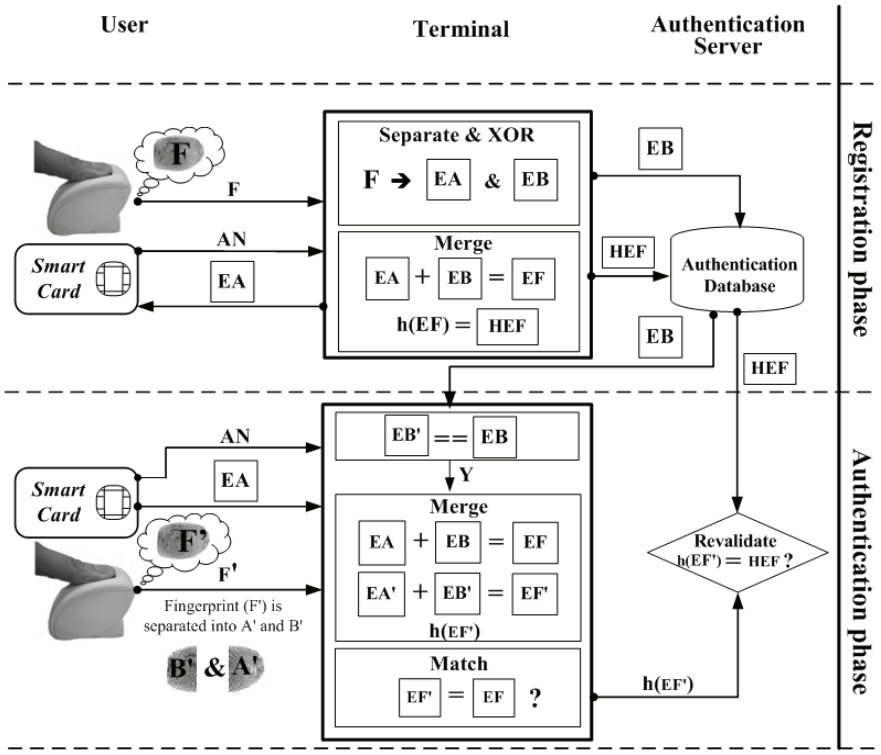


Fig. 6. Proposed fingerprint matching concept

In the initialization phase, the manufacturer produced a smart card and wrote a set of unique security parameters (AN) into it. In the registration phase, the user registers with a CA organization, and verifies their legal identity by means of traditional physical identity documents such as an identity card or a social security card. Encrypted fingerprint template A (EA') is generated from the information extracted by a fingerprint scanner (EA) and the smart card information obtained from a card reader (AN), and the remaining part of the encrypted fingerprint template B (EB') is directly extracted from the authentication database. Once the two templates (EA', EB') have been combined into a complete template by the terminal, the comparison results are sent to the server to verify the legality of the user, that is, (EF = EF'). Note that this step is designed to prevent counterfeit attacks in which a malicious hacker sends a "legal user" message directly from the terminal in order to deceive the server.

Fig. 7 presents the function flow diagram of the proposed remote authentication scheme. The details of each phase in the scheme are presented in Sections 3.1~3.3.

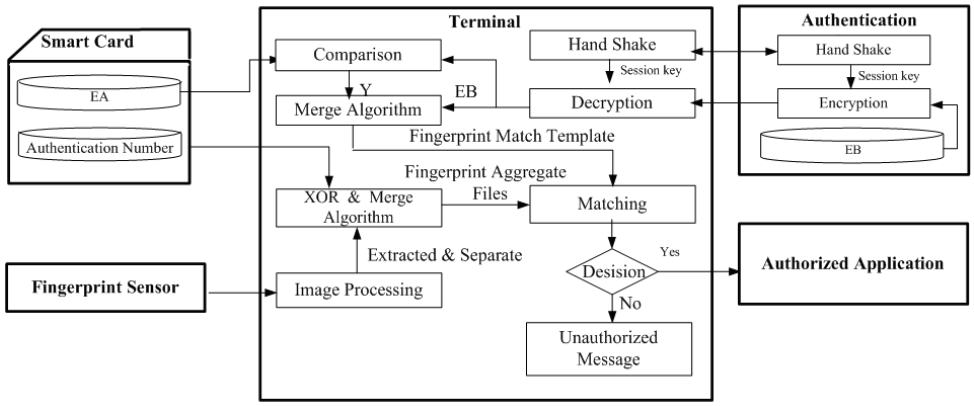


Fig. 7. Function flow diagram of proposed remote authentication scheme

3.1 Initialization phase

When the smart card manufacturer accepts an order from the CA, it writes various security parameters into the cards (e.g., the card number or authentication number (AN)) and then sends the cards to the CA. The detailed procedure is shown in Fig. 8

Step 1.1: Manufacturer randomly chooses a large prime number p and determines its root α.

Step 1.2: Manufacturer generates a unique Authentication Number (AN) based on a pre-defined coding rule.

Step 1.3: Manufacturer randomly selects a 128-bit string K as a key for symmetric encryption and keeps (p, α, AN, K) secret.

Step	Executor	Actions
1.1	*Manufacturer*	Randomly choose a large prime number *p* and determines its root α
1.2	*Manufacturer*	Generate a unique Authentication Number (*AN*)
1.3	*Manufacturer*	Randomly select a 128-bit string *K* as a key for symmetric encryption and keep [*p*, α, *AN*, *K*] $_{\text{Smart card}}$ secret.

Fig. 8. Initialization phase

3.2 Registration phase

The user registers with the CA and receives a smart card once he or she has confirmed their legal identity using some form of physical identity document. As shown in Fig. 9, the registration phase comprises five steps, namely:

Step 2.1: Let user U_i with identity ID_i be about to register with the server. The user chooses a card password, PWi , the password is then saved to the smart card, and then protected by the encryption mechanism of smart card.

Step 2.2: The fingerprint image of User U_i is obtained via a sensor and the minutiae are extracted from this image to form a fingerprint template F_i. The terminal separates F_i into two parts, F_{iA} and F_{iB}, where F_{iA} and F_{iB} represents part A and part B of fingerprint template, respectively.
Step 2.3: The terminal computes $EA_i = h(F_{iA} \oplus AN)$, $EB_i = h(F_{iB} \oplus AN)$, and $HEF_i = h(EA_i \cup EB_i)$, where $\cup$ is a merge operation and h(.) is a public one-way hash function.
Step 2.4: The terminal sends (ID_i, hEB_i, p, α, K, HEF_i) to the server over a secure channel
Step 2.5: The terminal stores (ID_i , PW_i, hEA_i) in the smart card.

Step	Executor	Actions
2.1	U_i	Determine a card password PW_i
2.2	U_i *Terminal*	Form a fingerprint template F_i using the fingerprint minutiae obtained via a sensor. (Note that F_i represents the fingerprint template of user *Ui*.) Separate F_i into two parts, F_{iA} and F_{iB} .
2.3	*Terminal*	Compute $EA_i = F_{iA} \oplus AN$, $EB_i = F_{iB} \oplus AN$ $HEF_i = h(EA_i \cup EB_i)$
2.4	*Terminal* ➔ *Server*	Send (ID_i, hEB_i, p,α,K, HEF_i)
2.5	*Terminal*	Store (ID_i , PW_i , hEA_i) on smart card
	Terminal ➔ U_i	[ID_i , PW_i, hEA_i, p ,α, AN, K] Smart card

Fig. 9. Registration phase

3.3 Authentication phase

Users insert their smart card, containing a partial authentication template into a card reader and a login request is then sent to the authentication server. The fingerprint information is checked using the following eight-step procedure (see Figs. 10 and 11):
Step 3.1: User U_i inputs his or her password PW_{i*} into the terminal. If the password is correct, the AN is extracted; else the login request is rejected.
Step 3.2: Users "provide their fingerprint via a sensor, and the fingerprint is then compared with that stored on the authentication server. Let F_{i*} represent the fingerprint minutiae extracted by the sensor. The terminal separates F_i* into F_{iA*} and F_{iB*}, and then computes $EA_{i*} = F_{iA*} \oplus AN$ and $EB_i* = F_{iB*} \oplus AN$. The two parts (i.e., EA_{i*} , EB_{i*}) are then merged to generate the full biometric template of the user, i.e., $EF_{i*} = EA_{i*} \cup EB_{i*}$. The server sends EBi to the terminal for comparison purposes in order to verify the user's legal identity. If a match is obtained (i.e., $EB_i == EB_{i*}$), the authentication process proceeds to Step 3.3; else it terminates.
Step 3.3: (Diffie-Hellman key exchange algorithm). The terminal randomly selects a number X_A such that $X_A < p$, and then computes $Y_T = \alpha^{X_A} \bmod p$ and $Y_A = ID_i \,||\, Y_T$, where α and p are both stored on the smart card. The terminal then sends YA to the server. Similarly, the server randomly selects a number X_B such that $X_B < p$, computes $Y_B = \alpha^{X_B} \bmod p$, and then sends Y_B to the terminal.

Step 3.4: The terminal uses Y_B to compute the session key $SK = (Y_B)^{X_A} \bmod p$. Similarly, the server uses Y_A to compute the common session key, $SK = (Y_A)^{X_B} \bmod p$. Note that SK is a shared secret between the terminal and the server.

Step	Executor	Actions
3.1	U_i	Input password PW_i^*
	Terminal	Examine PW_i^* and gain AN
3.2	U_i	Scan finger to provide information required to construct fingerprint template F_i^*
	Terminal	Separate F_i^* into F_{iA}^* and F_{iB}^*, where $EA_i^* = F_{iA}^* \oplus AN$, $EB_i^* = F_{iB}^* \oplus AN$, and $EF_i^* = EA_i^* \cup EB_i^*$
	Server ➔ *Terminal*	Extract EB_i from server. If a match is obtained (i.e., $EB_i == EB_i^*$), go to Step 3.5; else terminate the authentication process
3.3	*Terminal*	Randomly select a number X_A such that X_A <p Compute $Y_T = \alpha^{X_A} \bmod p$.
	Terminal ➔ Server	$Y_A = ID_i \,||\, Y_T$
	Server	Randomly select a number X_B such that X_B <p
	Server ➔ *Terminal*	Send Y_B to terminal
3.4	*Terminal*	$SK = (Y_B)^{X_A} \bmod p$
	Server	$SK = (Y_A)^{X_B} \bmod p$

Fig. 10. Authentication phase (Steps 3.1~3.4).

Step 3.5: The server generates a one-time symmetric key RK, computes $M = E_{sk}(EB_i \,||\, RK)$, and then sends M to the terminal. Note that $E_{sk}(.)$ denotes a symmetric encryption function (such as the *AES* method) based on the session key SK.

Step 3.6: The terminal acquires EB_i and RK by performing the decryption process $D_{SK}(M)$, and extracts EA_i from the smart card. EA_i and EB_i, are then merged to obtain $EF_i = EA_i \cup EB_i$, where $D_{sk}(.)$ denotes a symmetric decryption function based on the session key SK.

Step 3.7: The terminal compares EF_i^* and EF_i. If a match is obtained, the legal user is successfully identified; else the terminal sends $RM = E_{RK}(h(EF_i) \,||\, CM)$ to the server for reconfirmation purposes. Note that E_{RK} is a symmetric decryption function based on the key RK, and CM is a message indicating the matching result.

Step 3.8: The server re-verifies the match $h(EF_i) == HEF_i$. If a match is obtained, the server accepts the login request of U_i; else it rejects the request.

Step	Executor	Actions
3.5	*Server*	Generate a one-time private key RK
	Server➔*Terminal*	Compute $M=E_{sk}(EB_i \| \| RK)$ and send M
3.6	*Terminal*	*Decrypt* $D_{SK}(M)$ to obtain EB_i and RK Extract EA_i using card reader, then merge two parts of template, i.e., $EF_i = EA_i \cup EB_i$
3.7	*Terminal*	If Match ($EF_i^* == EF_i$), then CM=true; else CM=false
	Terminal ➔*Server*	Return the Comparison Message (CM) and EF_i with encryption $RM=E_{RK}(h(EF_i) \| \| CM)$
3.8	*Server*	*Decrypt* $D_{RK}(RM)$ to obtain $h(EF_i)$ and CM Verify ($h(EF_i) == HEF_i$) Accept the login request of U_i if match is obtained; else reject login request.

Fig. 11. Authentication phase (Steps 3.5~3.8).

Summarizing the procedures shown in Figs. 9~11, the overall sequence diagram of the proposed remote authentication scheme can be illustrated as shown in Fig. 12.

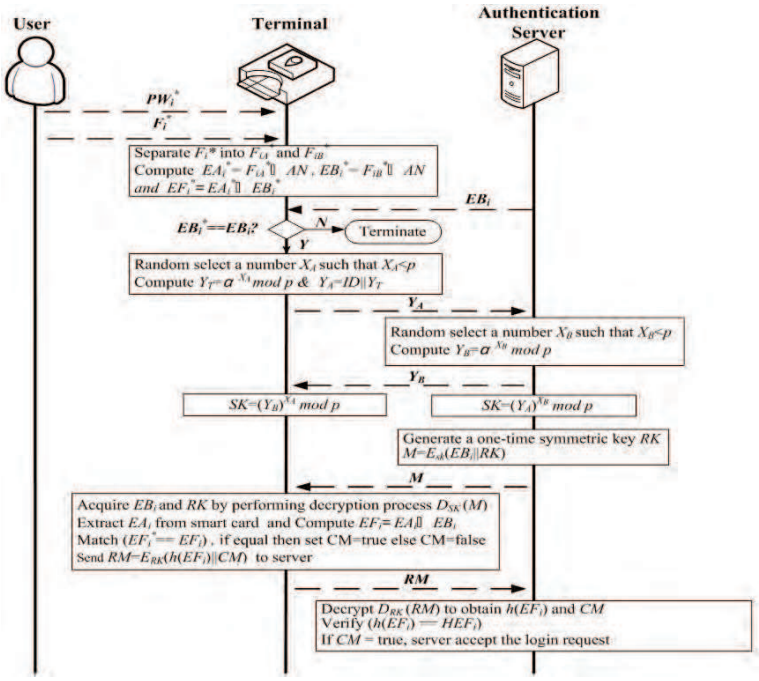


Fig. 12. Sequence diagram of proposed remote authentication scheme

4. The security performance and computational efficiency

This section discusses the security performance and computational efficiency of the proposed remote authentication scheme.

4.1 Security analysis

This sub-section demonstrates the robustness of the proposed authentication scheme toward three common forms of attack, namely (i) authentication factor attacks; (ii) network attacks; and (iii) interior attacks originating from the card-issuing organization.

4.1.1 Authentication factor attacks

Given a three-factor authentication scheme (i.e., password, smart card and user biometrics), a hacker requires all three factors in order to successfully complete the authentication process. It is possible that the smart card and password may be stolen or duplicated. However, in the scheme proposed in this study, the biometrics template is strongly protected using a secret-splitting technique. Thus, even if a hacker manages to obtain the partial fingerprint template EB_i, he or she cannot generate the partial template EA_i without possessing the knowledge of the authentication number (AN) stored on the smart card. Besides, hackers have no matters to generate the other part of biometrics template (EA_i), except they crack the program which is used for merging EA_i* and EB_i*, however, this program generally is an executive binary code and burn in the *ROM* of card issuing machine. In other words, it is extremely difficult for a hacker or a dishonest member of staff to obtain all three authentication factors for a particular user, and thus the proposed scheme is as safe as other multi-factor authentication schemes.

As described above, in the proposed approach, the biometric data of a user is separated into two parts (EA_i , EB_i), encrypted and stored on a smart card and a server, respectively. This approach not only preserves the privacy of the users in the login and authentication phases, but also helps protect the users' information against the theft of the user's fingerprint minutiae by interior dishonest staff.

4.1.2 Network attacks

This section demonstrates the robustness of the proposed authentication scheme toward three common types of network attack, namely (i) man-in-the-middle attacks, (ii) dictionary attacks, (iii) replay attacks.

Strong encryption authentication helps prevent *man-in-the-middle* attacks. In the proposed scheme, the authentication template, encrypted using a *128-bit* AES symmetric encryption algorithm, is split into two parts; stored on the smart card and the server, respectively. To prevent from the man-in-the-middle attacks, the data transmissions between the terminal and the server are protected by a session key generated using the Diffie-Hellman key exchange algorithm. Therefore, hackers are not easily able to steal the complete set of biometric data. Thus, the security of the biometric data is further enhanced since solving the Discrete-Logarithm Problem (DLP) in order to crack the Diffie-Hellman protected transmissions is extremely hard within a finite period of time [14]. In addition, the decryption process is further complicated (from the hacker's perspective) by the fact that the session key is changed on a periodic basis. Thus, a hacker not only faces a major challenge in determining the AN of the smart card and the coding used to construct the partial authentication template EA_i, but also encounters severe difficulties in cracking the encrypted transmission packets exchanged between the terminal and the server.

For *dictionary* attacks, cracking a password needs either weak password strength or large quantity of hash of the target password; two cases can be prevented by both strong hash function algorithms such as MD5 and the SHA family and long character password with numbers, mixed case, and symbols in Step 2.1.

Assume that a hacker has attained the formation of the terminal (AN, EA_i^* , EB_i^*) in Steps 3.1~3.4 from the terminal and smart card, and then launches a *replay attack* to counterfeit a legal user in the authentication process. In Step 3.5, a one-time session key (RK) is randomly generated by the server. This key is valid only for the current authentication process. In other words, old session keys cannot be re-used, and thus imitation attacks are thwarted.

4.1.3 Attacks originating within card issuing organization

This section demonstrates the robustness of the proposed scheme toward interior staff attacks in the registration phase and authentication phase, respectively.

Registration phase

In the registration process, the users scan their finger in order to provide the system with the fingerprint minutiae required to construct the finger template (see Step 2.2). The fingerprint template F_i, stored in the Random Access Memory (RAM) of the terminal is utilized only in the subsequent registration process. That is, to prevent exposure of the user's biometric data to any unauthorized third party, F_i and its related parameters are deleted as soon as the authentication process is complete. Therefore, interior staff and external hackers have little chance of acquiring F_i since it exists within the system for only a short period of time and, moreover, its location within the terminal RAM varies dynamically.

Authentication phase

As shown in Fig. 6, the three components of the authentication template generated in the proposed scheme are stored separately in the cards, terminal and servers ("on two different physical components, namely (i) EA_i is stored on the smart card; (ii) and (iii) EB_i is stored at the authentication server. Thus, even if the template data at the authentication server is stolen by a dishonest member of staff, the authentication process cannot be completed since the remaining template information is missing. In practice, a dishonest member of staff can only complete the authentication without password and smart card, except someone is capable of copying process by somehow copying the user's card and acquiring the user's fingerprint from the imprint cup.

4.2 Computational complexity

In this section, the computational complexity of the proposed scheme is compared with that of the schemes presented by Fan *et al.* (2006), Lin and Lai (2004), Kim *et al.* (2003) and J.K. Lee *et al*. (2002) (see Table 1). Among the various computations performed by the different schemes, the exponential operation in the decryption procedure (E) is the most time consuming. It is observed that the number of exponential operations in the schemes proposed by Lee *et al.* and Lin and Lai, respectively, is slightly higher than that in the proposed scheme and significantly higher than that in the scheme proposed by Fan et al. In addition, it is seen that the overall computational complexity of the scheme proposed in this study is slightly higher than that of the scheme proposed by Fan *et al*. due to the separation of the authentication data and the encryption of the symmetric keys during transmission.

Compared to the scheme proposed by Fan et al., the proposed scheme requires three additional exponential operations and two additional merge operations. However, the number of symmetric decryption operations is reduced by one, while the number of hash and XOR operations is reduced by three and one, respectively. Significantly, the scheme proposed by Fan *et al*. utilizes the Rabin algorithm (Rabin, 1979) to protect the symmetric keys during transmission. Whilst this approach reduces the number of exponential operations required, the security of the communications between the terminal and the

authentication server cannot be guaranteed in an open environment. By contrast, the scheme proposed in this study uses the Diffie-Hellman key exchange /agreement algorithm to protect the terminal-server communications. Thus, while a greater number of exponential operations are required (i.e., to solve the Discrete-Log Problem), the security of the transmissions is significantly improved relative to that in Fan *et al*.'s scheme.

It is acknowledged that the proposed scheme has certain limitations. For example, in the event that the user loses his or her smart card, the CA cannot immediately re-issue a new card since they do not possess the complete fingerprint template. In other words, the users must repeat the registration process in order to obtain a new card. Furthermore, the computational complexity of the proposed scheme is slightly higher than that of existing schemes. However, compared to existing methods, the proposed scheme ensures the security of the users' biometric information even if the contents of the authentication database are stolen. In other words, the proposed scheme achieves a compromise between the need to reduce the computational cost of the remote authentication process and the need to minimize the security threat posed by dishonest interior staff.

Scheme	Characteristic		
	Computational cost of login and authentication phases	Store complete biometric template	Clock synchronization
Proposed scheme	4E+3SE+3SD+H+2X+2M	No	No
Fan et al. (2006)	E+3SE+4SD+4H+3X	Client	No
Lin and Lai (2004)	5E+3H+4X	Client	Yes
Kim et al. (2003) (Timestamp-based)	4E+2H	Server	Yes
Kim et al. (2003) (Nonce-based)	4E+1H	Server	No
J.K. Lee et al. (2002)	7E+2H+2X	Server	Yes

Table 1. Comparison of related schemes (revised from Lee S.W. et al., 2005)

Note that *E* represents the computational time required to perform modular exponentiation; SE denotes the computational time required to perform modular symmetric encryption; *SD* is the computational time required to perform modular symmetric decryption computation; *H* denotes the computational time required to perform a one-way hash function; X is the computational time required to perform a modular exclusive-or operation; and *M* represents the computational time required to perform a modular merge operation.

5. Conclusions

This paper has presented a novel remote authentication scheme based on a secret-splitting concept for cloud computing applications. Compared to existing methods, the proposed scheme has a number of important advantages, namely (i) the users can choose passwords (PW_i) for their smart cards at will; (ii) the smart card and server each store a partial biometric template rather than the full template; and (iii) the partial templates are integrated only when the users have successfully completed the login process in the authentication phase. The proposed scheme is robust toward three common forms of attack, i.e., man-in-the-middle attacks, dictionary attacks and replay attacks. As a result, it provides an effective solution for enhancing the security of cloud computing applications, and is therefore beneficial to SaaS service providers in improving user acceptance of their services.

6. Acknowledgements

This study was supported partly by TWISC@NCKU, and by the National Science Council under the Grants Nos. NSC100-2219-E-006-001 and NSC 99-2219-H-168-001.

7. References

Diffie W. & Hellman M. E. (1976). Multiuser Cryptographic Techniques, *Proceedings of National Computer Conference*, New York, June 7-10, 1976

ElGamal T. (1985). A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *Proceedings of IEEE Transactions on Information Theory*, Vol.31, No. 4, pp. 469–472, ISSN 0018-9448

Fan C. I.; Lin Y. H. & Hsu R. H. (2006). Remote Password Authentication Scheme with Smart Cards and Biometrics, *Proceedings of 49th annual IEEE Global Telecommunications Conference (GLOBECOM)*, pp.1-5, San Francisco, California, USA, 27 Nov, 2006

Jeong J.; Chung M. Y. & Choo H. (2006). Secure User Authentication Mechanism in Digital Home Network Environments, *Lecture Notes in Computer Science (LNCS)*, Vol.4096, pp.345-354

Kim H. S.; Lee S. W. & Yoo K. Y. (2003). ID-based Password Authentication Scheme Using Smart Cards and Fingerprints, *ACM SIGOPS Operating Systems Review*, Vol.37, No.2, pp.32-41, ISSN 0163-5980

Lee J. K.; Ryu S. R. & Yoo K. Y. (2002). Fingerprint-based remote user authentication scheme using smart cards, *Electronics Letters*, Vol.38, No.12, pp.554-555, ISSN 0013-5194.

Lee S. W.; Kim H. S. & Yoo K. Y. (2005). Efficient nonce-based remote user authentication scheme using smart cards, *Applied Mathematics and Computation*, Vol.167, No.1, pp. 355-361, ISSN 0096-3003

Lin C. H. & Lai Y. Y. (2004). A flexible biometrics remote user authentication Scheme, *Computer Standards & Interfaces,* Vol. 27, No.1, , p.19-23, ISSN 0920-5489

Mark K. H. (2006). Data theft scandal - what we can learn from India Opinion, In: Offshoring, 6 Oct 2006. Available from http://services.silicon.com/offshoring/0,380000487 7,39163049,00.htm

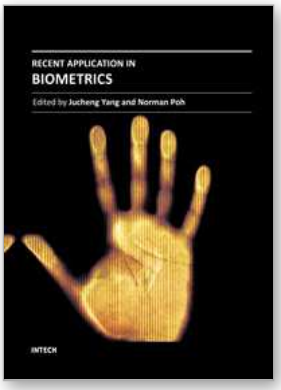
Mitchell C. J. & Tang O. (2005). Security of the Lin-Lai smart card based user authentication scheme, Technical Report, Royal Holloway, University of London, 2005 Available from from http://www.rhul.ac.uk/mathematics/techreports

Miura N.; Nagasaka A. & Miyatake T. (2005). Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles, *Proceedings of the 9th IAPR Conference on Machine Vision Applications (MVA2005)*, pp.347-350, Tsukuba Science City, Japan, 2005.

Pfitzmann A. (2008). Biometrics---How to Put to Use and How Not at All, In: TrustBus 2008, Furnell S.M.; Katsikas S.K. & Lioy A. (Ed.), LNCS 5185, pp. 1–7, Springer-Verlag, ISSN 0302-9743

Rabin M. O. (1979). Digitalized Signatures and Public-key Functions As Intractable As Factorization, *Technical Report of MIT/LCS/TR212, MIT Labatory*, Computer Science Cambridge, MA, USA

Scott M. (2004). Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints, *ACM SIGOPS Operating Systems Review*, Vol. 38, No. 2, pp.73-75, ISSN:0163-5980



Recent Application in Biometrics

Edited by Dr. Jucheng Yang

ISBN 978-953-307-488-7
Hard cover, 302 pages
Publisher InTech
Published online 27, July, 2011
Published in print edition July, 2011

In the recent years, a number of recognition and authentication systems based on biometric measurements have been proposed. Algorithms and sensors have been developed to acquire and process many different biometric traits. Moreover, the biometric technology is being used in novel ways, with potential commercial and practical implications to our daily activities. The key objective of the book is to provide a collection of comprehensive references on some recent theoretical development as well as novel applications in biometrics. The topics covered in this book reflect well both aspects of development. They include biometric sample quality, privacy preserving and cancellable biometrics, contactless biometrics, novel and unconventional biometrics, and the technical challenges in implementing the technology in portable devices. The book consists of 15 chapters. It is divided into four sections, namely, biometric applications on mobile platforms, cancelable biometrics, biometric encryption, and other applications. The book was reviewed by editors Dr. Jucheng Yang and Dr. Norman Poh. We deeply appreciate the efforts of our guest editors: Dr. Girija Chetty, Dr. Loris Nanni, Dr. Jianjiang Feng, Dr. Dongsun Park and Dr. Sook Yoon, as well as a number of anonymous reviewers.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821