International Journal of Engineering and Technology Vol. 1, No. 2, June, 2009
1793-8236

An Efficient and Reliable Three-Entity Remote User and Server Authentication Technique

C. Koner, *Member, IACSIT*, C. T. Bhunia, *Sr. Member, IEEE* and U. Maulik, *Sr. Member, IEEE*

***Abstract*— Authentication of remote user and server is a great research challenge in today's advanced wired and wireless communication. Recently Das proposed a flexible remote system authentication using smart card [7]. Xu et al. proved that Khan et al.'s fingerprint based remote user authentication is vulnerable to the impersonation and parallel session attack [10]. In this paper, we show that Das's scheme is not withstand the reverse XOR and adversary system attack. We also propose an improved remote user and server authentication that verifies the authenticity of user by user's password, smart card and biometric property of user. The technique is insulated from the reverse XOR, adversary system, impersonation and parallel session attacks**

***Index Terms*— Authentication, Remote System, Password, Smart card, Biometric.**

I. INTRODUCTION

User authentication technique ensures that a legitimate user is accessing the services provided by a remote server. Previously password based user authentication was the basic and popular authentication technique in public networks. Remote user password authentication technique is a scheme to authenticate a remote user who is communicating with a remote server over a public channel. Remote user password authentication technique is based on one-way hash function chaining, was first designed by Lamport in 1981 [2]. Haller [3] proposed secret key based one time password technique (a modified version of Lamport's technique) that eliminates hash function chaining and password set again problem of Lamport's technique. But in both of those techniques, it is required to maintain user password database in remote server. Thus, an attacker can hack and change the password of users and involvement of remote server is needed for change of user password. To solve the problem authentication token by mean smart card is introduced for storing the user information (Password, Identity etc). Remote user password authentication technique with smart card was developed by Chang and Wu in 1993 [4].

After that, there is history of advancement of remote user password authentication technology with smart card. Several new remote user password authentication techniques with smart card have been planed and developed. Remote user authentication using smart card, introduced by Hwang and Li in 2000 [5], is an application of ElGamal's [6] public-key scheme to authenticate a user. After that, few public-key based authentication techniques have been invented and improved. But all of the techniques check only the authenticity of user but can not check the authenticity of server. In 2006, Das et al. [7] developed a flexible remote user authentication scheme using smart card that authenticates user as well as remote sever. The remote server authentication is necessary by which the user can check whether he is communicating with the intended server or not. In all these techniques user authenticity is verified by applying only password (what user know) and smart card (what user have) but no biometric entity of user (what user are) is applied.

User biometric authentication is a technique to check a valid user by user physical characteristic. Human physical characteristics are called Biometric property such as Fingerprint, Voiceprint, Retinal scan and Face recognition etc. User fingerprint-based authentication technique was first proposed by Lee et al. in 2002 [8], is a biometric authentication to check the validity of a user by user biometric property. In 2006, Khan et al. [9] introduced modified version of Lee's techniques that requires only a secret key but in 2008 Xu et al. [10] showed that it is vulnerable to the parallel session attack and impersonation attack.

Three-Entity (3-E) user authentication technique is a scheme to authenticate a communicating user according to what you know (Password), what you have (Smart card), and what you are (Biometric entity). We propose an efficient and reliable three entity user authentication technique that verifies the authenticity of user as well as remote server. User authenticity is verified by applying password, smart card and biometric property of user simultaneously. Our 3-E technique is insulated from parallel session attack and impersonation attack. It has a user friendly password changing facility.

II. CRYPTANALYSIS OF DAS'S TECHNIQUE

We present a cryptanalysis of Das's remote system authentication technique in this section. Das showed that, although his technique is secured from replay, stolen verifier, impersonation, guessing and denial-of-service attack but his technique is still vulnerable to reverse XOR attack and

Chandan Koner is an Assistant Assistant Professor in the Department of Computer Science and Engineering, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India., he is pursuing PhD course. He is member of IACSIT and IAENG. (Phone No.+91-9434535556)

Chandan Tilak Bhunia is an Director, Bengal Institute of Technology and Management, Santiniketan, P.O. Doranda, West Bengal, Pin-731236, India. He is a Senior Member of IEEE and FIE.
(Phone No. +91-9434033157)

Ujjwal Maulik is currently a Professor in the Department of Computer Science and Technology, Jadavpur University, Kolkata, India. He is a Senior Member of IEEE.
(Phone No. 91-33-24131766)

adversary system attack. We demonstrate these attacks.

Reverse XOR attack: During the registration phase, the secret key x has to be applied. Now based on the reversible property of XOR operation, if the primary secret key of remote system (x) is hacked, user password (PW_i) is guessed and mode of hash function is leaked, then nonce, N_i can be easily obtained. Hence Das's technique is vulnerable to the reverse XOR attack.

Adversary system attack: Suppose the processors in remote system and card reader are very hasty and the transmission of data between user and server is happening in very speedily. In this type of communication, the timestamp of user Tu in user authentication phase and the timestamp of server Ts* in remote system authentication phase will be equal. During remote system authentication phase, remote system sends X_i [= h(N_i⊕ Tu⊕Ts*) or h (h (PW_i, ID_i)⊕ h(x) ⊕ T⊕ Ts*)] to the user over a public channel. As Tu and Ts* are same so X_i = h (N_i). Again suppose an adversary has stolen the user smart card for one time and just extract the N_i and mode of hash function is known to him so he can easily compute X_i which is h(x). Now if the adversary is also a user and accessing another server then he can send X_i to the user by that illicit sever over the public channel before the original server sent. Then user can easily certify that server as an authentic server and communicates with that illicit server. The adversary, thus, can trick the user by connecting him with a wrong server. Das's technique is therefore insecure from the adversary system attack.

III. The Proposed Three Entity Authentication Technique

Our proposed Three Entity (3-E) authentication technique is a collection of five parts, namely, User Enrollment Phase, User Login Phase, User Authentication Phase, Remote System Authentication Phase and User Password Change Phase.

User Enrollment Phase

To get access to the Remote Server S_R, firstly the Remote User U_R has to take entry to the S_R. In the execution of user enrollment phase, the U_R is enrolled to the S_R. This phase is executed only once for one U_R.

UE1: The user U_R chooses his identifier I and password P and sends to the S_R through a private channel. The user also imprints his biometric entity at the biometric device.

UE2: The S_R has received the enrollment request from U_R and executes the following tasks.

UE2.1: Computes G = h (I ⊕P ⊕B), where B is the extracted template of biometric entity of the U_R, h (.) is a one-way hash function and ⊕is a bitwise XOR operation.

UE2.2: Computes K= h (s) ⊕ G, where s is a secret key of S_R.

UE2.3: Stores the parameters {h (.), e, I, B, K and G} into a Smart Card C_S, where e is a secret number stored in each enrolled user's smart card.

UE2.4: Sends the C_S to the U_R through a private channel.

User Login Phase

This phase is executed every time when the U_R wants to access the S_R.

The U_R inserts his C_S to a card reader, enters his identifier I and password P′ and imprints his biometric entity B′ at the biometric device.

UL1: The C_S computes L= h (s) ⊕G ⊕h (I ⊕P′ ⊕B′). Then checks whether L is equal to the h(s) or not. If it is equal then C_S perform the following tasks otherwise rejects the login request.

UL2: Computes O = G ⊕h (T), where T is the current time of user login.

UL3: Computes N = h (h (e)⊕ K ⊕ h (T)).

UL4: Sends the login request {O, N, T} to the S_R through a public channel.

User Authentication Phase

This phase is executed after the login phase when the U_R wants to access the S_R.

UA1: The S_R has received the login request {O, N, T} at time T* and executes the following tasks.

UA1.1: Checks the difference between T* and T is valid time interval for transmission delay. If it is correct then the S_R performs the next tasks.

UA1.2: Computes N' = h (h (e) ⊕ h(s) ⊕ O).

UA1.3: The S_R checks whether N = N'. If it holds, the S_R accepts the login request of U_R. Otherwise the S_R rejects the login request of U_R.

Remote System Authentication Phase

The correctness of S_R is verified in this phase and executed when the remote user is authentic.

RSA1: S_R computes M= h (T** ⊕ h (T⊕h (s)⊕ h (I ⊕ P ⊕ B))) where T** is the current time of S_R.

RSA2: S_R sends (M, T**) to the U_R through a public channel. Suppose U_R receives (M, T**) at time T***.

RSA3: C_S checks the difference between T*** and T** is valid time interval for transmission delay. If it is correct then the C_S performs the next tasks.

RSA3.1: C_S computes M′= h (T** h (T⊕ K)) ⊕

RSA3.2: The C_S checks whether M = M'. If it holds, the S_R is correct and gives permission to U_R for accessing the resources of S_R. Otherwise U_R terminates the communication with the S_R.

User Password Change Phase

This phase is executed when the U_R wants to replace his password P by the new password P'.

The U_R inserts his C_S to a card reader, enters his identifier (I) and password (P) and imprints his biometric entity at the biometric device. The C_S verifies the entered I and P with the stored values of I and P in the C_S, and the biometric entity of U_R with the stored values of B in the C_S. If all of the verifications are passed correctly, then C_S executes the following tasks.

UP1: Asks the U_R to enter a new password and he chooses a new password P' and submits it.

UP2: Computes G′= h (I ⊕ P'⊕ B) and K'= h (s) ⊕G′

UP3: The P', G′ and K' are stored in the place of P, G and K respectively.

IV. Security Evaluation of OUR 3-E Technique

We analysis that how our Three Entity authentication technique is protected from the various security parameters. We discuss the defense of the technique from the various

attacks by which previous techniques are suffered.

a) Reverse XOR attack

In 3-E authentication technique, G [= h (I ⊕P ⊕B)] is computed in the registration phase. If P is guessed and mode of hash function is leaked by an adversary, he never gets G because G is a function of the biometric property B which is the physical characteristics of user. Without the physical existence of correct user, the B can not be obtained. As G will not get so K [= h (s) G] will not be obtained by adversary.

Hence 3-E technique is undoubtedly not vulnerable to the reverse XOR attack.

b) Adversary system attack

In remote system authentication phase, remote system sends M [= h (T**⊕ h (T ⊕ h (s)⊕ h (I⊕ P ⊕ B))) or h (T** ⊕ h (T ⊕K))] to the user over a public channel. For a very first system where T and T** are same M will not be equal to the h (K). So if an adversary extracts the K by stoling the user smart card for one time and mode of hash function is known to him then he never gets M. So the user always authenticates a correct server.

Hence 3-E technique is firmly secured from the adversary system attack.

c) Parallel Session Attack

In this attack an adversary eavesdrops the login request in login phase and sends it to the server in authentication phase. So the adversary can easily access the server's resources as a legitimate user can. Basically when the symmetric information is passed between the user and server in the login and authentication phases, this phenomenon is happened.

In our proposed 3-E authentication technique, the information exchanged between the user and the remote server in the login phase N [= h (h (e) ⊕ h(T))] and in the authentication phase N' [= h (h(e) ⊕(s) ⊕O)] are not symmetric. This means that our 3-E technique is insulated from parallel session attack.

d) Impersonation Attack

This attack happens when an adversary has stolen the user smart card and extracted the stored information. Then he constructs the login request and communicates with the server as a legitimate user. In impersonation attack an adversary acts as legitimate user to the server by forging the login request.

In our 3-E technique, if the adversary steals the user's smart card and extracts the stored value G and K but he could not able to construct N [= h (h (e) K h (⊕))] because it requires e. The user himself can not construct N because he also does not know e. So an adversary as well as a legitimate user can't forge a login request. Hence we can claim that our 3-E technique is secured from this attack.

User Password (P)	Smart card sends N to the remote server in user authentication phase.	Remote system sends M to the smart card in remote system authentication phase.
55736572	0114f18e	36e7a841
27734175	0a9d2eda	fc686b8c
7468656e	15f0912d	d04b71f0
74696361	86e0ad65	dc979d10
74696f6e	f36bab48	2a5e7312

V. RESULTS AND DISCUSSION

User Password (PW_i)	Smart card sends C_i to the remote server in user authentication phase.	Remote system sends X_i to the smart card in remote system authentication phase.
55736572	785b8d4d	fd48d41c
27734175	2f199456	3cb75052
7468656e	55714236	cefaeb42
74696361	e8f019a6	c0d7fa43
74696f6e	0421a554	fc788588

A) *Results of Das's Technique*

User Password (PW_i): User'sAuthentication
User Identifier (ID_i): IdentityofRemoteUser
Secret Key (x) of Remote System: 71
Secret number (y) of Remote System: 255
Tu: - 13-03-2008, 10:10
Tu*: - 13-03-2008, 10:11
Ts: - 13-03-2008, 10:11

TABLE 1: RESULTS OF DAS'S TECHNIQUE

Ts*: - 13-03-2008, 10:12

b) Results of Khan et al.'s Technique

User Password (PW): User'sAuthentication
User Identifier (ID): IdentityofRemoteUser
User Fingerprint (F): BiometricFingerprint
Secret Key (x) of Remote System: 71
T: - 13-03-2008, 10:10
T′: - 13-03-2008, 10:11
T″: - 13-03-2008, 10:12

TABLE 2: RESULTS OF KHAN ET AL.'S TECHNIQUE

Password (PW)	Smart card sends C_1 to the remote server in login phase.	Remote system sends C_2 to the smart card in authentication phase.
55736572	b07b368d	b92150a9
27734175	10f6066b	25f0910c
7468656e	6c45603d	91ad7afe
74696361	01fbfb7c	b60bcf05
74696f6e	db9d9246	ade38848

c) Results of our 3-E Technique

User Password (P): User'sAuthentication
User Identifier (I): IdentityofRemoteUser
User Biometric Entity (B): BiometricFingerprint
Secret Key (s) of Remote System: 71
Secret number (e) of Remote System: 255
T: - 13-03-2008, 10:10
T*: - 13-03-2008, 10:11
T**: - 13-03-2008, 10:12
T***: - 13-03-2008, 10:13

TABLE 3: RESULTS OF 3-E AUTHENTICATION TECHNIQUE

VI. Analysis of Results

This section discusses the analysis of results of the three authentication techniques. We compare the techniques using three parameters: Distance, Redundant Character and Pair Character. Distance is defined as the summation of modulus of deviation between characters of plain text and cipher text. Redundant character measures by same character if they are in same position in plain text and cipher text. Pair character measures by same character if they are in consecutive position in cipher text.

a) Das's Technique

(a) Comparison between PW_i and C_i

A = 55736572 27734175 7468656e 74696361 74696f6e B = 785b8d4d 2f199456 55714236 e8f019a6 0421a554

(i) Distance = Deviation of A and B= $\sum$ Deviation of a_{ij} from b_{ij} = ((2+3+2+8+2+8+3+11) + (0+8+6+6+5+3+2+1) +(2+1+1+7+2+3+3+8)+(7+4+9+9+5+6+4+5)+ (7+0+4+8+4+10+1+10))
= 39 + 31 + 27 + 49 + 44 = 190

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If ($a_{ij} = b_{ij}$) then the character is redundant. Here 2 characters are redundant out of 40 characters ($a_{10=} b_{10,} a_{41=} b_{41}$). So the probability of redundant character is 1/20. The probability of redundant character increases the probability of authentication failure.

(iii)Pair Character: If ($b_{ij} = b_{ik,}$ where k= j+1) then the characters are called Pair Character. Here is 1 pair character out of 20 pair ($b_{20}b_{21}$). So the probability of pair character is 1/20. The probability of pair character increases the probability of authentication failure.

(b) Comparison between PW_i and X_i

A = 55736572 27734175 7468656e 74696361 74696f6e B = fd48d41c 3cb75052 cefaeb42 c0d7fa43 fc788588

(i) Distance = Deviation of A and B = $\sum$ |Deviation of a_{ij} from b_{ij} |
=(10+8+3+5+7+1+6+10)+(1+5+4+4+1+1+2+3)+(5+10+9+ 2+8+6+2+12)+5+4+7+2+9+7+2+2) + (8+8+1+1+2+10+2+6)
= 50 + 21 + 54 + 38 + 38 = 201

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If ($a_{ij} = b_{ij}$) then the character is redundant. Here no character is redundant out of 40 characters. The probability of redundant character increases the probability of authentication failure.

(iii)Pair Character: If ($b_{ij} = b_{ik,}$ where k= j+1) then the characters are called Pair Character. Here is 1 pair character out of 20 pair ($b_{46}b_{47}$). So the probability of pair character is 1/20. The probability of pair character increases the probability of authentication failure.

b) Khan et al.'s Technique

(a) Comparison between PW and C_1

A = 55736572 27734175 7468656e 74696361 74696f6e B = b07b368d 10f6066b 6c45603d 01fbfb7c db9d9246

(i) Distance = Deviation of A and B = $\sum$ Deviation of a_{ij} from b_{ij} = (6+5+0+8+3+1+1+11) + (1+7+8+3+4+5+1+6) + (1+8+2+3+0+5+3+1)+(7+3+9+2+9+8+1+11)+ (6+7+3+4+3+13+2+8)
= 35 + 35 + 23 + 50 + 46 = 189

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If ($a_{ij} = b_{ij}$) then the character is redundant. Here 2 characters are redundant out of 40 characters ($a_{02=} b_{02,} a_{24=} b_{24}$). So the probability of redundant character is 1/20. The probability of redundant character increases the probability of authentication failure.

(iii) Pair Character: If ($b_{ij} = b_{ik,}$ where k= j+1) then the characters are called Pair Character. Here is no pair character out of 20 pair.

(b) Comparison between PW and C_2

A = 55736572 27734175 7468656e 74696361 74696f6e B = b92150a9 25f0910c 91ad7afe b60bcf05 ade38848

(i)Distance = Deviation of A and B = $\sum$ Deviation of a_{ij} from b_{ij} = |(6+4+5+2+1+5+3+7) + (0+2+8+3+5+0+7+7) + (2+3+4+5+1+5+9+0)+(4+2+6+2+6+12+6+4)+ (3+9+8+6+2+7+4+6)
= 33 + 32 + 29 + 42 + 45 = 181

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If ($a_{ij} = b_{ij}$) then the character is redundant. Here 3 characters are redundant out of 40 characters ($a_{10=} b_{10,} a_{15=} b_{15,} a_{27=} b_{27}$). So the probability of redundant character is 3/40. The probability of redundant character increases the probability of authentication failure.

(iii)Pair Character: If ($b_{ij} = b_{ik,}$ where k= j+1) then the characters are called Pair Character. Here is 1 pair character out of 20 pair ($b_{44}b_{45}$). So the probability of pair character is 1/20. The probability of pair character increases the probability of authentication failure.

c) 3-E Authentication Technique

(a) Comparison between P and N

A = 55736572 27734175 7468656e 74696361 74696f6e B = 0114f18e 0a9d2eda 15f0912d 86e0ad65 f36bab48

(i)Distance = Deviation of A and B = $\sum$ |Deviation of a_{ij} from b_{ij} = (5+4+6+1+9+4+1+12) + (2+3+2+10+2+13+6+5) + (6+1+9+8+3+4+4+8)+ (1+2+8+9+4+10+0+4) + (8+1+0+2+4+4+2+6)
= 42 +43 + 43 + 38 + 27 = 193

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If ($a_{ij} = b_{ij}$) then the character is redundant. Here 2 characters are redundant out of 40 characters ($a_{36} = b_{36}$, $a_{42} = b_{42}$). So the probability of redundant character is 1/20. The probability of redundant character increases the probability of authentication failure.

(iii)Pair Character: If ($b_{ij} = b_{ik}$, where k= j+1) then the characters are called Pair Character. Here is no pair character out of 20 pair. The probability of pair character increases the probability of authentication failure.

(b) Comparison between P and M

$$A = \begin{bmatrix} 55736572 \\ 27734175 \\ 7468656e \\ 74696361 \\ 74696f6e \end{bmatrix} \quad B = \begin{bmatrix} 36e7a841 \\ fc686b8c \\ d04b71f0 \\ dc979d10 \\ 2a5e7312 \end{bmatrix}$$

(i)Distance = Deviation of A and B = $\sum$ Deviation of a_{ij} from b_{ij} =(2+1+7+4+4+3+3+1) + (13+5+1+5+2+10+1+7) +(6+4+2+3+1+4+9+14)+(6+8+3+2+3+10+5+1)+ (5+6+1+5+1+12+5+12)
= 25 + 44 + 43 + 38 + 47 = 197

The probability of authentication depends on the distance. Smaller distance increases the probability of authentication failure.

(ii) Redundant Character: If ($a_{ij} = b_{ij}$) then the character is redundant. Here no characters are redundant out of 40. The probability of redundant character increases the probability of authentication failure.

(iii)Pair Character: If ($b_{ij} = b_{ik}$, where k= j+1) then the characters are called Pair Character. Here is no pair character out of 20 pair. The probability of pair character increases the probability of authentication failure.

VII. COMPARATIVE STUDY BY RESULT

This section discusses comparison between the user authentication phases of Das's, Khan et al.'s and 3-E authentication technique and remote system authentication phases of the three authentication techniques. We compare the phases by the Distance, Redundant character and Pair character parameters.

a) User Authentication Phase

The distance is highest in 3-E technique that means the probability of authentication failure is lowest in 3-E technique among the three. The probability of redundant character is same (i.e. 1/20) in all the three techniques. The probability of pair character in Das's technique is 1/20 but in Khan et al.'s technique and 3-E technique is 0. So comparing by pair character Khan's technique and 3-E technique are best than Das's technique. But distance is most valuable criteria for checking the security of the authentication techniques. Hence User authentication phase of 3-E technique is the most efficient.

b) Remote System Authentication Phase

The distance is highest in Das's technique that means the probability of authentication failure is lowest in Das's technique among the three. The probability of redundant character in Khan et al.'s technique is 3/40 but in Das's technique and 3-E technique is 0. The probability of pair character is lowest (i.e. 0) in 3-E technique among all the three techniques. So comparing by redundant character and pair character 3-E technique is the best among them. But distance is most valuable criteria for checking the security of the authentication techniques. Hence Remote system authentication phase of Das's technique is the most efficient.

VIII. CONCLUSION

We have discussed the proposed Three Entity remote user and server authentication technique to counter the various attacks of previous techniques.

The advantages of the proposed technique are,

(i) This technique is secured against the vulnerabilities of user password authentication and public key based authentication.

(ii)User authentication is checked by the physical characteristics of the user.

(iii) Simple one way hash function and XOR operation are only used.

(iv) Many users with same login identity can not able to log in.

(v) Any user password database is not required in remote sever.

(vi) Smart card and Remote server have secret key and secret number respectively. That enhances the security of the technique.

(vii) The user can freely choose and change his password without any involvement of remote server.

(viii) The technique is free from the reverse XOR, adversary system, impersonation and parallel session attacks.

In future we propose to work to minimize the computational cost of our scheme.

REFERENCES

[1] C. T. Bhunia, Information Technology Network and Internet, New Age International Publishers, India, 5th Edition (Reprint), 2006.
[2] L. Lamport. Password authentication with insecure communication. Communication. ACM, Vol. 24, No. 11, pp. 770-772, 1981.
[3] N. M. Haller, A one-time password system. RFC 1704, 1994
[4] C. C. Channg and T. C. Wu, Rmote password authentication with smart cards, IEEE Proceeding-E, Vol. 138, no. 3, pp. 165-168, 1993.
[5] M. S. Hwang and L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, pp. 28-30, February 2000.
[6] T. ElGamal, A public key based cryptosystem and a signature scheme based on discrete algorithms, IEEE Transactions on Information Theory, Vol. 31, No. 4, pp. 469-472, 1985.
[7] M. L. Das. Flexible and Secure Remote Systems Authentication Scheme Using Smart Cards., HIT Transaction on ECCN, Vol. 1, No.2, pp.78-82, April 2006.
[8] J. K. Lee, S. R. Ryu, and K. Y . Yoo, Fingerprint-based remote user authentication scheme using smart cards, Electronics Letters, Vol. 38, No. 2, pp. 597-600, 2002.
[9] M. K. Khan and J. Zhang, An efficient and practical fingerprint-based remote user authentication scheme with smart cards, IPSEC 2006, Lecturer Notes in Compueter Science 3903, pp 260-269, 2006.

[10] Jing Xu, Wen-Tao Zhu, Deng-Guo Feng, Improvement of a Fingerprint-Based Remote User Authentication Scheme, ISA 2008, pp. 87-92, 2008