Authentication protocol for fingerprint feature extraction and IBC in monitoring systems

Changgeng Yu; Liping Lai
School of Mechanical and Electronic Engineering,
Hezhou University,
No.18, xihuan Road, Hezhou,
China
yuchanggen66@163.com, lailiping66@163.com

Abstract: - Authentication methods based on biometric parameters are gaining importance over the years. But they require the storage and transmission security of fingerprint templates to perform this task. In this work an efficient method based on digital fingerprint random encryption IBC is introduced. The process works by user's fingerprint feature and asymmetric authentication technology to security implementation in monitoring system. Firstly, Fingerprint feature vector was extracted based on the digital fingerprint point extraction method for details feature. Then user identity information had good uniqueness and prevent speculative by the digital fingerprint characteristic vector was encrypted. Finally user identity certificate was generated based on the RSA random fusion method, and the user's identity was determined by random value. The proposed protocol has been modeled and tested with datacenter computer monitoring system (DCRMS) and is found to be safe.

Key-Words: - Authentication, Random Encryption, Smart Cards, Monitoring Systems

1 Introduction

Along with the computer and network communication technology in the intelligent monitoring system application, using open protocols, general structure, embedded hardware and the modular software to develop the intelligent monitoring system, become a trend. The environment of industrial system is thread by network attack, information manipulation, and virus Trojan [1]. In a Datacenter Computer Room Monitor System (DCRMS), usually an authentication technology is an important part of the trusted technology.

Biometric-based remote user authentications are inherently more reliable and secure than usual traditional password-based remote user authentication schemes. Server biometric-based remote user authentications schemes have been proposed in the literature [2]-[13]. Lee *et al*. [2] proposed a fingerprint-based remote user authentication scheme using smart cards in 2002. Lin and Lai [3] pointed out that Lee's scheme cannot prevent forgery attack, and proposed an authentication scheme by user freely change password in 2004. To overcome only unilateral authentication, Khan and Zhang (2006) [4] proposed a mutual authentication between login user and remote server. To prevent user biometric information leakage, Bhargav - Spantzel *et al*. (2007) [5] carry out a multi-factor remote authentication scheme that can hide the identity of the users. Fan and Lin (2009) study an authentication scheme that can be realized privacy protection [6]. In 2010, Time stamp scheme prevent serious time synchronization problem, Li and Hwang proposed a remote authentication scheme based on random numbers and one-way hashing function [7], Li-Hwang's scheme is vulnerable to the existing authentication problem and the DoS attack, Li (2011) [8] propose an improvement of Li-Hwang's scheme in order to withstand their design flaws.

Smart card and biometrics authentication technology, remote user authentication based on fingerprint has already been recognized as the most widely applications, ease of use, and the highest identity authentication technology, but biometric templates is security is the key problem biometric security system. At present, the fingerprint, smart card, and password remote authentication and encryption technology collection scheme will become a new research direction [8]-[13].

In this paper, we study user authentications in DCRMS. We propose a remote user authentication scheme. Our scheme, which is based on Digital

Fingerprinting Random Encryption IBC (DFRE-IBC), does not require a system to maintain a password table. The remainder of the paper is organized as followed: in Section 2, we proposed an authentication scheme based on DFRE-IBC. Key technology of authentication scheme based on DFRE -IBC in Section 3. In section 4, we present a detailed comparison between our scheme and other scheme with validity, security, and functionality properties. Section 5 shows the application and analysis experiments. Finally, we drew our conclusion in Section 6.

2 Digital fingerprint feature extraction method

The fingerprint feature extraction pre-processing aim is to improve the quality of the image. Fingerprint characteristics including overall features and details, the details of the two fingerprints features can't completely the same [14].The most frequently used are the ridge ending and ridge bifurcation [15].

Select the appropriate coordinate system, the topology of the ridge ending data set T as follows:

$$\boldsymbol{T}=\{(x_{t0},y_{to}), (x_{t1},y_{t1}), \ldots,(x_{tn},y_{tn}) \} \quad (1)$$

The topology of the ridge bifurcation data set C as follows:

$$\boldsymbol{C}=\{(x_{c0},y_{co}), (x_{c1},y_{c1}),\ldots,(x_{cn},y_{cn}) \} \quad (2)$$

Topology information of fingerprint feature points as the user's fingerprint uniqueness identification, take the fingerprint characteristics ridge ending before i points and the ridge bifurcation before j points constitute the user's fingerprint characteristic matrix vector G, then

$$\boldsymbol{G}=\{(x_{t0},y_{to}), (x_{t1},y_{t1}),\ldots,(x_{ti},y_{ti}), (x_{c0},y_{co}), (x_{c1},y_{c1}), \ldots, (x_{cj},y_{cj}) \} \quad (3)$$

Conventions to matrix vector G of ridge ending data before $i\times8$ bytes and the ridge bifurcation before $j\times8$ bytes, as the user's fingerprint initial vector, insufficient bit padded with 0, denoted by Xu. Then:

$$\boldsymbol{X}_u=0\text{X } x_{t0}y_{to}x_{t1}y_{t1}\ldots x_{ti}y_{ti}x_{c0}y_{co}x_{c1}y_{c1}\ldots x_{cj}y_{cj} \quad (4)$$

Xu will division according to 32 bytes for the unit, the fingerprint characteristic vectors W: $\{W_1, W_2, W_3, \ldots\}$.

3 User credentials generation method Based on the digital fingerprint

User registration based on the DFRE – IBC as shown Fig.1. During the registration, the user sends samples of her fingerprint feature to the PKG server, who obtains a credential of the user. The identity information are encrypted and sent to the authentication server, and a notification is sent back to the user. The overall's algorithm of the user credentials generation method in given in Algorithm 1.

Algorithm 1: User credentials generation method

1. Initial State: the user ID, password are encrypted: k_u
2. User collects multiple sample of her fingerprint, Feature vector, W
3. Computer an authenticating threshold, τ
4. Feature vector are encrypted using the user ID and password: $E(W_i)$
5. The user's identity be generated: C_u
6. The user is then notified about success

Step 1: The PKG server is used to elliptic curve Diffie-Hellman $\boldsymbol{E_p}$ and G is basis points for Elliptic curve $\boldsymbol{E_p}$ on the order of n, makes user ID meet mapping function: $F_{ID}:\{0,1\}^m \rightarrow E_p$. PKG server computers $P_m=k_m \bullet G$, where k_m is a large prime number, Calculation of user private key k_u meet: $U_{ID}= k_u \bullet G$, Finally, PKG server stores k_m, k_u.

Step 2: PKG server generate user private key digital signature Su using a $Sig(k_m, k_u)$ as follows:

$$S_u=\{k_u, Sig(k_m, k_u)\} \quad (5)$$

Where k_u is user private key, $Sig(k_m, k_u)$ is a digital signature function. And along with user private key k_u sent to the user. The user verifies whether k_u is legal or not. If k_u is legal, k_u send to the user.

Step 3: users input the person fingerprint on the fingerprint collection device to extract fingerprint characteristic vector W: $\{W_1, W_2, W_3,\}$, and to generate the fingerprint feature matching threshold τ. The fingerprint characteristic vectors W are encrypted using **RSA** algorithm, and result as fingerprint characteristics cipher $E(W_i)$. $E(W_i)$, and

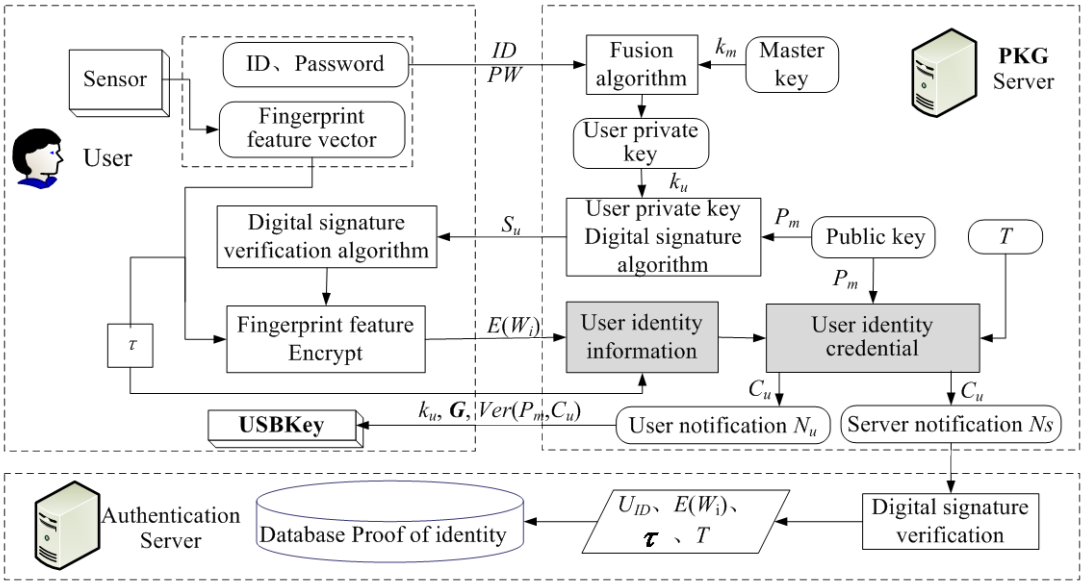

Fig.1 User registration based on the DFRE - IBC

The threshold τ, are sent to the PKG server. among them:

$$E(W_i)=E(U_{ID}, W_i) \quad (6)$$

Step 4: The PKG server according to the user ID, password, fingerprint characteristics cipher $E(W_i)$ and user identity proof time period T to generate the user identity credential,

$$C_u=\{U_{ID}, PW, E(W_i), \tau, Sig(k_m, \tau \| T \| E(W_i))\} \quad (7)$$

And will be sent to the user authentication server.

Step 5: The authentication server using a digital signature verification function *Ver* (P_m, *Cu*) verifies whether C_u is legal or not. If C_u is legal, then, the user ID, password, E (W_i), threshold τ and identity certificate time period T sends to Database Proof of identity

Step 6: PKG server is then notified about success, sends parameters {k_u, ***G***, *Ver* (P_m, *Cu*)} to USBKey.

4 User authentication method based on DFRE-IBC

User authentication based on the DFRE -IBC as shown Fig. 2. After receiving the user registration phase, the authentication has to perform the following steps with the user to authenticate each other. The overall's algorithm of the User authentication method in given in Algorithm 2.

Step 1: users computers fingerprint feature vector X_u: {x_1, x_2, x_n} from the person fingerprint on the fingerprint collection device. Each feature X_u is encrypted E (x_i) using RSA algorithm and sends to authentication server. As the encryption used RSA algorithm is homomorphic to multiplication, we can computer, $E(W_i x_i)= E(W_i) E(x_i)$, at the authentication sever.

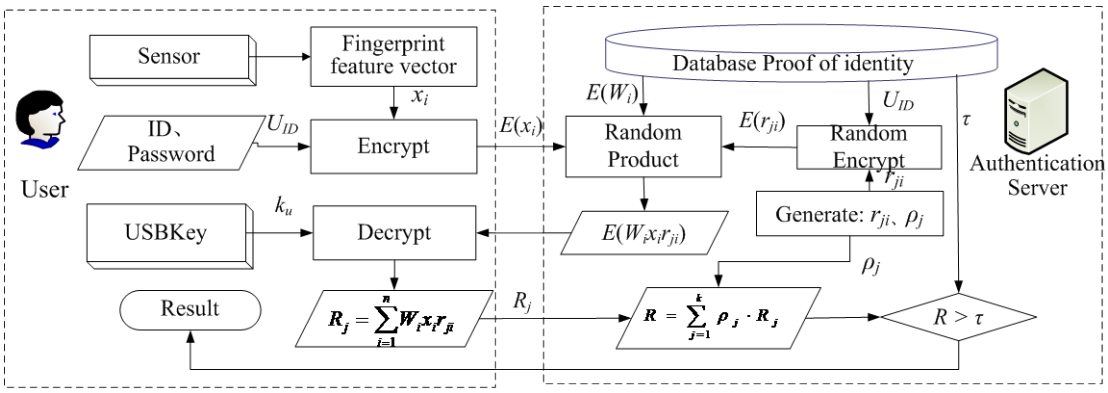

Fig.2 Flow chart of user authentication based on the DFRE – IBC

Algorithm2: User authentication method

1: User computers feature vector, $\boldsymbol{X_u}$: $\{x_1, x_2, \ldots, x_n\}$, from test data
2: Each feature x_i is encrypted using RSA ($E(x_i)$) and send to authentication server
3: Authentication server computers $kn+k$ random numbers, ρ_j and r_{ji},
such that, $\forall i,\ \sum_{j=1}^{k} \rho_j \cdot r_{ji} = 1$
4: Random number r_{ji} is encrypted ($E(r_{ij})$)
5: Authentication server computers $E(W_i x_i r_{ij}) = E(W_i)E(x_i)\ E(r_{ij})$
6: The user decrypted the products to obtain $W_i x_i r_{ij}$
7:The user returns $R_j = \sum_{i=1}^{n} W_i x_i r_{ji}$ to the authentication server
8: The authentication server computer $R = \sum_{j=1}^{k} \rho_j \cdot R_j$
9: **If** $R>\tau$ **then**
10: return *Accepted* to the user
11: **else**
12: return *Rejected* to the user
13: **end if**

Step 2: the authentication sever computer $kn+k$ random numbers, ρ_j and r_{ji}, we impose the following condition on ρ_j s and r_{ji} s during its generation:

$$\forall i,\ \sum_{j=1}^{k} \rho_j \cdot r_{ji} = 1 \tag{8}$$

Step 3: Random number r_{ji} is encrypted $E(r_{ij})$ using RSA algorithm.

Step 4: the authentication sever computers $E(W_i x_i r_{ij}) = E(W_i)E(x_i)\ E(r_{ij})$, and send $E(W_i x_i r_{ij})$ to user.

Step 5: The user decrypted the products $E(W_i x_i r_{ij})$ to obtain $W_i x_i r_{ij}$. User returns $R_j = \sum_{i=1}^{n} W_i x_i r_{ji}$ to the authentication server.

Step 6: Authentication server carries out all its computation in the encrypted domain, and hence does not get any information about fingerprint feature vector ($\boldsymbol{X_u}$ or W). We thus assume the authentication server has an access to a random number generator (PRANG), the ρ_j and r_{ji} are generated using PKNG while ensuring that (8) holds.

Substituting the above equality in the expansion of user fingerprint feature validation values sum (R), we get

$$R = \sum_{j=1}^{k} \rho_j \cdot R_j = \sum_{j=1}^{k} \rho_j \sum_{i=1}^{n} W_i x_i r_{ji} = \sum_{i=1}^{n} \sum_{j=1}^{k} \rho_j W_i x_i r_{ji}$$
$$= \sum_{i=1}^{n} W_i x_i \sum_{j=1}^{k} \rho_j r_{ji} = \sum_{i=1}^{n} W_i x_i \tag{9}$$

If $R>\tau$ holds, the users passed the authentication verification. On the contrary, if $R<\tau$, the users does not pass the verification. Return *Accepted*/*Rejected* to the users.

5 Validity, Security, and Functionality in Authentication based on DFRE-IBC

In this section, we analysis the validity, security, and functionality properties of our proposed scheme.

5.1 Validity analysis

Burrows, *et al.* (1989) proposed BAN logic is to analyze the correctness of the identity authentication protocol formal method [15]. BAN logic is a formal analysis tool based on faith, through the modal logic analysis of authentication protocol, research involved in certification both sides communication is correct.

The C (the user) and S (the authentication server) on both sides of the initial belief assumptions as follows:

(1)**C** has $\boldsymbol{U_{ID}}$, PW, x_i, k_u
(2)**S** has $E(W_i)$, τ
(3)**S** *fresh* (r_{ji}, ρ_j)
(4)**S** believes **C** said $E(W_i)$
(5)**C** believes **S** *fresh* ($E(W_i x_i r_{ji})$)
(6)**S** believes **C** said R_j

The authentication of messages change into corresponding BAN logic language, ideal authentication model based on DFRE-IBC is set up as follows:

messages 1: **C**→**S**: U_{ID}, $E(x_i)$
messages 2: **S**→**C**: *fresh*($E(W_i x_i r_{ji})$)
messages 3: **C**→**S**: R_j

In the *messages* 1, **S** believes **C** said U_{ID}, $E(x_i)$, S will match user ID in the 1: N with U_{ID} and database proof of identity(DB). If the DB in existence and matching the user ID, come to the conclusion that the U_{ID} is existent. The authentication success; Otherwise come to the conclusion that the U_{ID} is inexistent. S send error message to the user, the authentication failure. S generator random number of *fresh* (r_{ji}, ρ_j), *fresh* r_{ji} encrypted using the user ID in the DB and calculate the *fresh* ($E(W_i x_i r_{ji})$), by the *message* 1 can also be concluded that **S** has U_{ID}.

In the *messages* 2, **C** believes **S** said *fresh* ($E(W_i x_i r_{ji})$). The *message* 2 decrypted by C use the k_u , further concluded that: **C** believes **S** said $W_i x_i r_{ji}$, and computers $R_j = \sum_{i=1}^{n} W_i x_i r_{ji}$.

In the *messages* 3, **S** believes **C** said R_j. Authentication server(S) computers $R_j = \sum_{i=1}^{n} W_i x_i r_{ji}$, and compared with the known threshold τ. If $R>\tau$ holds, the users passed the authentication verification. On the contrary, if $R<\tau$， the users does not pass the verification.

The above analysis shows that under the premise that a certain initial belief, identity authentication scheme based on DFRE-IBC through a series of certification means, to be able to authenticate users correctly legitimacy to achieve expected results.

5.2 Security analysis

Attack test method can test authentication system based on DFRE-IBC for defensive identity certificate, the illegal invasion ability, determine its security system

Let us consider the following attack scenarios:

Case 1: *Preventing Replay Attack*

An attacker pretending to be a legal user may attempt to login to the server by sending U_{ID}， PW， $E(x_i)$ and R_j messages. In our scheme, the authentication server will choose random number r_{ji} and ρ_j to prevent replay attack, and both values will be different in each time. Thus, an attacker has no opportunity to successfully replay used messages.

Case 2: *Preventing Insider Attack*

The insider attack is when the user's USBKey is obtained by the server. Therefore, the user must conceal his/her USBKey from the server to pretend, Attacker steal users USBKey tried to pretend, fingerprint characteristic encrypt used in our scheme could not succeed.

Case 3: *Invasion of terminal operation*

The attack is when the user's ID and password are obtained in the login phase, because user's private key stored in USBKey can't export, the attacker can't get it, attacker cannot decrypt the authentication server send back the random value $E(W_i x_i r_{ji})$. Thus, our scheme can successfully prevent invasion of terminal operation.

Case 4: *Preventing Forgery Attack*

If the attacker can't obtain the user's ID, user's template of fingerprint characteristic values $E(x_i)$, and the secret values, the attacker can't decrypt the user's fingerprint information. or used user's fingerprint to spy out other information, the attack cannot be authenticated.

Case 5: *Preventing Guessing Attack*

i) It is impossible for attacker to obtain private key and fingerprint feature within the effective time limit from user's private key and the fingerprint characteristic, because of RSA algorithm robustness and the complexity of the fingerprint characteristics. ii) Attacker guesses R_j constantly, attempting to threshold verification by the fingerprint characteristic. In each time the authentication through the random number to the authentication server check product R_j features. The attacker can't obtain random numbers, so a brute force attack is not successful.

5.3 Functional analysis

(1)*Without password table, maintaining verification table and fingerprint characteristic database*

In the process of identity authentication scheme, digital fingerprint feature vector have been encrypted by user ID, password and public-key, the result is a fingerprint feature vector cipher $E(W_i)$. Authentication server through identity credential database constructed stochastic integration value $E(W_i x_i r_{ji})$, authentication server does not require user password table, verification table and the fingerprint characteristic database. This solution need to maintain the user registry to store each registered user identity certificate, the table is small and do not keep secret.

(2)*Users can freely choose and update passwords*

Our scheme offers registered for users the freely choose and update passwords, as a result, registered users of the scheme is convenient to manage their password.

(3) *Without synchronized clocks*

To prevent replay attacks using different random numbers (r_{ji}, ρ_j) instead of a timestamp, overcome problem of the certification both sides need to keep the clock. Therefore, our scheme there is no clock synchronization problem within certification process.

(4) *The user identification and fingerprint feature data to be protected*

User identification method is combined with the public key algorithm of elliptic curve cryptographic algorithm, RSA encryption algorithm. The elliptic curve for 163 bit key length, RSA password length is 1024 bits, within the limited time, the algorithm in computing is a safe [17]. User authentication server identity resolution process, our scheme doesn't get the user ID, password, and the original fingerprint information, so protects user privacy.

We compare the performances and functional of our scheme with those for Lee *et al.*'s scheme[2], Lin *et al.*'s scheme[3] and Khan *et al.*'s[4] scheme. Performances and functional comparison of our scheme with those related schemes are shown in Table 1.

Table 1 Performances and Functionality comparison with other related scheme

Performances and Functionality	**DFRE-IBC**	**Lee** *et al.* [2]	**Lin** *et al.*[3]	**Khan** *et al.*[4]
Resistance replay attack	Yes	Yes	Yes	Yes
Resistance insider attack	Yes	Yes	No	No
Impersonation attack	Yes	No	Yes	Yes
Resistance guessing attack	Yes	Yes	Yes	Yes
Preventing Server spoofing attack	Yes	No	No	Yes
Mutual Authentication	Yes	No	No	Yes
without synchronized clocks	Yes	No	No	No
Without password table, maintaining verification table and fingerprint characteristic database	Yes	Yes	Yes	Yes
Freely choose and update password	Yes	No	Yes	Yes
fingerprint feature data to be protected	Yes	No	No	No
the user identification to be protected	Yes	No	No	No

Form Table 1. we see that DFRE-IBC scheme, compared with Lee *et al.*'s scheme[2], Lin *et al.*'s scheme[3] and Khan *et al.*'s scheme[4], has high security and functional. As a result, DFRE-IBC scheme is fully meet the requirements of authentication in DCRMS environmental.

6 Application and analysis Experiments

We have performed an experiment to evaluate the performance and function of our scheme. A datacenter machine room monitoring system was implemented based on a client-server model that can perform verification over the Internet. Fingerprint collection device is U.are.U 4000 by the SUPCON company, USBKey is the eToken NG-FLASH 64k.

As shown in fig. 3 DCRMS client login screen, the implemented system work properly as user needs to registration, the admin click on the "register" button to enter the user registration screen.

Fig.3 Interface of client login

User registration screen as shown in Fig.4. Enter the registered user interface, the system automatically verifies of digital fingerprint. If its integrity verification through, the system can carry out the new user registration. Otherwise, the system alarm record and automatically returned to the client login screen.

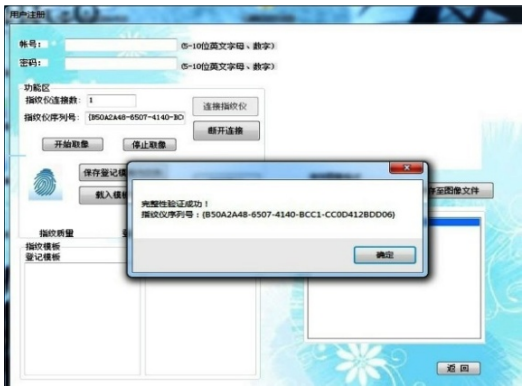

Fig.4 Interface of user registration

After the success of the user registration, the client login screen enters your user name and password, DCRMS user authentication interface as shown in Fig. 5. The system again to integrity verification of digital fingerprint, the success of the validation, digital fingerprint acquisition instrument collect user's fingerprint. The client extract fingerprint feature template, and trusted authentication server interact to identity authentication.

Fig.5 Interface of user authentication

The user identity were certified by using the login information of right and wrong respectively, in DCRMS system user login process, Certification results and time was recorded. Based on DFRE - IBC identity authentication system function is validated by False Rejection Rate (FRR) and False Acceptance Rate (FAR), and real-time function is validated by the user authentication time. Based on DFRE-IBC identity authentication system test results as shown in Table 2.

Table2 Result of authentication system based on DFRE-IBC

Number /time	False Rejection /time	False Acceptance /time	FRR /%	FAR /%	Correct Rate /%	Mean time /s
1200	22	0	1.83	0	98.17	0.94

The experimental results show that the authentication system which false reject rate is 1.83%, false acceptance rate is 0, and the average login time is 0.94 s.

7 Conclusions

(1) An authentication method based on DFRE-IBC both cryptography and fingerprint recognition technology is proposed by taking into account the security, privacy, and non-repudiation, so more suitable for DCRMS among entity authentication.

(2) The method is mainly fusion user's fingerprint characteristic and asymmetric authentication technology to security implementation in DCRMS environment, it does not reveal any information about fingerprint samples to the authentication server.

(3)We analysis the validity, security, and functionality properties of our proposed scheme. As a result, DFRE-IBC scheme is fully meet the requirements of authentication in DCRMS environmental.

Acknowledgements

This research was supported by the doctor`s scientific research foundation of Hezhou University, the project of Guangxi university of science and technology research (No.2013YB242).

References:

[1] United States Government Accountability Office, Information security: Cyber threats and vulnerabilities place federal systems at ris, *Congressional Testimony GAO-09-661T*, 2009.

[2] Lee J K, Ryu S R, Yoo K Y, Fingerprint-based remote user authentication scheme using smart cards, *Electronics Letters*, vol.38, no.12, pp:554-555, 2002.

[3] Lin C H, Lai Y Y, A flexible biometrics remote user authentication scheme, *Computer Standard and Interfaces*, vol.27, no.1, pp:19-23, 2004.

[4] Khan M K, Zhang J, Improving the security of 'a flexible biometrics remote user authentication scheme', *Computer Standards and Interfaces*, vol.29, no.1, pp: 82-85, 2007.

[5] Bhargav-Spantzel A, Squicciarini A C, Bertino E, et al, Privacy preserving multi-Factor authentication with biometrics, *Journal of Computer Security*, vol.15, no.5, pp:529-560, 2007.

[6] Fan C I, Lin Y H, Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics, IEEE *Transactions on Information Forensics and Security*, vol.4, no.4, pp: 933-945.

[7] Li C T, Hwang M S, An efficient biometrics-based remote user authentication scheme using smart cards, *Journal of Network and Computer Applications*, vol.33, no.1, pp: 1-5, 2010.

[8] D. S. Wang, J. P. Li, Y. Tang, et al, Authentication scheme of remote users by using multimodal biometric and smart cards, *2007 International Conference on Information Computing and Automation*, no.1, pp: 98-101, 2007.

[9]. D. S. Wang, J. P. Li, A new fingerprint-based remote user authentication scheme using mobile devices, *2009 International Conference on Apperceiving Computing and Intelligence Analysis*, pp: 65-68, 2009.

[10] Li X, Niu J W, Ma J, et al, Cryptanalysis and improvement of a biometrics-based remote user authentication scheme using smart cards , *Journal of Network and Computer Applications*, vol.34, no.1, pp: 73-79, 2011.

[11] Madhusudhan R., Mittal R. C, An enhanced biometrics-based remote user authentication scheme using mobile devices, *International Journal of Computational Intelligence Studies*, vol.1, no.4, pp: 333-348, 2012.

[12] Meghanathan, Natarajan, Identification and removal of software security vulnerabilities using source code analysis: A case study on a java file writer program with password validation features, *Journal of Software*, vol.8, no.10, pp: 2412-2424, 2013.

[13] Bu, Wei Wang, Kuanquan, Wu, Xiangqian, et.al., Hand segmentation for hand-based biometrics in complex environments, *Journal of Software*, v 8, n 10, p 2439-2446, 2013.

[14] Sutthiwichaiporn P., Areekul V, Adaptive boosted spectral filtering for progressive fingerprint enhancement, Pattern *Recognition*, vol.46, no.9, pp: 2465-2486, 2013.

[15] David Z, Feng L, Qijun Z, et al, Selecting a reference high resolution for fingerprint recognition using minutiae and pores, *IEEE Transactions on Instrument and Measurement*, vol.60, no.3, pp: 863-871, 2011.

[16] Burrows M., Abadi M., Needham R., logic of authentication, *ACM transactions on Computer Systems*, vol.8, no.1, pp: 18-36, 1990.

[17] Lauter K., The advantages of elliptic curve cryptography for wireless security, *IEEE Wireless Communications*, vol.11, no.1, pp: 62-67, 2004.