Authentication Methods Based on Digital Fingerprint Random Encryption IBC

Changgeng Yu
School of Mechanical & Automotive Engineering, South China University of Technology, Guangzhou, China
School of Mechanical and Electronic Engineering, Hezhou University, Hezhou, China
Email: yuchanggen66@163.com

Guixiong Liu
School of Mechanical & Automotive Engineering, South China University of Technology, Guangzhou, China
Email: megxliu@scut.edu.cn

Abstract—**Aiming at the problem of the storage and transmission security of fingerprint templates in datacenter computer monitoring system (DCRMS), an authentic method based on digital fingerprint random encryption IBC is proposed in this paper, combined with the feature of fingerprint vector encryption algorithms. The method is mainly based on fusion user's fingerprint characteristic and asymmetric authentication technology which is to secure the implementation in DCRMS environment. The analysis about the safety of authentication scheme indicated that scheme can authenticate the users right legality, while the attacker can't get users' privacy information. It is difficult to find the solution in limited time. Users' identification and fingerprint template is to be protected. The experimental results show that the false reject rate of the authentication system is 1.83% while its false acceptance rate is 0, and the average login time is 0.94 s.**

Index Terms—**Digital Fingerprinting, Authentication, Random Encryption, USB Key, DCRMS**

I. Introduction

With the developing of intelligent monitoring system application computer and network communication technology as well as the using of open protocols, general structure, embedded hardware and the modular software, the intelligent monitoring system is becoming a trend. Environment of the industrial system is threatened by network attacks, information manipulation, and virus Trojan [1]. Usually in a Datacenter Computer Room Monitor System (DCRMS**)**, the authentication technology is one of the important parts of the trusted technology.

Biometric-based remote user authentications are inherently more reliable and more securable than the usual traditional password-based remote user authentication schemes. Server biometric-based remote user authentications scheme had been proposed in several literature works [2]-[13]. Lee *et al* [2] proposed a fingerprint-based remote user authentication scheme which using the smart cards in 2002. Lin and Lai [3] pointed out that Lee's scheme cannot prevent forgery attack, and proposed an authentication scheme which users could change their password freely in 2004. To acquire the one and 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) had been studied on an authentication scheme which can realize the privacy protection [6]. In 2010, Time stamp scheme prevented the serious time synchronization problem. At that time, Li and Hwang proposed a remote authentication scheme based on random numbers and one-way hashing function [7]. Li-Hwang's scheme is vulnerable against the existing authentication problem and the DoS attack. So, Li (2011) [8] proposed an improved version of Li-Hwang's scheme in order to avoid their design flaws.

Smart card and biometrics authentication technology based on fingerprint which can remote users' authentication has already been recognized as the most widely used applications. It is easy to use with its highest identity authentication technology, but the biometric templates security is a key problem in the biometric security system. At present, the research about fingerprint, smart card, password remote authentication and encryption technology collection scheme is becoming a new research trend [8]-[13].

In this paper, we will study on the user authentications in DCRMS, and will propose a remote user authentication scheme. Our scheme, which is based on Digital Fingerprinting Random Encryption IBC (DFRE-IBC), does not require any system to maintain the password table. Our remainder of the paper is organized as followed: in Section 2, we will propose an authentication scheme based on DFRE-IBC. And the key technology of authentication scheme based on DFRE -IBC will be proposed in Section 3. In section 4, we will present a very detailed comparison between our scheme and others' on different aspects such as validity, security, and functionality properties. Section 5 will show our application and analysis experiments. And our conclusion will be given in the Section 6.

II. Authentication Scheme based on DFRE –IBC

The frame of authentication scheme based on the DFRE–IBC is shown in Fig.1. The design process of our scheme can be divided into the following steps.

doi:10.4304/jsw.9.6.1612-1618

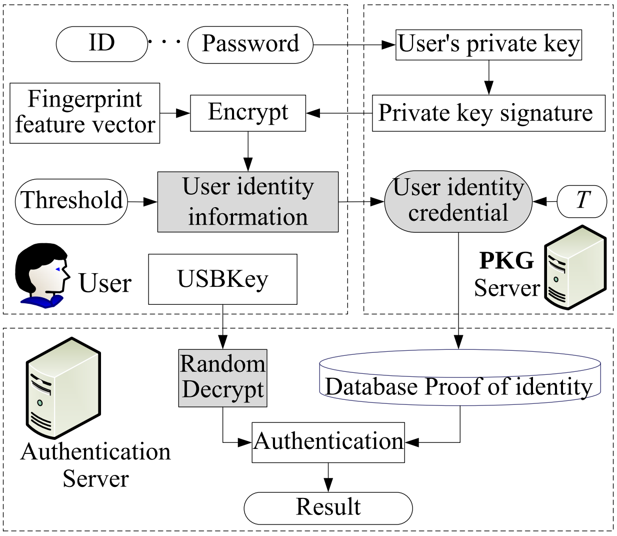


Figure 1. Frame of authentication scheme based on DFRE- IBC

(1) The Private Key Generator (PKG) generates those corresponding private keys. During operation, the PKG will publish a master public key while user private key is produced by the user ID, password and the system master key. The user identity information, also called fingerprint characteristic information, will be encrypted by using the user private key.

(2) The fingerprint feature vectors, encrypted by PKG server along with user ID and password, will be sent into the authentication server.

(3) The authentication server generates random numbers, and is randomly generated by the cipher text of user's fingerprint characteristics. The threshold of fingerprint characteristic shows its authenticity by being saved in the database according to user authentication credentials, so as to infer the authenticity of user identity information.

III. Key Technology of Authentication Scheme Based on DFRE – IBC

This section is mainly about digital fingerprint feature extraction, user credentials generation, and user authentication, which are key technologies working based on the DFRE-IBC identity authentication scheme.

A. Digital Fingerprint Feature Extraction Method

The fingerprint feature extraction pre-processing is aiming to improve the quality of image. Fingerprint characteristics include the overall features and the details. The detailed features of two fingerprints can not be the same completely [14]. The features mentioned most frequently are ridge ending and ridge bifurcation [15].

Select an appropriate coordinate system and set *T* to present the topology of ridge ending data as follows:

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

Set *C* to present the topology of ridge bifurcation data as follows:

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

Point the topology information of fingerprint feature as user's fingerprint uniqueness identification. Assuming that the fingerprint characteristics ridge ends before *i* points, then the ridge bifurcation which before *j* points will construct a user's fingerprint characteristic matrix vector *G*:

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

Assuming that the ridge matrix vector G ends its data before *i*×8 bytes, the ridge bifurcates before *j*×8 bytes, and *Xu* presents the insufficient bit padded with 0 as the user's fingerprint initial vector. Then:

$$\boldsymbol{X}_u=0\mathrm{X}\ x_{t0}y_{to}x_{t1}y_{t1}\ldots x_{ti}y_{ti}x_{c0}y_{co}x_{c1}y_{c1}\ldots x_{cj}y_{cj} \tag{4}$$

Xu will divide the fingerprint characteristic vectors *W* to 32 bytes, and one unit for each: $\{W_1, W_2, W_3,...\}$.

B. User Credentials Generation Method Based on the Digital Fingerprint

User registration based on the DFRE – IBC is shown on Fig.2. During registration, user may send the sample feature of her fingerprint to a PKG server which could obtain her credential. The identity information will be encrypted and sent to the authentication server, and then a notification is going to be sent back to user. The general method of user credential overall algorithm will be 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, $\tau$
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: PKG server is used for the elliptic curve Diffie-Hellman $\boldsymbol{E_p}$, and *G* is a basis points to elliptic curve $\boldsymbol{E_p}$ on the order of *n*, which makes user ID meet this mapping function: $F_{ID}:\{0,1\}^m \rightarrow E_p$. PKG server computers $P_m=k_m \bullet G$. Among which, k_m is a large prime number. The calculation of user private key k_u satisfies $U_{ID}= k_u \bullet G$. In the end, the PKG server stores k_m and k_u.

Step 2: PKG server generates the user private key digital signature *Su*, and formula $Sig(k_m, k_u)$ is as follows:

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

Among which, k_u is the user private key, and $Sig\ (k_m, k_u)$ is a digital signature function which would be sent to the user along with the user private key k_u. The user verifies whether k_u is legal or not. If k_u is legal, k_u will be sent to the user .

Step 3: users input their personal fingerprint in the fingerprint collection device to extract fingerprint characteristic vector *W*: $\{W_1, W_2, W_3\ \ldots\}$, as well as to generate the fingerprint feature which matches the threshold τ. Encrypt the fingerprint characteristic vectors *W* by using **RSA** algorithm, and make the fingerprint characteristics cipher $E\ (W_i)$. $E\ (W_i)$. Through the threshold τ, they will be sent to the PKG server. Among which, there is:

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

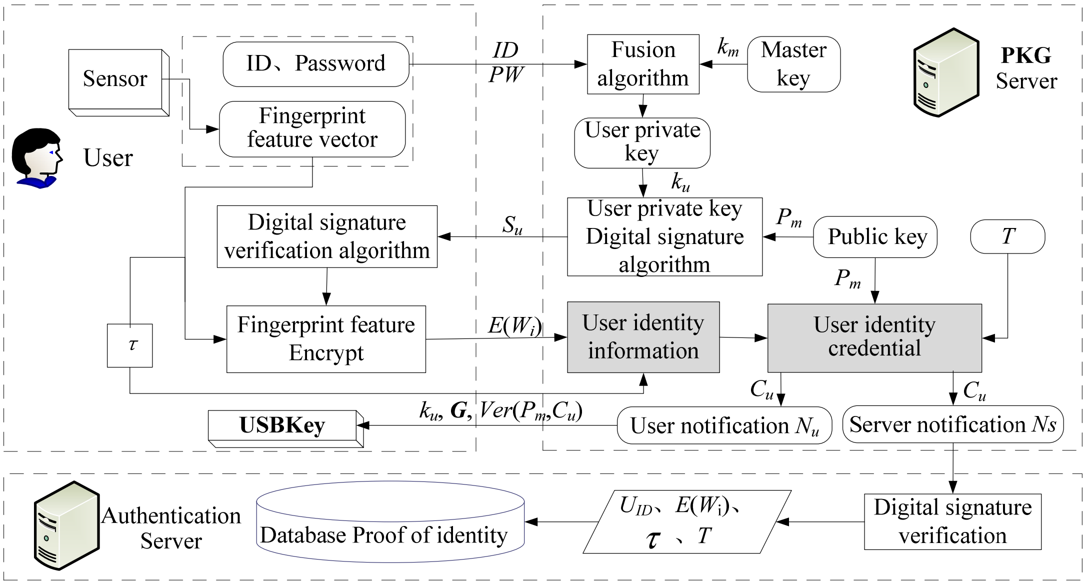

Sensor
ID、Password
Fingerprint feature vector
User
ID
PW
Fusion algorithm
k_m
Master key
PKG Server
User private key
k_u
Digital signature verification algorithm
S_u
User private key Digital signature algorithm
P_m
Public key
T
P_m
τ
Fingerprint feature Encrypt
$E(W_i)$
User identity information
User identity credential
C_u
C_u
USBKey
k_u, $\boldsymbol{G}$, $Ver(P_m,C_u)$
User notification N_u
Server notification Ns
Authentication Server
Database Proof of identity
U_{ID}、$E(W_i)$、τ 、T
Digital signature verification

Fig.2 User registration based on the DFRE - IBC

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

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

and it will be sent to the user authentication server.

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

Step 6: then the PKG server would be notified succeed. It would send parameters $\{k_u,\boldsymbol{G},Ver(P_m,C_u)\}$ to the USB Key.

C. User Authentication Method Based on DFRE-IBC

User authentication based on the DFRE -IBC is shown in Fig.3. After receiving the user registration phase, the authentication shall perform with user the following steps to authenticate each other. Ps: the overall algorithm of the User authentication method is given in Algorithm 2.

Step 1: users computers fingerprint feature vector X_u: $\{x_1, x_2 \ldots x_n\}$ are based on the personal fingerprint from the fingerprint collection device. Each feature X_u is an encrypted E (x_i) by RSA algorithm, and will be sent to the authentication server. The process of encryption by using the RSA algorithm is a process of changing from homomorphism to multiplication. We can compute $\mathrm{E}(W_\mathrm{i}x_\mathrm{i})=\mathrm{E}(W_\mathrm{i})\mathrm{E}(x_\mathrm{i})$ on the authentication sever.

Step 2: the authentication sever computes $kn+k$ random numbers, ρ_j and r_ji. We shall impose the following condition on ρ_j s and r_ji s during its generation:

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

Step 3: random number r_{ji} is an encrypted $E(r_{ij})$ by RSA algorithm.

Step 4: the authentication sever computes $E(W_ix_ir_{ij})= E(W_i)E(x_i)\ E(r_{ij})$ and sends $E(W_ix_ir_{ij})$ to user.

Step 5: user decrypts the product $E(W_ix_ir_{ij})$ so as to obtain $W_ix_ir_{ij}$, and then returns $R_j = \sum_{i=1}^{n} W_i x_i r_{ji}$ to the authentication server.

Algorithm2: User authentication method

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

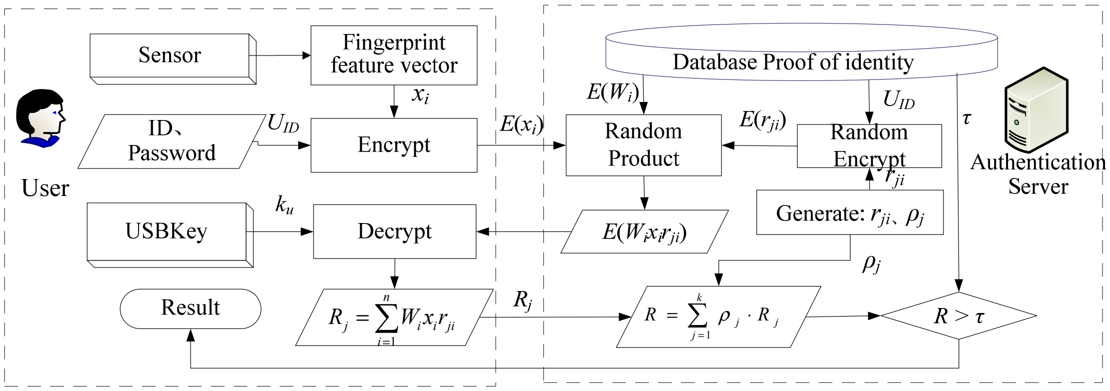


Fig.3 Flow chart of user authentication based on the DFRE – IBC

Step 6: authentication server carries out all its computation from the encrypted domain. Hence, it will not get any information about the fingerprint feature vector ($\boldsymbol{X_u}$ or W). Thus we assume that the authentication server has an access to the random number generator (PRANG). The ρ_j and r_{ji} will be generated after using PKNG, and they'll ensure what (8) holds at the same time.

By substituting the equality above during the expansion of user fingerprint feature validation, and by valuing the sum (R), we can get:

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

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

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

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

A. Validity Analysis

Burrows, *et al.* (1989) had once proposed BAN logic which is used for analyzing the correctness of identity authentication protocol formal method [15]. BAN logic is a formal anglicizing tool based on faith. It analysis the authentication protocol as well as the research about certificating whether both sides' communication is correct or not through the modal logic.

The user (denoted by C) and the authentication server (denoted by S) on each side of the initial belief assumptions as follows:

(1)**C** has $\mathbf{U_{ID}}$, 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

Messages authentication changes 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 the user ID in 1: N with U_{ID} and database proof of identity (DB). If the DB exists and matches the user ID, then the U_{ID} exists. So, the authentication succeeds. Otherwise, the U_{ID} is inexistent. S sends error message to user. The authentication fails. S generates the random number *fresh* (r_{ji}, ρ_j), *fresh* r_{ji} encrypted by using the user ID in the DB, and calculates the *fresh* ($E(W_i x_i r_{ji})$). That **S** has the U_{ID} can also be concluded through *message* 1.

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

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

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

B. Security Analysis

Attack test method can test the defensive identity certification of authentication system based on DFRE-IBC, and the illegal invasion ability as well, to decide its security system.

Let us consider the following attack scenarios:

Case 1: *Preventing Replay Attack*

The attacker who pretended to be a legal user might be attempted to login the server by sending U_{ID}, PW, $E(x_i)$ and R_j messages. But in our scheme, authentication server would choose the random number r_{ji} and ρ_j to prevent the replay attack so that both values could be different at each time. Thus, the attacker would have no opportunity at all to replay used messages successfully.

Case 2: *Preventing Insider Attack*

It is called the insider attack when the user's USB Key is obtained by server. So the user should conceal his/her USB Key from the server, just in case. Attacker steals user's USB Key and tries to pretend, but it shall fail due to the fingerprint characteristic encryption mentioned in our scheme.

Case 3: *Invasion of terminal operation*

The attack is going to happen when the user's ID and password are obtained in the login phase. If the user's private key stored in USB Key could not be exported, then the attacker could not get it. So that the attacker couldn't decrypt the authentication server and send back the random value $E(W_i x_i r_{ji})$. Thus, our scheme could prevent the invasion of terminal operation successfully.

Case 4: *Preventing Forgery Attack*

If the attacker couldn't obtain user's ID, user's fingerprint characteristic values template $E(x_i)$, and the secret values, then the attacker couldn't decrypt user's fingerprint information or spy other information by using user's fingerprint. So the attack could not be authenticated.

Case 5: *Preventing Guessing Attack*

i) It is impossible for attackers to obtain the private key and the fingerprint feature within effective time which is limited by user's private key and fingerprint characteristic. It is due to the RSA algorithm robustness and the complexity of fingerprint characteristics. ii) The attacker constantly attempts to dope out the R_j and to pass the threshold verification by using the fingerprint characteristics. Each time, the authentication would check the product R_j features through random numbers in the authentication server. And of course the attacker couldn't obtain those random numbers. Which means the brute force attack fails.

C. Functional Analysis

(1) *Maintain the verification table and the fingerprint characteristic database without a password table*

In the scheme of identity authentication, digital fingerprint feature vectors have been encrypted by user ID, password and public-key. And the result is the fingerprint feature vector cipher $E(W_i)$. Authentication server constructs a stochastic integration value $E(W_i x_i r_{ji})$ through identity credential database without the requirements of user password table, verification table and fingerprint characteristic database. It is necessary to store every registered user's identity certificate by maintaining their registries in this solution; however the table is too small to keep those secrets.

(2) *Choose and update passwords freely*

The freedom of choosing and updating passwords is ensured in this scheme for all registered users. So, it is convenient for them to manage their own passwords.

(3) *No synchronized clocks*

It is necessary to keep the clock while preventing the replay attacks by using different random numbers (r_{ji}, ρ_j) instead of a timestamp and overcoming the problem of certification. Therefore, there will be no clock synchronization problem during the certification process in our scheme.

(4) *Protect user's identification and fingerprint feature data*

User identification method is related to the public key algorithm of elliptic curve cryptographic algorithm and RSA encryption algorithm. The key length of an elliptic curve is 163 bits while a RSA password is 1024 bits. The algorithm in computing shall be safe within limited time [17]. In the user authentication server identity resolution process, user ID, password, and original fingerprint information will not be obtained. So, user's privacy is well protected in our scheme.

The performances and functions mentioned in our scheme had once been compared with those in Lee *et al.*'s scheme[2], Lin *et al.*'s scheme[3] and Khan *et al.*'s[4] scheme. These comparisons above 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 can see that our DFRE-IBC scheme, compared with theirs, could ensure higher security and better functioning. It shows that our DFRE-IBC scheme can perfectly meet the authentication requirements in DCRMS environment.

V. APPLICATION AND ANALYSIS EXPERIMENTS

We had performed an experiment before to evaluate the performance and function of our scheme. In our experiment, a datacenter machine room monitoring system was implemented based on a client-server model which could perform verification over the Internet. The fingerprint collection device we used is U.are.U 4000 from the SUPCON Company, and the USBKey is eToken NG-FLASH 64k.

As shown in fig. 4, the DCRMS client login screen, the implemented system works as proper as users needed during the registration. Admin shall enter the user registration screen by clicking on the "register" button.

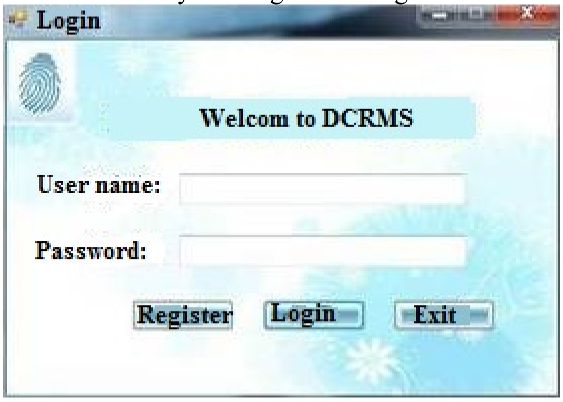
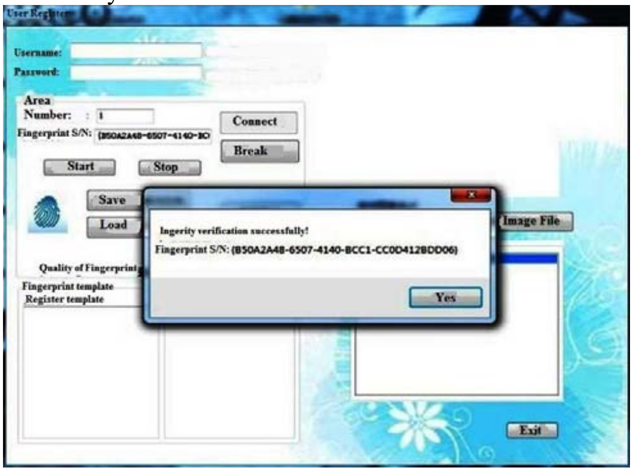


Fig.4 client login Interface

The User Registration Interface is shown in Fig.5. Enter the registered user interface, and the system will verify the digital fingerprint automatically. If its integrity verification passed through, the system would carry out a new user registration. Otherwise, the system would send alarm record and then return to the client login interface automatically.



Area Number: 1

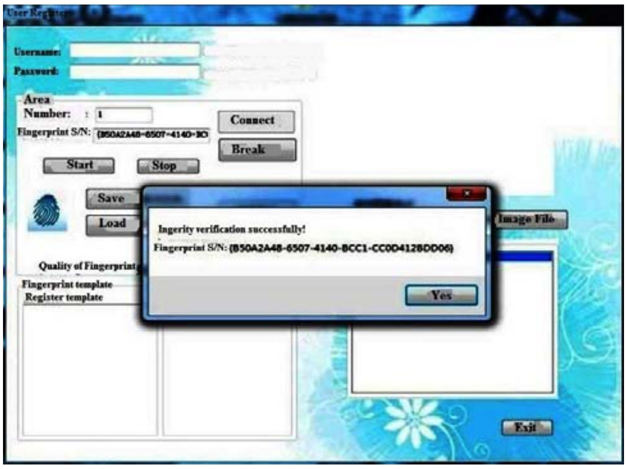
Fingerprint S/N: (B50A2A48-6507-4140-BC

Ingerity verification successfully!

Fingerprint S/N: (B50A2A48-6507-4140-BCC1-CC0D412BDD06)

Fig.5 user registration interface

After passing through the user registration successfully, the clients may get into the login interface and input their user names and passwords. DCRMS user authentication interface is shown in Fig. 6. The system would come to verify whether the validation is success or not by checking the integrity verification of digital fingerprint again. And the digital fingerprint acquisition instrument would collect user's fingerprint. Clients may extract the fingerprint feature template. And the trusted authentication server would have interactions with the identity authentication.



Area Number: 1

Fingerprint S/N: (B50A2A48-6507-4140-BC

Ingerity verification successfully!

Fingerprint S/N: (B50A2A48-6507-4140-BCC1-CC0D412BDD06)

Fig.6 user authentication interface

User's identity shall be certified by judging whether the login information is right or not. During the DCRMS system user login process, the certification results and the time used shall be recorded. The function of identity authentication system based on DFRE -IBC is validated by False Rejection Rate (FRR) and False Acceptance Rate (FAR), while the real-time function is validated by the user authentication time. The test results of identity authentication system based on DFRE -IBC is 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 false reject rate of authentication system is 1.83% while the false acceptance rate is 0, and the average login time is 0.94 s.

VI. CONCLUSION

Here in this paper, an authentication method based on DFRE-IBC is presented. It owns the following features and advantages:

(1) An authentication method based on DFRE-IBC is not only a kind of cryptography but also a kind of fingerprint recognition technology. Taking the elements of security, privacy, and non-repudiation into account, it is more suitable for DCRMS among entity authentication.

(2) The method is mainly a fusion of user's fingerprint characteristic and asymmetric authentication technology, which is to secure the implementation in DCRMS

environment. It will not expose any fingerprint samples information to authentication server.

(3) We have analyzed the validity, security, and functionality properties of our proposed scheme. And it comes to a conclusion that the DFRE-IBC scheme could totally meet the requirements of authentication in DCRMS environmental.

ACKNOWLEDGMENT

This work was partially supported by the New Century Excellent Researcher Award Program from Ministry of Education of China (NCET-08-0211), the project of Guangxi university of science and technology research (No.2013YB242) and the foster special provincial level project of Hezhou university (No.2012PYZK06).

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] Fenghua Liu. “Efficient Two-Factor Authentication Protocol Using Password and Smart Card”. Journal of computers, vol.8, no.12, pp: 3257-3263, 2013.

[9] Chunguang Ma, Jiuru Wang, Peng Wu,et al. “Identity Authentication and Key Agreement Integrated Management Protocol for Heterogeneous Sensor Networks”. Journal of computers, vol.7, no.8, pp: 1847-1852, 2012.

[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, pp: 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.. “A 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.

Changgeng Yu was born in 1974, is currently a lecturer in Hezhou University, Hezhou, China. He received the M.S. degree from Guilin University of Electronic Technology in 2009. Now he is pursuing his doctorate at School of Mechanical and Automotive Engineering in South China University of Technology. Major in Manufacturing Engineer Intelligent Detection and Instrument, Research area includes modern testing and automation equipment, information system modeling theory and application.

Guixiong Liu was born in 1968, is currently a professor and doctoral supervisor in South China University of Technology, Guangzhou, China. He received doctor degree from Chongqing University, Chongqing, China, in 1995. His research interests include modern detection technology and networked control, intelligent sensing theory and method, information system modeling theory and application.