International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

AN EFFICIENT AND PRIVACY-PRESERVING BIOMETRIC IDENTIFICATION SCHEME IN CLOUD COMPUTING

N Ashok [1],Somysetty Tejaswini[2], Sama Tharun Reddy[3],Mettu Manisha Reddy[4], Penumula Uday Sagar[5]

[2,3,4,5] UG Scholars, Department of CSE, **AVN Institute of Engineering and Technology,**Hyderabad, Telangana, India.

[1] Assistant Professor, Department of CSE, **AVN Institute of Engineering and Technology**, Hyderabad, Telangana, India.

ABSTRACT

Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which however brings potential threats to users' privacy. In this paper, we propose an efficient and privacy-preserving biometric identification outsourcing scheme. Specifically, the biometric data is encrypted and outsourced to the cloud server. To execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over the encrypted database and returns the result to the database owner. A thorough security analysis indicates the proposed scheme is secure even if attackers can forge identification requests and collude with the cloud. Compared with previous protocols, experimental results show the proposed scheme achieves a better performance in both preparation and identification procedures.

INTRODUCTION

BIOMETRIC identification has raised increasingly attention since it provides a promising way to identify users. Compared with traditional authentication methods based on passwords and identification cards, biometric identification is considered to be more reliable and convenient. Additionally, biometric identification has been widely applied in many fields by using biometric traits such as fingerprint, iris, and facial patterns, which can be collected from various sensors.

In a biometric identification system, the database owner such as the FBI who is responsible to manage the national fingerprints database, may desire to outsource the enormous biometric data to the cloud server (e.g., Amazon) to get rid of the expensive storage and computation costs. However, to preserve the privacy of biometric data, the biometric data has to be encrypted before outsourcing. Whenever a FBI's partner (e.g., the police station) wants to authenticate an individual's identity, he turns to the FBI and generates an identification query by using the individual's biometric traits (e.g., fingerprints, irises, voice patterns, facial patterns etc.). Then, the FBI encrypts the query and submits it to the cloud to find the close match. Thus, the challenging problem is how to design a protocol which enables efficient and privacy- preserving biometric identification in the cloud computing.

A number of privacy-preserving biometric identification solutions have been proposed. However, most of them mainly concentrate on privacy preservation but ignore the efficiency, such as the schemes based on homomorphic encryption and oblivious transfer for fingerprint and face image identification respectively. Suffering from performance problems of local devices, these schemes are not efficient once the size of the database is larger than 10 MB. Later, Evans presented a biometric identification scheme by utilizing circuit design and ciphertext packing techniques to achieve efficient identification for a larger database of up to 1GB. Additionally, Yuan and Yu proposed an efficient privacy-preserving biometric identification scheme. Specifically, they constructed three modules and designed a concrete protocol to achieve the security of fingerprint trait. To improve the efficiency, in their scheme, the database owner outsources identification matching tasks to the cloud. However, Zhu pointed out that Yuan and Yu's protocol can be broken by a collusion attack launched by a malicious user and cloud. Wang proposed the scheme Cloud BI-II which used random diagonal matrices to realize biometric identification. However, their work wasproven insecure.

In this paper, we propose an efficient and privacy- preserving biometric identification scheme which can resist the collusion attack launched by the users and the cloud. Specifically, our main contributions can be summarized as follows:

- We examine the biometric identification scheme and show its insufficiencies and security weakness under the proposed level-3 attack. Specifically, we demonstrate that the attacker can recover their secret keys by colluding with the cloud, and then decrypt the biometrictraits of all users.
- We present a novel efficient and privacy-preserving biometric identification scheme. The detailed security analysis shows that the proposed scheme can achieve a required level of privacy protection. Specifically, our scheme is secure under the biometric identification out-sourcing model and can also resist the attack proposed.
- Compared with the existing biometric identification schemes, the performance analysis shows that the pro- posed scheme provides a lower computational cost in both preparation and identification procedures.

LITERATURAL SURVEY

1) Privacy-preserving fingercode authentication.

AUTHORS: Mauro Barni, Mario Di Raimondo, Tiziano Bianchi, and Dario Catalano

We present a privacy preserving protocol for fingerprint based authentication. We consider a scenario where a client equipped with a fingerprint reader is interested into learning if the acquired fingerprint belongs to the database of authorized entities managed by a server. For security, it is required that the client does not learn anything on the database and the server should not get any information about the requested biometry and the outcome of the matching process. The proposed protocol follows a multi-party computation approach and makes extensive use of homomorphic encryption as underlying cryptographic primitive. To keep the protocol complexity as low as possible, a particular representation of fingerprint images, named Fingercode, is adopted. Although the previous works on privacy-preserving biometric identification focus on selecting the best matching identity in the database, our main solution is a generic identification protocol and it allows to select and report all the enrolled identities whose distance to the user's fingercode is under a given threshold. Variants for simple authentication purposes are provided. Our protocols gain a notable bandwidth saving (about 8 − 24%) if compared with the best previous work and its computational complexity is still low and suitable for practical applications. Moreover, even if such protocols are presented in the context of a fingerprint based system, they can be generalized to any biometric system that shares the same matching methodology, namely distance computation and thresholding.

2) Efficient privacy-preserving biometric identification

AUTHORS: Yan Huang, Lior Malka, David Evans, and Jonathan Katz

We present an efficient matching protocol that can be used in many privacy-preserving biometric identification systems in the semi-honest setting. Our most general technical contribution is a new backtracking protocol that uses the byproduct of evaluating a garbled circuit to enable efficient oblivious information retrieval. We also present a more efficient protocol for computing the Euclidean distances of vectors, and optimized circuits for finding the closest match between a point held by one party and a set of points held by another. We evaluate our protocols by implementing a practical privacy-preserving fingerprint matching system.

3. Collusion-resisting secure nearest neighbor query over encrypted data in cloud

AUTHORS Youwen Zhu ; Zhikuan Wang ; Jian Wang

It is a challenging problem to securely resist the collusion of cloud server and query users while implementing nearest neighbor query over encrypted data in cloud. Recently, CloudBI-II is put forward to support nearest neighbor query on encrypted cloud data, and declared to be secure while cloud server colludes with some untrusted query users. In this paper, we propose an efficient attack method which indicates CloudBI-II will reveal the difference vectors under the collusion attack. Further, we show that the difference vector disclosure will result in serious privacy breach, and thus attain an efficient attack method to break CloudBI-II. Namely, CloudBI-II cannot achieve their declared security. Through theoretical analysis and experiment evaluation, we confirm our proposed attack approach can fast recover the original data from the encrypted data set in CloudBI-II. Finally, we provide an enhanced scheme which can efficiently resist the collusion attack.

4. Security analysis on privacy-preserving cloud aided biometric identification schemes

Biometric identification (BI) is the task of searching a pre-established biometric database to find a matching record for an enquiring biometric trait sampled from an unknown individual of interest. This has recently been aided with cloud computing, which brings a lot of convenience but simultaneously arouses new privacy concerns. Two cloud aided BI schemes pursuing privacy preserving have recently been proposed by Wang et al. in ESORICS '15. In this paper, we propose several elaborately designed attacks to reveal the security breaches in these two schemes. Theoretical analysis is given to validate our proposed attacks, which indicates that via such attacks the cloud server can accurately infer the outsourced database and the identification request.

SYSTEM ANALYSIS

Existing System:

Biometric identification has become increasingly popular in recent years. With the development of cloud computing, database owners are motivated to outsource the large size of biometric data and identification tasks to the cloud to get rid of the expensive storage and computation costs, which however brings potential threats to users' privacy.

In a biometric identification system, the database owner such as the FBI who is responsible to manage the national fingerprints database, may desire to outsource the enormous biometric data to the cloud server (e.g., Amazon) to get rid of the expensive storage and computation costs.

Proposed System:

We propose an efficient and privacy-preserving biometric identification scheme which can resist
The collusion attack launched by the users and the cloud. Specifically, our main contributions can be summarized as follows:

We examine the biometric identification scheme and show its insufficiencies and security weakness under the proposed level-3 attack. Specifically, we demonstrate that the attacker can recover their secret keys by colluding with the cloud, and then decrypt the biometric traits of all users.

We present a novel efficient and privacy-preserving biometric identification scheme.

The detailed security analysis shows that the proposed scheme can achieve a required level of privacy protection. Specifically, our scheme is secure under the biometric identification outsourcing model and can also resist the attack proposed.

Compared with the existing biometric identification schemes, the performance analysis shows that the proposed scheme provides a lower computational cost in both preparation and identification procedures.

Advantages:

- To realize the efficiency and secure requirements, we have designed a new encryption algorithm and cloud authentication certification.

- The detailed analysis shows it can resist the potential attacks.

IMPLEMENTATION

MODULES

- ❖ Database Owner
- ❖ Data
- ❖ Cloud Server

MODULES DESCRIPTION:

Database Owner:

- ➢ The database owner holds a large size of biometric data (i.e., fingerprints, irises, voice, and facial patterns etc.), which is encrypted and transmitted to the cloud for storage.

- ➢ After receiving the request, the database owner generates a ciphertext for the biometric trait and then transmits the ciphertext to the cloud for identification.

- ➢ Database owner computes the similarity between the query data and the biometric data associated with the index, and returns the query result to the user.

Data User:

- ➢ When a user wants to identify himself/herself, a query request is be sent to the database owner.

Cloud Server:

- ➢ The cloud server figures out the best match for the encrypted query and returns the related index to the database owner.

SYSTEM DESIGN

SYSTEM ARCHITECTURE

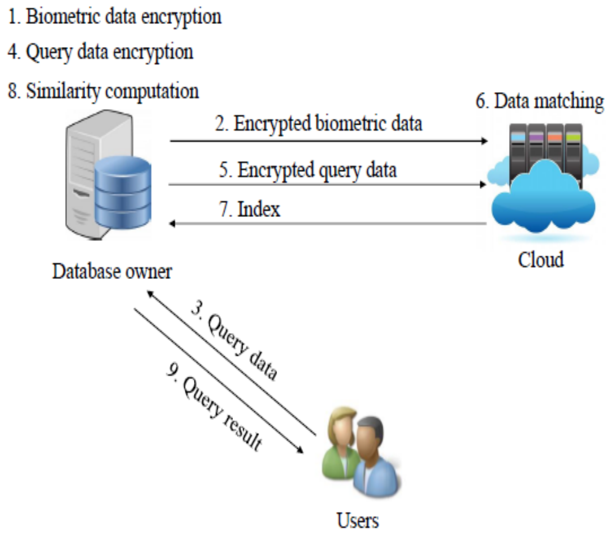
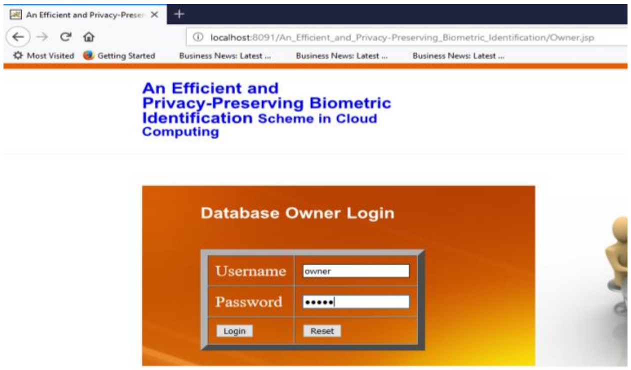


Fig. System Architecture

Results :

Home Page

Database Owner Login



localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Identification/Owner.jsp

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

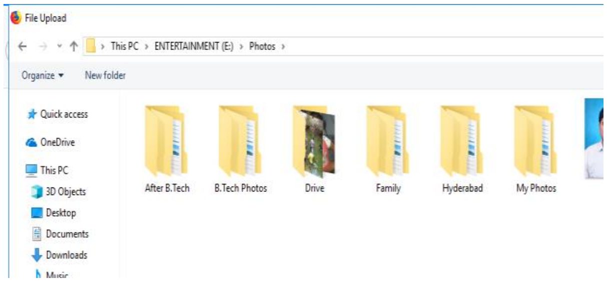
Database Owner Login

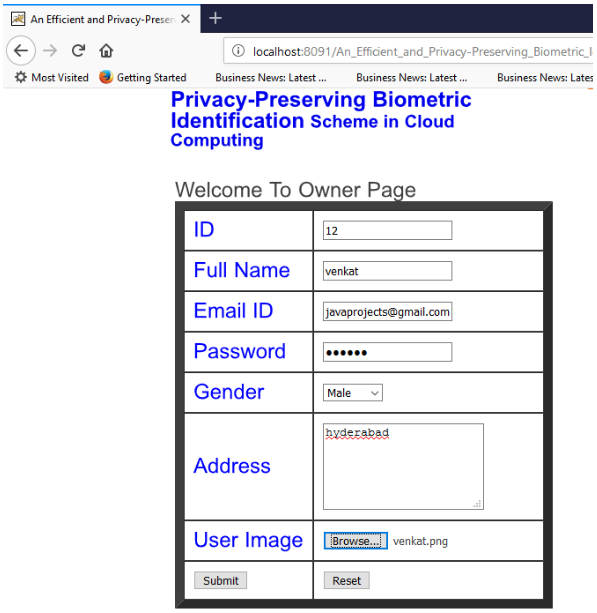
Username: owner

Password: •••••

An Efficient and Privacy-Preser
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
Login
Reset

… .





localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_I

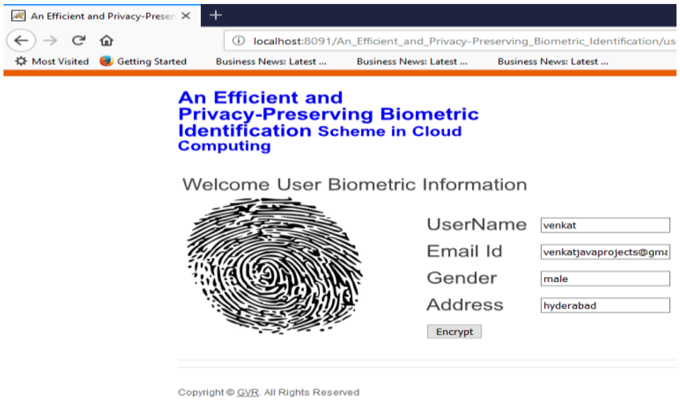
Privacy-Preserving Biometric Identification Scheme in Cloud Computing

Welcome To Owner Page

ID	12
Full Name	venkat
Email ID	javaprojects@gmail.com
Password	••••••
Gender	Male
Address	hyderabad
User Image	Browse... venkat.png
Submit	Reset

An Efficient and Privacy-Preser
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Lates

Biometric Information



localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Identification/us

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

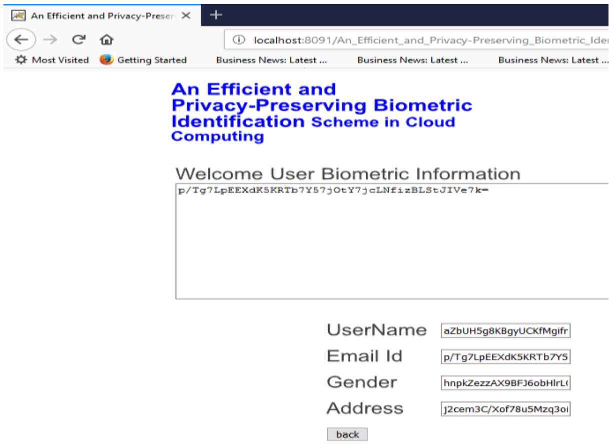
Welcome User Biometric Information

UserName	venkat
Email Id	venkatjavaprojects@gma
Gender	male
Address	hyderabad

Copyright © GVR. All Rights Reserved

An Efficient and Privacy-Preser
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
Encrypt

Encrypted Details



localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Ide

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

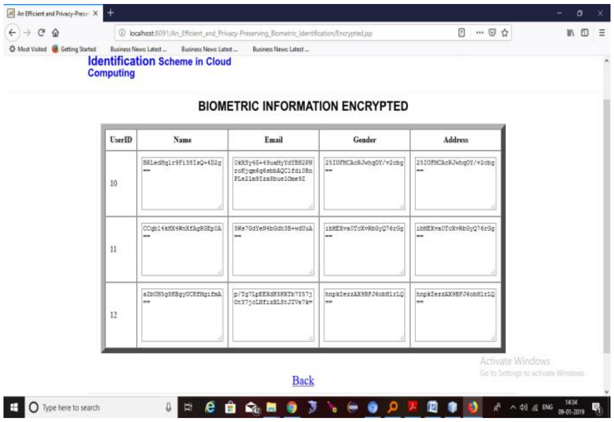
Welcome User Biometric Information

p/Tg7LpEEXdK5KRTb7Y57jOtY7jcLNfizBLStJIVe7k=

UserName	aZbUH5g8KBgyUCKfMgifr
Email Id	p/Tg7LpEEXdK5KRTb7Y5
Gender	hnpkZezzAX9BFJ6obHlrL(
Address	j2cem3C/Xof78u5Mzq3oi

An Efficient and Privacy-Preser
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
back

Biometric Information Encrypted



localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Identification/Encrypted.jsp

Identification Scheme in Cloud Computing

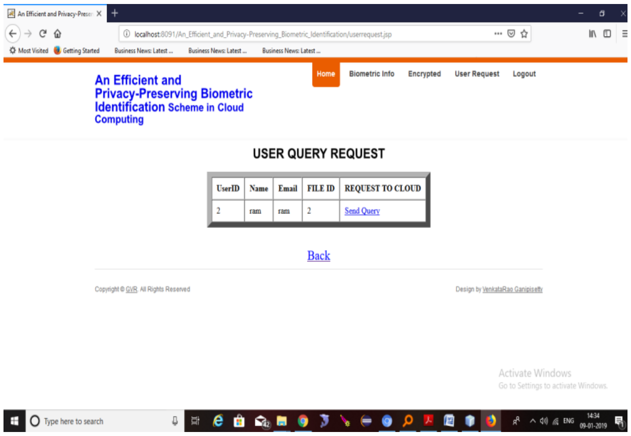
BIOMETRIC INFORMATION ENCRYPTED

UserID	Name	Email	Gender	Address
10	BRLedHqlr9Fi38IsQ+4D2g==	0kKSy4G+49uaMyYdYBH2PNroKjqm6q6sbbAQClfdi0RnPLe2lm9Iza8bue1Ome9Z	25IOFMCAcRJwhqOY/v2cbg==	25IOFMCAcRJwhqOY/v2cbg==
11	CCqb14kMX4WnXfAgRGEp0A==	5Ws7GdYeN4bGdh3B+wdUuA==	ibMEXva0TcXvRbGyQ76rGg==	ibMEXva0TcXvRbGyQ76rGg==
12	aZbUH5g8KBgyUCKfMgifmA==	p/Tg7LpEEXdK5KRTb7Y57jOtY7jcLNfizBLStJIVe7k=	hnpkZezzAX9BFJ6obHlrLQ==	hnpkZezzAX9BFJ6obHlrLQ==

Back

An Efficient and Privacy-Prese
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
Activate Windows
Go to Settings to activate Windows.
Type here to search
ENG
14:34
09-01-2019

User Query Request


An Efficient and Privacy-Preser
localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Identification/userrequest.jsp
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
Home
Biometric Info
Encrypted
User Request
Logout
Activate Windows
Go to Settings to activate Windows.
Type here to search
14:34
09-01-2019

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

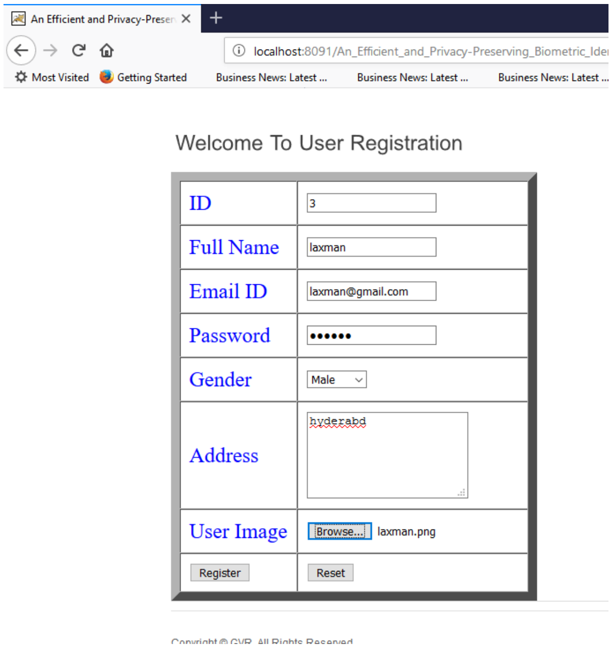
USER QUERY REQUEST

UserID	Name	Email	FILE ID	REQUEST TO CLOUD
2	ram	ram	2	Send Query

Back

Copyright © GVR. All Rights Reserved   Design by VenkataRao Ganipisetty

User Registration

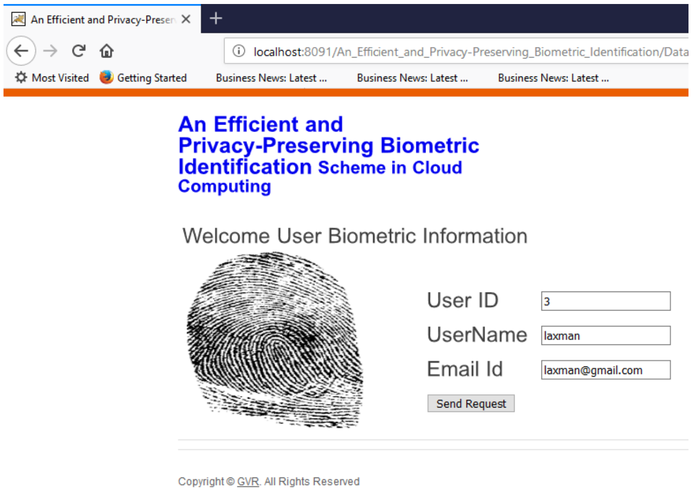

An Efficient and Privacy-Preser
localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Ide
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
Browse...
Register
Reset

Welcome To User Registration

ID	3
Full Name	laxman
Email ID	laxman@gmail.com
Password	••••••
Gender	Male
Address	hyderabd
User Image	laxman.png

Copyright © GVR. All Rights Reserved

Data Request To database owner


An Efficient and Privacy-Preser
localhost:8091/An_Efficient_and_Privacy-Preserving_Biometric_Identification/Data
Most Visited
Getting Started
Business News: Latest ...
Business News: Latest ...
Business News: Latest ...
Send Request

An Efficient and Privacy-Preserving Biometric Identification Scheme in Cloud Computing

Welcome User Biometric Information

User ID	3
UserName	laxman
Email Id	laxman@gmail.com

Copyright © GVR. All Rights Reserved

CONCLUSION

In this paper, we proposed a novel privacy-preserving biometric identification scheme in the cloud computing. To realize the efficiency and secure requirements, we have designed a new encryption algorithm and cloud authentication certification. The detailed analysis shows it can resist the potential attacks. Besides, through performance evaluations, we further demonstrated the proposed scheme meets the efficiency need well.

REFERENCES

[1] A. Jain, L. Hong and S. Pankanti, “Biometric identification,” Communications of the ACM, vol. 43, no. 2, pp. 90-98, 2000.

[2] R. Allen, P. Sankar and S. Prabhakar, “Fingerprint identification technology,” Biometric Systems, pp. 22-61, 2005.

[3] J. de Mira, H. Neto, E. Neves, et al., “Biometric-oriented Iris Identification Based on Mathematical Morphology,” Journal of Signal Processing Systems, vol. 80, no. 2, pp. 181-195, 2015.

[4] S. Romdhani, V. Blanz and T. Vetter, “Face identification by fitting a 3d morphable model using linear shape and texture error functions,” in European Conference on Computer Vision, pp. 3-19, 2002.

[5] Y. Xiao, V. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A survey of key management schemes in wireless sensor networks,” Journal of Computer Communications, vol. 30, no. 11-12, pp. 2314-2341, 2007.

[6] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, “An effective key management scheme for heterogeneous sensor networks,” Ad Hoc Networks, vol. 5, no. 1, pp. 24-34, 2007.

[7] X. Du and H. H. Chen, “Security in wireless sensor networks,” IEEE Wireless Communications Magazine, vol. 15, no. 4, pp. 60-66, 2008.

[8] X. Hei, and X. Du, “Biometric-based two-level secure access control for implantable medical devices during emergency,” in Proc. of IEEE INFOCOM 2011, pp. 346-350, 2011.

[9] X. Hei, X. Du, J. Wu, and F. Hu, “Defending resource depletion attacks on implantable medical devices,” in Proc. of IEEE GLOBECOM 2010, pp. 1-5, 2010.

[10] M. Barni, T. Bianchi, D. Catalano, et al., “Privacy-preserving fingercode authentication,” in Proceedings of the 12th ACM workshop on Multimedia and security, pp. 231-240, 2010.