An Efficient And Privacy-Preserving Biometric Identification Scheme In Cloud Computing

[1]Dr.P.PRATHUSHA [2]K.ADI LAKSHMI ,[3] K. HARITHA ,[4]B.SAI DIVYA,[5]B.VEERA NAVYA
[1]GUIDE Assistant Professor, [2,3,4] U.G Scholar

[1,2,3,4] DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
RAVINDRA COLLEGE OF ENGINEERING FOR WOMEN

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 project, 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.

I. INTRODUCTION

1.1 Overview of the Project

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 [1]. Additionally, biometric identification has been widely applied in many fields by using biometric traits such as fingerprint [2], iris [3], and facial patterns [4], which can be collected from various sensors [5]–[9]. 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.

1.2 Objective of the Project

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 number of privacy-preserving biometric identification solutions [10]–[17] 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 in [10], [11] for fingerprint and face image identification respectively.

1.3 Motivation

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.

1.4 Exisisting System

- Related works on privacy-preserving biometric identification are provided in this section. Recently, some efficient biometric identification schemes have been proposed.
- Wangand Hatzinakos proposed a privacy-preserving face recognition scheme [22]. Specifically, a face recognition method is designed by measuring the similarity between sorted index numbers vectors.
- Wong and Kim [23] proposed a privacy preserving biometric matching protocol for iris codes verification. In their protocol, it is computationally infeasible for a

malicious user to impersonate as an honest user.

- Barni et al. [10] presented a Finger Code identification protocol based on the Homomorphic Encryption technique.
- However, all distances are computed between the query and sample Finger codes in the database, which introduces too much burden as the size of fingerprints increases.
- To improve the efficiency, Evans et al. [12] proposed a novel protocol which reduces the identification time.
- They used an improved Homomorphic encryption algorithm to compute the Euclidean distance and designed novel garbled circuits to find the minimum distance.
- By exploiting a backtracking protocol, the best match Finger-Code can be found. However, in [12], the whole encrypted database has to be transmitted to the user from the database server.
- Wong et al. [24] proposed an identification scheme based on kNN to achieve secure search in the encrypted database.

1.5 Disadvantages

- The system doesn't implement Biometric Identification Scheme.
- There is no an affective privacy preserving encryption techniques in this system.

1.6 Design Challenges and Issues

In order to achieve practicality, both security and efficiency are considered in the proposed scheme. To be more specific, design goals of the proposed scheme are described as follows:

- Efficiency: Computational costs should be as low as possible at both the databaseowner side and the user side. To gain high efficiency, most biometric identification operations should be executed in the cloud.
- Security: During the identification process, the privacy of biometric data should be protected. Attackers and the semi-honest cloud should learn nothing about the sensitive information.
- Thus, the challenging problem is how to design a protocol which enables efficient and privacy preserving biometric identification in the cloud computing. Most of them mainly concentrate on privacy preservation but ignore the efficiency, such as the schemes based on homomorphic encryption and oblivious transfer.
- A number of privacy-preserving biometric identification solutions [10]–[17] 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 in [10], [11] 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.

1.7 Applications of the Project

- With the rapid growth in the development of smart devices equipped with biometric sensors, client identification system using biometric traits are widely adopted across various applications.
- Among many biometric traits, fingerprint-based identification systems have been extensively studied and deployed.
- However, to adopt biometric identification systems in practical applications, two main obstacles in terms of efficiency and client privacy must be resolved simultaneously.
- Border control and airport: A key area of application for biometric technology is at the border. Biometric technology helps to automate the process of border crossing. Reliable and automated passenger screening initiatives and automated SAS help to facilitate international passenger travel experience while improving the efficiency of government agencies and keeping borders safer than ever before.
- Healthcare: In the field of healthcare, biometrics introduces an enhanced model. Medical records are among the most valuable personal documents; doctors need to be able to access them quickly, and they need to be accurate. A lack of security and good accounting can make the difference between timely and accurate diagnosis and health fraud.
- Security: As connectivity continues to spread around the world, it is clear that old security methods are simply not strong enough to protect what is most important. Fortunately, biometric technology is more accessible than ever, ready to provide added security and convenience for everything that needs to be protected, from a car door to the phone's PIN.

II. LITEREATURE SURVEY

Kannavara and Bourbakis [1] summarized a series of biometric recognition methods based on neural networks by using voice, iris, fingerprint, palm-print and face and pointed out potential ways to improve these methods.

Shunmugam and Selvakumar [2] believed that unimodal biometric methods are limited. Multimodal biometric methods are much more reliable for building up a safer authentication system. They discussed

such multimodal methods as multiple sensors, multiple algorithms, multiple instances, multiple samples and hybrid models.

Meng et al. [3] surveyed 11 types of biometric authentication methods on mobile phones.He pointed out a series of potential attacks in a generic biometric authentication system.

Blasco et al. [4] focused on sensors in wearable devices and classified the biological signals that can be collected by wearable devices. They discussed the difference between biometric authentication methods and traditional ones and analyzed the computational cost of different signal processing techniques.

Borra et al. [5] focused on fingerprint recognition technologies. They discussed different types of fingerprint structures and studied different fingerprint recognition approaches including pattern recognition, wavelet and wave atom.

Sreeja and Misbahuddin [6] discussed deoxyribonucleic acid (DNA) based cryptography methods.
A couple of surveys [7], [8] focused on keystroke dynamics.

Padma and Srinivasan [9] reviewed the existing biometric authentication mechanisms in a cloud computing environment. In this paper, biometric authentication was classified into two categories: physical based biometric authentication and behavioral based authentication.

Barni et al. [10] presented a FingerCode identification protocol based on the Homomorphic Encryption technique. However, all distances are computed between the query and sample Fingercodes in the database, which introduces too much burden as the size of fingerprints increases.

González-Jiménez and Alba-Castro [11] proposed a point distribution model to deal with the pose variation in 2-D face recognition. They used pose eigenvectors and pose parameters to synthesize pose corrected images based on thin plate splines-based warping. In the evaluation, the proposed methods achieved state-of-the-art results, outperforming a 3-D morphable model and other approaches in a set of rotation angles ranging from -45° to 45° . This face recognition's accuracy is not high, only about 30%.

Evans et al. [12] presented a biometric identification scheme by utilizing circuit design and ciphertext packing techniques to achieve efficient identification for a larger database of upto1GB. He proposed a novel protocol which reduces the identification time. They used an improved Homomorphic encryption algorithm to compute the Euclidean distance and designed novel garbled circuits to find the minimum distance. By exploiting a backtracking protocol, the best match FingerCode can be found.

Yuan and Yu [13] 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.

Wang et al. [14] proposed the scheme CloudBI-II which used random diagonal matrices to realize biometric identification. Based on [13], Wang et al. presented a privacy-preserving biometric identification scheme in [14] which introduced random diagonal matrices, named CloudB I-II.

Pillai et al. [15] proposed a unified framework based on random projections and sparse representations. Its algorithm can deal with common distortion in iris image collection. Thus, this iris recognition method can achieve very high accuracy, over 99%.

Thavalengal et al. [16] analyzed the feasibility of iris recognition applied to non-contact handheld devices. They argued that pixel resolution still limits the application of iris recognition, while existing optical design and smartphone volume cannot allow the embedment of this system.

Thavalengal et al. [17] focused on critical factors for system implementation such as iris size, image quality and acquisition wavelength. They discussed system requirements for unconstrained acquisition in smartphones.

Zhu et al. [18] pointed out their protocol can be broken if a malicious user colludes with the cloud server in the identification process. He showed an attack for Yuan and Yu's scheme. In their attack, the attacker observes the cloud and gets the values of relative distance.

Czajka et al. [19] presented a biometric smart card that can support multi-factor verification. The experimental results show that the method achieves 100% accuracy, and the average time consuming to complete the recognition process is 8.465 seconds. This scheme uses an iris coder based on Zak-Gabor transform and includes an eye aliveness detection.

Rigas and Komogortsev [20] applied the difference between a paper-printed iris and a natural eye iris to propose a method based on the utilization of eye movement to deal with the iris fake attack. Due to the similarities between eye tracking and iris capturing systems, the method they proposed can be used in the existing iris authentication systems with a minimal cost.

Bodade and Talbar [21] proposed a method to detect the inner boundary of iris based on pupil size variation. Since pupil size changes with different light levels, its variation can be used to detect the aliveness of iris. 384 images of both

eyes of 64 subjects were used in experimental tests.

Wang and Hatzinakos proposed a privacy-preserving face recognition scheme [22]. Specifically, a face recognition method is designed by measuring the similarity between sorted index numbers vectors.
Wong and Kim [23] proposed a privacy preserving biometric matching protocol for iris codes verification. In their protocol, it is computationally infeasible for a malicious user to impersonate as an honest user.

Wong et al. [24] proposed an identification scheme based on kNN to achieve secure search in the encrypted database. However, their scheme assumes that there is no collusion between the client side and cloud server side.

Kumar and Ravikanth [25] presented a new approach for personal authentication by using finger-back surface imaging. This paper introduced a pegfree imaging technology. The finger- back surface images of each user are normalized to minimize their scale, translation, and rotational variations in knuckle images.

2.3 Proposed System

In this project, we propose an efficient and privacypreserving 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:

- The proposed system examines the biometric identification scheme [13] and shows 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.
- The system presents 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 by the proposed system.
- 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.

2.4 Advantages of Proposed System

- An efficient and privacy preserving biometric identification scheme which can resist the collusion attack launched by the users.
- Attackers can only observe the encrypted data stored in the cloud. In order to avoid, the well-known cipher text-only

attack model has been implemented.

SYSTEM ANALYSIS AND DESIGN

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

Output Design

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rests with the administrator only.The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients.

III. Modules

The project working is divided into 3 modules.

- Data owner

- Cloud Server
- Users

3.1.1 Data Owner

In this module, the data owner uploads their Biometric images with their contents data to the Cloud server. For the security purpose the data owner assigns the digital sign and then store in the Cloud and also performs the following operations such as Upload Biometric image with its digital sign based on title, desc, List all uploaded Biometric images, Verify Biometric image details, and Delete Biometric image details.

3.1.2 Cloud Server

The Cloud service provider manages a Cloud to provide data storage service. And performs the following operations such as Store all Biometric image files with their signature, View all Biometric image Files with its details, View all Biometric image comments, View all Data owners and Users, and View all attackers.

3.1.3 Users

The Cloud User who has a large amount of data to be stored in Cloud Servers and have the permissions to access and manipulate stored Biometric image and its data. The consumer will search the data and accessing the Biometric image data if he is authorized and performs the following operations such as Search Biometric image , Access Biometric image and its details, Download Biometric image & make comments.

IV. IMPLEMENTATION

4.1 Homomorphic Encryption Alogirthm

Homomorphic Encryption algorithms utilize some basic four-step process:

1. The sender retrieves the recipient's public key.
2. The sender uses the public key to encrypt plaintext.
3. The sender sends the ciphertext to the recipient.
4. The recipient uses the recipient's private key to decrypt the ciphertext. The recipient can now view the plaintext.

Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

Homomorphic encryption can be used for privacy-preserving outsourced storage and computation. This allows data to be encrypted and out-sourced to commercial cloud environments for processing, all while encrypted. In highly regulated industries, such as health care, homomorphic encryption can be used to enable new services by removing privacy barriers inhibiting data sharing.

4.2 Explanation of Alogirthm

4.2.1 Structural Similarity

Homomorphic encryption is a form of encryption with an additional evaluation capability for computing over encrypted data without access to the secret key. The result of such a computation remains encrypted. Homomorphic encryption can be viewed as an extension of either symmetric- key or public-key cryptography. Homomorphic refers to homomorphism in algebra: the encryption and decryption functions can be thought of as homomorphisms between plaintext and ciphertext spaces.

We construct a novel biometric identification scheme to address the weakness of Yuan and Yu's scheme[13]. To achieve a higher level of privacy protection, a new retrieval way is constructed to resist the level-3 attack. Moreover, we also reconstruct the ciphertext to reduce the amount of uploaded data and improve the efficiency both in the preparation and identification procedures.

In the remaining part of this section, we will introduce the preparation process and the identification process.

Preparation process

In the preparation process, bi is the i-th sample feature vector derived from the finger print image using a feature extraction algorithm [19]. To be more specific, bi is an n-dimensional vector with l bits of each element where n = 640 and l = 8. For ease of identification, bi is extended by adding an (n+ 1)-th element as Bi. Then, the database owner encrypts Bi with the secret key M1 as follows:

Ci = Bi ×M1. (9)

The database owner further performs the following operation: Ch = M−1 2 ×HT. (10)

Each Finger Code Bi is associated with an index Ii. After execute the encryption operations, the database owner uploads (Ci,Ch,Ii) to the cloud.

Testing

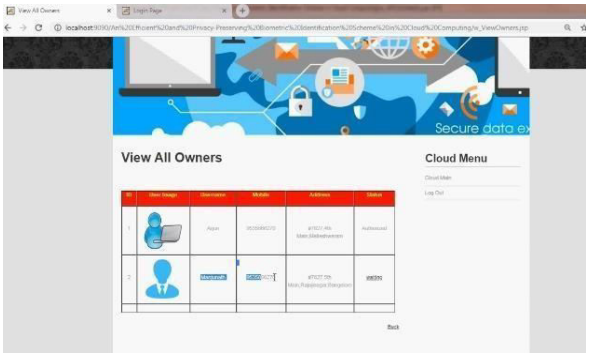
The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

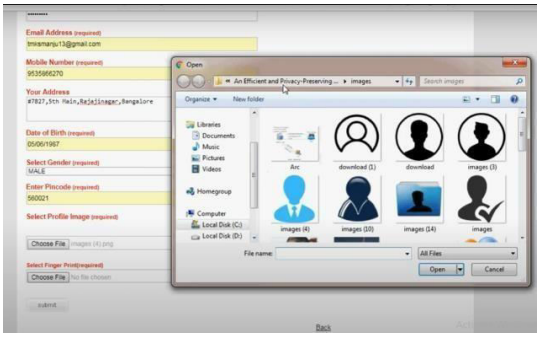
V. Experimental Results

Extensive Experimental Results on the encrypted data generated by various methods show that our proposed system is well generalized and very robust Analysing Concept.We Analyse the data using Homomorphic encryption algorithm that internally generate the secret key in order to provide communication between the database owner and the user.

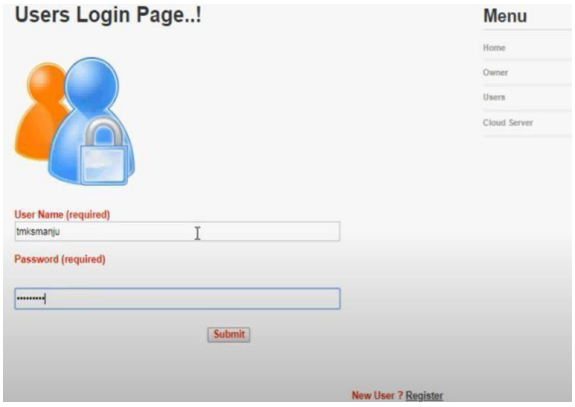
5.2 Screen Shots

Cloud Server login page

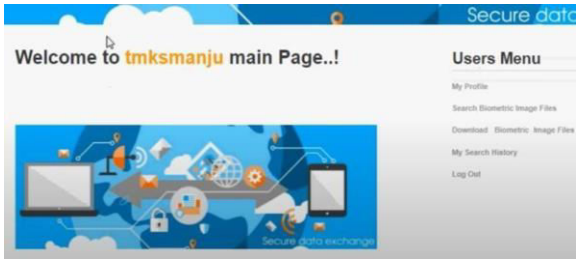




User registering by



Usr's Login page

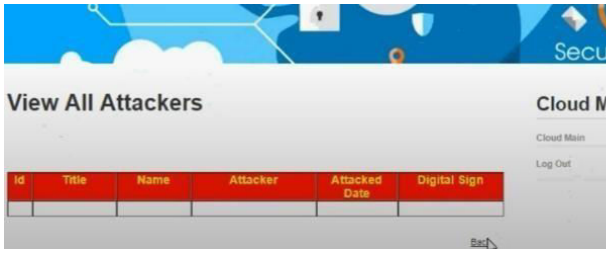


User main page after login

User requesting owner to get details from cloud using secret key

Details of Users

Attacker is modifying the data of the user



View of Attackers

Image showing that user has been attacked successfully

Image showing that the attacked file does not exists

Owner is again checking the details of the user after the result

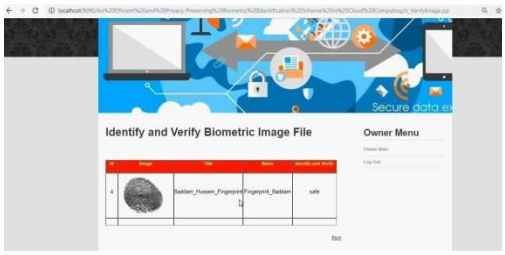


Image showing that the user data is safe

VI Conclusion

In this project, 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.

VI. Future Scope

Biometrics helps in verifying the identity of a person based on physiological or behavioral characteristics. Specifically, traditional authentication methods such as magnetic cards, personal identification cards, passwords or keys are vulnerable to attacks and can be easily stolen. Biometrics technology identifies an individual on the basis of their fingerprints, face, signature, DNA, iris, typing rhythms etc and provides convenient and secure authentication.

With the thriving Internet-based commerce such as online banking and rising need for precise verification while accessing accounts, biometrics technology is considered to be the most convenient and simplest solution.

Biometrics systems are used across several industries including government, defense services, banking and finance, consumer electronics, healthcare, home safety & security, commercial safety & security, transport/visa/logistics among others.

VII. 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] [6]X.Du, Y.Xiao, M.Guizani, and H.H.Chen, "An effective key management scheme for heterogeneous sensor networks," AdHoc 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 IEEEGLOBECOM2010, 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.

[11] M. Osadchy, B. Pinkas, A. Jarrous, et al., "SCiFI-a system for secure face identification," in Security and Privacy (SP),2010 IEEE Symposiumon, pp. 239-254, 2010.

[12] D.Evans, Y.Huang, J.Katz, etal., "Efficient privacy-preserving biometric identification," in Proceedings of the 17th conference Network and Distributed System Security Symposium, NDSS, 2011.

[13] J.Yuan and S.Yu, "Efficient privacy-preserving biometric identification in cloud computing, " in Proc.of IEEEINFOCOM2013, pp.2652-2660, 2013.

[14] Security, pp. 186-205, 2015.

[15] Y.Zhu, Z.Wang and J.Wang, "Collusion-resisting secure nearest neighbor query over encrypted data in cloud," In Quality of Service (IWQoS), 2016 IEEE/ACM 24th International Symposium on, pp. 1-6, 2016.

[16] S. Pan, S. Yan, and W. Zhu, "Security analysis on

privacy-preserving cloud aided biometric identification schemes," in Australasian Conference on Information Security and Privacy, pp. 446-453, 2016.

[17] C. Zhang, L. Zhu and C. Xu, "PTBI: An efficient privacy-preserving biometric identification based on perturbed term in the cloud," Information Sciences, vol. 409, pp. 56-67, 2017.

[18] Y.Zhu, T.Takagi, and R.Hu,"Security analysis of collusion-resistant nearest neighbor query scheme on encrypted cloud data,"IEICETransactionson Information and Systems, vol. 97, no. 2, pp. 326-330, 2014.

[19] A.Jain,S.Prabhakar,L.Hong,etal.,"Filterbank-based fingerprint matching," IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846-859, 2000.

[20] H. Delfs, H. Knebl, and H. Knebl, "Introduction to cryptography," Berlin etc.: Springer, 2002.

[21] K. Liu, C. Giannella, and H. Kargupta, "An attacker's view of distance preserving maps for privacy preserving datamining,"KnowledgeDiscovery in Databases, pp. 297-308, 2006.

[22] Y. Wang, and D. Hatzinakos, "Face recognition with enhanced privacy protection," in IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 885-888, 2009.

[23] [23]K.Wong, and M.Kim, "A privacy-preserving biometric matching protocol for iris codes verification," in Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC), pp. 120-125, 2012.

[24] [24] W. Wong, D. Cheung, B. Kao B, et al., "Secure kNN computation on encrypted databases," in Proceedings of the 2009 ACM SIGMOD International Conference on Management of data, pp. 139-152, 2009.