Feasibility of Deploying Biometric Encryption in Mobile Cloud Computing

Kao Zhao, Hai Jin, Deqing Zou, Gang Chen, Weiqi Dai
Services Computing Technology and System Lab
Cluster and Grid Computing Lab
Huazhong University of Science and Technology, Wuhan, 430074, China
hjin@hust.edu.cn

***Abstract*—*Biometric Encryption* (BE) is a new issue in the information security field which is based on biometric identification and cryptosystems and it will be a key research subject in the future. At the same time the development of cloud computing is not restricted to PC anymore, some cloud computing services for mobile terminals such as cellphones have already appeared due to the booming of mobile internet. However, security problems still exists in *mobile cloud computing* (MCC) inherited from cloud computing and mechanisms are needed to cope with these problems. In this paper, we examine various aspects of using BE in MCC to solve security problems: first, we describe the background and related work of BE and MCC, and second we demonstrate several scenarios of deploying BE in MCC. Specifically, we analyze the new critical issues in these situations that can be used by an adversary to disable the operation of cloud computing environment. We then discuss different BE methods that applying in MCC, and explore scenarios where each method shows its strengths and weaknesses. In particular, we address the problem of using BE to protect privacy for users in MCC. Further, we propose an advanced protocol that employ BE for transferring private data in cloud computing environment, and design a conceptual cloud platform supporting biometric authentication to serve as future data center.**

***Keywords*-Biometric Encryption; Mobile Cloud Computing; Security**

I. Introduction

As mobile network infrastructures continuously improve, their data transmission becomes increasingly available and affordable. It becomes popular for clients to consume web resources instead of using mainstream PC. With the development of wireless access technologies, cloud computing is expected to expand to mobile environments, where mobile devices and sensors are used as the information collection nodes for the cloud. Therefore, MCC appears as an emerging cloud service model following the trend to extend the cloud to the edge of networks. It includes numerous mobile devices closely associated with users. It will be directly involved in many cloud activities that extend the cloud boundaries into the entire cyber physical system. As predicted by Gartner, mobile phones will overtake PCs as the most common web access devices worldwide by 2013 [1]. Thus mobile devices will become more important and will be involved in almost all aspects of our daily life.

To protect private data for users of cloud service, traditional solutions provide cryptographic schemes to enhance the security of data storage and transfer. Compared to security mechanisms based on secret key, biometric encryption is more reliable because it has features of difficult to forget, lose, share and forge. There does not exist a mobile phone that can combine biometric sensor module in its chip to the best of our knowledge. We firmly believe that in near future, mobile phones will support biometric identification with the development of the hardware and BE of mobile computing will be a hot spot in this area. This paper examines how BE can work on mobile device in cloud environment, explores the task of protecting data privacy under various attacks, and provides solutions for deploying BE in MCC.

We begin in section 2 by describing the background of MCC and biometric encryption, as well as the related work. In section 3, we present several application scenarios of MCC using BE, and emphasize the critical issues in these scenarios. We provide a security analysis of using BE in mobile computing in section 4, and explore the situations in which attacks can break the security of it. We introduce our improved method for designing a conceptual mobile cloud platform in section 5. We provide discussion in section 6 and present conclusions in section 7.

II. Background and Related Work

A. Mobile Cloud Computing

MCC refers to the provision of computational resources on demand via mobile internet, moreover it is an application on mobile internet of cloud computing. One important feature of mobile cloud applications is functional collaboration. For example, mobile social network based data mining requires collaborations among mobile users. To this end, mobile cloud will serve as not only a nexus that interconnects information sources gathered from both cloud computing service domain and mobile computing domains, but also a knowledge center to help mobile users in their daily activities.

MCC allows resources in cloud computing platforms such as Amazon EC2, Microsoft Azure, and Google AppEngine to be used to overcome the lack of local resources in mobile devices. Integration between mobile devices and cloud computing is presented in several previous works. Christensen [2] presents general requirements and key technologies to

978-0-7695-5058-9/13 $26.00 © 2013 IEEE
DOI 10.1109/ChinaGrid.2013.10

achieve the vision of MCC. The author introduces an analysis on smart phones, context awareness, cloud and restful based web services, and explains how these components can interact to create a better experience for mobile phone users. Luo [3] introduces the idea of using cloud computing to enhance the capabilities of mobile devices. The main goal of this work is to show the feasibility of such implementation, introducing a new partition scheme for tasks. Giurgiu et al. [4] use the cloud as the container for mobile applications. Applications are pre-processed based on the current context of the user, so only the bundles that can run on the local device and minimize the communication overhead with the cloud are offloaded to the mobile device from the cloud. Marinelli [5] introduces Hyrax, a MCC client that allows mobile devices to use cloud computing platforms. Based on Hadoop, the main focus of this work is to port a client into a mobile device to enable the integration.

B. Biometric Encryption

In traditional identification and authentication solutions, cryptography occupies an important position, especially in the area of access control, security audit, intrusion detection etc. However, in perfect cryptography mechanism, how to protect the secret key becomes the Achilles' heel of a security system [6]. Biometric identification is a science of using physiological or behavioral features of human to identify the person's identity. Physiological features includes fingerprint, iris, face and so on, behavioral features includes signature, voice and tread. Biometric features is more reliable than secret key because they are difficult to forget, lose, share and forge. Recently, biometric identification is gradually accepted as ultimate solution applying in public security, bank and other confidential industries [7].

As security risks exist in biometric identification, a technology which combines biometric identification and cryptography appears: *biometric encryption* (BE). BE combines secret key and biometric feature, and they cannot be achieved in the templates stored in the system, only when a living biometric feature was proposed to the system the secret key would be regenerated. BE was first proposed in a patent by Bodo [8] and completely by Tokmo. Soutar [9] proposed a version of BE. In terms of the actual product, so far Philips has developed encryption system based on face detection. Aratek has developed FDS250 hard disk based on fingerprint authentication. Motorola proposed the Motorola MC7x *Enterprise Digital Assistant* (EDA) rugged handheld mobile device to be the core of mobile biometric identification solution. Jennifer [10] developed a cell phone-based biometric identification system, which uses phone-based acceleration sensors, called accelerometers, to identify and authenticate cell phone users. This is a form of behavioral biometric identification.

Encryption system based on BE technology generally uses following 3 models: key release, key binding and key generation. Key release model simply superposes the secret key and the biometric feature to be the biometric feature template, only if the biometric feature matches the secret key released. Key binding model combines the biometric feature and the key materials to be the biometric feature templates in encryption scheme, only if the biometric feature matches the secret key will be extracted by corresponding algorithm. These two models both combine biometric feature and secret key, the security of these systems are based on secret key, once the secret key is missing, the security of system is broken. Based on these considerations people extract secret key from the signal directly instead of external input. We call this key generation model.

III. Problem Formulation

Mobile applications gain increasing share in a global mobile market. Various mobile applications have taken the advantages of MCC. There are several typical MCC applications such as mobile commerce, mobile learning, mobile healthcare, mobile gaming. Some applications involving confidential data require encryption technology. To address the problem of implementing BE in MCC, we study a sequence of scenarios applying BE technology.

A. BE in Mobile Commerce

Mobile commerce (m-commerce) is a business model for commerce using mobile devices. The m-commerce applications generally fulfill some tasks that require mobility. The m-commerce applications have to face various challenges (e.g., low network bandwidth, high complexity of mobile device configurations, especially security). We try to focus on finance-related applications or services as they involve more sensitive data and need higher-level security mechanism.

Scenario 1. Alice is going to purchase something on a website by her mobile phone, and she uses her e-bank to pay the bill. After installing a bank-related application on her device, Alice enters the password and finishes the payment. Later, Bob borrows Alice's mobile phone and installs a key logger program stealthily, by analyzing the record of keystroke he gets the password successfully, then Bob transfers Alice's property from her account to another.

Discussion. Traditional secret key is still susceptible to be stolen or forged, this leads to a psychological barrier for people to accept m-commerce. Implementing BE technology in m-commerce can mitigate the threat because malicious attacker cannot steal one's finger or other organs stealthily, and people provide unique biometric feature as identification to finish trade instead of remembering a series of complex passwords. Moreover, BE can be an additional method coexisting with traditional encryption scheme.

B. BE in Mobile Healthcare

Mobile healthcare provides medical services and information by mobile technology, it can be the solution for

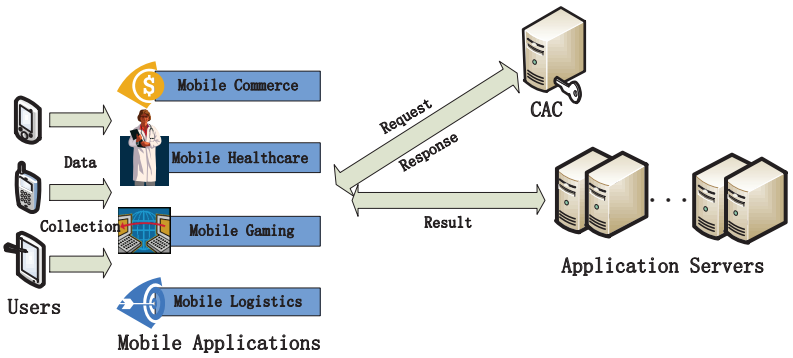

Figure 1. BE applying in MCC

developing country of lacking medical resources. During mobile healthcare progress, in order to diagnose, research or teach, medical institutions have to collect or publish a large number of medical data, which probably contains users' personal privacy information, and it could be used for diagnosis, treatment or disease tracking. Information leakage of medical treatment will bring a huge influence to patients' personal life involving dignity and property.

Scenario 2. Cathy feels sick one day and she tries to see a doctor using mobile healthcare service in her community, then she provides her electric medical record and her symptom to an online doctor by her mobile phone. Unfortunately, the electric medical records stored on the server of hospital are stolen by a hacker, and he sells the information to a personal drugstore. A few days later, Cathy receives many spam messages of selling medicines.

Discussion. In normal situation, both patients and doctors should be authenticated before the treatment, and the data generated during the treatment should be encrypted and kept in safe, then all the access to the patients' data should be authorized. With the advantages of biometric encryption, it can improve the security of mobile healthcare system to a high level. On the other hand, for elder or forgetful patients who may have difficulty to remember a long password, BE can provide convenience for them.

C. BE in Mobile Gaming

In recent years mobile gaming is a popular industry in the area of mobile application development, hundreds of new games are on line in Apple app store and Android app market every day. However, mobile game companies (e.g. iOS game development company) face these threats: in-apple purchase cracking, ipa cracking, save data modification, package hijacking and game process debugging. These tricks harm the profit of game software development companies and the rights of legal users. We take in-apple purchase cracking as an example, the theory of this tool is to modify the transaction status returned from in-apple purchase, then it cheats the software to believe the purchase is successful, at last the user can purchase things for free.

Scenario 3. David often plays games on his tablet computer, to buy equipments in the game he plans to purchase some game coins using his apple account. One day he sees someone on the internet claims that he can buy everything for free in the game and the article shows the procedures of cheating on the game. With curiosity David tries it and has experience of purchasing goods for free, even though he enjoys the sense of accomplishment by buying the best equipments in the game, he loses interest of that game soon.

Discussion. We suppose the application accepts biometric information from the user after he clicks something in the store, then the application verifies with a specific server and the response should not be forged, after the operation is proven to be legitimate the application can trade with app store. With BE the users who buy legitimate software can be protected from pirated copies, BE can be also used in signing in game center instead of user name and password.

D. BE in Mobile Logistics

Nowadays people can not only shop by mobile phone, but also trace the logistics online to know where the goods are anytime. In majority situation, people receive the goods by waiting the delivery courier calling them to take delivery at some place. Regardless of morality and other factors, due to the delivery courier only checks the name or phone number of receivers, it is possible that the goods are taken by an impostor who may be familiar with the owner. To avoid this happening by introducing BE mechanisms, receivers get authenticated on a handheld device by fingerprints or some other biometric features instead of signing.

Summary. Though applying BE in mobile applications is reasonable, there are still many challenges of deploying BE in mobile services. Analyzing and verifying encrypted biometric data, and responding requests from users may make a great burden for the application server. To this end, we consider establishing a cloud authentication center (CAC) between BE applications and their servers. We expect CAC as an infrastructure of credibility like banks. Applications

send the biometric data to CAC for analyzing, and CAC sends the result to the corresponding application servers. The servers need not to know the details of authentication but the result of success or fail. We show this progress in Figure 1.

IV. Security Analysis

Implementing BE in MCC faces security issues inherited from both of BE and cloud computing. The security-related issues are introduced in two categories in the following: the security for mobile users and the security for data.

Security for mobile users. Mobile devices such as cellular phone, personal digital assistant, and smartphone are exposed to numerous security threats like malicious codes (e.g., virus, worm, and Trojan horses) and their vulnerability. Installing and running security softwares such as Kaspersky, McAfee, and AVG antivirus programs on mobile devices are the simplest ways to detect security threats on the devices. However, mobile devices are constrained in their processing and power; protecting them from the threats is more difficult than that for resourceful device. In addition, with mobile phones integrated *global positioning system* (GPS) device, they can cause privacy issues for subscribers when mobile users provide private information such as their current location. This problem becomes even worse if an adversary knows the user's important information.

Securing data on clouds. Although both mobile users and application developers benefit from storing a large amount of data/applications on a cloud, they should be careful of dealing with the data/applications in terms of their integrity, authentication and digital rights.

Some low level attacks against BE systems are still possible. In the low level attacks an attacker is supposed to be familiar with the algorithm and to be able to access the stored helper data. The attacker can also collect or generate a biometric database to use it offline. The most important attacks of BE include: Inverting the hash; *False acceptance* (FAR) attack; Hill Climbing attack [11]; Nearest Impostors attack; *Running Error Correcting Code* (ECC) in a soft decoding and/or erasure mode; ECC Histogram attack; Non-randomness attack against Fuzzy Vault [12]; Other attacks that have been considered include Non-randomness attack against Fuzzy Vault and quantization schemes [13], and Blended Substitution. FAR attack is conceptually the simplest. The attacker needs to collect or generate a biometric database of a sufficient size. The attack can be mitigated by using a secret transform [14], preferably controlled by a users password; by using slowdown functions; and by using BE within a framework of a homomorphic cryptosystem [15].

As we mentioned before, encryption system based on BE technology generally uses 3 models: key release, key binding and key generation. The key release model is easy to implement while it has two defects. First, the biometric feature template is not safe enough, the template is critical in biometric identification system and it is inevitable for templates being stolen. Second, although the authentication and the key release proceed separately, the attacker may evade the biometric feature matcher using trojans, therefore it can not fulfill high security requirements. Both of key release and key binding model are based on secret key, the security breaks if the key is missing, therefore we tend to use key generation model in our platform.

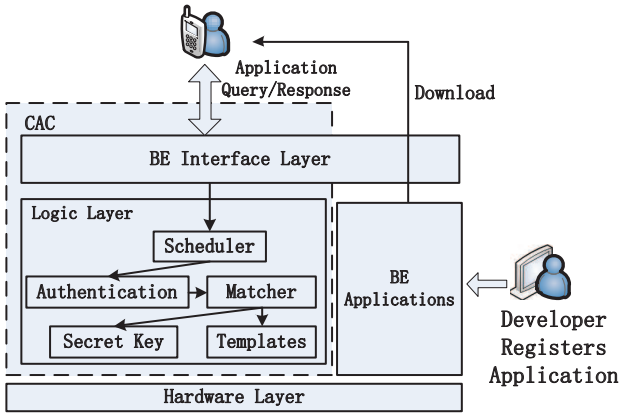

Figure 2. Mobile cloud platform architecture

V. Mobile Cloud Computing Platform

We try to integrate BE technology in our MCC platform, which has never been proposed before. The MCC platform should consider application developers, users and operators based on existing mobile network architecture, rather than build without foundation.

A. Architecture

The architecture depicted in Figure 2 is similar to that of an (non-transparent) Internet proxy requiring registration. The steps towards using BE MCC platform are as follows: BE application developers should register in the platform when they release their products. Users download registered applications to mobile devices from app market in the platform, and the biometric data will be transferred to the platform through specific interface. Before an user begins to use the applications he should create a record containing his biometric features on the platform. In the platform, thousands of requests are scheduled and analyzed, and the original templates of users are stored in database encrypted. After the requests are disposed by CAC, the results will be sent back to the applications.

At design time, the developer has to register the application with BE MCC platform. Application registration informs request parameters, including the category of the application, biometric features requested, security requirement level etc. The applications will be examined strictly in case of malwares disguising legal software, then the

```
{
    app_id,  // The identity of application
    app_category,  // The category of application
    biometric_feature_flag,  // Whether application need to collect
biometric feature
    biometric_feature_type,  // The type of biometric feature
    security_level,  // The importance of data
    rank_and_comment
    . . . . . .
}
```

Figure 3. The format of application information

```
{
    app_id,  // The identity of application
    app_signature,  // The evidence of legal application
    user_id,  // The identity of user
    biometric_id,  // The code of biometric feature
    biometric_data, // Data containing biometric information
    result
    . . . . . .
}
```

Figure 4. The format of request message

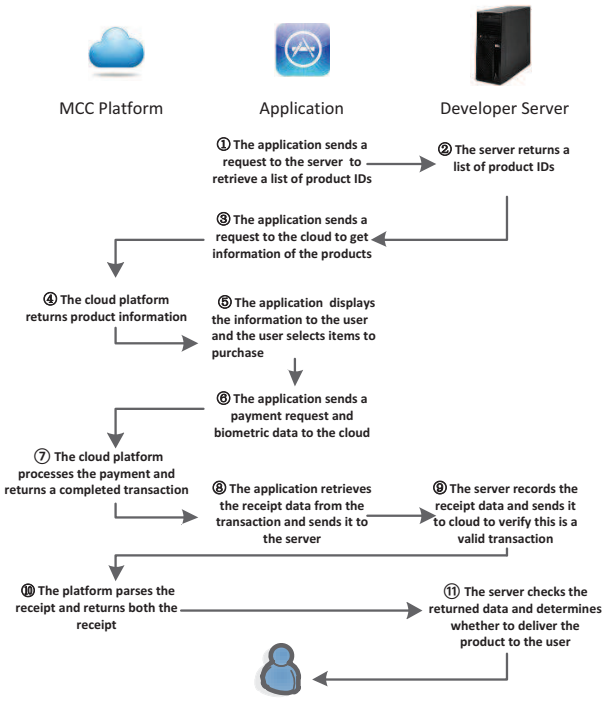

Figure 5. The progress of purchasing with MCC platform

application will have a record data in the platform containing its information. Besides version, size, and users' data, we list some special items of BE application in Figure 3.

CAC is the core module of the platform, scheduling the requests from clients, matching the submitted biometric data with the original ones, while managing the biometric feature templates and secret keys. It must be a authority to make license for all the applications and users, the creation of users' biometric data record should be a real-name system. The scheduling module plays a vital role in processing requests from clients, searching the data and responding the request in real time, and some technologies of massive data processing would be required such as partitioning, indexing, caching, establishing temporary tables and views. To store and manage users' data, the storage architecture of platform could be a distributed file system like Hadoop and MapReduce.

B. Communication with Mobile Cloud Computing Platform

When a BE embedded application needs to receive biometric feature from the user, it calls a BE module on the mobile device. The module should base on hardware level and its security mechanism must be integrated in the chip, thus to defend attacks from system and application level. We show the request message format in Figure 4, as shown in the figure, application ID needs to be provided to correlate corresponding application and the user ID to locate the individual database.

To communicate with MCC platform and the BE applications on it, a secure protocol should be proposed. We learn some mechanisms from mobile gaming and design a suitable protocol for our platform. Considering integrity, dependability and uniqueness, every operation involving sensitive data should generate a receipt for verification. Taking mobile shopping as an example, a receipt data should be produced both in market application server and the cloud platform, to verify whether it is a valid request the market server may check the consistency of receipts by requesting the platform, Figure 5 shows the progress of purchasing something in an application using MCC platform.

VI. Discussion

Statistics show that 10% of human's fingers can not be identified by biometric feature system due to the quality of fingerprint, and other fingers may become dry, wet or distorted and fail to be collected. Moreover, fingerprint image changes with applied pressure, temperature, moisture, sweat, oil, dirt on the skin, cuts and other damage, changes in body fat, and with many other factors. Therefore improving the robustness of fingerprint identification algorithm to deal with fingerprints of low quality, is a major problem in this area. In addition, aging, illness, environmental factors, etc., have a bearing on the quality and variability of captured biometric data. Therefore, a comprehensive mechanism is required to help those people keep their biometric features available by some methods, such as multiple finger recording or updating the biometric data combining user's other authenticated information.

We point out several obstacles to overcome in implement-

ing BE in MCC, though some of them are usual problems inherited from BE or MCC, they still need to be solved.

- Extending battery lifetime. Battery is one of the main concerns for mobile devices. Existing solutions require changes in the structure of mobile devices, or they require a new hardware that results in an increase of cost and may not be feasible for all mobile devices. With BE technology integrated in mobile devices, frequent operations of authentication or authorizations consume more battery power, and the collection cannot be moved to the cloud.
- Improving data storage capacity and processing power. Storage capacity is also a constraint for mobile devices. MCC is developed to enable mobile users to store/access the large data on the cloud through wireless networks. MCC also helps in reducing the running cost for compute-intensive applications that take long time and large amount of energy when performed on the resource-limited devices. BE related applications should authenticate the biometric feature efficiently and send back the result to the user precisely.
- Improving reliability. Storing data or running applications on clouds is an effective way to improve the reliability because the data and application are stored and backed up on a number of computers. This reduces the chance of data and application lost on the mobile devices. Biometric features are privacy of users, both the client and the cloud should guarantee the security of all the operations including collecting, sending and authentication.

VII. Conclusion

We make a forward-looking research about deploying BE technology in mobile cloud computing. We demonstrate several scenarios applying BE in mobile applications and introduce the concept of implementing BE in our life to the readers, then we analyze the security problems of them. At last, a secure mobile cloud platform is depicted serving for applications with BE technology. Though the platform is conceptual and there are still many challenges for practical implementation (e.g. appropriate request scheduling, efficient match algorithm, secure storage of templates and secret keys), we believe that in near future we can overcome these obstacles with the development of mobile internet, and people will enjoy the convenience brought by mobile cloud computing with BE technology.

References

[1] M. Walsh, "Gartner: Mobile to outpace desktop web by 2013," *Online Media Daily*, 2010.

[2] J. Christensen, "Using restful web-services and cloud computing to create next generation mobile applications," in *Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications*. ACM, 2009, pp. 627-634.

[3] X. Luo, "From augmented reality to augmented computing: A look at cloud-mobile convergence," in *Proceedings of the International Symposium on Ubiquitous Virtual Reality (ISUVR'09)*, Gwangju, South Korea. IEEE, 2009, pp. 29-32.

[4] I. Giurgiu, O. Riva, D. Juric, I. Krivulev, and G. Alonso, "Calling the cloud: Enabling mobile phones as interfaces to cloud applications," in *Proceedings of the 10th ACM/IFIP/USENIX International Conference on Middleware (Middleware'09)*. New York, NY, USA, ACM, 2009, pp. 1-20.

[5] E. Marinelli, "Hyrax: Cloud computing on mobile devices using mapreduce," *Master Thesis Draft*. Computer Science Department, CMU, September, 2009.

[6] A. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Transaction on Information Forensics Security*. 2006, vol. 1, No. 2, pp. 125-143.

[7] A. Cavoukian, A. Stoianov, and F. Carter, "Biometric Encryption: Technology for Strong Authentication, Security and Privacy," in *Proceedings of Polices and Research in Identity Management (IDMAN'07)*. Rsm Erasmus University, Rotterdam, the Netherlands, October 11-12, 2007, Springer, pp. 57-77.

[8] A. Bodo, Method for producing a digital signature with aid of a biometric feature, German patent DE 42 43 908 A1. June 30, 1994 (Priority date : Dec. 23, 1992).

[9] G. Tomko, C. Soutar, and G. Schmidt, Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, July 30, 1996 (Priority date: Sept.7, 1994).

[10] J. Kwapisz, G. Weiss, and S. Moore, "Cell phone-based biometric identification," in *Proceedings of 2010 Fourth IEEE International Conference on. Biometrics: Theory Applications and Systems (BTAS'10)*. IEEE, 2010, pp. 1-7.

[11] A. Adler, "Vulnerabilities in biometric encryption systems," *Audio-and Video-Based Biometric Person Authentication*. Tarrytown, NY, USA, 2005, pp. 1100-1109.

[12] E. Chang, R. Shen, and F. Teo, "Finding the original point set hidden among chaff," in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*. ACM, 2006, pp. 182-188.

[13] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," *Technical Report*. University of Twente, 2006.

[14] J. Anil K, N. Karthik and N. Abhishek, "Biometric template security," *Journal on Advances in Signal Processing, Special Issue on Biometrics*. January, 2008, pp.1-7.

[15] J. Bringer and H. Chabanne, "An authentication protocol with encrypted biometric data," in *Proceedings of the Progress in Cryptology, AFRICACRYPT, Lecture Notes in Computer Science.* vol. 5023, Berlin, Heidelberg: Springer-Verlag, 2008, pp. 109-124.