International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 3, Issue 9 (September'2017)

A STUDY OF SECURITY IN MOBILE AND SMART SYSTEM

R. Ramya,
Department of Computer Science,
Rajah Serfoji Govt. College,
Thanjavur, Tamilnadu,India.

V. Roja Shree,
Research Scholar,
Department of Computer Science,
Sri A.V.V.M. Pushpam College,
Poondi, Tamilnadu,India.

J.Gnana Jayanthi,
Department of Computer Science,
Rajah Serfoji Govt. College,
Thanjavur, Tamilnadu,India.

Abstract: The increased usage of mobile phones and the user's interest for using phones for mobile commerce application has lead to an urge for strict security authentication of the users. The password based authentication is becoming insane as there are many passwords too very simple. The biometric based authentication systems are becoming common place and are used widely as it is more stable and unique. The researchers are developing more and more fuzzy logic based multi-modal biometric authentication systems to verify the identity of the mobile phone users. This article presents one such authentication work that involves three parts of work. First part deals with the study of various models of mobile commerce authentication in a number of multi-model biometric authentication levels are defined to balance between the usability and security. Second part is a study of a multi-model biometric authentication system involving typing behavior recognition; face recognition and speaker recognition techniques to establish the identity of the user of mobile phone using m-commerce in it. Finally the fuzzy logic model proposed is studied to find out the transaction risk in m-commerce as there are some issues in the deterministic biometric authentication system.

Keywords: m-commerce, biometric authentication, fuzzy logic, mobile phone authentication, Security, Smart system.

I.INTRODUCTION

The development of mobile phone industry has lead to the increase in the subscription of more and more mobile phones. There is a substantial increase in the use of smart phones and has become the part and parcel of every man's life. In recent years the smart phones are ubiquitously used by people not only for communication but also for business, and to manage their day to day work. This leads to storage of large amount of personal and sensitive information in the mobile phone and applications. In the mean time mobile theft and remote mobile attacks are rising and are haunting the mobile phone users. In this pre-research work a multi-model mobile security and smart system has been studied to provide efficient and good mobile commerce performance authentication engine for future users.

For every individual user the authentication mechanism is very essential part of information security. Lack of secure authentication may lead to disclose the personal information and may also to heavy financial loss. Thus an authentication mechanism with high safety-critical, ease of use and ease of managing is essentially desired. The current authentication systems and the challenge can be broken down into three area:

1. How to use biometric techniques to establish a user's identity?
2. How to adjust the authentication mechanism according to the transaction risk in mobile commerce?
3. How to achieve the balance between usability and security in a multi media authentication system?

Initially, this paper work presents a number of authentication mechanisms in the system according to the transaction risks. This multi-level authentication system for mobile commerce provides a systematic safety mechanism which is also user friendly. Rather than using only a password security, this multi-level authentication system allows many techniques (like biometrics) for authenticating a mobile system.

Biometric authentication techniques allow uniquely identifying humans based on their intrinsic physical or behavioral traits [Jain et al., 2000]. Biometrics is used as a form of identity access management and access control and is also used to spot individuals in groups that are under surveillance. Unlike the widely used passwords-based methods the biometrics will never be forgotten or lost and is difficult to forge at the same time easy to use. The multi-level biometric model presented in this pre-thesis includes three biometric techniques listed below are presented in section 4,5,6.

In this paper a multi-model biometric authentication system involving three biometric techniques are studied to ascertain the identity of the mobile phone user. Secondly, a smart model was developed to authenticate the mobile-commerce. The traditional methods used a one-time password mechanism to authenticate the user which was verified by an Application Programming Interface (API) and the access control service provider. This method does not meet the

current security threats and hence there is a need for new and better mechanisms.

II. LITERATURE REVIEW ON MOBILE COMMERCE

2.1 Overview

Since the first generation of the wireless technology (IG) in 1980s, there is an overwhelming development in the mobile industry that has not stopped [Carney, 2002]. More than normal mobile phones, people prefer and use the smart phones like Android and I-phones, which has increased with the increase in its manufacturers. Smart phones are effectively a small computer that can conserve enormous amount of personal information, provide various services like mobile commerce and mobile identification. As the other forms of mobile commerce also has some security risks. This research paper takes a study on the mobile security systems, to protect user's information to assure the transaction security and authenticate the mobile phone users.

The current mobile user authentication is achieved by username and password or Personal Identity Number (PIN), which can be easily lost or forgotten [Uludag et al, 2004]. Moreover, hackers can use variety of methods to find the PIN or password. Recently many researchers have introduced biometric methods instead of PIN and password. Research studies like Clarke and Furnell [2007_b] have anticipated the use of user's keystroke behavior, Chen et al. [2010] have built a face detection and recognition system for a mobile device, finger print [Xi et al., 2011] or voice prints [Lee, 2009] as biometric techniques to achieve mobile user identification.

In 2000 when Internet was made available on mobile phones, the mobile commerce was born [Sukumar, 2011]. The significant development in mobile commerce has been marked as a drift from "wired world" to a "wireless world" with the advantage of smart phones, which has entered to a new era of mobile computing [Ramakrishnan, 2008]. The users of mobile commerce can collect real-time business information and make decisions at anytime and anywhere.

2.2 Generations

There are three generations of mobile commerce development

(i) First Generation: Based on Short Message Service (SMS) technology born in 1997, when a vending machine accepted payment via SMS text messages. There were a few major flaws in the 1G mobile commerce: poor security, unprotected transaction and limit in the SMS message length which have made the information incomplete.

(ii) Second Generation: Based on Wireless Application Protocol (WAP), where in the user was able to browse the information on the web through their mobile device thus leading to a rapid development in mobile based commerce in early 2000. 2G solved some mobile access issues but still had some security risks and limited interaction ability.

(iii)Third Generation: Based on combined usage of smart phones, Virtual Private Network [VPN], database synchronization identity authentication, web service and other mobile communication technologies. 3G provided a secure and speedy mobile commerce mechanism. The various functions of 3G mobile commerce system are as follows:

- SMS function – The system sends an SMS alert to the user about the transaction and an electronic receipt with the detailed transaction is generated.
- Comment function – Users can comment on the product and so the communication between the user and the traders becomes effective and allows the traders to receive the feedback and suggestions about the product from the user.
- Display function – a complete description about the product is displayed on the web.
- Shopping guide function – Online query service provided by the mobile commerce allows the user to contact the trader directly and then order online.
- Authenticate function – The identity of the mobile user is determined by username and password authentication technique. Mobile Payment is also done by enabling online mobile payment by turning the mobile phone into a wireless payment tool using Near Field Communication (NFC) or 2D barcodes combined with biometric techniques. It is potentially secure, fast and convenient for the user.

2.3 M-Commerce Model

The traditional payment methods will gradually get replaced by the appearance of mobile commerce, which is widely accepted and is being used as a popular method [Jahanshahi et al., 2011]. Nowadays a mobile phone with NFC chip can replace a bank card to complete a purchase. A "mobile wallet" is an m-commerce service based on Near Field Communication (NFC) and Radio Frequency Identification (RFID) techniques, which uses the mobile phone as a client tool, link with the user's bank account, via SMS, Interactive Voice Response (IVR) and many other means to accomplish mobile payment or balance enquiry. A mobile phone can replace cash, cheque or credit cards and allow a user to shop at any place with a Point of Sale (POS) machine such as store, shopping centre or bus station. Mobile payment has become a trend of mobile phones. "Mobile wallet solutions are our top priority" says PayPal boss [clark, 2010].

2.4 Global Status

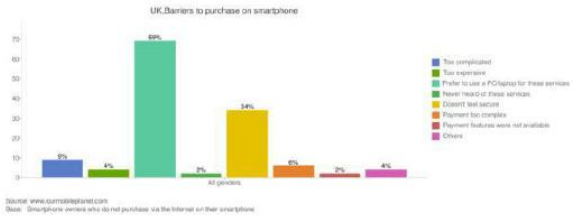

Figure 2. 1- Why users are reluctant to use mobile payment methods

Figure 2.1 above depicts the detail data of the survey from Intersperience (2011). It can be seen that the 'complexity' to use and 'security' are the major issues that most of the mobile phone users were concerned about. Thus the new

mobile commerce techniques must ensure excellent security measures with enough publicity and simplified payment methods.

3. LITERATURE REVIEW OF CONVENTIONAL MOBILE SECURITY

3.1 Mobile Phone Theft

Mobile phone theft also increases with the increase in the growth of mobile phone market every year. Purchase, sale and other transactions are the main purpose of m-commerce which purely relies on personal information. As these personal information which includes residential address, credit card details or purchase history could be accessed by criminals if the mobile phone is stolen. This may lead to a tragic loss of the users private details, mobile device and at the worst financial loss. Alan Campbell, Minister for Crime Prevention, also said in the report [BBC news, 2010], "firms have a social and a corporate responsibility to tackle crime". So if a method can ensure the personal and financial data safety even when the mobile phone is stolen may reduce the risks for the victims and thereby the number of mobile commerce users could also be increased.

3.2 Conventional Authentication Mechanisms

The conventional authentication mechanism includes PIN, username-password, dynamic password (One Time Password), and challenge-response is the most commonly used user identification technologies [Borde, 2007]. A password verification system is very simple as shown in figure below.

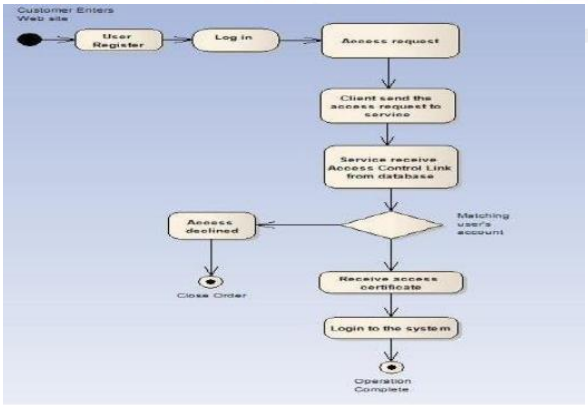

Figure 2.2 Password verification flowchart

In the password authentication system first the user needs to register as a new user and store the username and password in the server. Then each time while using the authentication interface the user is asked to login with a username-password which is send to the server to check for the matches with the data in the database. If the credentials match the user is allowed to login and the operation is carried out. If the credentials do not match the user is rejected to access the system. However some drawbacks exist in the password-based authentication system which allows the hackers to attack the system. There are a variety of methods used by the hackers to steal the password. In mobile commerce the user credentials are stored by default in the device, which when stolen all the private data and financial information of the user are at risk. Hence some new methodology is required to ensure the mobile security system.

3.3 Conventional Mobile Transaction Model

Apart from the password authentication methods mobile commerce also implements biometric authentication methods. At present a single authentication technology is used which is difficult to achieve high accuracy rate [Dave et al., 2010; Campisiet al., 2009]. The use of multiple authentication technology may slow down the speed and also increase the complexity of the system. The current mobile commerce security system has some flaws like poor reliability, poor usability, lower security, transaction risks cannot be measured and the user behavior is not recorded. Thus, the primary challenge of this research is to develop a smart secure system which is more convenient and secure in mobile commerce.

3.4 Biometric Authentication

Biometrics, which is concerned with the reliable, stable and unique personal physiological characteristics such a facial features, fingerprint, iris pattern, retina and hand geometry or some aspects of behavior like handwriting and typing behavior is emerging as the most fool proof means of automated personal identification [Miller, 1994; Lawton, 1998; Jain et al., 1999; Zhang, 2000; Amayeh et al., 2009]. The biometric system is a personal identification technique which verifies the authenticity of a specific behavioral and physiological characteristic possessed by the user. These methods are widely studied in the recent research area. Each method has its own scope and area of application and not all are applicable to mobile system authentication.

Features of biometric authentication techniques:

- Portability: the biological characteristics are always with the user and need not be remembered and will not be lost or forgotten
- Generality: Everyone has a biological behavior or characteristic
- Uniqueness: everyone's biological characteristics are unique [Jain et al., 1999]
- Stability: The biological characteristics will not change with time and conditions.
- Security: Biological characteristic is the best testimony of personal identity which is hard to steal and imitate and has high level of security.

At present, many researches are done on biometric authentication techniques. In some cases of biometric authentication like finger print recognition and signature recognition a specific hardware like finger print reader or sweep device is required in a mobile phone device. But most mobile devices have keyboard, microphone and camera. So face recognition, typing behavior and speaker recognition techniques are more convenient to be used in mobile phone authentication system [Clarke and Furnell, 2007_a].

4. STUDY OF TYPING BEHAVIOR RECOGNITION

4.1 Keystrokes as a Biometric

Keystroke dynamics or typing dynamics is a details timing information of about when a specific key is pressed and released by the user while typing on the keyboard [Moskovitch, 2009]. The authentication engine compares the

user's registration pattern with the input keystroke data; and then validates the identity of the claimer. The mobile client does not preserve any data and hence very secure and reliable. In this authentication technique the user is asked to enter the username and password which is verified as usual and the user's behavior is monitored based on the following two metrics.

- ***The keystroke latency (Interval):*** The time between successive keystroke. The measure of time from when a key is released and the next subsequent key is pressed.
- ***The key hold-time (Duration***): The time taken to press and release the key. The measure of time from when a key is pressed and the same key is released.

So if the password is "abertay2011" then there are 10 *keystroke latency* and 11 *key hold-time* recorded. The user may have to train the system by a number of repeated entries of the same password and an average of these latency and duration will be stored in the database for validation. The system flow is shown in the figure4.1 below.

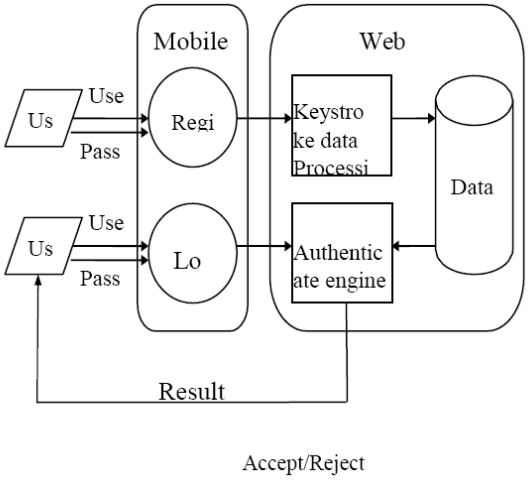

Figure 4. 1 Typing Behavior Recognition System

These metrics are registered with the help of the following algorithm:

$$\text{Average Duration} = \frac{(\text{Duration t1} + \text{Duration t2} + \ldots\ldots + \text{Duration t6})}{6}$$

$$\text{Average Interval} = \frac{(\text{Interval t1} + \text{Interval t2} + \ldots\ldots\ldots + \text{Interval t6})}{6}$$

In this system each user has to type the same username and password six times and the average of these user's keystroke data is stored into the database as the user's pattern.

In the above algorithm a new parameter 'α' is introduced and it determines how near to the registered pattern is the user's attempt to be accepted by the system. The 'α' For example, the higher 'α' values says that the system is more likely to accept the wrong user and reject the actual user and a lower 'α' value means the system is more secure. Equal Error Rate(EER) is a statistic which is used when qualifying the success of biometric system. The FRR is where the FAR and FRR are equal to each other. It is the best single description of the Error Rate of an algorithm. The lower the EER the more successful and secure the biometric system is [Griaule Biometrics, 2008]

The suggested mechanism of username and password authentication simultaneously with keystroke behavior authentication can effectively prevent the potential attacks from cyber crimes.

V. STUDY OF FACE RECOGNITION

A facial recognition is a computer based application program that identifies a person from a digital image or a video frame from a video source [Animetrics, 2008]. The captured facial image is compared with a stored facial database for authentication. It is very difficult to recognize face because of the following reasons:

- The images of various facial expressions of the same person varies greatly
- The face will change with age
- The quality of the facial image will vary with exposure to light, angle and distance of imaging.
- Computer based facial recognition is carried out using image processing, computer vision, neural network and pattern recognition.

All these factors make the research on facial recognition a challenging task.

5.1 Face Recognition Engine

The face.com provides a free face recognition API. They have used "faces in crowd" method to allow the system to accurately identify the location of a face by referring to the key points such as the eyes, nose and mouth. The method can detect multi-face in one picture as shown in figure 5.1 below. This API of face.com has a fast processing speed, minimal hardware requirement and as a highlight it supports multi-person face tracking at real time so that it could be used by mobile users even when they are in public places. So the face.com API is used for face recognition in mobile authentication engine in this research.

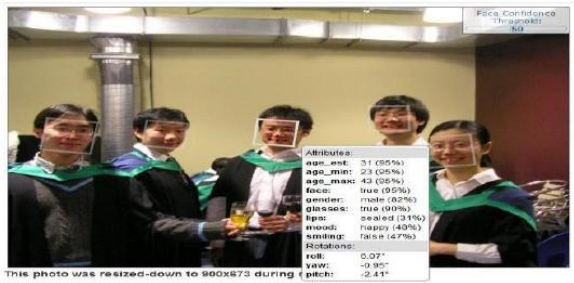

Figure 5. 1 Face recognition API window of Face.com

5.2 Methodology

The face recognition system framework has two functional parts: the mobile client and the web server. In the client the researcher has designed two mobile interfaces: the registration and the login that helps the user to register and identify them on the mobile phone. The API used in the system is from face.com which includes the following functional modules: face detector, feature extractor and authentication engine. The working of the system is shown in figure 5.2 shown below.

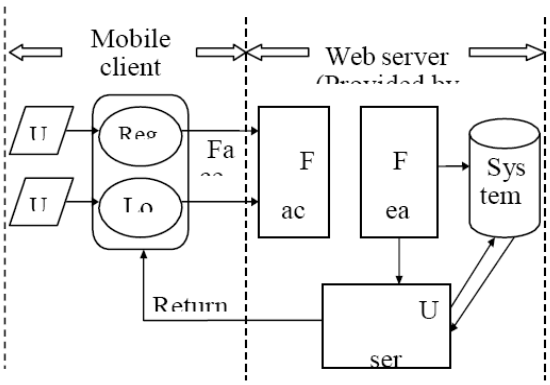

Figure 5. 2 The face recognition system

The main task of mobile client is to capture the user's face and send it to the web server where the authentication engine uses the recognition API from face.com for image processing and identity verification.

The entire process is carried out as in the following steps given below.

(i) User registration: If the user is entering the system for the first time they are asked to register their identity in two ways: shooting a photo using the mobile camera or uploading a photo from the internet. Shooting a photo from mobile camera the user will be shown the image shot on the screen and by clicking the capture button the "face detection" method will be used to identify the face image and extract the features. Finally the user will be prompted to enter a unique username to finalize the image. Similarly while uploading a image from the internet too on clicking the capture button the face detection is used and the user can register with the unique username. Figure 5.3 below show the window of face registration.

Figure 5. 3 Face registration window

(ii) Face recognition process: There are three steps in this process as follows-

- Face Detection: The API provided by face.com has a set of services that allows computers to analyze facial information found in photos and tries to identify the faces against a known set of users. The technology allows detecting specific user from many faces, mark face region out the image and display the position and size of each face. In order to achieve these functions on mobile phone a click function is introduced into the Flex application (an application to process face image and receive recognition result from face.com). When the mobile phone user enters the face from a complex background the application allows to manually touch the face target that they want to choose thus and hence increasing the system usability.
- Face feature extract: This requires an index of known faces before recognition can be performed. This function is used to detect position and shape of major facial feature like eyes, nose and mouth. The facial detects results consists of two categories of information- Attribute [such as gender, wearing glasses and smiling] and geometric information of the tag [eye, nose and mouth].
- For each user's login attempt a near likely use ID is returned or an empty result is displayed for unrecognized faces. The face.com API generates only a recognition score for each trial and so we need to compare this result with a threshold [also considered to be the acceptance standard] in the system.

(iii) Operating environment: The face detection system is designed to run on mobile phones. So the requirements of mobile phones and operating system are:

- IPhone 3GS and above, operating system IOS 3.1 or above.
- Android phone, operating system Android 2.2 or above
- Android phone install Adobe Air 2.6

The flex application on the client side was developed using Adobe Flash Builder 4.5 and written using Action script language.

The main task in this experimental work is to examine whether face recognition could be used in mobile authentication methods. This is achieved by finding out the FAR and FRR by using the threshold value analysis from the output received from face.com API. The tables below summarized the FAR and FRR values obtained from different experimental inputs and the EER is obtained to be 4%.

Accept Standard / Results	≥90	≥80	≥70	≥60	≥50	≥40
Unsuccessful login	14 times	10 times	8 times	5 times	3 times	1 Times
FRR	35%	25%	20%	12.5%	7.5%	2.5%

Table 5. 1 FRR of face recognition system

Accept Standard / Results	≥10	≥20	≥30	≥40	≥50
Unsuccessful login	19 times	14 times	12 times	9 times	5 times
FAR	10%	7.4%	6.3%	4.7%	2.6%

Table 5. 2 FAR of face recognition system

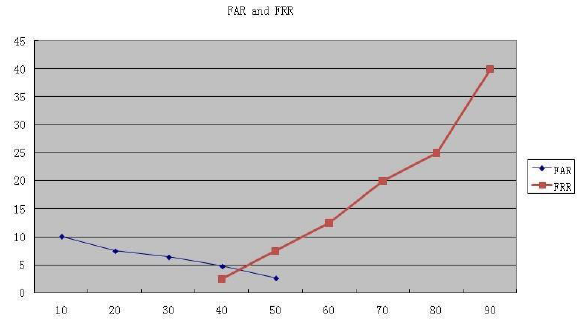

Figure 5. 4 FAR and FRR of face recognition system

5.3 Summary

Face recognition is a non-intrusive that people do not have any problem in accepting face as a biometric characteristic [Hong and Jain, 1998]. In normal lighting condition the system provides a good recognition rate: the experimental outputs show that the ERR in the system is 4% when the acceptance standard is set at over or equal to 44 points. Face recognition techniques has some limitation in lighting of the environment in spite of which it aims to achieve higher recognition efficiency and increase the implementation speed.

6. STUDY OF SPEECH RECOGNITION

6.1 Speech Recognition Technique

Voice print pattern analysis and speech signal processing are the two different methods that can be used in speaker recognition [Finan et al., 1997]. The first method sets up a physical model using the captured voice print, and then gets the parameters for the model through solving differential equations. The second method uses signal processing technology and extracts some individual characteristic parameters form the speech signal, and uses these parameters as standard to achieve recognition. "Securivox approach" is a system that judicially combines these two models and is provided by Speech Sentinel Limited Company [speechsentinel.co.uk]. The preprocessing part in the frontend of the system includes voice signal digital processing, pre-emphasis, and extraction of the voice parameters. High accuracy, insensitivity to the background noise and text independent recognition are the advantages of SecuriVox and is suitable for mobile speaker recognition system.

6.2 Methodology

In general the speaker recognition methodology includes the speaker identification (does the person match one to the templates stored in the database) and speaker verification (confirmation of the person's claimed identity based on unique characteristics of the voice). The system structure of speaker recognition system is similar to the face recognition system with two parts: mobile client and web server as shown in the figure 6.1 below.

As shown in the figure above the Flex application allows a new user to register into the server by repeatedly training the system to recognize the voice by repeating a same phrase a number of times, which on succeeding is stored to a database. Later when the user tries to log in the authentication engine processes the voice file and compares with the database registered values. If a sufficient match is found an acceptance result is returned to the user else the user's login request is rejected.

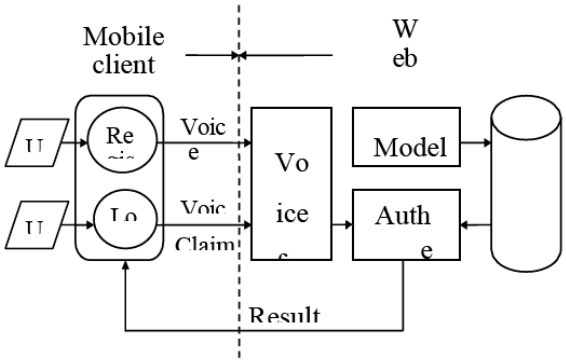

Figure 6. 1 Speaker Recognition System Model

In the speaker recognition system, the recognition mechanism is: each user attempts to login, they are required to speak a phrase and the recognition results returned will contain five digits.

To accept a user: when the result contains three or more "1"s,
To reject a user: when the result contains three or more "0"s.

The above algorithm is used to calibrate the acceptance rate of the user login. Hence the number of ones is fixed as the threshold in the system. Table 6.1 below shows the changes in FRR and FAR with changing threshold value in a noisy and quite environment.

How many "1" to accept a user?		3 or more	2 or more	1 or more
Group 1[Quiet environment]	FRR	20%	10%	0
	FAR	0	0	0
Group 2[Noisy environment]	FRR	50%	10%	10%
	FAR	0	0	10%
Overall	FRR	35%	10%	5%
	FAR	0	0	5%

Table 6. 1 Summary

6.3 Summary

Thus the results show that the speaker recognition techniques has a better result in quite environment than in a noisy environment. The false acceptance did not happen when the system accept a user when the recognition result contains 3 or more '1's the FRR was 35% and when the sytem accept a user when the recognition result contains 2 or more '1's the FRR was reduce to 10%. But the FRR are equal to the FAR when the system accept a user if the recognition result contains 1 or more '1's. Thus the accept threshold in the system as 1 or '1's, FAR=FRR which means the system can achieve an ERR of 5%.

VII. CONCLUSION

he mobile security and smart system in mobile commerce in future will focus on three parts: more biometric techniques to indentify the user of the mobile phone; study the feasibility of building a mobile commerce model for disabled users and improve a smarter model than the current models. If the three parts of work can be achieved in future may increase the usability and security of the mobile commerce.

REFERENCES

[1]. Abdolahi, M., Mohamadi, M. and Jafari, M. "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic". Volume 2, Issue 6, pp. 504–510, January 2013.

[2]. Alsaade, F. "Neuro-Fuzzy Logic Decision in a Multimodal Biometrics Fusion System". Scientific Journal of King Faisal University, Volume 11, Issue 2, pp. 163–176, 2010.

[3]. Amayeh, G., Bebis, G., Erol A. and Nicolescu, M. "Hand-based verification and identification using palm–finger segmentation and fusion". Computer Vision and Image Understanding 113, pp.477–501, 2009.

[4]. Arabacioglu, B. C. "Using fuzzy inference system for architectural space analysis". Applied Soft Computing, vol. 10 (3), pp. 926–937, 2010.

[5]. Araujo, L., L. S., Lizarraga, M. L., Ling, L. and YabuUti, J.B. "User Authentication Through Typing Biometrics Features". IEEE Transactions on Signal Processing, vol. 53, Issue 2, Part 2, pp. 851–855, 2010.

[6]. Awang, S. and Yusof, R "Fusion of Face and Signature at the Feature Level by using Correlation Pattern Recognition". World Academy of Science, Engineering and Technology, Vol. 59, pp. 2291-2296, 2011.

[7]. Bai, Y., Zhao Z.D., Qi Y.C., Wang, B. and Guo, J.Y. "Research on Text-Independent Speaker Recognition Methods Using Wavelet Neural Networ"k. Chinese Journal of Electronics & Information Technology, Vol.28, No.6, 1036–1039, 2006.

[8]. Baker, O.AI., Benlamri, R and Qayedi, A.AI. "A gprs-based remote human face identification system for handheld devices". Wireless and Optical Communications Networks, WOCN, Second IFIP International Conference. Pages 367–371, 2005

[9]. BBC news "Government calls for action on mobile phone crime". Technology correspondent http://news.bbc.co.uk/1/hi/technology/8509299.stm, 2010.

[10]. Berto. R, and Poggio. T "Face recognition: Feature versus templates". IEEE Transactionson Pattern Analysis and Machine Intelligence, Volume 15, No.10, pp.1042-1052. 1993.

[11]. Blender, S. and Postley, H. "Key sequence rhythm recognition system and method". Patent No. 7 206 938, U.S. Patent and Trademark Office, 2007.

[12]. Borde, D. "Selecting a two-factor authentication system. Network Security", Volum Issue 7, pp.17-20. July 2007,

[13]. Broekhoven, E.V. and Baets, B.D. "Fast and accurate center of gravity defuzzification of fuzzy system outputs defined on trapezoidal fuzzy partition"s. Fuzzy Sets and Systems 157, pp. 904 – 918. 2006.