

# **Mobile Security & Smart systems: Multi-modal biometric authentication on mobile devices**

**Xuan Huang**

A thesis submitted in partial fulfilment of the requirements of  
the University of Abertay Dundee for the degree of Doctor of Philosophy

July 2013

I certify that this thesis is the true and accurate version of the thesis approved  
by the examiners

Signed \_\_\_\_\_ Date \_\_\_\_\_

(Director of Studies)

## Declaration

I, Xuan Huang, hereby certify that the thesis has been written by me, and the work presented in this thesis is my own. Where information has been derived from other sources, I can confirm that this has been indicated in the thesis.

Signed \_\_\_\_\_

Date \_\_\_\_\_

To my beloved family!

More than 30 years ago, people call their friends use the lined phone...

**... today we do it use mobile phone**

20 years ago, the PC has an operating system...

**... today the mobile phone has**

10 years ago, people only install application into their PC...

**... today Apple and Android can tell you how many mobile applications can be installed into their phone**

Today people know their mobile phone...

**... tomorrow mobile phones will know their owner**

“Innovation has no limits. The only limit is your imagination.”

— Steve Jobs

## **Abstract**

With increased use of mobile phones that support mobile commerce, there is a need to examine the authentication of users. The password-based authentication techniques are not reliable with many passwords being too simple. A biometric authentication system is becoming more commonplace and is widely used in security fields because of its special stability and uniqueness. Within this context, the researcher has developed a fuzzy logic based multi-modal biometric authentication system to verify the identity of a mobile phone user.

The research presented in this thesis involves three parts of work. Firstly, a model to support the authentication of mobile commerce has been proposed. Within this model, a number of different authentication levels have been defined in the system which sought to achieve the balance between usability and security. Secondly, the researcher has developed a multi-modal biometric authentication system which involves typing behaviour recognition, face recognition and speaker recognition techniques to establish the identity of the user on the mobile phone. However, there are some issues with deterministic biometric authentication systems. Because of this, a fuzzy logic model which can determine the transaction risk in m-commerce and the recognition result

from biometric authentication engine has been built.

In the experimental stage, the researcher simulates a mobile commerce environment. At one extreme, users will just want to obtain the item and not enter any identity. They are prepared to accept the low level of risk when the transaction is of low value. On the other extreme for a high value transaction users will accept multiple levels of security and would not want the transaction to go through without any checking. The experimental results showed that the fuzzy logic based multi-modal authentication system can achieve a low equal error rate (EER) of 0.63%, and by using the fuzzy logic model, it can effectively reduce the false rejection rate (FRR). There is also a reduction in the environmental influence in the fuzzy logic based biometric authentication.

There are three contributions of the thesis: firstly, this research has proposed a model to support the authentication in mobile commerce. Secondly, a multi-modal biometric authentication system was developed. Another major contribution is the development of a fuzzy logic based multi-modal biometric authentication system which is able to overcome the issues of deterministic biometric systems. Overall, the results gained in this thesis prove that using the multi-modal biometric authentication system, it is possible to establish the identity of the user on a mobile phone. The fuzzy logic based authentication

model can make the multi-modal biometric system more accurate, and also reduce the influence of external environmental factors. A holistic interpretation of the research indicated that the mobile security and smart system can help mobile commerce become more secure and more flexible in future.

## **Acknowledgements**

Firstly, I would like to give my special thanks and appreciation to my lead PhD supervisor Dr Geoffrey Lund, who have teach me more than seven years since my MSc studies in Abertay. Thanks for introduced me into the amazing mobile application development world, and gave me an opportunity to research in the project that I am really interested in. I know how difficult to be a PhD supervisor of an oversea student, thanks again for all his help, support and patience. Thanks to Mr Andrew Sapeluk, who was my technical supervisor and gave me a lot of help and ideals when I develop the applications. I am grateful to him for taking the time to guide me through all the research. Thanks to Mr Victor Bassilious, who was the first Abertay lecture I have met (2005, in China), and also my MSc supervisor, thanks for his great help in a long time through my research. I can't finalise my thesis writing and publish papers without his help.

I would also thanks to my friends for help me to finish the experimental work in this thesis; I know it was a boring process and thanks for all your times. I am grateful to all academic staff within the school of Computing and Engineering systems at the University of Abertay Dundee who assisted me between 2007 and 2013. I cannot finish my research work without all your help.



Finally I'd like to express my greatest thanks and love to my family, six and half years is a long time, thousands of miles is a long distance, but I can feel your love at every second, thanks for your support and tolerance. Thanks to my parents, to my wife and to my son, love you forever!

Xuan Huang

Dundee

April 2013

# Table of Contents

Declaration .....	II
Abstract .....	V
Acknowledgements .....	VIII
List of figures and tables .....	XVI
<b>1. Introduction .....</b>	<b>p1</b>
1.1 Mobile security and smart system.....	p1
1.2 Research background .....	p3
1.3 Objective of the project .....	p7
1.4 Structure of the thesis .....	p9
<b>2. Literature review .....</b>	<b>p12</b>
2.1 Research background .....	p12
2.2 Overview of mobile commerce.....	p13
2.2.1 History of m-commerce.....	p14
2.2.2 The status of mobile commerce in the UK.....	p17
2.3 Overview of the mobile security.....	p19
2.3.1 Mobile phone theft.....	p19
2.3.2 The current authentication technology on mobile device .....	p20
2.3.3 The issues exist in mobile commerce .....	p22
2.4 An overview of biometric authentication .....	p24
2.4.1 Typing behaviour recognition .....	p27
2.4.2 Face recognition .....	p30
2.4.3 Speaker recognition .....	p31
2.5 Smart and multi-modal authentication system .....	p32

2.6 Summary .....	p33
<b>3. A model to support the mobile transaction .....</b>	<b>p35</b>
3.1 Introduction .....	p35
3.2 An overview of existing m-commerce model .....	p36
3.3 Model builds up .....	p39
3.4 Results and user tests .....	p46
3.5 Discussion .....	p48
<b>4. Typing behaviour recognition on mobile device .....</b>	<b>p50</b>
4.1 Introduction .....	p50
4.2 Keystroke as a biometric .....	p51
4.2.1 Keystroke analysis .....	p51
4.2.2 Two metrics .....	p52
4.2.3 Recognition algorithms .....	p54
4.3 Methodology .....	p56
4.3.1 System overview .....	p56
4.3.2 Client side design .....	p58
4.3.3 Web server .....	p60
4.3.3.1 Registration .....	P60
4.3.3.2 Validate .....	p62
4.3.4 Database .....	p62
4.3.4.1 Users information .....	P63
4.3.4.2 Keystroke data .....	p63
4.4 Experimental work .....	p65
4.4.1 Experimental environment .....	p65
4.4.1.1 Hardware .....	p65
4.4.1.2 Software .....	p66

4.4.2 Experiment arrangement .....	p66
4.4.2.1 Aims of the work .....	p66
4.4.2.2 Participants .....	p67
4.4.2.3 Methodology .....	p68
4.4.3 Results .....	p72
4.4.3.1 FAR and FRR in different groups .....	p72
4.4.3.2 Result summary .....	p74
4.4.3.3 Usability discussion .....	p76
4.5 Conclusions .....	p77

## **5. Face recognition on mobile device ..... p80**

5.1 Face recognition engine.....	P81
5.2 Research objectives and tasks .....	P82
5.3 Methodology .....	p83
5.3.1 System overview .....	p83
5.3.2 System achievement .....	p85
5.3.2.1 User register.....	p85
5.3.2.2 Face recognition process .....	p87
5.3.3 Operating environment .....	p90
5.3.3.1 Hardware .....	p90
5.3.3.2 Software .....	p91
5.4 Experimental work .....	p91
5.4.1 Aims of the work .....	p91
5.4.2 Methods .....	p92
5.4.3 Result .....	p93
5.4.4 Result summary .....	p100
5.5 Discussion .....	p100

<b>6. The Speaker's Identity Recognition system .....</b>	<b>p102</b>
6.1 The speaker recognition technique used in this research.....	p102
6.2 Research aim and tasks .....	p105
6.3 Methodology .....	p105
6.3.1 System overview .....	p105
6.3.2 Mobile application .....	p109
6.3.2.1 Voice record and user enroll .....	p109
6.3.2.2 User recognition and login .....	p112
6.3.3 Web service .....	p113
6.4 Experimental work .....	p114
6.4.1 Aims and method .....	p114
6.4.2 Result .....	p115
6.4.3 Result summary.....	p118
6.5 Discussion .....	p122
 <b>7. The multi-modal biometric authentication system .....</b>	 <b>p123</b>
7.1 Overview of the multi-modal authentication system.....	p123
7.1.1 The registration process .....	p125
7.1.2 The identification process .....	p126
7.1.2.1 A mobile-commerce model .....	p126
7.1.2.2 Authentication levels determination .....	p127
7.1.2.3 Authentication interfaces .....	p129
7.2 Evaluation .....	p131
7.4 Discussion .....	p134
 <b>8. A smart model in mobile-commerce .....</b>	 <b>p137</b>
8.1 Authentication levels determination .....	p138

8.2 A Fuzzy logic model used in m-commerce .....	p140
8.2.1 Why we need Fuzzy logic? .....	p140
8.2.2 Introduction of the algorithm .....	p141
8.2.2.1 Fuzzy subsets and membership functions .....	p141
8.2.2.2 Control rules.....	p143
8.2.2.3 Defuzzification.....	p145
8.2.3 Methodology .....	p146
8.2.3.1 The fuzzy inference engine .....	p146
8.2.3.2 The definition of input/output fuzzy subset.....	p148
8.2.3.3 Fuzzy rules .....	p154
8.2.4 Example test.....	p157
8.3 Experimental work.....	p168
8.3.1 Aim and objectives of the experiments.....	p168
8.3.2 Methods.....	p168
8.3.3 Results summary.....	p178
8.4 Discussion .....	p179
 <b>9. Conclusion and future work .....</b>	 <b>p182</b>
9.1 Conclusion .....	p182
9.1.1 A model to support the authentication on mobile device .....	P183
9.1.2 Development of the multi-modal biometric authentication system .....	p184
9.1.3 Development of a smart m-commerce model .....	p185
9.2 A holistic interpretation of the research.....	p185
9.3 Implications and limitations of the research.....	p187
9.4 Future work.....	p190

**Appendices** ..... p192

**Reference**..... p195

## List of figures and tables

<b>Figure 1.1:</b> The trends of mobile commerce .....	p4
<b>Figure 1.2:</b> The mobile ticket system used in Fandango.com .....	p5
<b>Figure 1.3:</b> The mobile marketing applications .....	p7
<b>Figure 1.4:</b> The outline of the thesis.....	p11
<b>Figure 2.1:</b> User Interface of 'Mobile Payment' .....	p18
<b>Figure 2.2:</b> The reason why user not choose mobile commerce .....	p20
<b>Figure 2.3:</b> Flow chart of password authentication system .....	p22
<b>Figure 2.4:</b> The different biometric characteristics.....	p26
<b>Figure 2.5:</b> The working principle of keystroke analysis system .....	p29
<b>Figure 2.6:</b> The face recognition system used in Olympic game.....	p33
<b>Figure 3.1:</b> Mobile commerce system flow chart .....	p42
<b>Figure 3.2:</b> The multi-modal authentication process .....	p47
<b>Figure 3.3:</b> NFC interface .....	p50
<b>Figure 4.1:</b> The comparison result between each participant.....	p57
<b>Figure 4.2:</b> The flow chart of typing behaviour recognition system .....	p61
<b>Figure 4.3:</b> The duration time and latency time in keystroke data .....	p62
<b>Figure 4.4:</b> Two tables in system database .....	p66
<b>Figure 4.5:</b> Experimental tools .....	p67
<b>Figure 4.6:</b> The system interface on windows phone .....	p69
<b>Figure 4.7:</b> The system interface on Android phone .....	p69
<b>Figure 4.8:</b> User registration page .....	p71
<b>Figure 4.9:</b> False rejection happens in the experiments .....	p71
<b>Figure 4.10:</b> False acceptance happens .....	p72
<b>Figure 4.11:</b> The flow chart of validation experiment .....	p73
<b>Figure 4.12:</b> The FAR and FRR in typing recognition experiment.....	p77
<b>Figure 5.1:</b> The face recognition algorithm used in Face.com .....	p83



<b>Figure 5.2:</b> The face recognition system .....	p86
<b>Figure 5.3:</b> The registration page .....	p88
<b>Figure 5.4:</b> The registration page .....	p89
<b>Figure 5.5:</b> User interface of face detect .....	p91
<b>Figure 5.6:</b> The experimental result interface.....	p95
<b>Figure 5.7:</b> The recognition results .....	p96
<b>Figure 5.8:</b> FRR of face recognition system .....	p97
<b>Figure 5.9:</b> The comparison of the FRR in experiment 1 and 2 .....	p99
<b>Figure 5.10:</b> The false acceptance happens .....	p100
<b>Figure 5.11:</b> FAR and FRR of the face recognition system .....	p101
<b>Figure 6.1:</b> The speaker recognition system model .....	p110
<b>Figure 6.2:</b> User registration interface on Android phone .....	p112
<b>Figure 6.3:</b> Speaker recognition web service .....	p113
<b>Figure 6.4:</b> Experimental interfaces .....	p116
<b>Figure 7.1:</b> The training interfaces of multi-modal system.....	p125
<b>Figure 7.2:</b> A mobile-commerce model .....	p128
<b>Figure 7.3:</b> Level 1 vilified interfaces .....	p129
<b>Figure 7.4:</b> Level 2 vilified interfaces .....	p130
<b>Figure 7.5:</b> Level 3 and 4 vilified interfaces .....	p131
<b>Figure 8.1:</b> The decision tree of a smart m-commerce model .....	p139
<b>Figure 8.2:</b> Fuzzy subsets and their membership functions .....	p142
<b>Figure 8.3:</b> The fuzzy inference engine methods .....	p147
<b>Figure 8.4:</b> The definition of fuzzy sets .....	p150
<b>Figure 8.5:</b> The definition of fuzzy sets .....	p152
<b>Figure 8.6:</b> The gained outcome fuzzy set after execute Rule 6 .....	p160
<b>Figure 8.7:</b> The gained outcome fuzzy set after execute Rule 10 .....	p161
<b>Figure 8.8:</b> The output result of Step 1 .....	p162
<b>Figure 8.9:</b> The Fuzzy Logic Controller Interface .....	p163

<b>Figure 8.10:</b> The final outcome fuzzy set .....	p165
<b>Figure 8.11:</b> The output result of Step 2 .....	p166
<b>Figure 8.12:</b> The Fuzzy Logic Controller Interface .....	p167
<b>Figure 8.13:</b> Fuzzy inference application Interfaces .....	p169
<b>Figure 8.14:</b> Output results after using fuzzy logic method in multi-modal biometric authentication system .....	p171
<b>Figure 8.15:</b> Fuzzy inference application Interface .....	p173
<b>Figure 8.16:</b> EER of the fuzzy logic based authentication system .....	p176
<b>Table 2.1:</b> The mobile commerce development history .....	p16
<b>Table 2.2:</b> Table 2.2: Comparison of related work .....	p38
<b>Table 3.1:</b> Authentication level set up .....	p43
<b>Table 3.2:</b> Experimental results .....	p50
<b>Table 4.1:</b> The experimental results .....	p76
<b>Table 4.2:</b> The different FRR and FAR when password length changed....	p79
<b>Table 4.3:</b> Comparison of related work .....	p80
<b>Table 5.1:</b> FRR of face recognition system .....	p97
<b>Table 5.2:</b> FRR in experiment 2 .....	p98
<b>Table 5.3:</b> FAR of face recognition system .....	p100
<b>Table 6.1:</b> Conventional SV versus SecuriVox SV .....	p106
<b>Table 6.2:</b> The recognition mechanism used in the system .....	p109
<b>Table 6.3:</b> The experimental results .....	p118
<b>Table 6.4:</b> The list table of experimental works .....	p119
<b>Table 6.5:</b> Results summary.....	p121
<b>Table 7.1:</b> The experimental results gained from Chapter 4, 5 and 6 .....	p124
<b>Table 7.2:</b> Potential parameters for inclusion into the multi-level authentication model.....	p125

<b>Table 7.3:</b> The recognition rate of a deterministic authentication system .....	<b>p133</b>
<b>Table 7.4:</b> Performance comparison of related works .....	<b>p135</b>
<b>Table 8.1:</b> The details of fuzzy sets .....	<b>p148</b>
<b>Table 8.2:</b> The details of fuzzy sets .....	<b>p151</b>
<b>Table 8.3:</b> The fuzzy rules 1 .....	<b>p156</b>
<b>Table 8.4:</b> The fuzzy rules 2 .....	<b>p157</b>
<b>Table 8.5:</b> Input values .....	<b>p158</b>
<b>Table 8.6:</b> The output fuzzy sets after conditional rules are executed.....	<b>p159</b>
<b>Table 8.7:</b> Input values and their membership.....	<b>p163</b>
<b>Table 8.8:</b> Input variables .....	<b>p171</b>
<b>Table 8.9:</b> The details of experimental results .....	<b>p173</b>
<b>Table 8.10:</b> The comparison of results which were gained from fuzzy .....	<b>p175</b>
<b>Table 8.11:</b> The difference between the two authentication models .....	<b>p177</b>
<b>Table 8.12:</b> Comparison of related works .....	<b>p180</b>
<b>Table 9.1:</b> Comparison of related works .....	<b>p186</b>

# Chapter 1

## Introduction

With the development of mobile phone industry, mobile phone subscriptions are increasing in recent years and Smartphone have become ubiquitous in modern society. More and more people are beginning to use mobile phones as business or communication tools but also as a means of planning and managing their work and daily life. Meanwhile, mobile security issues such as mobile theft and remote attacks are rising and haunting the mobile phone user. The large amount of private information stored in mobile phone makes mobile security an increasingly important issue in recent years. In this research, a mobile security and smart system has been presented which aims to provide an efficient and good performance authentication engine for mobile commerce.

### **1.1 Mobile security and smart system**

The work of this research project is two-fold. Firstly, a multi-modal biometric authentication system which involves three biometric techniques was developed

to establish the identity of a user on a mobile phone. Secondly, a smart model was build to support the authentication of mobile commerce transactions. The traditional methods to implement identity authentication is achieved through an API (Application Programming Interface) between the authentication and access control service provider with an application strengthened with one-time password. This method does not meet the current security demands and a new identification mechanism is required.

Primarily, this thesis presents a multi-level authentication mechanism which defines a number of authentication levels in the system according to the transaction risk. This model can be used to support the authentication of mobile commerce; it will not only introduce systematic safety, but will also be more convenient to the user. Based on this model, it can use a number of authentication techniques (like biometrics) rather than a password to ensure the system security.

Biometrics (or biometric authentication) consists of methods for uniquely recognising humans based upon one or more intrinsic physical or behavioral traits (Jain et al., 2000). Particularly in computer science, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Compared with the widely used password-based technologies, biometrics will never be lost or forgotten, hard to forge and easy to use. In this thesis, the presented multi-modal biometric system involves three biometric techniques: typing

behaviour recognition, face recognition and speaker's identity recognition. At the end of the thesis, a fuzzy inference model has been built to determine the transaction risk in mobile commerce, and to also determine the recognition rate of the biometric authentication results. From this research work, further research questions were addressed on whether the biometric techniques can be used instead of password, and whether the smart model is possible to achieve the balance between safe and convenience of use in mobile commerce. The performance test and experimental results in this thesis will aim to find out the answer.

## **1.2 Research background**

At present, nearly everyone has a mobile phone in UK and some people even have more than one (Cellular-news.com, 2009); and over a quarter of adults and nearly half of all teens now own a Smartphone (Ofcom News, 2011), the mobile phone is becoming an important part of our daily life. More and more people begin to use Smartphone to plan and organise their work and private life. A report (InternetRetailing, 2011) released in 2011 said, Across France, Germany, Italy, Spain and the UK, 13.5 million users accounting for 5.8% of all mobile subscribers – accessed online retail sites in the three month average period ending May 2011. This growth is even stronger in the UK, with a 163% increase in Smartphone users accessing retail sites since May 2010. In mobile commerce, the need for security is even greater. If we can establish the identity of the user on a mobile phone, a number of mobile commerce services can be

provided, such as mobile banking, mobile ticketing, mobile marketing, NFC transaction, and even make a payment in store. Examples are shown in Figure 1.1.



Figure 1.1: The trends of mobile commerce

## 1. Mobile banking

Since the first mobile phone with WAP support enabling the use of the mobile web in 1999 (Itavisen, 1999), the mobile banking has been one of the fastest growing markets in the world. Many banks in UK like Barclays, RBS and TSB have provided their mobile banking service, but most of the authentication mechanisms are based on User ID/Password or One-time password, if a more

secure mechanism like biometric authentication been used in mobile banking, more customers will choose to use the mobile banking service.

## 2. Mobile ticketing

The working process of a mobile ticketing system is: buy tickets online and the web server will send the electric tickets to customer's mobile device, and then the customer can go straight to the ticket-taker. It is shown in Figure 1.2.

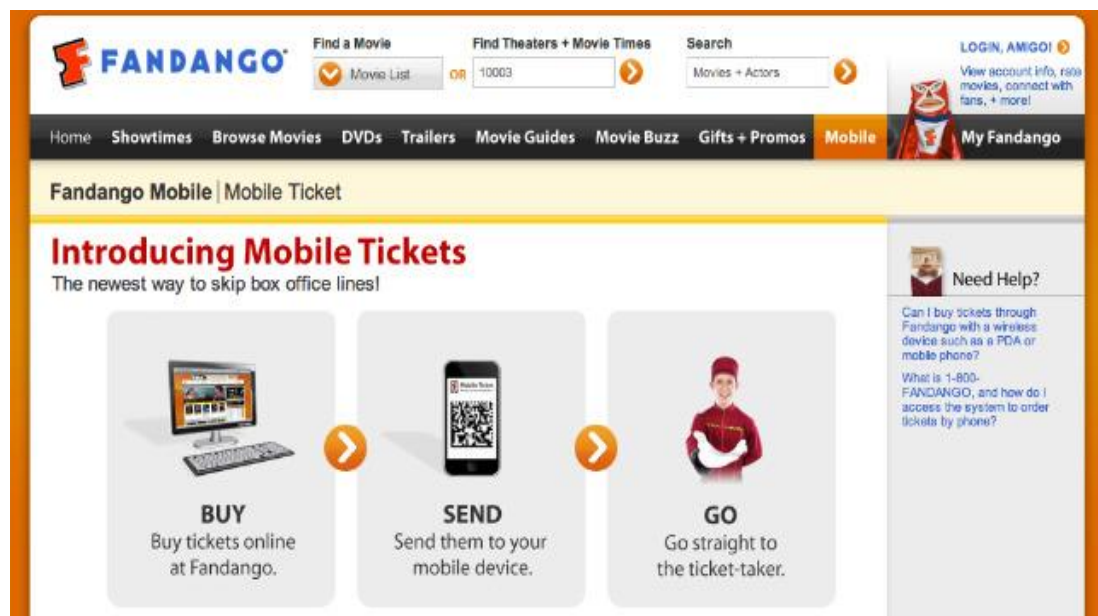


Figure 1.2: The mobile ticket system used in Fandango.com (2012)

Particularly in the mobile ticketing system, if a mobile application has been installed on client side and an authentication mechanism is used to identify the identity of the user, it is not necessary to purchase a ticket from the PC side. Customers can order, pay for and validate tickets from their mobile phone at anytime and anywhere. Obviously, the convenience of mobile ticketing will make



it more popular in future.

### 3. NFC & Tangible goods

According to a survey by the Mobile Marketing Association (MMA, 2010), 17% of mobile commerce was used for applications or ring tones, 6% used their mobile phones for coupons and or discounts, and another 6% used their phones for physical goods. NFC (Near Field Communication) is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows user to share small payloads of data between an NFC tag and a mobile phone (AndriodDevelopers, 2013), this has provided the opportunity to build “Touch and Go” applications. Using an NFC phone allows the user to touch a tag and walk out of the shop, leaving the payment to the back-end system. On the other hand, a user requires assurance that the system would restrict the use of their phone if it fell into the hands of a thief; some form of authentication system is needed. Anyone can image a scene: maybe in future, no cashier and no check out point in store and just by use a mobile phone, actual goods that you can put in your hands.

### 4. Mobile marketing

Mobile commerce is growing and it is directly related to the amount of mobile marketing that companies are investing in (Rogers, 2010). Another report (Mulpuru, 2010) indicates that 74% of online retailers either already have or are developing a mobile strategy. One in five has a fully-implemented mobile

strategy in place already. As shown in Figure 1.3, Amazon and eBay have launched their mobile App.

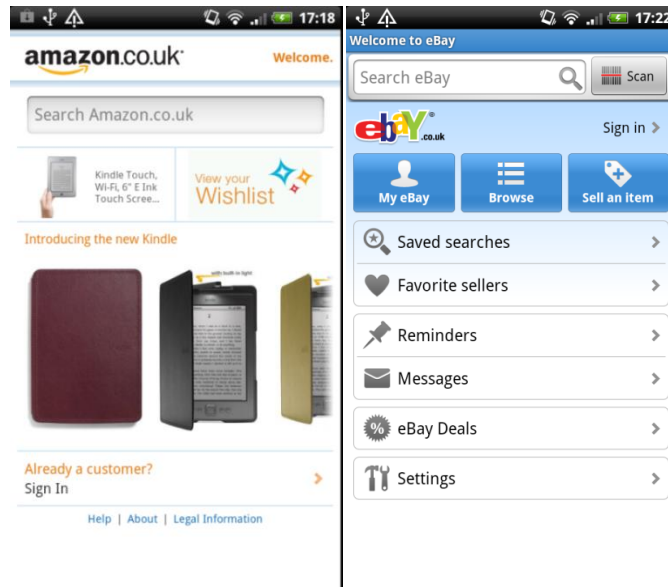


Figure 1.3: The mobile marketing applications

Amazon and eBay's mobile store are two examples which illustrate that the mobile marketing is considered by more and more retailers.

Overall, with the increase of mobile marketing and mobile transaction, there is a burgeoning need for mobile commerce services. Whilst the ability to purchase goods and access information in mobile commerce is convenient, it also has security risk existed. Due to the risk factor, there is a need to provide a comprehensive security system on mobile phones, verifying the identity of the user. This research therefore seeks to develop a smart multi-modal biometric authentication mechanism to ensure the security of mobile commerce.

### **1.3 Objectives of the project**

For the individual user, an authentication mechanism is the most important part of information security. If the authentication system is compromised, that means all the users' information is disclosed, and moreover can cause huge financial loss. Therefore, an authentication mechanism with high safety-critical, easy to manage, easy to use is always desired. With the fast development of information technology in the latest decades, many scientists and researchers have presented number of security technologies. Although these techniques may have many differences in principle, they can encrypt the information and protect the system against unauthorised access. More differences are reflected in the level of security they can achieve, technical stability, and usability. An overview of the current authentication systems, and the challenge can be broken down into three areas:

1. How to use biometrics 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-modal authentication system.

The objectives of the thesis are shown as follows:

1. Build up a multi-level authentication based on password to make

system more reliable and convenient.

2. Explore the biometric in mobile authentication.

3. Combines typing behaviour recognition, face recognition and speaker recognition techniques to build a multi-modal biometric authentication system.

4. Use fuzzy logic method to build a smart model.

5. Evaluate the developed system.

## **1.4 Structure of the thesis**

Chapter 1 has presented an introduction to the topic area, and the current development situation of mobile business in the worldwide. It has also discussed the challenge of mobile authentication, and the aim of the project. Additionally, at the end of chapter 1 summarises the outline of the thesis, shown as Figure 1.4.

Chapter 2 is literature review, which contains an overview of mobile phone services and mobile business/commerce, focus on the security issues on mobile transactions. Following on, the current authentication techniques will be discussed, in particular, general biometrics will be presented, with an emphasis placed on face recognition, speaker's identity recognition and typing behaviour recognition.

Chapter 3 will present a model to support the authentication of mobile business.

In this chapter, four different authentication levels will be set up in the system according to user's transaction details.

Chapter 4, 5 and 6 will detailed discuss how to build a multi-modal biometric authentication system, which includes model build up, the implement on mobile phones, software and hardware used to capture and analyse user's biometric data, experimental works and a discussion and analysis of the experimental results to show the performance of biometric authentication system.

Chapter 7 will focus on discusses the performance of a deterministic system model and the accuracy rate of multi-modal biometric authentication system. This chapter aims to provide an evaluation of the authentication mechanism.

Chapter 8 will present a smart model which can be used in mobile-commerce. This model uses a fuzzy logic method to determine the transaction risk and recognition result. A comparison between these two models will be presented then, and the discussion section will investigate the flexibility, accuracy rate, usability and performance of these two models.

Finally, conclusions and future work will be discussed in Chapter 9.

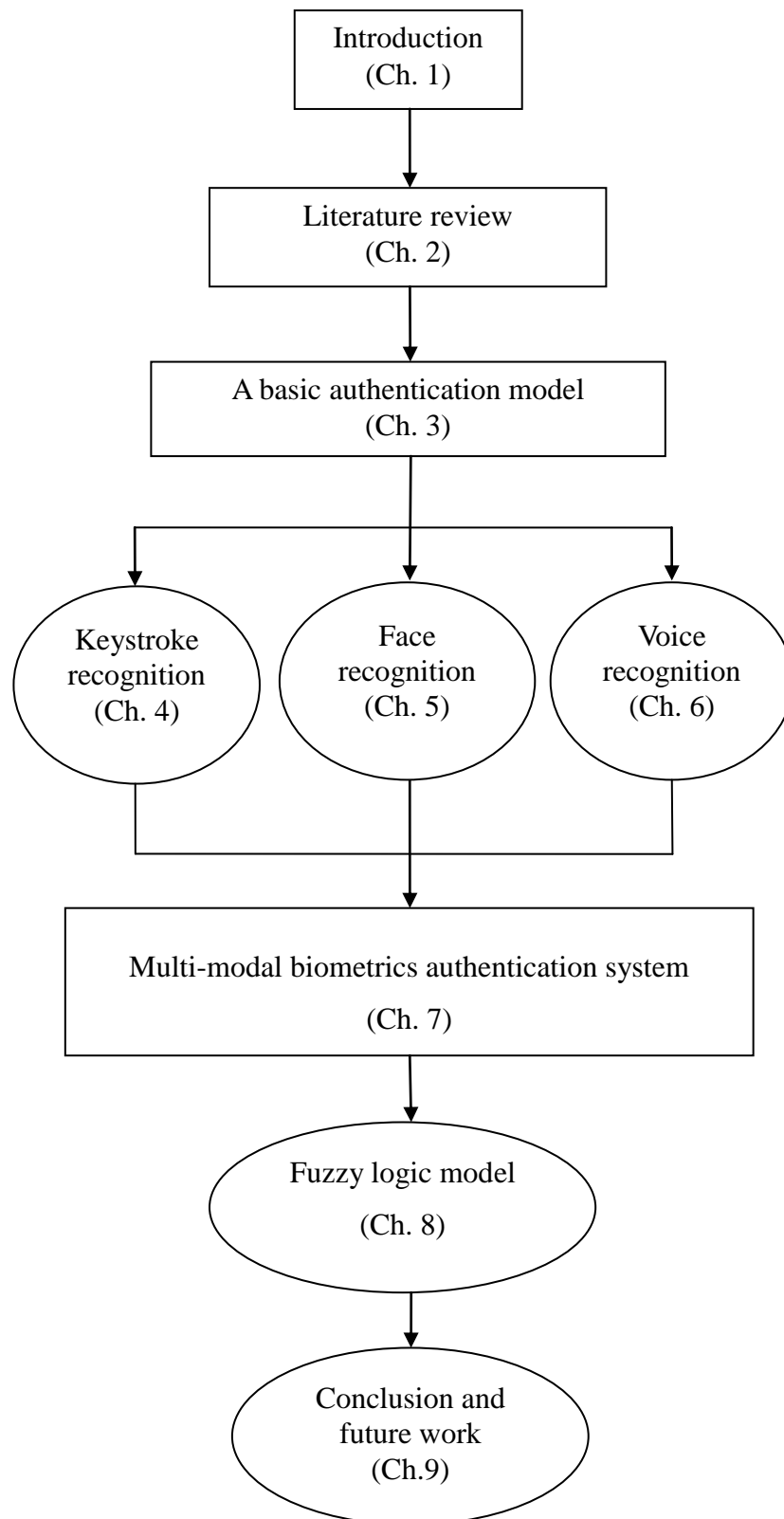


Figure 1.4: The outline of the thesis

## Chapter 2

### Literature review

#### **2.1 Research background**

Since the first generation wireless technology (1G) was launched in the 1980s (Carney, 2002), the development of mobile industry has not stopped. The number of mobile users is increasing every year. A report (CBS News, 2010) in February 2010, said there were worldwide 4.6 billion mobile phone subscribers, a number that is estimated to grow throughout the next few years. Meanwhile, more and more mobile phone manufacturers have released their latest smart-phone like Iphone and Androids phone. Compare with non-smart phones, smart-phone is effectively a small computer and as such has the ability to preserve a large amount of personal information. It also can provide various services including mobile commerce and mobile identification. Mobile commerce can be used to purchase goods, tickets or make a payment. A report (realwire.com, 2011) revealed that 10 million online consumers in the UK made

a transaction using a mobile device in 2011. On the other hand, as other forms of commerce, there is a security risk within mobile commerce. The UK government (BBC news, 2010) has called on the mobile phone industry to do more to protect handset owners against theft. But some other criminals are beginning to use mobile spyware to purloin the user's financial information in their mobile phone (Figliola, 2006). Based on this research background, a new mobile security system which aims to protect user's information and assure the transactions security has been proposed in this thesis. The primary challenge of the system is to establish the identity of a user on mobile phones. At present, the most popular methods to achieve mobile identification are based on username and password or PIN. PIN and Password can easily be lost or forgotten (Uludag et al, 2004). Additionally, hackers or criminals can use a variety of methods to steal a password or PIN. In the past several years, many researchers have introduced the use of biometric techniques instead of a PIN or password. Some related studies such as Clarke and Furnell (2007<sub>b</sub>) have proposed the use of a user's keystroke behaviour as a biometric to identify the user; Chen et al. (2010) have built a face detection and recognition system for a mobile device. Many other researchers have used finger print (Xi et al., 2011) or voice print (Lee, 2009) as biometric to achieve identification.

## **2.2 Overview of mobile commerce**

Mobile commerce refers to the distribution of business data to mobile phone such as smart-phones and tablet computers. It is a new e-commerce model



which achieves data transmission through the mobile communication network and then uses a mobile phone to participate in various business activities. Mobile commerce started around the year 2000, when the internet was available on a mobile phone (Sukumar, 2011). Mobile commerce has shown a significant growth in the last few years, and this change has been partly encouraged by a change from the 'wired world' to a 'wireless world' with the advantage of smart phones which has led to a new era of mobile computing (Ramakrishnan, 2008).

Mobile commerce users can collect real-time business information and make decisions at any time and any place. They can communicate with others accurately for the first time, or interact with a business information centre, let customers release the constraints of fixed equipment and wired network environment completely. According to a report from InformationWeek (Hatch, 2008), many companies have moved to mobile and remote workforce strategies, with the aim of improvement in employee productivity (for example, the time spent looking for information) to better and faster decision making, better customer service, and delivery of real-time bi-directional data access to make decisions anytime and anywhere.

### **2.2.1 History of m-commerce**

Mobile commerce development has been through three generations. The first generation was based on Short Message Service (SMS) technology; it was born

in 1997 when the first two mobile phone enabled Coca Cola vending machines were installed in the Helsinki area in Finland (Mobile commerce – white paper, 2010). The machines accepted payment via SMS text messages. The first mobile phone-based banking service was launched in 1997 by Merita Bank of Finland, also using SMS (Barnes and Corbitt, 2003). There were a few serious flaws in the first generation mobile commerce: poor security, the transaction was not protected; SMS message length limit also makes the information incomplete.

Second generation systems were based on Wireless Application Protocol (WAP) technology. The user can search information on browser web pages through their mobile device. Other Mobile-commerce-related services spread rapidly in early 2000. For example, Norway launched mobile parking payments, Austria offered train ticketing via mobile device, and Japan offered mobile purchases of airline tickets (Mobile commerce – white paper, 2010). The second generation systems partly solved some mobile access issues, but there were still security risks and limited interaction ability.

The third generation mobile commerce system came with the launch of the smart phone, with the appearance of the Iphone and Android phone. Mobile commerce has moved away from SMS systems and simple WAP into actual applications. The third generation mobile commerce system which combines smart phone, Virtual Private Network (VPN), database synchronisation, identity

authentication, web service and other mobile communication techniques are able to provide a secure and fast mobile commerce mechanism. The follow table shows the different between each generation:

Generation \ Feature	Functions	Technology
G1	Question & answer	SMS-based
G2	Information service	WAP
G3	Identity determine Mobile payment	NFC, 3G, Web server

Table 2.1: The mobile commerce development history

The functions of the 3rd generation mobile commerce systems are shown as follows:

- (1) SMS function – The system can send text messages to users after transaction; and the electronic receipt will inform the user of about the transaction detail.
- (2) Comment function -- Users can comment on the product. This function achieves direct and effective communication between user and the trader, and lets the trader receive feedback and suggestions from the customers.
- (3) Display function -- The complete product descriptions displayed on the web

page can help user resolve the restriction of time and space imposed by 2G.

(4) Shopping guide function -- Mobile commerce systems can provide online query service. The user can contact the trader directly and then order online.

(5) Authenticate function – Determine the user's identity on mobile device using username and password or other authenticate technology; potentially includes biometric data.

(6) Mobile payment -- The mobile phone can be turned into an wireless payment tool by using the NFC or 2D barcodes combined with biometric techniques. This has the potential to make the system more convenient and secure for the user.

Because of the greatly improved performance, the third generation mobile commerce system can provide a significant number of services on a mobile phone. Many of these services rely on the user of the phone being the owner; these services can interact with private and personal information. For example:

- Mobile banking where the user can pay bills, move cash between accounts
- Mobile ticketing where the mobile phone can be used to purchase tickets that are delivered to the phone in electronic format
- Mobile commerce where the phone is used as the medium through which the user can make a purchase
- Mobile phones for airport boarding passes: e-passport, e-identity
- Tracking of individuals via their phone

- Mobile wallet, mobile money

### **2.2.2 An existing m-commerce model**

Since the appearance of mobile commerce, M-Commerce is not only being widely accepted but also it is being more used as a popular way of business/commerce, and traditional payment method will gradually be replaced (Jahanshahi et al., 2011). At present, a mobile cell phone with a NFC (Near field communication) chip can replace bank cards to complete a purchase. "Mobile wallet" is one of the m-commerce services; it is based on NFC and RFID (Radio frequency identification) techniques. In such a system, it uses mobile phone as the client tools, link with the user's bank account, via SMS, IVR (Interactive Voice Response) and other means to achieve mobile payment or view an account balance. Replacing cash, cheque or credit cards, a consumer can use a mobile phone to shop at any place with a POS (point of sale) machine (such as store, shopping centre or bus station), as shown in Figure 2.1.



Figure 2.1: User Interface of 'Mobile Payment' (Source from [www.baike.baidu.com](http://www.baike.baidu.com))

With the development of mobile recognition and NFC techniques, mobile payment has attracted interest by more and more mobile phone manufacturers and mobile Communication Companies. Mobile payment is undoubtedly the trend of the future of mobile phones. Japan already has more than 50 million mobile phone users that use them as a "mobile wallet". 'Mobile wallet solutions are our top priority' says PayPal boss (Clark, 2010), and the market analysts Juniper Research expected in 2013, "Mobile Wallet" user will increase from the current 50 million to 700 million.

### **2.2.3 The status of mobile commerce in the UK**

Will people hesitant to use mobile payments? What are the barriers to purchase on mobile phone? According to the survey from Intersperience (2011), 8% of UK adults buy through their mobile phones, while 21% intend to in the future. But this report also said 37% of UK adults are hesitant to use a mobile phone to buy something. Another report (Richards, 2011) indicated that 69% of smart-phone users who do not buy via mobile simply prefer to use their PC or laptop for shopping. 34% people said mobile commerce 'doesn't feel secure', and 9% felt the payment process is too complex. A further 2% of those surveyed said they did not know sufficiently about mobile payments, and 4% thought that the cost was too high. The detail of data within the survey report is shown in Figure 2.2.

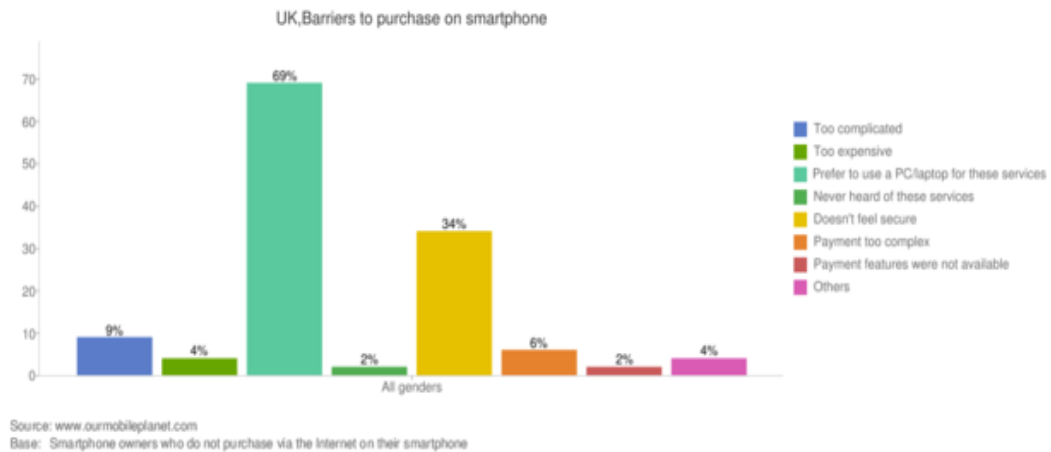


Figure 2.2: The reason why users not choose mobile commerce (Source: [www.ourmobileplanet.com](http://www.ourmobileplanet.com))

From the results in these reports, it can be seen that ‘security’ and ‘complexity’ were the most important issues that the mobile phone users were most concerned about. Therefore, the promotion of mobile commerce should be based on good security measures which can resolve potential security problems, excellent publicity, and simplified mobile payment methods.

## 2.3 Overview of the mobile security

### 2.3.1 Mobile phone theft

As the mobile phone market grows every year, the mobile phone theft problem is becoming more and more serious. In 2010, a report (BBC news, 2010) states that around 2% of British mobile phone users report they have suffered a theft in the last year, and 228 mobile phones are reported stolen in the UK every hour. One can imagine that the main purposes of an m-commerce user are purchase,

sale or make some other transactions. All of these actions rely on personal information. The mobile phone, as the main implementation tool in mobile commerce, will always store a user's private information for example home address, credit card details or purchase history. This feature could give criminals the chance to access the victim's private information or bank account if their mobile phone was stolen. When this happens, the user loss is not only a cell phone but also the loss of personal information and lots of money. 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". Due to the reliance on mobile phones in a modern society, only providing the security of mobile phones is not enough, they must also provide security of user's personal data. If a method can ensure data safety, even when the mobile device is stolen, a victim does not need to worry about their private financial information and any more loss.

### **2.3.2 The current authentication technology on mobile device**

Password-based authentication technology which includes PIN, username-password, dynamic password (one-time password), and challenge-response is the most commonly used individual user identification technology (Borde, 2007). Logging into an operating system and e-mail user authentication are both based on this method. The system will open the access authority only when the password matches the initial set. Such a password



verification system is very simple: it includes client side and server. The Figure 2.3 shows how the system works.

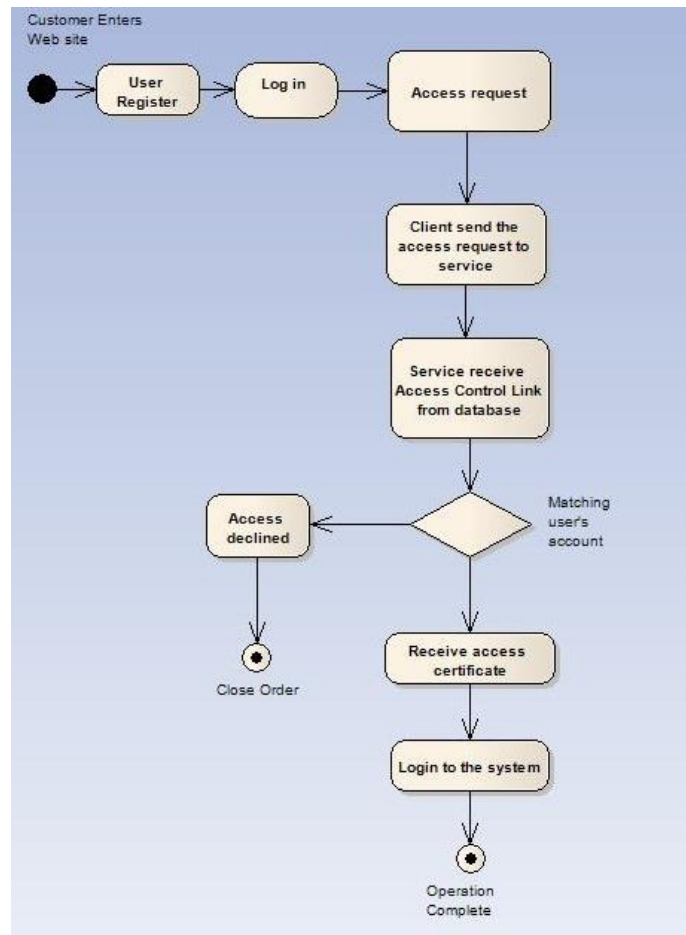


Figure 2.3: Flow chart of password authentication system

The client provides a system access interface where users can enter their user name, password and such information will be immediately sent to the server-side. The server-side matches the “username / password “with its own database to check if the corresponding entries can be found. If the information matches, access to the system is authorised. Otherwise, where there is no such corresponding entries, or user input information are not fully compatible with the database, the system will reject the access request.

The password-based authentication method is easy to achieve and can provide basic protection, it is widely used in security systems like: online banking, account management, and credit cards systems. However, some shortcomings in password-based authentication are in existence, which provides Hacker opportunities to attack the system. At present, there are a variety of hacking methods can be used by criminals to steal a password. For example, attackers can use social networking information to guess a user's password; capture weak passwords to decrypt whole passwords; or use the "Trojan horse" program to intercept and capture the password. Due to these hackings, many users often report to their bank because of their accounts and passwords were stolen. In mobile commerce, users usually link their bank account with the mobile phone. If the mobile phone is stolen, then that means all user's private information and bank account are open to the criminal. And the phone loss will lead to huge financial losses. Therefore, some new authentication models are required to enhance the defense capabilities of the mobile security system.

### **2.3.3 The issues exist in mobile commerce**

Besides the password-based authentication technique, there are other authentication techniques like biometric authentication and user behaviour recognition which can be used in a mobile security system. At present, most of existing authentication model use single technology, but it is difficult to achieve a high accuracy rates (Dave et al., 2010; Campisi et al., 2009). The use of multiple authentication technologies can slow down the speed and increase the

complexity of system. Basically, the current mobile commerce has a list of issues:

1. **Poor reliability**, transaction message or electric tickets are easy to lost or be stolen.
2. **Poor usability**, a user need to register a password for each independent system. If the password is forgotten, the system will reject all the access requests.
3. **Security**, password is the most popular technology in mobile payment, biometrics and other techniques has not been widely used.
4. **Dumb system**, most of the mobile shops use dumb system: the transaction risk cannot be measured; the authentication process is always the same for every transaction; the transaction is over when consumers finish the purchases and user's behaviour will not be recorded on the system.

In summary, the identification of individuals based upon user name and password has existed for hundreds of years (Crisman, 1965). Passwords have been used with computers since the earliest days of computing (Morris and Thompson, 1979). Researchers have presented a variety of favorable results and most have shown the password based system is feasible to authenticate users based upon username and password (Lin and Chang, 2009; Yang and Chang, 2009; Ross et al., 2005). But this is facing more and more security risks and hacker attack, the password-based authentication is not enough to protect the system. A well-developed biometric authentication system on mobile phones

has not been widely implemented. Therefore, the primary challenge of this research work is to develop a smart and security system which is more convenient and secure in mobile commerce.

## **2.4 An overview of biometric authentication**

Biometrics, which is concerned with the unique, reliable and stable personal physiological characteristics such as fingerprints, facial features, iris pattern, retina and hand geometry, or some aspects of behavior, such as typing behaviour and handwriting, 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). A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by the user. A system that uses physiological biometrics can identify an individual by use physical feature of an individual. Conversely, behavioural biometrics attempt to characterise the way in which an individual does things, the system use behavioural biometrics can identify an individual though voiceprint, signature or the keystrokes way. Many research works found the biometric identification model has the potential to create a substantial value in the future. In 2007, IBG (International biometric group) released an annual report of the global biometric market (IBG, 2007), it lists several widely used biometric technologies, and the report also predicted the market scale for the next five years: more than 3 billion U.S. dollars in 2007, reached 38 billion

dollars in 2008, and it will exceed 7.4 billion by 2012, and actually Visiongain's (Visiongain, 2013) analysis indicates that the Biometrics market is set to be worth 7.59 billion dollars in 2012. Figure 2.4 shows a number of different biometric characteristics which can be used for biometric authentication (Lin, 1998; Huang et al., 2012). These recognition techniques are the most popular and widely studied in the related research area. Each method has its own scope of application, not all being suitable for mobile authentication.

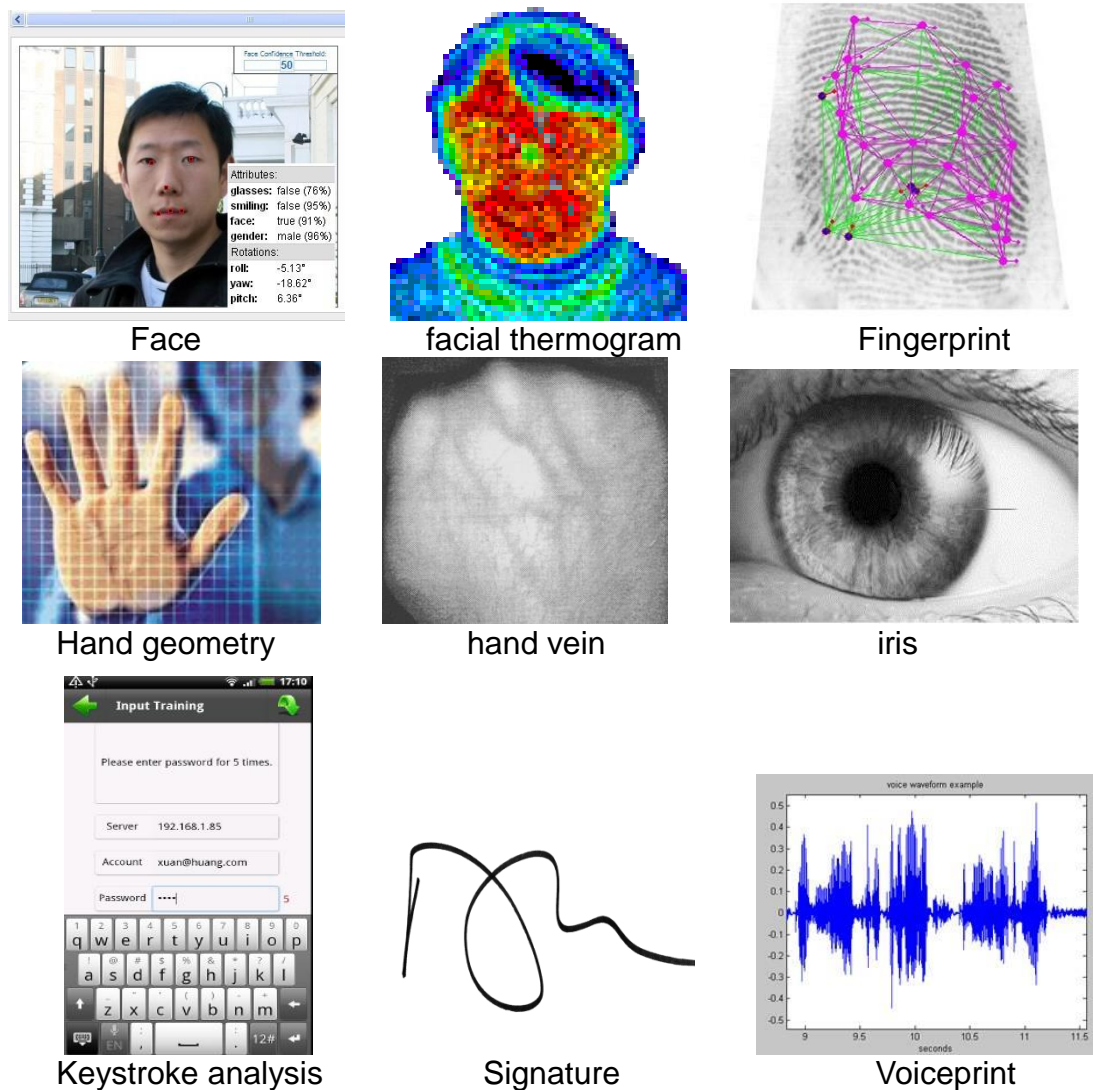


Figure 2.4: The different biometric characteristics

Compared with password-based identification methods, biometric recognition technologies have the following features:

1. **Portability:** biological characteristics are the inherent characteristics of human body. It can be carried to anywhere at any time.
2. **Generality:** everyone has biological characteristics.
3. **Uniqueness:** everyone's biological characteristics are different (Jain et al., 1999).
4. **Stability:** most of the biological characteristics such as fingerprints and iris will not change with time and conditions (Pankanti et al., 2000)
5. **Security:** biological characteristic is the best proof of personal identity and it is hard to steal or imitate. It can satisfy high level security requirement.
6. **Collectable:** at present, there are several pieces of equipment (such as: camera, microphone, fingerprint reader and so on) that can be used to collect biological characteristic from an individual.

Based on the above features, biometrics authentication provides several significant advantages compared to traditional techniques. It is not necessary to set and remember your password, and it is more secure and convenient to use. At present, many studies have proposed biometric authentication system on mobile phone. Dave et al. (2010) built a face recognition system on a mobile phone; Ricci et al. (2006) use the e-signature as the identification tool; Clarke and Furnell (2007<sub>b</sub>) use keystroke analysis to achieve mobile authentication. Wang et al. (2007) built a J2ME application which can implement fingerprint

authentication on mobile phone.

In consideration of the specific hardware configuration of mobile phone, signature and fingerprint recognition system required a mobile device with fingerprint reader or a sweep sensor. But most mobile phones only have keyboard, microphone and camera. Therefore, face recognition, speaker recognition and typing behaviour recognition techniques are recommended to be used in the mobile authentication system (Clarke and Furnell, 2007<sub>a</sub>).

#### **2.4.1 Typing behaviour recognition**

Keystroke dynamics, or typing dynamics, is the detailed timing information that describes exactly when each key was pressed and when it was released as a person is typing at a computer keyboard (Moskovitch, 2009). The typing behaviour recognition technique combines Keystroke dynamics with the traditional password-based authentication method. The research into keystroke dynamics as an authentication method relies on developing a technique that is robust, inexpensive, and has the potential to be transparent to the user (Crawford, 2010). The first research work based on typing behavioural recognition was reported in 1975 (Spillane, 1975), and in the following decades, its feasibility has been examined on both computers (Monrose and Rubin, 2000; Zahid et al. 2009; Araujo et al. 2005) and mobile phones (Campisi et al. 2009; Clarke et al., 2002). As shown in Figure 2.5, there are two key times in the system: hold time and inter-key latency. The hold-time characteristic is calculate

by recording the time between pressing the key and releasing it; and the inter-key latency or time between successive keystrokes, is calculate by recording the time between release the first key and pressing the next one.

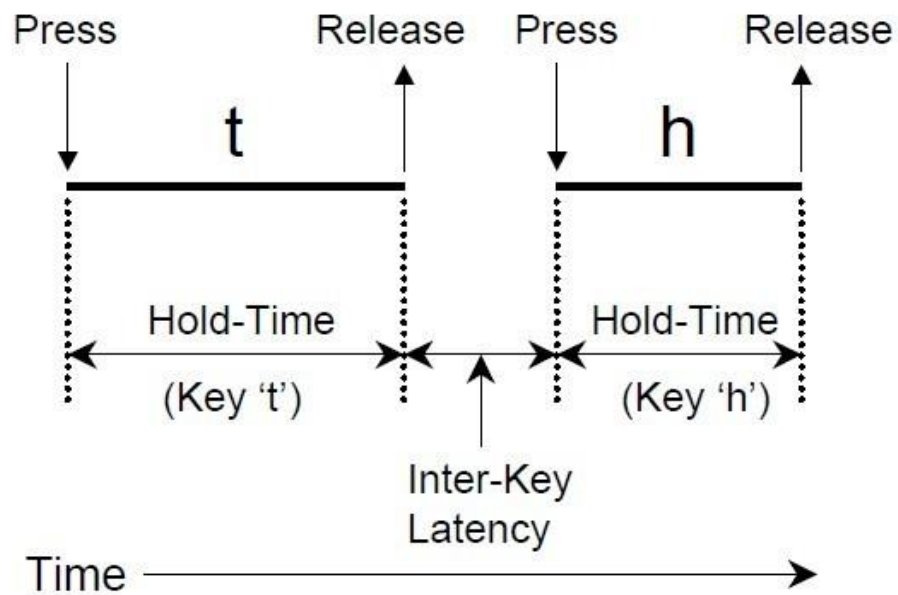


Figure 2.5: The working principle of keystroke analysis system (Karatzouni and Clarke, 2007)

Hold time and inter-key latency are the two standard metrics in a keystroke analysis system (Crawford, 2010); these metrics can be used to identify the typing speed of a user, therefore, keystroke is considered to be a typing behaviour whereby the typing pattern of a user creates a unique signature. Keystroke dynamics are not expected to be unique to each individual since there is likely to be similarities between individuals' typing style, but it is known to be sufficiently different between users to be useful as a method of verifying a user's identity. In Blender and Postley's (2007) work, they found that if a system



can achieve recording and analysis of user's input mode at the same time with user password identification, this dual protection mode will not only guarantee the user's data security, but also effectively prevent the attacks of hackers. On the other side, typing behaviour recognition is not only used on a desktop or laptop, Clarke and other's (2002) work is based on mobile phones, and they have proposed a neural network pattern classification method. The drawback is that mobile phones lack the computing power necessary to employ a neural network in situations where the processing is done on the device itself (Crawford, 2010). Overviews of the current research work, show that most of the studies are based on desktop and laptop keystroke dynamics (Garcia, 1986; Denning, 1999; Araujo et al., 2005), and others are based on numeric keyboard phone or Personal Digital Assistants (PDA) (Clarke and Furnell, 2007<sub>b</sub>; Zahid et al., 2009; Campisi et al., 2009). At present, the latest mobile phones like the Iphone and the Android phone have similar full size QWERTY keyboards which could help developers to improve the performance on such devices.

### **2.4.2 Face recognition**

A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source (Animetrics, 2008). One of the ways to do this is by comparing selected facial features from of the image and with those of a facial database. Although the human has a great ability to recognize faces to remember and identify thousands of different face (Zhao et al., 2003), it is more difficult for

computer to do so because of these following reasons: images of different facial expressions of the same person differ greatly; the face will change with age; the quality of face image will be affected by light, angle and imaging distance. In addition, face recognition is also related to image processing, computer vision, pattern recognition and neural network. These related factors make research of face recognition a challenging task.

The research on automatic face recognition has over 20 years' history (Kirby, and Sirovich, 1990). The early research of face recognition can be divided into two main directions: one is the face geometric feature extraction method, and the other is template matching method which use the analysis of templates and image gray correlation to achieve face recognition. In 2000 (Lin, 2000), the main research of face recognition has another two new directions: the first one is based on the overall properties of face; while the second is based on characteristics analysis methods which constitute recognition eigenvector. These methods analyse benchmark of human detection/recognition and other relative facial features parameters or category parameters to describe the shape of the face. Comparing these two categories of methods, the whole face feature based recognition method will not only retain the topological relationship between the parts of face, but also retained other part's information (Zhang and Su, 2000). While the second method based on characteristics analysis boasts a specific identification algorithm through extracted local contour information and gray information. Berto and Poggio (1993) said the method based on the whole

face analysis is superior to the method based on parts analysis; the reason is that the former method retains more information. But such a view is rather defective, because if the whole face image is used as a model, light, angle of view and face size will influence recognition result. Therefore, how to effectively remove this interference is the main crux. In contrast, the identification method based on face parts analysis is much more intuitive; it extracts and uses the most useful features, such as the position of key points or the shape of the component. Until recently, a new method combining whole face recognition with characteristics analysis has been proposed: Tremblais and Augereau (2004) use multi-scale edge detection and characteristics recognition method to locate human faces; The Flexible Model proposed by Lanitis et al. (2002) can explain the whole face image and codes the features points. In Li and Prince's (2009) work, they have built a model to find the key point positions, treat the location of each key point as a hidden variable and marginalise over it in a Bayesian manner. This algorithm greatly improved recognition accuracy, but it poses high requirement for image quality. The authentication web service provides by Face.com (2012) can analyse the physiological characteristics of human face, given age, genders and other related information. Face.com's API provides fast and real-time face recognition.

As an important method of biometric authentication, face recognition has been widely used in banking, customs, post offices and other commercial departments. In the 2008 Beijing Olympic Games, many gymnasiums have

been equipped with face recognition monitoring alarm system, which established an automatic face recognition and alarm network. When the system detected unauthorised person attempting to enter the gymnasium, it sends off an alarm to the security center. As one of the security measures, the face recognition system greatly enhanced the security of the Olympic Game in Beijing, and also improved the tourist identification work. The pictures in Figure 2.6, which were shot on the 8<sup>th</sup> August, 2008, show the audiences undergoing face recognition checkpoints before entering the National Stadium.

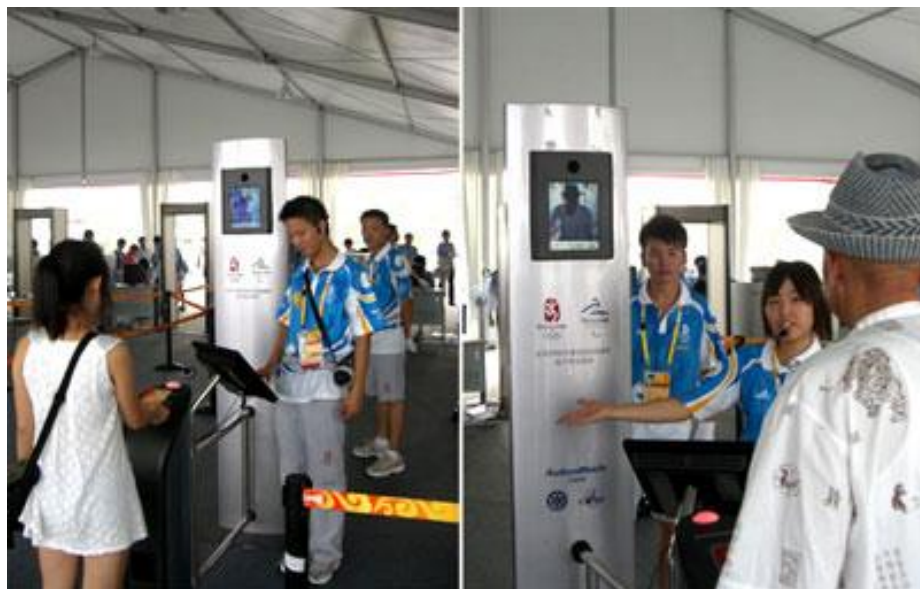


Figure 2.6: The face recognition system used in Olympic game

Compared with fingerprints, retinal and other biological authentication techniques, face recognition is intuitive, friendly, and easy to use (Hong and Jain, 1998). Based on this reason, face recognition research has attracted extensive attention in recent years. However, most face recognition equipment and

hardware is larger, has poor mobility, and it is widely used in public place but not suitable for personal use. In recent years, the developments of multimedia techniques have promoted the spread of digital cameras and mobile phones. /Anyone with such a device can readily take their facial photos at anytime and anywhere, this make it possible to use face recognition techniques to establish the identity of the user on a mobile phone.

### **2.4.3 Speaker recognition**

Speaker recognition is the computing task of validating a user's claimed identity using characteristics extracted from their voice (Saquib et al., 2011). Speaker recognition has a history dating back some four decades and uses the acoustic features of speech that have been found to differ between individuals (Kinnunen and Li, 2010). These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). Speaker recognition has a mature theory and can reach a high accuracy in laboratory conditions, and is beginning to be considered by companies: since 1998, some companies like AT&T, ITT, Keyware, T-NETIX, Motorola and Visa also have related research work on speaker recognition (Hong and Yu, 2009).

The commonly used speaker recognition algorithms include: Pattern Match, Vector Quantization, Gaussian Mixture Model, Support vector machine and Artificial Neural Network. In Reynolds and other's (Reynolds and Rose, 1995)

research work, they use Gaussian mixture models (GMM) to achieve robust text-independent speaker identification. It can achieve an 80.8% accuracy rate by using 15 second telephone speech utterances. Gaussian mixture models have been used in the earliest research work in this area, but it is hard to achieve a high recognition rate. In order to solve this issue, support vector machine (SVM) have been proposed. This is a powerful discriminative classifier that has been recently adopted in speaker recognition (Kinnunen and Li, 2010). In Huang's (2004) work, the researcher distilled the speech parameters from individual's speech features, and the identity of the speaker is automatically recognised according to these speech parameters. In Campbell et al. (2006) and Shriberg et al.'s (2005) work, they have successfully used combined SVM and GMM to increase the accuracy rate. In recent years, artificial neural network is another method which has been widely used in the speaker recognition system because it has strong anti-interfere and adaptive learning ability (Bai, 2006). But this method is slow in terms of inherent convergence speed, and prone to trap into a local minimum. Scheffer and others (2011) have proposed a speaker recognition systems based on MLLR (Maximum Likelihood Linear Regression) transforms, which has the ability to process a large amount of speech data.

As with a camera, the microphone is an indispensable part of a mobile device. A human speech signal is easy and convenient to obtain on a mobile phone. On the other hand, a noisy environment, and a change of human acoustic

characteristics will also affect the system accuracy rate. Overall, the speaker cognition technique has many advantages but also has its own flaws. As an important part of the multi-modal biometric authentication system, it is used to improve the system performance.

## **2.5 Smart authentication model**

The simplest authentication model requires the user to identify themselves via a password for every transaction. When a user uses it to process a low level transaction frequently, this repeated entering of a password is annoying. At the other extreme, a password is not secure enough to protect the high level transactions. For example, if an application used a single password on start-up, this would leave the user open to a significant loss if they were to lose their phone. In order to solve this issue, the multi-modal authentication system can provides a balance between repeated password entry and single password entry whilst adhering to the principle of higher value transactions requiring more security. In recently years, researchers have begun to use multi-modal authentication mechanism in personal identification systems. In Clarke and Furnell's work (2007<sub>a</sub>), they proposed a four authentication levels mechanism and used a set of biometric methods to achieve the authentication work.

In this project, a model to support the authentication in mobile commerce is proposed in Chapter 3; and then a multi-modal biometric authentication system is developed to combine with the model. Unfortunately, the biometric is not

always reliable; therefore, a fuzzy logic model has been built into the m-commerce environment. The fuzzy logic is a form of many-valued logic or probabilistic logic; it deals with reasoning that is approximate rather than fixed and exact (Novák and Perfilieva, 1999). Fuzzy set theory was firstly proposal by Zadeh in 1965 (Zadeh , 1965). Generally, a fuzzy logic method always focuses on what the system should do rather than find out how it works. In recent decades, this method has been widely used in control theory and artificial intelligence area. Mamdani and Assilian (1975) first used the technique in a linguistic synthesis system. Höppner et al. (1999) use this method for classification, data analysis and image recognition. Arabacioglu's work (Arabacioglu, 2010) uses a fuzzy inference system for architectural space analysis. Moreover, a number of researchers (Song et al., 1997; Büyükožkan and Feyzioğlu, 2004) have successfully used the fuzzy logic control algorithm in economic and business fields. All these research work demonstrated that fuzzy logic is a good method for sorting and processing data. The fuzzy model proposed in this project is aimed to provide high level flexibility and conventional decision support for the system when it is used in mobile commerce.

## **2.6 Summary**

This Chapter has presented an introduction of mobile phone as the device to deliver mobile commerce, and then discuss the background of mobile commerce and biometric authentication techniques. The comparison of related research work is shown in Table 2.2.



	Campisi et al. (2009)	Dave et al. (2010)	Kinnunen and Li (2010)	Koreman et al. (2006)	Clarke and Furnell (2007 <sub>a</sub> )
Mobile phone	Yes	Yes	No	Yes	Yes
Biometrics	Keystroke	Face	Voice	Voice Face Signature	Keystroke Face Voice
Authentication levels	No	No	No	No	4
Model	Single biometric	Single biometric	Single biometric	Multimodal biometric	Multimodal biometric
Accuracy rate	EER: 16%	EER: 25%	EER: 2.49%	EER: 0.83 – 2.39%	FRR: 0.001-0.4(%) FAR: 0.000001-0.000 02(%)

Table 2.2: Comparison of related work

The use of biometric authentication on mobile phone can effectively solve password stolen issues. Campisi et al. (2009), Dave et al. (2010), Kinnunen and Li's (2010) research work proved a single biometric authentication mechanism is possible to achieve mobile authentication. Koreman et al. (2006) and Clarke and Furnell's (2007<sub>a</sub>) work have shown that the combination of biometrics of voice, face, signature or keystroke can achieve a level of authorisation accuracy which should be acceptable for the wide range of applications which is normally secured by a PIN or signature.

## Chapter 3

# A model to support the authentication of mobile commerce

The International Bank Card Association raised security issues in the early 70s: how to use individual authentication mechanism to protect systems from attack (Samal and Iyengar, 1992). With the fast development of communication technology in the last four decades, the mobile phone is not just a device to call a colleague. As discussed in Chapter 2, in mobile commerce, there are a significant number of services can be provided on a mobile phone. One can imagine the expansion of these services as phones get more sophisticated. At the same time as services becoming more personal, the authentication method on mobile phones is usually password-based, including PIN, username-password, dynamic password (one-time password), and challenge-response question. Hackers or criminals can use a variety of methods to steal PIN, passwords and security information. Most of the existing mobile commerce systems use single authentication technology which does not solve

the weakness in the password system. Using a number of these authentication technologies at the same time will slow down the speed of implementation and increase the complexity for the user. This chapter proposes a smart authentication model to make system more convenient and less susceptible to break in.

### **3.1 Research aim and task**

Although mobile commerce is widely used and the number of subscribers are increasing, security risk is still exist. How do the users identify themselves within an application on the phone? There are 3 different mechanisms to verify the person who they claim to be from within an application:

- 1 they have something
- 2 they know something
- 3 some aspect to their physical being – biometrics

Most of the current m-commerce systems use only one or two of these three actions, for example, in a NFC based system, it allow a user to employ a “Touch and Go” approach to shopping, which means no security is required other than just having the phone. In other password based systems, the account number and password information are transmitted by wireless which makes the transaction relatively simple, but when a user loses their mobile phone or it is stolen, it is difficult to protect their linked bank account effectively. Therefore,

people will usually be concerned about the security issues, and a new authentication mechanism is required.

In this research, the authentication mechanism defines a number of additional authentication levels; it aims to achieve the balance between usability and security. The authentication levels are determined by the transaction value and each level corresponds to a different authentication method: pin, password and security question. The model proposed here provides a balance between repeated password entry and single password entry whilst adhering to the principle of higher value transactions requiring more security. It will greatly enhance the security of mobile commerce, and eliminate potential safety problems.

### **3.2 Model build up**

The described authentication system in this chapter consists of four parts: client side, the authentication level manager, authentication engine and database. The main components and their functions are shown in Figure 3.1:

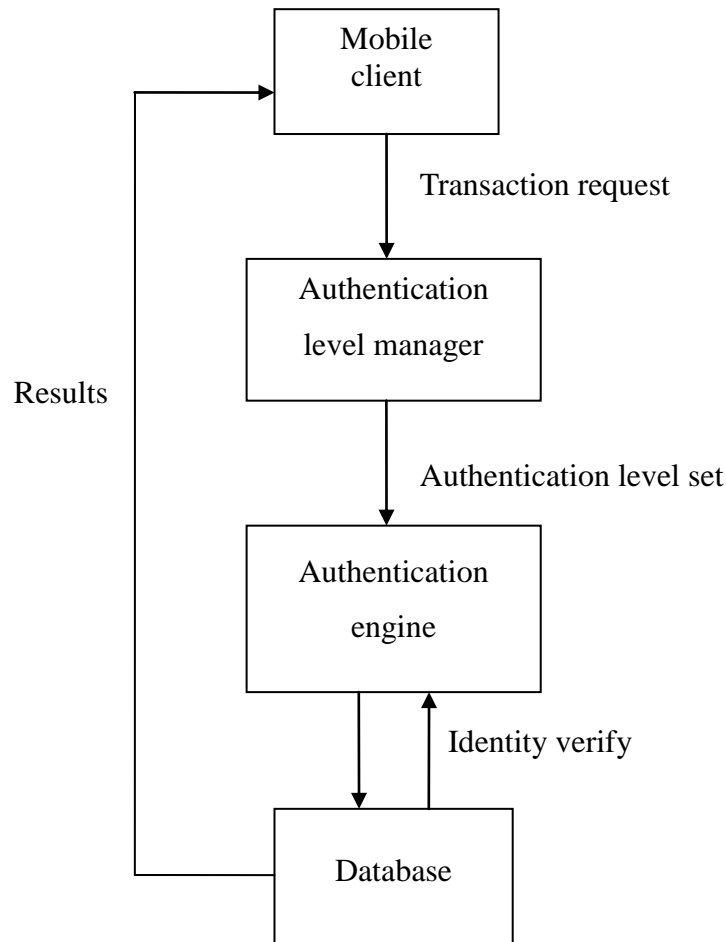


Figure 3.1: Mobile commerce system flow chart

**Mobile client:** The first of these is built into the phone; the user of an application has the phone. The phone is a personal device so by using the phone there is some degree of certainty that the user is the phone owner. People protect their phone as they would their wallet; it is a personal item and not shared. In this system, the mobile device is used to capture user's access request; set up connection with a server; send user information and access requests to the server; and receive server response messages.

**Authentication level manager:** receives user information and access requests which were sent from client side; define the authentication level according to the system transaction level; send this information to the corresponding user authentication server. The authentication level is defined as shown in Table 3.1.



	AL=0	AL=1	AL=2	AL=3	AL=4
Transaction level	Very Low	Low	Medium	High	Very High
Authentication technique	Direct Access	Pin	PIN and Password	Third level of security	Fourth level of security
Duration	Stay as long as the phone is on	Stay t1 minutes then revert to lower level	Stay t2 minutes then revert to lower level	Stay t3 minutes then revert to lower level	Stay only for the duration of the transaction then revert lower level
Security	Weak  Strong				
Usability	Easy  Complex				

Table 3.1: Authentication level set up

(AL=Authentication level, t1, t2 & t3 can be set by the system administrator)

The present model can be used with more or fewer levels of security, the number of authentication levels will affect the usability and security of the

system. Less authentication levels system can provide more usability but less security, conversely, more authentication levels system provides more security but less usability. At present, most of the mobile banking systems (such as Barclays mobile banking and Lloyds TSB mobile banking) are using two authentication levels model, but only two levels is not clear enough to identify the transaction risk. However, too many authentication levels like nine or ten levels are not user friendly. The reason why five levels are built into the model is considering the balance between security and usability. Compare with Clarke and Furnell's work (2007<sub>a</sub>), they also proposed a similar four Alert levels based authentication model (but no level 0), and the model has proven to be a good model in mobile authentication. In this research, an additional level 0 is defined which allowed the user to process some very low risk transactions when they have the phone. Therefore, five authentication levels are defined in this research.

There are two purposes to set a number of authentication levels in the system: the first purpose is to achieve the balance between security and usability. Another purpose is to build a multi-modal authentication system. Obviously phones are stolen but there are well established mechanisms for reporting these and blocking the phone and SIM. So for AL=0 transactions the phone is relatively safe; a user may be prepared to allow some low risk transactions without any further security protection for the ease of use. The standard security mechanisms use items the user knows and is used to identify them. These

include PIN, password or answer to personal questions such as “name of first school” or “Mother’s maiden name”. There are well known insecurities in using these items, as they are prone to eavesdropping, dictionary attacks, and user insecurity (for example user writing them down). But knowledge of one or more of these items achieves better level of security on their mobile system. For high level transactions (for example  $AL=3$  or  $AL=4$ ), biometric authentication techniques can be used instead of password, this will be discussed in the next three chapters.

***A. Balance between security and usability***

Whenever a mobile application requires to access any secure data the user may be required to enter some token to prove it is them. Perhaps the user must input the username, password and PIN. The more tokens required the more secure the application. Think of this as more locks on a safe. However the more tokens requested the less useable the application. Using the safe analogy; if the user puts all their money in a safe, whenever they require 20p for a paper they must undo 3 locks, prior to getting the cash. This is the same as the user being requested for all 3 tokens for a low risk low value transaction. For ease of use many users will just want to get the item and not enter any token as they are prepared to accept the low level of risk as the transaction is of low value. On the other extreme for a high value transaction many users will require the more levels of security and would not want the transaction to go through without any checking.



***B. Authentication level in the system***

It is argued that for any user they can balance their expected security for a transaction against the ease of use. Within the model below we are suggesting a 5 level model: 0 is a normal 'phone switch-on' level, level 1-4 we can use PIN and other three biometric techniques to achieve authentication.

Level 0 – no security required other than just having the phone.

Level 1 – simple security of 1 token (PIN).

Level 2 – medium security requiring 2 tokens (PIN and Password).

Levels 3 & 4 – higher security requiring further security.

In this chapter, we are not arguing that PIN, password and security questions are the best tokens to use, these are used for illustrate the model. Biometric authentication techniques can be used to instead of PIN and password, in the next three chapters we will further discuss about the multi-modal biometric system.

**Authentication engine:** To achieve authentication in this system, two security mechanisms must be imperative: authentication level and duration. Based on these mechanisms, the system workflows chart is shown in Figure 3.2:

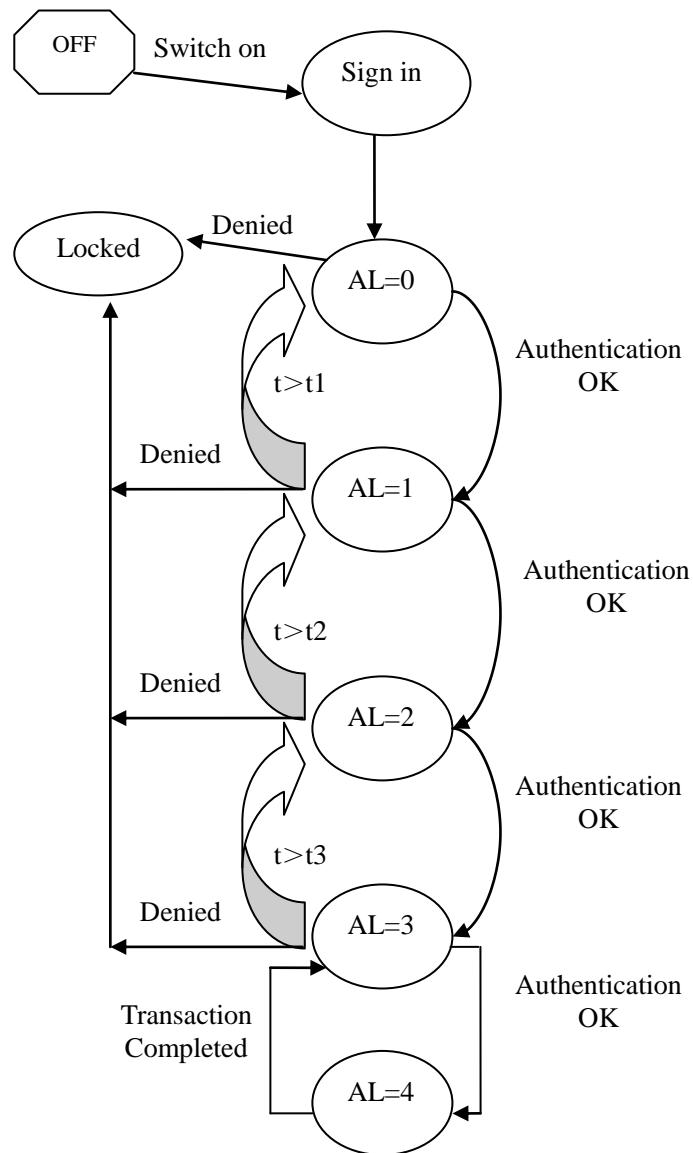


Figure 3.2: The multi-modal authentication process

(1) When the mobile phone is switched on it is set to AL=0 (Authentication level). When the client requests a very low transaction this will automatically be authenticated. If the transaction is at a higher level, then the phone needs to be at a higher AL. To achieve this user is required to enter their PIN. When they

have attempted to do this and they succeeded then AL is set to 1; otherwise the phone is locked.

(2) If the phone is currently at  $AL=1$  then transactions of low or very low are carried out without any further authentication. If the transaction is a medium or higher rated transaction then the client must authenticate the phone. The user is asked for their password and they have 3 attempts at entering the password. If it is successful the AL is set to 2; otherwise the AL is reset to 0. If the phone is on  $AL=1$  for longer than  $t_1$  minutes it reverts to  $AL=0$ .

(3) If the phone is set to  $AL=2$  then transactions of medium, low or very low are carried out without any further authentication. If the transaction is rated as high or very high then the client must authenticate the phone. The user is asked a third level of security and they also have 3 attempts for successful operation. If it is successful the AL is set to 3; otherwise the AL is reset to 1. If the phone is on  $AL=2$  for longer than  $t_2$  minutes it reverts to  $AL=1$ .

(4) If the phone is currently at  $AL=3$  then transactions of high, medium, low or very low are carried out without any further authentication. If the transaction is a higher or very high rated transaction then the client must authenticate the phone. The user is asked fourth level of security and they also have 3 attempts for successful operation. If it is successful the AL is set to 4; this allows the transaction to be executed only and the AL is reset to 3 immediately after the

transaction; otherwise the AL is reset to 3. If the phone is on AL=3 for longer than t3 minutes it reverts to AL=2.

**Database:** The system database used to store user account information and biometric data. It manages user's registration and access information. The typical management task including: add and delete user account, add or delete access control list, set up resources access control list.

### **3.3 Experimental work**

The experimental work aims to test the performance of the discussed multi-level authentication model and compare it with a basic mobile commerce model which has no authentication levels. In this stage, the researcher has designed two simulated mobile shopping cart models and used Nokia 6131 NFC phone to test them. The server application was written in ColdFusion with access to a database. An application written in J2ME was used on the phone to emulate the shopping. Before the experiment, item information will post to the associated tag. When the client wishes to purchase an item they touch the tag with the NFC phone. The information from the tag is then downloaded to the server application which will initiate a dialogue with the client to complete the authentication process.

Two models were designed in the experiments. Model 1 is a basic mobile commerce model with no authentication levels and PIN is the only authentication

method. Participants can purchase any item after they enter a correct PIN. Model 2 use the mechanism presented in this chapter. In experiment 1, 12 participants were asked to register on the phone. Following this, they were required to purchase some items by use both model 1 and model 2. In order to calculate the false acceptance rate of the system, in experiment 2, other 12 non-registered users were asked to login into the system. The system interface is shown in Figure 3.3, and the experimental results are shown in Table 3.2.



Figure 3.3: NFC interface

	Authentication levels	Authentication techniques	Experiment 1	Experiment 2
Model 1	No	PIN	FR = 0	FA = 2
Model 2	5 levels	PIN, password and security questions	FR = 0	FA = 2 (AL=1) FA = 0 (AL=2,3,4)

Table 3.2: Experimental results

During the testing phase both true and false data was entered into the system to check the adherence to the model. This worked as designed. In experiment 1, two shopping models were tested by 12 participants. They did not report any errors with two of the systems with no false rejections being recorded. In experiment 2, two non-registered participants access the model 1 and AL=1 in model 2, but no participants can access to AL=2, 3, 4 in model 2. This result indicated that the authentication model developed in this chapter can reduce the risk of unauthorised users gaining access to the system.

### **3.4 Discussion**

The presented mechanism defined five authentication levels which can effectively protect the system. At the top authentication level, it is difficult to perform the attack on the system. Obviously, the proposed system not only provides a number of password-based authentication techniques but also set up authentication levels. Moreover, the password-based authentication techniques can be replaced by biometrics. On the client side, NFC based mobile device is used, as a prototype, the mobile shopping application using NFC technique to capture transaction information and achieve authentication level defined. The experimental results show that the multi level authentication model provides a fast authentication for low level transactions, and the use of multiple authentication techniques enables the system to achieve a low false acceptance rate at high authentication levels. Overall, it can conclude that the presented system is more effective and more secure for mobile authentication.

The proposed model has been shown to achieve network applications and controllable resources access. It simplifies the authentication process and also makes the Internet services more secure and convenient. Through adding a number of authentication levels to the authentication process, it is no longer a matter of providing a pass or fail response providing a one-time authentication. It provides the correct level of authentication to achieve the intended transaction and no more. With mobile device functionality increasing, the ability to perform suitable user authentication becomes ever more important. Existing password-based techniques are under-utilised, and in any case provide an inadequate level of protection when compared to the sensitivity of data and services accessible through the devices. In the next chapters, a number of biometric authentication techniques involve typing behaviour recognition, face recognition and speaker recognition will be used instead of a password. When biometric authentication techniques combines with the model proposed in this chapter, it can provide valuable enhancements to mobile commerce.

## Chapter 4

# Typing behaviour recognition on mobile device

### 4.1 Introduction

This chapter discusses a biometric authentication system which is password-based and uses behavioural traits (typing behaviours) authentication technology to establish a user's identity on a mobile phone. Compared with the traditional PIN and password, typing behaviour will never be lost or forgotten, hard to forge and easy to use. In the proposed system, a mobile application was developed to capture user's keystroke data when they typed the password. The authentication engine will compare the input keystroke data with the user's registration pattern; and then establish whether the claimer's identity is genuine or fraudulent. The mobile client does not keep any data and the whole process is reliable and secure.

The main task of this chapter is to develop a mobile application to investigate



whether it is possible to use metrics based on typing behaviour to establish the identity of the user on a mobile phone. Therefore, the objectives are:

- Develop an application which can run on mobile phone platform.
- Perform a number of experiments to investigate the effectiveness of the authentication system.
- Investigate the accuracy rate and the usability of the developed system.

## **4.2 Keystroke as a biometric**

The identification of individuals based upon user name and password has existed for hundreds of years in the history (Clarke and Furnell, 2007<sub>b</sub>). Researchers have presented a variety of favourable results and most of researches have shown their systems are feasible to authenticate users based upon username and password. However, biometric authentication models have not been widely used on mobile phones. The typing behavioural recognition system developed in this chapter can analysis user's keystroke data at the same time when they input the user name and password. By using this authentication mechanism, it is hypothesised that it will greatly reduce the probability of password theft.

### **4.2.1 Keystroke analysis**

The operating principle of a typing behaviour recognition system is that when a user input their username or password through their computer or mobile phone

keyboard, the system is not only able to identify the password to log on, but also analyse the keystroke data (usually how long they hold the key and the intervals between they press each key). Generally in a typing behaviour recognition system, there are two keystroke characteristics can be utilised to solve the interactions between individuals and computer or mobile phone keyboards.

#### **4.2.2 Two metrics**

- ***The keystroke latency (Interval)***, or time between successive keystrokes is a measure of the amount of time between when a key is released and the subsequent key is pressed.
- ***The key hold-time (Duration)***, or the time to press and release a key. It is a measure of the amount of time between when a key is pressed and when the same key is released.

Many of the related studies (Obaidat and Sadoun, 1997; Haidar et al., 2000; Araujo et al., 2005) beginning with Obaidat and Sadoun in 1997, used these two keystroke characteristics in the keystroke recognition systems with good results (Crawford, 2010). Both metrics are common in studies that examine keystroke dynamics on desktop and laptop keyboards. Particularly in this research, these two metrics can be captured from a full-size (QWERTY) mobile phone keyboard.

In keystroke analysis, the keystroke data is recorded when the user types in the password. So for example if the password is “abertay2011”, there are 10 “*keystroke latency*” and 11 “*Key hold-time*” recorded. During the training phase, the user must enter their username and password a number of times in order to register. Capturing a higher number of keystrokes during the registration process, will ensure more accurate results, however the repetition of entering a username and password is not user friendly. Therefore a decision was made, defining six times as a standard is based on other researcher’s work. This matches Szymkowiak et al.’s (2009) research, six times was the selected standard during the registration stage. When the system captures a user’s registration data, it records the duration and interval and calculates the average time. Subsequently, the data will be converted to xml format, sent to a web server and stored in a database. In order to study the feasibility of typing behaviour recognition, a simple account (username: abertaytest; password: abertay2011) was stored. A number of participants were asked to try to login using the same username/password. For illustrative purposes, three random participants were chosen, and their “*Key hold-time*” plotted together with that of the original, the difference between them is shown in Figure 4.1.

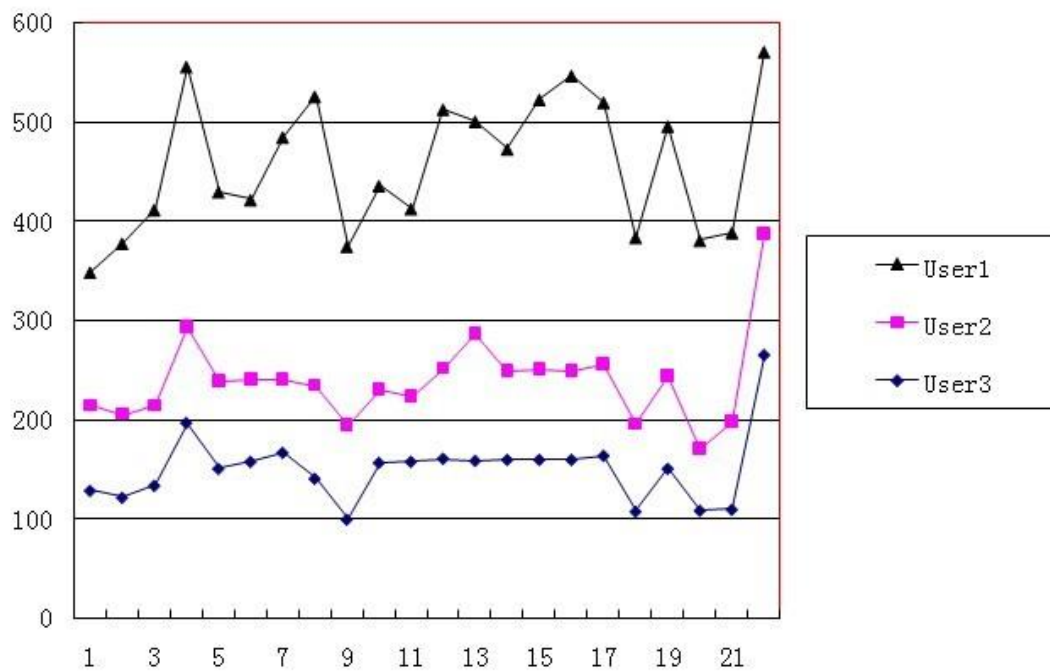


Figure 4.1: The comparison result between each participant

Figure 4.1 shows the “key-hold times” of participants keystroke data, each participant has their own input timing pattern and they are different from each other. Compared with User 1’s keystroke pattern, it can be found that other user’s patterns are different in the database. There is a fairly consistent upward and downward pattern to the lines of each participant. Obviously, some participants tended to press certain keys for much longer than others, and also require much longer transition time to press the next key.

### 4.2.3 Recognition algorithms

In this system, each user has to type in the same username and password six times to register; and the mean of these captured keystroke data will be stored

in database as the user's pattern. This pattern contains two keystroke metrics: Pattern Duration (also consider as *the key hold-time*) and Pattern Interval (also known as *the keystroke latency*). In order to improve the data process efficiency, the client side will firstly calculate the mean times; and then upload it to the web server.

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

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

When a user's typing pattern is compared to the target, there are two kinds of authentication results: Accept or Reject.

*A. To accept a user:*

$$\frac{\text{Pattern Average Duration}}{\alpha} \leq \text{Attempt Duration} \leq \text{Pattern Average Duration} \times \alpha$$

And

$$\frac{\text{Pattern Average Interval}}{\alpha} \leq \text{Attempt Interval} \leq \text{Pattern Average Interval} \times \alpha$$

If the attempt duration time is less than the pattern average duration time, the user is recognised as the owner of the claimed identity.

*B. To reject a user:*

$$\begin{aligned} \text{Attempt Duration} &> \text{Pattern Average Duration} \times \alpha \quad \text{or} \\ \text{Attempt Interval} &> \text{Pattern Average Interval} \times \alpha \end{aligned}$$

And

$$\begin{aligned} \text{Attempt Duration} &< \frac{\text{Pattern Average Duration}}{\alpha} \quad \text{or} \\ \text{Attempt Interval} &< \frac{\text{Pattern Average Interval}}{\alpha} \end{aligned}$$

In the algorithm above, a new parameter ‘ $\alpha$ ’ is introduced. The value of ‘ $\alpha$ ’ determines how near to the registered pattern the attempt is needed to be to accept the individual. The proposed algorithm is possible to calculate an accurate ‘ $\alpha$ ’ value by compare the attempt keystroke data with the pattern keystroke data. As shown in Figure 4.1, user’s keystroke data is a skewed distribution rather than a normal distribution. In this research, we define an interval of acceptance  $[p / \alpha, p \times \alpha]$  (‘ $p$ ’ indicated Pattern Keystroke data) where  $\alpha$  can be chosen to represent a known FRR level. Moreover, In Curtin and other’s work (Curtin et al., 2006), they also suggest to use ‘ $x$ ’ and ‘ $s$ ’ for calculation with a good result. The more usual interval  $[p - \alpha \times s, p + \alpha \times s]$  (‘ $s$ ’ indicated a standard deviation) requires a normal distribution and as the distribution is skewed, the lower bound in the interval will typically be negative – a meaningless value. But the use of ‘ $x$ ’ and ‘ $s$ ’ in this algorithm can avoid appearing negative value in the interval. Therefore, the proposed algorithm use

'x' and '/' to measure the deviation.

In this research, a change of the ' $\alpha$ ' value will determines the FRR (False rejection rate) and FAR (False acceptance rate) of the system. For example, the higher ' $\alpha$ ' value means the system is less likely to reject the right user or accept the wrong user; on the other extreme, a lower ' $\alpha$ ' value can make the system more secure. By using the model proposed in this chapter, the ' $\alpha$ ' value can be easily changed to achieve the balance between usability and security. Compared with neural network algorithms (Clarke and Furnell, 2007<sub>b</sub>) and Minimum and Maximum method (Szymkowiak et al., 2009), the proposed algorithm is faster, simpler, more flexible and convenient to adjust the standard deviation.

## **4.3 Methodology**

### **4.3.1 System overview**

The main purpose of this section is test the performance of the typing behaviour recognition system on mobile phones, therefore, an application was built on a mobile phone to record and analyse user's keystroke data. The system model includes two parts, registration and authentication. The purpose of registration is to record user's keystroke data for comparison. To achieve this, users have to enter their user name and password for a number of times, then the data will be collected and an algorithm will calculate the average keystroke time. When user

tries to log in, a keystroke array will send to the web server, and then the authentication engine will compare the attempts with the user pattern and identify the individual user. System flow chart is shown in Figure 4.2.

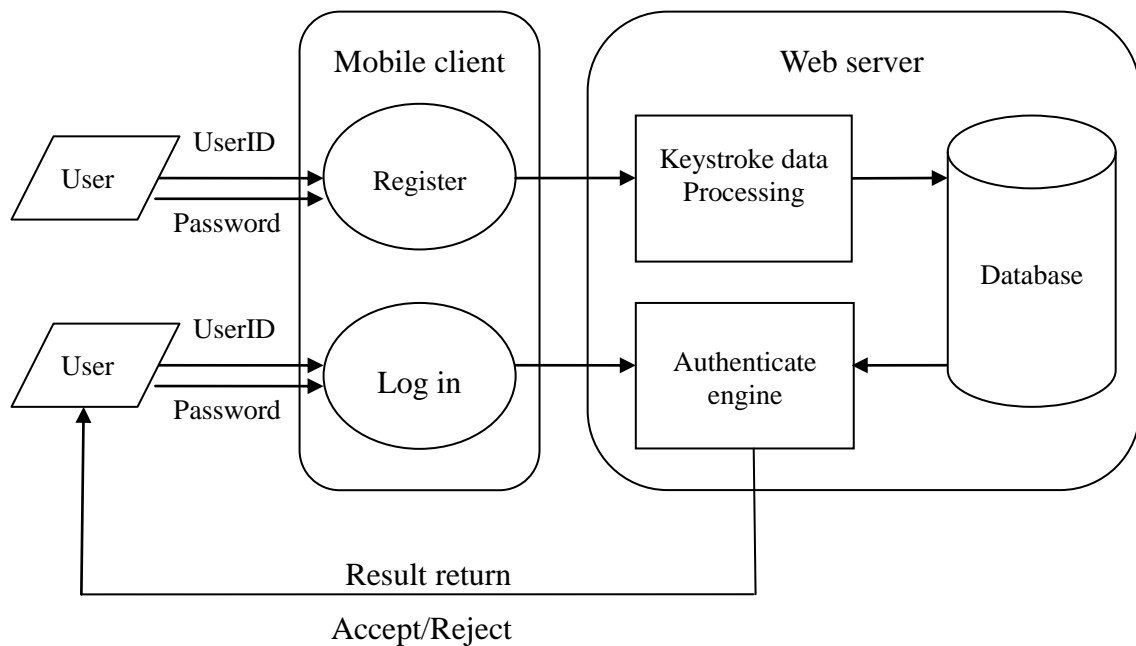


Figure 4.2: The flow chart of typing behaviour recognition system

The main task of the mobile client is to capture keystroke data from the user and calculate the average time. The collected data will be converted to an XML file and stored in the database. The authentication engine processes the keystroke data within the web server, and compares the input data with the user pattern and establishes if a user is genuine or fraudulent. In order to test the performance of authentication engine, a set of experiments were planned. The application will run on a mobile phone with a full keyboard, with the aim to find out the accuracy rate of the system.



### 4.3.2 Client side design

The client side was designed to capture the keystroke data from user, analyse them and then transmit it to the web server. The first step is registration, it require each user to enter username and password six times to complete. After the keystroke data is uploaded, the system will analyse it. Figure 4.3 shows the duration time and latency time in a user's keystroke data. For example, if a user uses "abertaytest" as a username and "abertay2011" as a password, when they type in these six times, there are 132 duration times and 120 latency times need to be recorded. In order to increase speed of data processing and reduce data transfer, the client side will analyse the data and calculate the average time before store it as a user pattern.

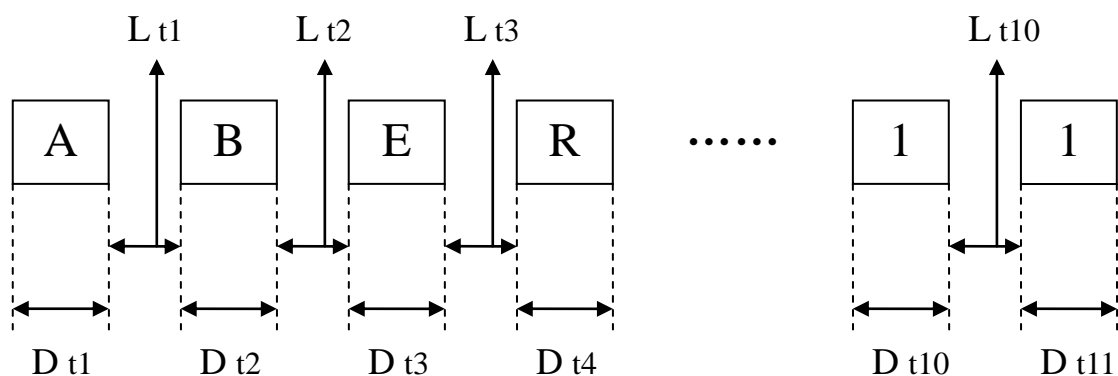


Figure 4.3: The duration time and latency time in keystroke data

According to the principle above, the keystroke duration time and latency time cab be calculated by using the follows algorithm:

The duration time  $t^1 = \text{keyUpTime}^{t^1} - \text{keyDownTime}^{t^1}$

Latency time  $t^1 = \text{keyDown}^{t^2} - \text{keyUp}^{t^1}$

The code in Appendix V (1) describes how the system captures user's keystroke data. After data collection, the client side will calculate the mean time of keystroke data. If the password is "abertay2011", there are 10 "*keystroke latency*" and 11 "*Key hold-time*" to be stored in the database.

### 4.3.3 Web server

In this project, there are two main tasks of the web server: analyse the keystroke data gained from the client side, and then inspect, and return an authentication result to the user. The next sections will explain each function of the web server and how it works.

#### 4.3.3.1 Registration

Registration is the first function of web server: When user types the username and password six times, the client side will process the gained keystroke data and connect the web server to add new user to the database. An xml file that contains the user name and the password plus the keystroke data will be transmitted to the web server via an upload request. This provides the reference point or signature for that user. The code in Appendix V (2) can achieve this function.

After database was created, two tables existed in the database: username password, and keystroke data which includes “*keystroke latency*” and “*Key hold-time*”. When registration is successful, the user can access to the next stage – validation.

#### **4.3.3.2 Validate**

There are two methods contained within the authentication engine: input validity check and verify user.

**Input validity check:** When the web server received a login request, the first step is to check the validity of input data, because it can only contains characters and numbers, when any illegal input is found, a warning message will be posted to the user. If all input characters are valid, the following verify work will carry on.

**Verify user:** There are three steps in this authentication stage:

- (1) Check whether the username exists in the database, if not, login failed; if exist, go to step 2.
- (2) Compare the password against the user ID in the database table, if the password match, go to step 3; otherwise, a denied message will send to the user;
- (3) The keystroke verification method will carry on comparing the attempts duration and latencies with the pattern in the database. The algorithm is

described in section 4.2.3. If the details match, the user has logged in successfully. The verify code is in the Appendix V (3).

#### **4.3.4 Database**

The keystroke data collected from user are stored in the database (an xml file), residing on the researcher's web server. There are two tables in the database: username password information and keystroke data information. The main purposes of database are to store user pattern and provide pattern for the web server to process the login attempts request. This section provides an overview of the database.

##### **4.3.4.1 Users information**

The user information table contains all users' username and password which was setup by the user when they registered. Any username or password shorter than 3 characters or longer than 17 characters cannot be inserting into the database table; any already existing usernames cannot be used either.

##### **4.3.4.2 Keystroke data**

The second table is the input table which contains all of the successful registered keystroke attempts; each user ID has two types of keystroke data: latency between key presses and how long they hold each key down. This data was collected and calculated on the client side and posted to the web server. It generates a keystroke signature which is stored as the pattern for each user.

This helps the authentication engine to verify the users' identity and also stores the experimental results. Figure 4.4 shows a user use 'abertaytest' as their ID and the details of his keystroke data.

```
- <Data>
  <UserName>abertay@huang.com</UserName>
  <Password>abertaytest</Password>
  - <Input>
    - <Duration>
      <Time>20</Time>
      <Time>20</Time>
      <Time>18</Time>
      <Time>15</Time>
      <Time>12</Time>
      <Time>13</Time>
      <Time>27</Time>
      <Time>31</Time>
      <Time>30</Time>
      <Time>22</Time>
      <Time>43</Time>
    </Duration>
    - <Interval>
      <Time>635</Time>
      <Time>675</Time>
      <Time>285</Time>
      <Time>311</Time>
      <Time>600</Time>
      <Time>467</Time>
      <Time>642</Time>
      <Time>480</Time>
      <Time>378</Time>
      <Time>407</Time>
    </Interval>
  </Input>
</Data>
```

Figure 4.4: Two tables in system database

This section has presented a typing behaviour recognition system, and has also discussed the system structure in details. In theory, it has the ability to identify

user's identity though analysis the keystroke data. The experimental works in next section will run this application on mobile phones.

## **4.4. Experimental work**

### **4.4.1 Experimental environment**

#### **4.4.1.1 Hardware**

The purpose of the experimental work is to capture biometric data from participants and test the performance of the system on different models of mobile phones. On the client side, the application can run on four different models of phones: Windows mobile phone, Android phone, iphone and blackberry phones. In addition the experimental data is gained from the O2 Xda Minis and HTC Sensation, as shown in Figure 4.5:



Figure 4.5: Experimental tools

The reasons why these phones were chosen are because each of them has a full size keyboard or simulate full size keyboard to capture keystroke data; and in addition, in consideration of the data transmission requirements, all the phones have the Wifi or GPRS function to connect to the internet.

#### **4.4.1.2 Software**

Two different client applications were designed in the system. The web server and windows mobile phone client interface were developed using the Microsoft Visual studio 2008 and was written in C#; the Flex application was designed for Iphone, Android phone and Blackberry phone. The application was developed by using Flash Builder 4.5 and written in ActionScript language. Both of the applications can run on Windows XP and Windows 7 machines. The system database is a XML file which was created on the client side when the user registered.

#### **4.4.2 Experiment arrangement**

##### **4.4.2.1 Aims of the work**

In order to test the system, the main task of client application is to capture keystroke data from volunteers. In this phase, the researcher has found 40 volunteers and recorded a number of their biometric items. Aims to test the system performance based on different mobile phones, 20 participants' keystroke data were collected from the windows mobile phone and the rest 20 participants' data were collected from Android phone. The experimental interfaces are shown in Figure 4.6 and 4.7.



Figure 4.6: The system interface on windows phone

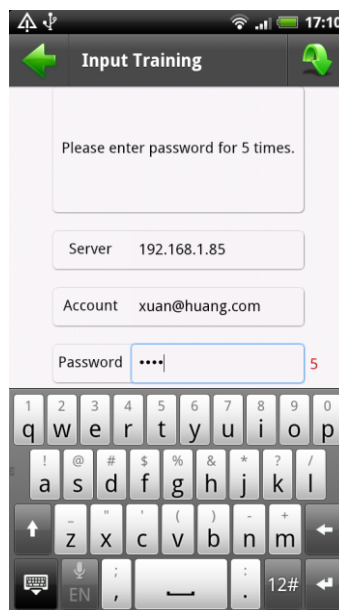


Figure 4.7: The system interface on Android phone

Another task of the experimental work is to test the accuracy rate of the system. In addition, a set of experiments are arranged to find out the relationship between the ' $\alpha$ ' value and the FAR and FRR of the system.



**4.4.2.2 Participants**

The participants are other students or staff in the University of Abertay and they were told the purpose of the work. The total of 40 participants aged from 22 to 61 years old and their mobile phone use experience is from 3 years to 10 years with the average of 6.2 years. In order to ensure the experiments accuracy, the participants were required to complete the experiment in a quiet environment.

**4.4.2.3 Methods**

The experiments include two parts of work, registration and validation. In the registration stage, participants were asked to register from the mobile phone; and the validate stage will find out the FAR and FRR in the system. Overall, there are three steps of work in the experiment:

(1) when user uses the system for the first time, they are required to enter a user name and a password six times to register. A message will display on the screen to tell user the registration was successful or not. The screen shot is shown in Figure 4.8.



Figure 4.8: User registration page

(2) The second step is the validate process. The researcher will ask participants try to login using their own user name and password. If the login attempts fail, it means false rejection happens; the result will be recorded to calculate the false rejection rate. Figure 4.9 shows this.



Figure 4.9: False rejection happens in the experiments

(3) In the last step, the researcher registered an account called “abertaytest”, and use “abertay2012” as the password. The account name and password are told to each participant and then the researcher asks them use this account to login again. If any participant login successfully, this means that a false acceptance happens, the result will be recorded to calculate the false acceptance rate. The screen shot is shown in Figure 4.10.



Figure 4.10: False acceptance happens

In order to find out the impact of different ‘ $\alpha$ ’ value on the FRR and FAR of the system, the validation experiment was divided into three groups. The ‘ $\alpha$ ’ value has been defined as 2 in group 1 and the value changed to 3 and 4 in the next two groups. After analysis of the validation experimental result, the difference between FAR and FRR when the ‘ $\alpha$ ’ value changed can be determined. The experimental flow chart is shown in Figure 4.11:

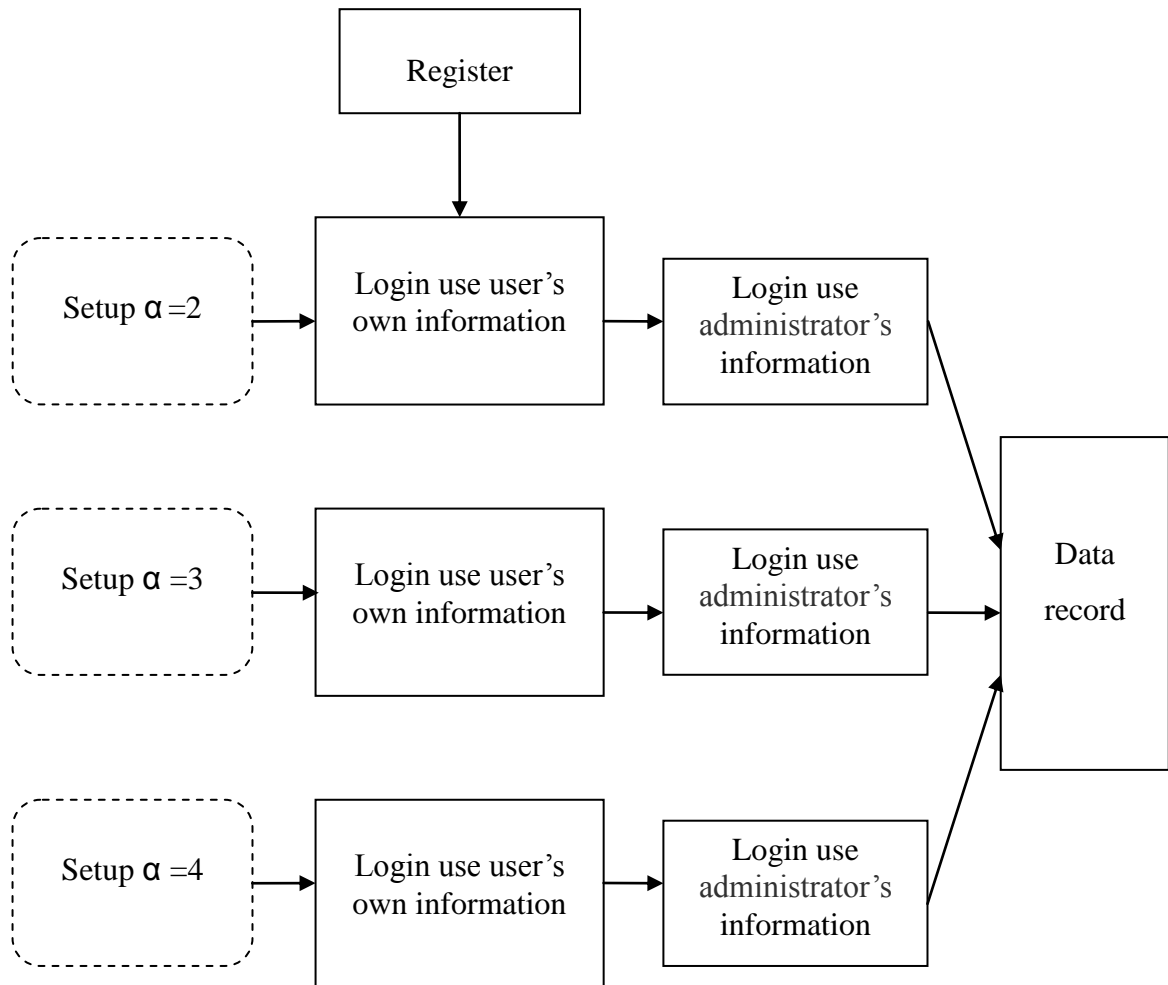


Figure 4.11: The flow chart of validation experiment

In these experiments, if a user failed to login when they use their own username and password, a “False rejection” happens; when a user successfully logs in using the administrator’s username and password, then a “False acceptance” happens. This data will be recorded in the experimental result and the next section will discuss these results.

### 4.4.3 Results

#### 4.4.3.1 FAR and FRR in different groups

The experimental result can help the researcher to find out the false rejection rate and false acceptance rate of the system. During the experiments, the research use O2 XDA minis and HTC Sensation phones as the experimental tools. All 40 participants register and login successfully, which means the system on mobile phones has run well. In group one; the 'α' value has been set to 2, which means when user try to login use their own account number, if

$$\frac{\text{Pattern Average Duration}}{2} \leq \text{Attempt Duration} \leq \text{Pattern Average Duration} \times 2$$

$$\frac{\text{Pattern Average Interval}}{2} \leq \text{Attempt Interval} \leq \text{Pattern Average Interval} \times 2$$

Then the identification result is accepted. On the reverse, when

$$\text{Attempt Duration} > \text{Pattern Average Duration} \times 2 \quad \text{or}$$

$$\text{Attempt latencies} > \text{Pattern Average Interval} \times 2$$

The identification result will be denied; or when

$$\text{Attempt Duration} < \frac{\text{Pattern Average Duration}}{2} \quad \text{or}$$

$$\text{Attempt latencies} < \frac{\text{Pattern Average Interval}}{2}$$

the result will also be denied.

According to this algorithm, in the first step, the researcher asks each participant to login using their username and password. If user's attempt duration and interval time is two times greater than the pattern average time or less than half of the pattern average time, the access request will be denied, a false rejection happens. Subsequently, the researcher asks participants to login using administrator's username and password. If a login is successful, this proves that false acceptance can occur. The experiment 1's result shows that 12 participants tried more than twice to login using their own account information.

This means false rejection happened 12 times and the  $FRR = \frac{12}{40} = 30\%$ . A login did not fail more than four times, the result being acceptable and no users were affected. During the first group's experiment, no participants were able to login using the administrator's account information. This means that false acceptance did not occur and the system did not permit unauthorised user access.

In experiment 2, the ' $\alpha$ ' value changes to 3. If user's attempt duration and interval time is three times greater than the pattern average time, the access request will be denied; false rejection happened 7 times during this experiment and false acceptance happened once. Therefore, the  $FRR = \frac{7}{40} = 17.5\%$  and the  $FAR = \frac{1}{40} = 2.5\%$ .

Similarly in experiment 3, the 'α' value was changed to 4. False rejection only happened twice but false acceptance happened three times. The  $FRR = \frac{2}{40} = 5\%$  and the  $FAR = \frac{3}{40} = 7.5\%$ .

These three groups of experiment results showed that different 'α' value will affect the FRR and FAR in the system, the summarised results in Table 4.1 show the difference between them.

	'α' value	False rejection (FRR)	False acceptance (FAR)
Experiment 1	2	12 times (30%)	None (0)
Experiment 2	3	7 times (17.5%)	Once (2.5%)
Experiment 3	4	2 times (5%)	3 times (7.5%)

Table 4.1: The experimental results

The results in Table 4.1 shows that when the 'α' value was set to 2 in experiment 1, the false acceptance not happened but the FRR is 30% which means the system is more likely to reject an authorised user. When the 'α' value changes to 3 and 4 in the next two experiments, the FRR reduced to 17.5% and 5% but the FAR increased to 2.5% and 7.5% which means the system is easier for the unauthorised user to access. In order to achieve the balance between

security and usability, a better solution is required to define the ' $\alpha$ ' value.

#### 4.4.3.2 Result Summary

From the results in Table 4.1, the Figure 4.12 can be used to display the relationship between the ' $\alpha$ ' value and the FAR and FRR of the system.

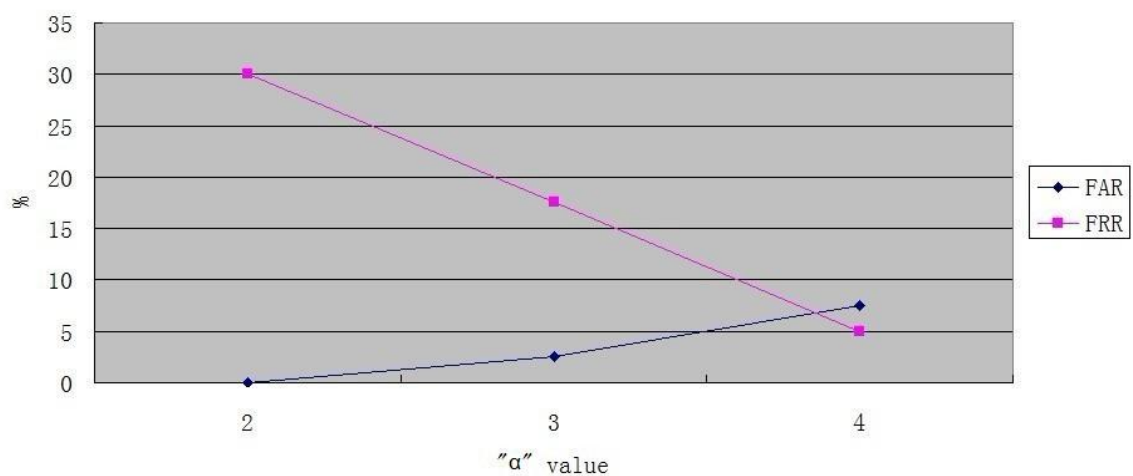


Figure 4.12: The FAR and FRR in typing recognition experiment

In the first group, the false acceptance did not happened — the lowest FAR in the set of experiments, but it also scored highest FRR of 30%. It can be seen that higher FRR restricts its practicability. When the ' $\alpha$ ' value changed to 3, the FRR reduced to 17.5%; in experiment 3, the FAR and FRR were extremely close to each other. From this diagram we can see the changes in direction have been plotted and these two lines crossed when ' $\alpha$ ' value come to 3.8, at that point FAR equal to FRR. EER (equal error rate) is a statistic which can be used when quantifying the success of a biometric system. The EER is where the FAR and the FRR are equal to each other, which is the best single description of



the Error Rate of an algorithm and the lower the EER, the more successful and secure the biometric system is (Griaule Biometrics, 2008). In this research, the EER is 7.5% when the ' $\alpha$ ' value is set to 3.8. To conclude, the experiment results showed that the typing behaviour recognition system is possible to capture user's keystroke data and identify the claimer's identity with accuracy rate of EER is 7.5%.

#### **4.4.3.3 Usability discussion**

Based on Karatzouni and Clarke's (2007) work, they have indicated that the length of the password will affect the system accuracy rate. In this experiment, in order to find out the FRR and FAR of system when user use different passwords, the researcher asked two users to register a 4 characters length password in experiment 1; 8 characters length password in experiment 2 and 16 characters length password in experiment 3. When the ' $\alpha$ ' value is set to 3.8, both users were asked to login 50 times in each experiment: 25 times using their own password (for calculate FRR) and 25 times using other user's password (for calculate FAR), gaining 300 (2 users  $\times$  3 experiments  $\times$  50 logins = 300 results) results in total. In each experiment, two users logged in 50 times to test the FRR and other 50 times to test the FAR. In experiment 1, false rejection happened 2 times, the FRR is 4%. False rejection happened 4 times in experiment 2, the FRR is 8%. When using a 16 character length password in experiment 3, false rejection happened 10 times, the FRR is 20%. On the other side, the FAR is also changed with different length of password. By using the 4

character password, false acceptance happened 43 times, the FAR is 86%; when using the 8 character length password, false acceptance happened 7 times, the FAR is 14%; when using the 16 character length password, false acceptance only happened 1 time, the FAR is 2%.

Password length	4	8	16
FRR	4%	8%	20%
FAR	86%	14%	2%

Table 4.2: The different FRR and FAR when password length changed

The Table 4.2 illustrates that: generally, short password can achieve a low FRR, but the FAR is out of our expected scope. With the password length increased, FAR reduced and FRR increased. In order to achieve a balance between low false rejection rate and low false acceptance rate, user's password length is suggested to set in a range between 4 and 16 when the typing behaviour recognition system used in mobile commerce.

## **4.5 Conclusions**

The presented mechanism builds a mobile identity recognition model and combines biometrics authentication in the system which can effectively prevent the potential attacks from criminals. The typing behaviour recognition enhances

username and password based authentication with keystroke analysis that periodically asks the user to re-verify their identity. In this research, a new parameter ' $\alpha$ ' is introduced; the experimental result shows that when the ' $\alpha$ ' value equal to 3.8, the system can achieve a low EER (7.5%). The comparisons of the system proposed in this chapter and other related research is shown in Table 4.3.

Techniques	Authentication systems				
	Zahid et al. (2009)	Campisi et al.(2009)	Karatzouni and Clarke (2009)	Clarke et al. (2007 <sub>b</sub> )	This work
Mobile device	Yes	Yes	No	Yes	Yes
Keyboard style	Not specified	Numeric	Thumb	Numeric	Full size
Experimental dataset size	25	25	50	32	40
Error rates (FRR/FAR or ERR)	FRR:2% FAR:5.6%	EER: 14.46%	EER: 12.2%	EER: 12.8%	EER: 7.5%

Table 4.3: Comparison of related works

Compared with other research works in Table 4.3, the proposed model in this chapter can work on most Smartphone platform and achieve a lowest equal error rate – 7.5%. On the other hand, the proposed algorithm is easy to implement, and the ' $\alpha$ ' value can be simply changed which makes the model become more flexible. From the above descriptions, it can be concluded that the proposed system is possible to establish the identity of the user on mobile phone, and it is

more effective, secure and convenient than other password-based authentication system on mobile phones.

Typing behaviour recognition is the first biometric technique proposed in this thesis because it can be easily achieved when mobile phone users type their password. The next chapters will focus on building a multi-modal biometric authentication system which uses face and speaker recognition techniques to combine with the typing behaviour recognition.

## Chapter 5

# Face recognition on mobile phones

With the development of mobile phones in recent years, most mobile phones have a high quality camera, and the mobile phone user can shoot and upload a face image at anytime and anyplace. This makes mobile face recognition become a reality. In this chapter, a face detection and recognition system based on mobile phones has been discussed. Within this model, a Flex application is designed by the researcher to capture and upload user's face image from a mobile phones. The web server provided by face.com will process the received face image, extract facial features, and then an authentication engine will finish the recognition work and return an authentication result. The authentication engine used in the system can achieve high recognition rate and fast processing speed. At the end of this chapter, experimental results indicate that the developed face recognition system can accurately establish the user's identity on a mobile phone.

## 5.1 Face recognition engine

The face.com's developers present a free face recognition API. They have proposed a "faces in the crowd" method which allows the system to accurately localise facial key points such as the eyes, nose or mouth. The method has the ability to detect multi-faces in one picture; the interface is shown in Figure 5.1:



Figure 5.1: The face recognition algorithm used in Face.com

There are lots of other studies in this research domain, but most of these studies are based on a PC rather than mobile phone. The API provided by face.com has

fast processing speed, minimal hardware requirements and in addition, it can also support real-time, multi-person face tracking which is helpful for mobile phone users when they use the system in a public place. It is suitable for the mobile face recognition system and can be used as the authentication engine in this research.

## **5.2 Research objectives and tasks**

The main purpose of this chapter is to design and develop a face recognition system based on mobile phone to establish the identity of the user. To achieve this aim, a number of objectives should be included:

- Develop a mobile application using an API which can run on mobile phone platform.
- Perform a number of experiments to investigate the effectiveness of the system.
- Test the system in different environments and prepare a comparison of the gained result.
- Collect experimental results and evaluate the system.

There are four tasks need to be described in this chapter:

- Develop a Flex application to process face image and receive recognition result from face.com.

- Calculate the False Rejection Rate (FRR) and False Acceptance Rate (FAR) of the face recognition system.
- Arrange three experiments in different environments and compare the experimental results.
- Evaluate the performance and usability of the developed system.

## **5.3 Methodology**

### **5.3.1 System overview**

The face recognition system framework can be divided into two parts: mobile client and web server. On the client side, the researcher has designed two mobile interfaces: registration and login; it allows user to register and identify themselves through the mobile phone. The API used in this system is provided by face.com, with the following functional modules included: face detector, feature extractor and authentication engine. The system works as shown in Figure 5.2.



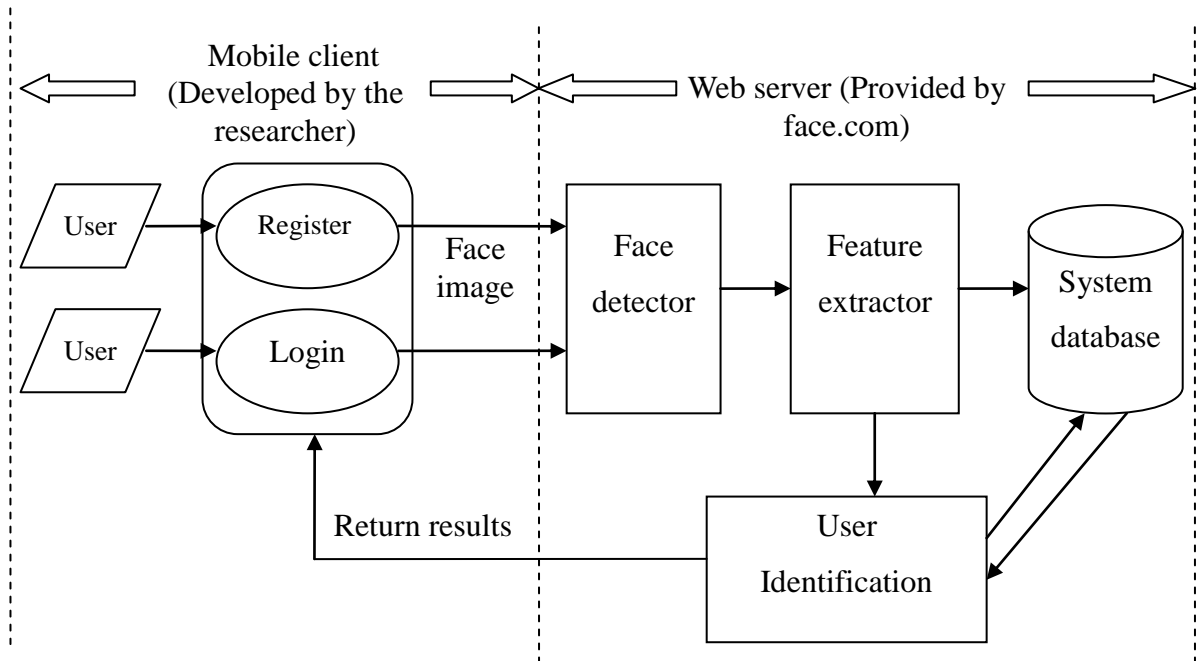


Figure 5.2: The face recognition system

**Mobile interfaces:** in this chapter, the mobile client is developed by the researcher; it is responsible for data collection and transmission. When the user registers or attempts to login, the application will automatically starts the mobile phone camera and ask users whether they'd like to take a photo. After that, the face image will be uploaded to face.com for further processing.

**Face detector:** this is the first step of processing work; when a user takes a picture in public place, one or more face target(s) may exist in one image, so the first thing is to find out the locations of human faces against the background and then choose the right one from all the faces.

**Feature extractor:** this can transform the pixels of the facial image into a useful vector representation (the key points in a facial image). Basically in face

recognition algorithm, eyes, nose and mouth are considered to be the most important features of human face. In face.com's work, the feature extractor will detect position and shape information of major facial parts and then display six position points in each face.

**Authentication engine:** There are two different models in a biometric authentication system: user verification and user identification. In term of this research, it uses user identification model to achieve face recognition. The working process is as follows: user shoots a face image from the mobile phones and posts it with user ID to the web server; the authentication engine will compare the image with user's pattern and finally return a result to user.

As shown in Figure 5.2, the main task of mobile client is capture user's face image and transmit it to the web server. On the web server's part, the authentication engine use recognition API from face.com, which is responsible for the image processing and identity verification. The following sections will continue introduce each part of the system in detail.

### **5.3.2 System achievement**

#### **5.3.2.1 User register**

The register interface was designed to allow user register though the phone. If a user runs the application for the first time, a page will appear to ask the user to register. There are two registration methods: shooting a photo though the

mobile phone camera or uploading an image from the internet. By using the first method, the user may see one or more face tags on the screen after shooting. By clicking the capture button, a “Face detection” method will be used to detect face image and extract features. After that, the user will be asked to enter a unique username to finish registration. If no face image exists, a warning message will appear to inform of the mistake. The screen shot of user interface is shown in Figure 5.3.

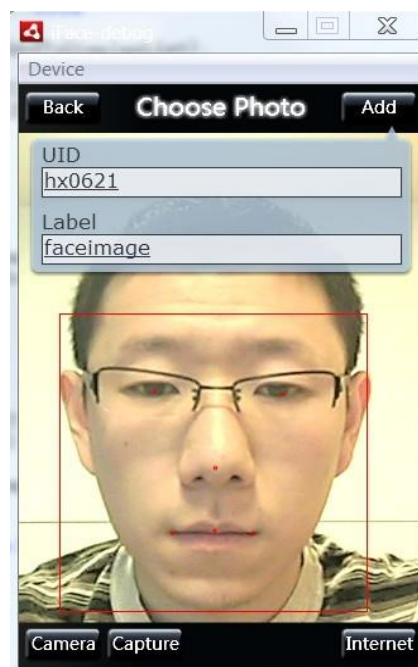


Figure 5.3: The registration page (shooting a photo with the mobile phone)

The other way to register is upload a face image from internet which can be achieved by entering a face image URL; the registration process is similar to that of the first method. By use this method, users can upload a higher quality

image to improve the recognition accuracy, the screen shot is shown in Figure 5.4.



Figure 5.4: The registration page (upload a photo from internet)

The same as with method one, the user can choose one face tag from the complex background and enter a unique username to complete the registration. When the user has been all set up in the index, the registration is successful. In addition, the user can upload more than one photo to the same account (because the researcher found that a high quality image or more saved tags for the same user can help the system to increase the recognition rate).

#### **5.3.2.2 Face recognition process**

There are three steps in face recognition process: (1) Face detection: when the

login page is opened, the mobile phone camera is automatically started, and user is prompted to shoot a photo. Before the user uploads the photo to web server, the Flex application will use the “detect API” from face.com to detect whether there are one or more faces in the image. If so, the application records face’s position and size as well as facial parts’ position. (2) Face feature extraction. Using this gained information, the “feature extractor” API can extract the face characteristics contained in each face prior to uploading it to the web server. (3) Face recognition. After receiving the uploaded information, the authentication engine will compare it with the corresponding face image in the database; identify whether the person is whom they claim to be and return the recognition result to user. Details of the whole recognition process details are shown as follows:

#### (1) Face detection

The face.com's API provides a set of services which allows computers to analyse facial information found in photos, and attempt to identify faces against a known set of users. The technology used in the server scales to many users, mark the face region out from the image and display the position and size of each face. In order to achieve this function on mobile phones, a “Click” function has been built into the Flex application. When users takes a face image in a public place and if the system has detected more than one face in the image, the user can manually click the face target which they want to choose. This method can effectively solve the problem of complex background and increase system usability.

## (2) Face feature extract

The process of face recognition requires an index of known faces before recognition can be performed. The function is used to detect the position and shape information of major facial parts such as eyes, mouth and nose. For example, the eyes are the most important feature of human face, the positioning of eyes is the key to recognition. The eyes produce gray valley area in the upper left and right of face image. Using this property, the system can accurately position both eyes. This process is also called 'training', and it works by adding face tags of known users to the index (or training-set), and then processing these photos to create a new index entry. More saved tags per user means higher accuracy. The Figure 5.5 shows how the system detect face image.

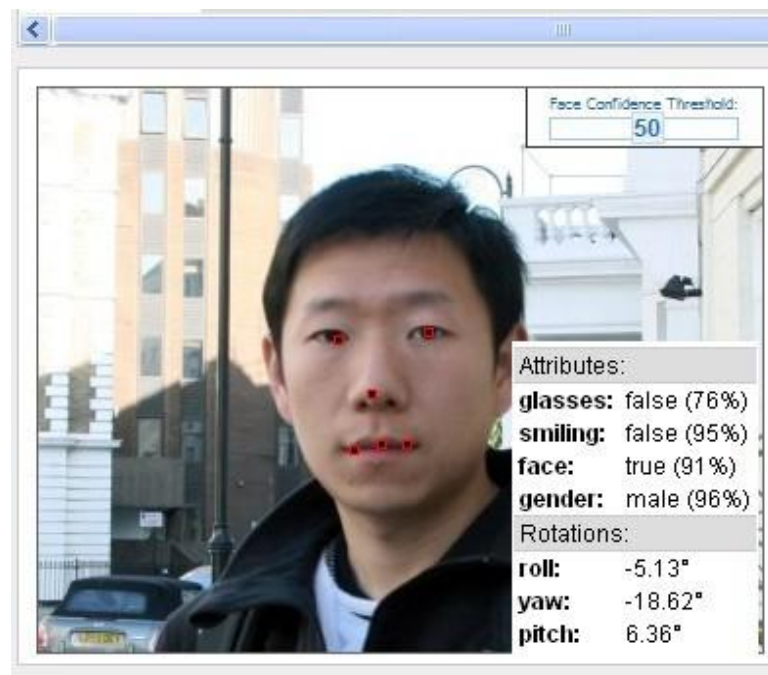


Figure 5.5: User interface of face detect

As shown in Figure 5.5, the faces detect results include two categories of information: Attributes (such as gender, wearing glasses, and smiling) and geometric information of the tag (eyes, nose and mouth).

### (3) Face recognition

After the face detection process, the user can start the recognition function by clicking the “Done” button. And then “Face. recognise” API will be used to analyse the gained results and compares them with the claimer’s pattern in the database. For each user’s login attempt, the face.com engine will return the most likely user IDs, or an empty result for unrecognised faces. This API provided by face.com’s has advantages such as: minimum calculation at rapid speed, realize real-time processing, and the ability to resist the interference of facial expression etc. Particularly in this research, face.com’s API only generates a recognition score for each trial, therefore, we need to compare the recognition result with a threshold (also consider as an acceptance standard) in the system. For example, if the threshold is 50, any recognition score greater or equal to this number is considered an acceptable result; and any recognition score below this number is considered a rejection result.

### **5.3.3 Operating environment**

The face recognition system was designed to achieve face detect and authentication in a mobile environment. On the client side, the application can run on a set of different mobile phones which includes HTC (Android phone),

apple (Iphone 3GS), and blackberry. The final experimental results were gained from the HTC Sensation phone.

The requirements of mobile phones and operating system are:

- (1) Iphone 3GS and above, operating system IOS 3.1 or above.
- (2) Android phone, operating system Android 2.2 or above.
- (3) Android phone install Adobe Air 2.6.

The Flex application on client side was developed by using Adobe Flash Builder 4.5, and written in ActionScript language.

## **5.4 Experimental Work**

### **5.4.1 Aims of the work**

In recently years, there are lots of studies based on face recognition, but most of the results of the related work are gained from PC (Bartlett et al., 2002; Yang, 2002; Blanz et al., 2002), only a few related work (Weinstein et al., 2002; Baker et al., 2005; Dave et al., 2010) focus on mobile application and the feasibility of mobile face recognition. Therefore, the main purpose of this experiment is to find out whether it is possible to use face recognition technique to establish the identity of the user on a mobile phone; if so, what is accuracy rate of the system. In order to find out the answers, the main tasks in this experimental work are: find out the false rejection rate (FRR) and false acceptance rate (FAR) of the system; to define an acceptance standard in the system, that is because the



face.com API only provide user verification method (after receiving the uploaded face image, the system will find out the best match pattern in the database and return a user ID and similar points), therefore, a threshold should be defined in face recognition system. In addition, though a set of experiments, the researcher tries to find out whether there is any potential factor which can affect the performance of the system.

#### **5.4.2 Methods**

In the experimental work, HTC sensation phone is chosen as the experimental tool, it is used to capture participant's face image and transmit data to web server. The face.com's API can analyse the received facial information and then establish user's identity. The database is provided by face.com, and it allows the creating of two namespaces and train 1000 private accounts. During the experiments, the researcher has found a total of 40 participants to test the system. There are few steps in the experiments:

(1) Registration: when running the application for the first time, users are asked to enter an ID and shoot a photo from mobile phone's camera or upload a face image to register.

(2) Login: researcher will ask each participant to login to use their registered ID; it is used to calculate the false rejection rate. In addition, a number of different experimental scenes are simulated to test the system practicality and performance.

(3) In the last step, the researcher will compare each participant's face image with the researcher's; any similar rate over the defined threshold score will be considered as false acceptance happens. The purpose of this work is to calculate the FAR of system.

### 5.4.3 Result

In the registration stage, all 40 participants had successfully registered through the phone. The photos taken from the mobile phone's camera can meet the requirement of system, and user can also use the photos from website as a user pattern. In general, the registration process takes 30-60 seconds. The user interface is shown in Figure 5.6.

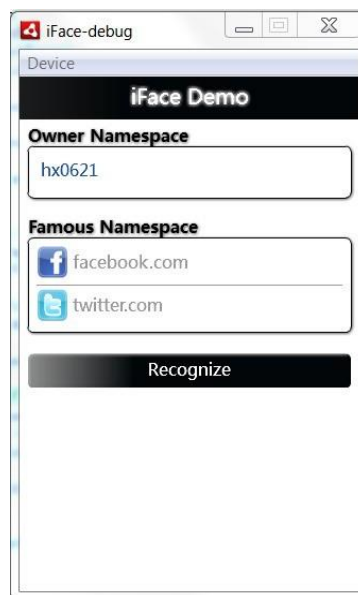


Figure 5.6: The experimental result interface

In the login stage, the researcher arranged three groups of experiments: in experiment 1, photos were taken under normal light condition (with bright light).

In experiment 2, photos were shot in a poor lighting environment. In experiment 3, the false acceptance rate of the system was tested.

(1) Experiment 1:

Experiment 1 aims to find out the FRR of the face recognition system. During the first experiment, the researcher has successfully registered two accounts by using different image uploading methods. The first account uses a photo shot by a mobile phone camera and second one uses a photo uploaded from internet. When the researcher logs in to the system, the first account gained 81 similar points and the second one gained 75 point. The interface was shown in Figure 5.7.



Figure 5.7: The recognition results

After the experiment, the results from 40 participants were analysed, it can be concluded that: 26 participants gained over 90 points; 4 participants gained

points between 80 to 90; 2 participants gained points between 70 to 80; 3 participants gained points between 60 to 70; 2 participants gained points between 50 to 60; 2 participants' gained points between 40 to 50 and 1 participant was unable to achieve a "verified" outcome because of the poor image quality. The FRR of the system can be shown as Table 5.1 and Figure 5.8.

Accept Standard Results	$\geq 90$	$\geq 80$	$\geq 70$	$\geq 60$	$\geq 50$	$\geq 40$
Unsuccessful login	14 times	10 times	8 times	5 times	3 times	1 time
FRR	35%	25%	20%	12.5%	7.5%	2.5%

Table 5.1: FRR of face recognition system



Figure 5.8: FRR of face recognition system

According to the result in Figure 5.8, the system FRR changes with acceptance standard. For example, if acceptance standard is set at over or equal to 90 points, the FRR will be 35%; and if acceptance standard is set at over or equal to 40 points, the FRR will be 2.5%. The next groups of experimental work will focus on testing the system performance when processing low quality images which were shot in poor lighting environments.

## (2) Experiment 2

In this experiment, the researcher has shot total 100 pictures in a poorly lit room. The researcher compares these photos with the registered pattern in database and gained 100 experimental results. The results indicate that the qualities of photos shot in poor lighting environment were greatly reduced. The details of the results are shown in Table 5.2 and the comparison of the FRR in experiment 1 and 2 is shown in Figure 5.9:

Accept Standard Results	$\geq 90$	$\geq 80$	$\geq 70$	$\geq 60$	$\geq 50$	$\geq 40$
Unsuccessful login	57 times	29 times	24 times	17 times	11 times	6 times
FRR	57%	29%	24%	17%	11%	6%

Table 5.2: FRR in experiment 2

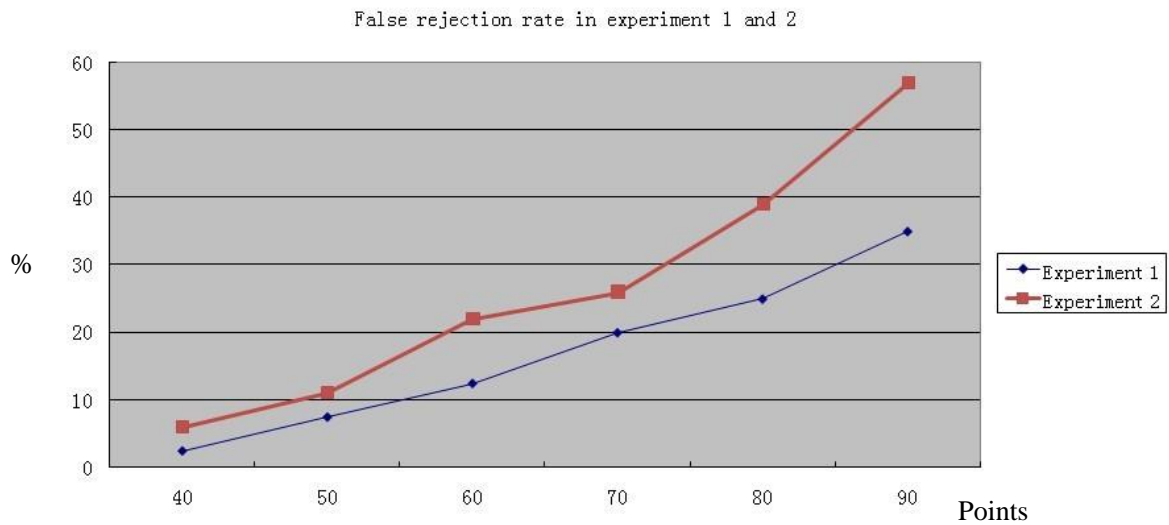


Figure 5.9: The comparison of the FRR in experiment 1 and 2

As shown in Table 5.2, the researcher has gained 43 results which were over 90 points; 28 results between 80 to 90 points; 5 results between 70 to 80 points; 7 results between 60 to 70 points; 6 results between 50 to 60 points; 5 results between 40 to 50 points, and 6 results are lower than 40 points. As shown in Figure 5.9, if we set the same acceptance standard in experiment 1 and experiment 2, the FRR in experiment 2 are significantly increased. This result shows that lighting condition is an important factor which will affect system accuracy rate. Therefore, the face recognition system is not suggested to be used in a poor lighting environment.

### (3) Experiment 3

Experiment 3 aims to find out the FAR of the face recognition system. In this experiment, the researcher has chosen a total of 20 participants' face image and compared it with other user's template. If system returns similar result, it

means false acceptance happens, as shown in Figure 5.10.

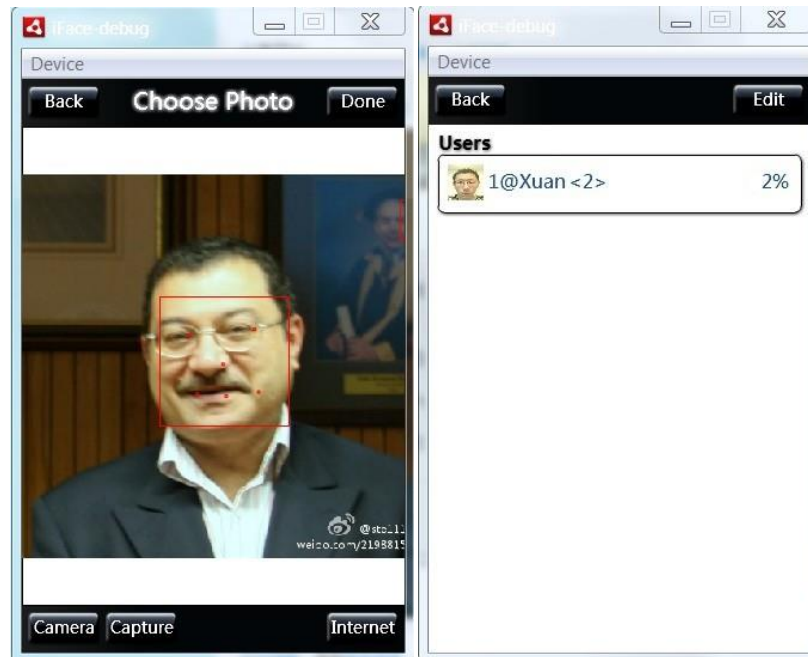


Figure 5.10: The false acceptance happens

After comparing each user's face image with the other 19 users' templates, the researcher has gained 190 results in total, the false acceptance happened 19 times, and the highest similar rate is 51% and the lowest 1%. The FAR changes with the acceptance standard, more details are shown in Table 5.3 and Figure 5.11.

Accept Standard Results	$\geq 10$	$\geq 20$	$\geq 30$	$\geq 40$	$\geq 50$
Success login	19 times	14 times	12 times	9 times	5 times
FAR	10%	7.4%	6.3%	4.7%	2.6%

Table 5.3: FAR of face recognition system

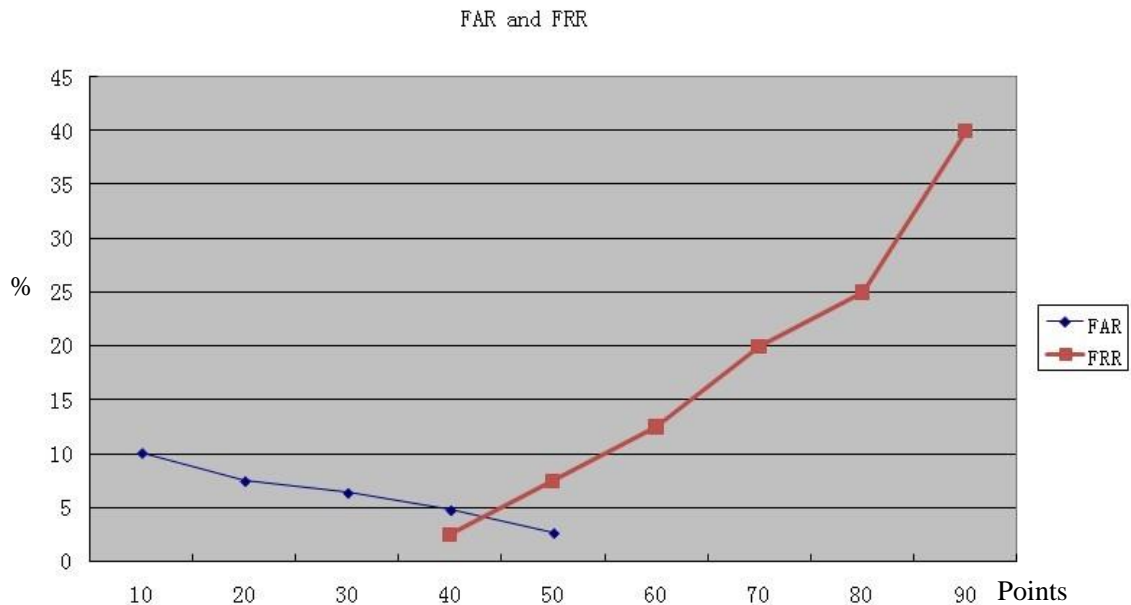


Figure 5.11: FAR and FRR of the face recognition system

From Figure 5.11, it can be seen that the system FAR changes with acceptance standard. When acceptance standard is set at to 10 points, the FAR is 10%; and if acceptance standard is set at over 50 points, the FAR reduced to 2.6%. Overall, the results gained in experiment 1 and 3 shows that, when acceptance standard is set at 44 points, FAR equal to FRR, this means that the system can achieve an EER (equal error rate) of 4%.

#### **5.4.4 Result summary**

In the face recognition experiments, 40 participants have successfully trained their face image and registered in the system. In experiment 1, when users log in to their own account, the best similar rate is 96% and the worst 41%. Experiment 2 tested the system in different environments and the gained results



show that the lighting condition has an influence on the recognition result. In experiment 3, the false acceptance happened: the highest similar rate is 51%, and the lowest 2%. The FAR is 10% when the acceptance standard is  $\geq 10$  points, and the FAR reduced to 2.6% when the acceptance standard is  $\geq 50$  points. According to the result gained in section 5.4.3, if we set the acceptance standard at  $\geq 44$  points and a user claims to be someone, the access request will be accept if the similar rate is over or equal to 44%. Otherwise, the request will be denied. In such circumstances, FAR equal to FRR which means the EER of the system is 4% in good lighting condition.

## **5.5 Discussion**

Face recognition is a non-intrusive technique. People generally do not have any problem in accepting face as a biometric characteristic (Hong and Jain, 1998). In particular, we use face recognition technique to replace the username and password identification method, which can better adapt to environmental changes. The overall experimental results covered in this chapter have demonstrated that, the proposed system can use face features to detect and facial geometry inherent characteristics to do automatic recognition work on a mobile phones. In normal lighting condition, the system can provide good identification rate: the experimental results indicate that the EER in the system is 4% when the acceptance standard is set at over or equal to 44 points.

However, the face recognition technique has its own limitations; the experimental results have shown that system accuracy rate is affected by the light condition. In dim light, some mobile phone without flash cannot successfully capture the user's face image. Therefore, the use of face recognition technique is conditioned by the environments. At present, some other individual biometric techniques such as speaker recognition and typing behaviour recognition can provide valuable enhancements in certain contexts. The next chapters will focus on the speaker's identity recognition technique and the design of a multi-modal biometric authentication system. It aims to achieve higher recognition efficiency and increase the implementation speed.

## Chapter 6

# The Speaker's Identity Recognition system

Humans have specific sound channel characteristics and pronunciation habit characteristics (Huang, 2004). A speaker's voice signals not only contain speech content, but also their personality characteristics. Therefore, speech signal digital processing technology on the computer side can be used to find out the difference between each user's voice characters and verify the speaker's identity. Since the 1960s, because of its unique convenience, economy and accuracy, speaker recognition techniques developed very fast and are widely used in the information security field, especially in the commercial application system (Saquib, 2011). The basic working process of a speaker recognition system is as follows: an individual must register a speech sample that is analysed and stored as a Voice Model, also called Voiceprint, or

Biometric Template in a system database. With the usage of the system for recognition, the test subject's utterance will be tested against the registered Voice Model and an identity decision will be made.

## **6.1 The speaker recognition technique used in this research**

Review the related work in context, there are two different methods that can be used in speaker recognition research. One is based on voice print pattern analysis, and other one is based on speech signal process (Finan et al., 1997). The former method set up a physical model using captured voice print, and then obtains the parameters for the model through solving differential Equations. The later method uses signal processing technology, extracts some individual characteristic parameters from the speech signal, and uses these parameters as standard to achieve recognition. The speaker recognition algorithm used in this research is provided by Speech Sentinel Limited Company ([speechsentinel.co.uk](http://speechsentinel.co.uk)), is a system called "Securivox approach" which judiciously combined the related two models. The speaker recognition system can be divided into two parts: preprocessing and recognition. In particular, the preprocessing part is the front end of the system, which includes voice signal digital processing, pre-emphasis, and extraction of the voice parameters. The comparison of the used system with other speaker recognition system is shown as Table 6.1.

CONVENTIONAL SV	SECURIVOX APPROACH
<ul style="list-style-type: none"> <li>• Developed for <b>speech recognition</b>, based on HMM/ANN technology</li> <li>• Uses thresholds to set the accept/reject score</li> <li>• Saturated performance – accuracy is around 93% to 95%</li> <li>• Sensitive to background noise</li> <li>• Text independent operation is difficult due to use of temporal information by HMM/ANN</li> <li>• Modelling is not extensible</li> </ul>	<ul style="list-style-type: none"> <li>• Developed for <b>speaker recognition</b></li> <li>• Does not use score thresholds</li> <li>• Accuracy is 99.5% +</li> <li>• Insensitive to background noise</li> <li>• Text independent operation is possible as temporal information is not used</li> <li>• Modelling paradigm is extensible</li> <li>• Scalable to large user bases; with deterministic error rates</li> </ul>

Table 6.1: Conventional SV versus ‘SecuriVox’ SV (Source from [speechsentinel.co.uk](http://speechsentinel.co.uk))

The Table 6.1 has illustrated that the SecuriVox approach has three advantages: high accuracy, insensitive to background noise and text-independent recognition. In addition, a major problem for speaker recognition systems is the variation in the quality of the channels. Speaker recognition systems have significant problems in maintaining the verification quality when channels vary (Finan et al., 2001). Typically this means that if a user is enrolled using a

landline telephone or a PC and then verifies using the same device the system will perform well. But, if the user then tries to verify using a mobile phone the recognition performance will deteriorate due to the differences between the landline, PC and mobile phone. Speech Sentinel has very good performance in the face of channel variations, and this method can reduce the system sensitivity to channel variations. Therefore, the 'SecuriVox' approach is suitable for the mobile speaker recognition system.

## **6.2 Research aim and tasks**

The aim of this chapter is to develop a mobile application to investigate whether it is possible to use user's voice print to establish the identity of the user on a mobile phone. To achieve this aim, a number of tasks must be completed:

- Develop a mobile application which can run on the same platform as the previous biometric authentication systems.
- Use the mobile phone to record user's voice and store it into the database.
- Perform a number of experiments to test the performance and accuracy rate of the system.
- Analysis the experimental results and evaluate the system.

## **6.3 Methodology**

### **6.3.1 System overview**

The general term speaker recognition denotes both Speaker Identification and

Speaker Verification.

**Speaker Identification** (SI) is a similar process of ascertaining a person's identity but here matches are made against multiple registered biometric templates, a watch set, and the test speaker matched to one of the set: i.e. *"does the person match one of the templates"*. In this case no identity claim is made and the identities are inherent in the watch set.

**Speaker Verification** (SV), which automatically confirms a person's claimed identity, based on the unique characteristics of the human voice. Speaker Verification Systems rely on extracting some unique features from an individual's speech and uses these features to differentiate him or her from other people.

The recognition method involves four mechanisms: speaker Identification, speaker verification, text-dependent and text-independent. Basically, the text-dependent recognition only models the speaker for a limited set of phonemes in a fixed context; it generally achieves higher recognition rates than text-independent recognition (Finan et al., 2001). But in practice, by using the text-independent recognition method, users are allowed to speak a random sentence rather than a fixed sentence. It is not necessary for the users to remember what they have spoken when registered. Therefore, the text-independent based speaker recognition system will be more flexible and easy to use. On the other hand, speaker recognition is one of the biometric

techniques used in the multi-modal authentication system, it is not a single method used to protect the system. Consider to the requirement of this research, the mechanism used in the system is speaker verification, and text-independent method, as shown in Table 6.2. It means that in the recognition process, when an individual claims to be someone, and speaks a random sentence or a paragraph, then the system makes a decision as to whether the claim is 'true' or 'false'.

	Speaker Identification	Speaker Verification
Text-dependent	/	/
Text-independent	/	√

Table 6.2: The recognition mechanism used in the system

The system structure of speaker recognition system is similar to that of the face recognition system. It can be divided into two parts: mobile client and web server. The client side can achieve voice file record and upload work, and two interfaces were designed: registration and login. In the web server, the following functional modules should be included: feature extraction, model training, authentication engine and database.



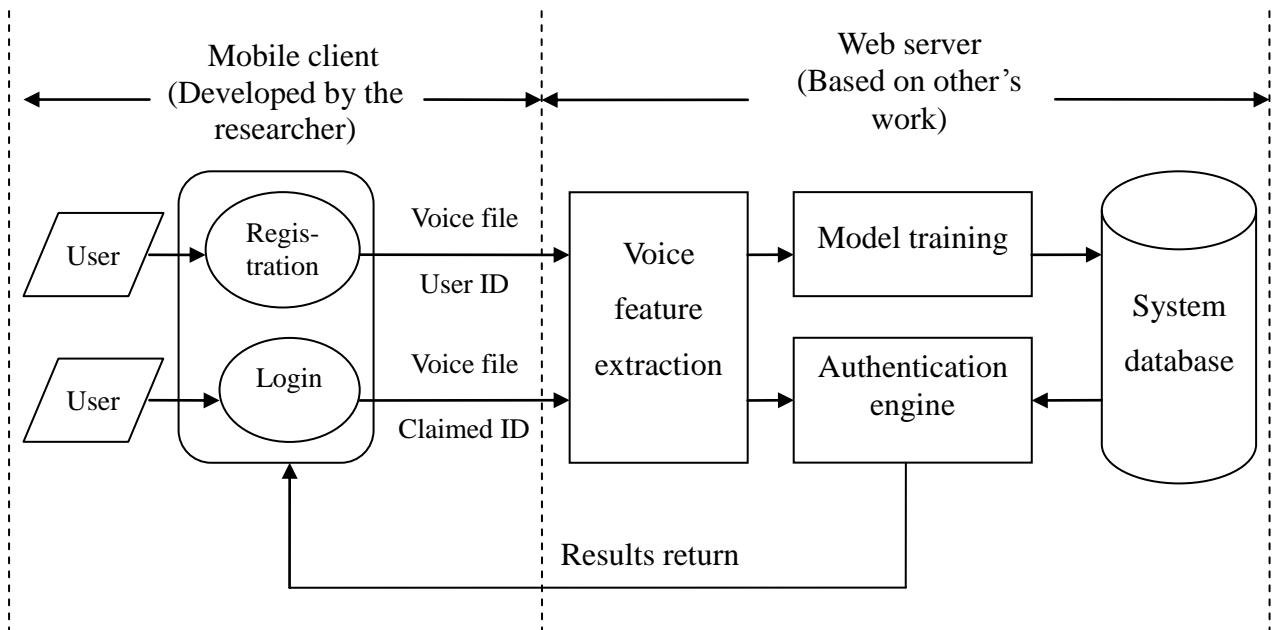


Figure 6.1: The speaker recognition system model

As shown in Figure 6.1, a Flex application has been developed by the researcher as a client, which allows users to register and login through a mobile phone. When user registration is successful, the voice file and username will be stored into the database. The task of the web server is to process the voice data recorded from mobile phone and complete the recognition work. When the web server receives the user's login request, it will ask user to enter a username and speak a random phrase. The authentication engine will subsequently process the voice file and compare it with other patterns they have registered. If a sufficient match is found, an acceptance result will be returned to user; otherwise, the user's login request will be rejected.

### **6.3.2 Mobile application**

#### **6.3.2.1 Voice record and upload**

The main tasks of the mobile client are to record the voice data from user and post it to the web server. A Flex application can use the device microphone to monitor audio sample data. When the data returned through the ActionScript Microphone API, the application can gather much information about the sound, and perform further process within web server. The code in Appendix V (4) can achieve the functions of capture audio data from an Android microphone. Within the 'audio data capture' code, when registering a "SampleDataEvent", the application can easily monitor the associated sample data being gathered and write the data to a "soundBytes" for later playback. As new samples come in, new data is added to the "soundBytes", building up the sound data over time. After the application gained the record data, the next step is convert it into a ".wav" file which can be accepted and processed by the web server. The code is given in Appendix V (5).

In this discussed speaker recognition system, speech recorded at 16 bit mono which can be PCM or mu-law encoded. The sampling rate, training times and recognition time can be set up in the system. Particularly, the sampling rate can be set between 8 kHz, 16 kHz, 11.025 kHz, 22.05 kHz and 44.1 kHz. In this research, 8 kHz ensures compatibility with telephony quality speech.

### 6.3.2.2 User registration and login

The developed Flex application allows users to register through the mobile phone. When a user runs the application for the first time, they are asked to enter a unique username (also referred to as Nick name in Figure 6.2) for distinction purposes. Users then speak a short random phrase such as their name or home address. To record the speech press the “Record” button and say the utterance. They repeat this five times and they can complete the registration by pressing the “Build” button. Once the model has been built, the voice files and user information are stored in a database. The screen shot of user interface is shown as Figure 6.2

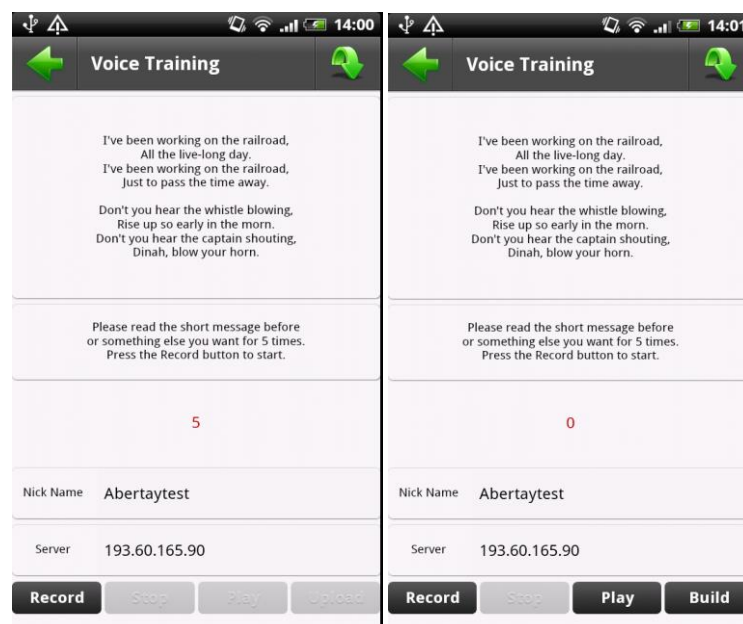


Figure 6.2: User registration interface on Android phone

Similarly, when a user attempts to login, they will be asked to speak a random phrase and upload the voice file again. After that, the web server will process the upload file and return an authentication result.

### 6.3.3 Web server

There are two main functions of the web server: model buildup and speaker's identity verification. When the user enter a username and upload five speech files, the model will be built up and stored in a database. The speaker verification server, also considered as the authentication engine is responsible for the verification work. The details are shown in Figure 6.3.

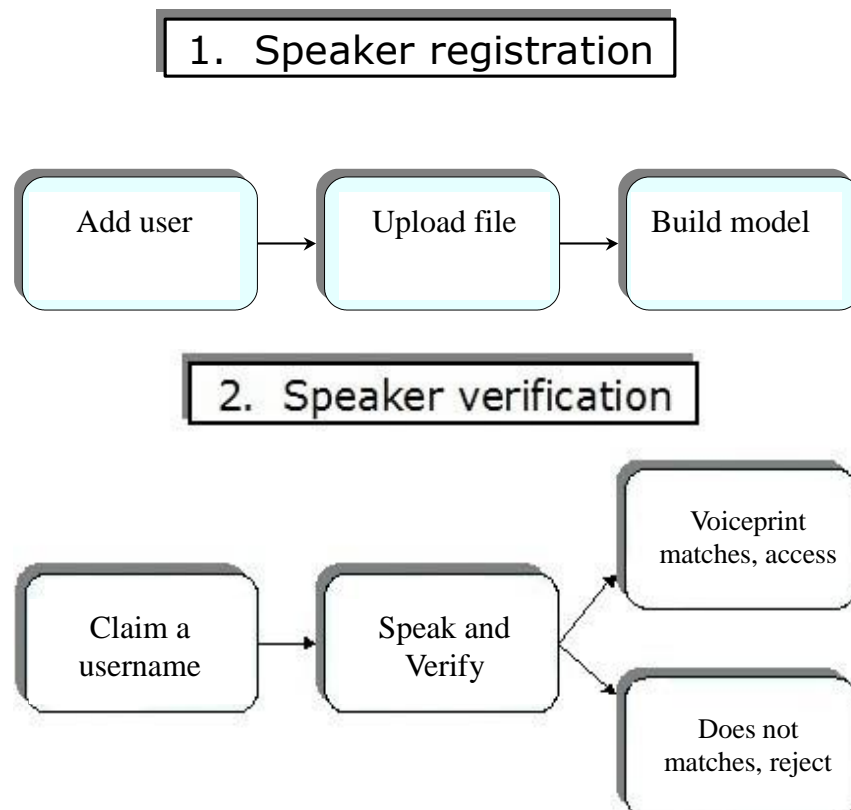


Figure 6.3 Speaker recognition web service

In the speaker recognition system, the user will be verified against a claimed identity. There are few steps in the recognition process. After receiving the user ID and uploading the voice file from the client, the web server can extract unique features from an individual's speech. Then, according to the claimed identity's information, the authentication engine will compare the voice print with the claimer's pattern in the database, and thus identify whether the person is who they claim to be. A passed or failed result will be returned to the user.

## **6.4 Experimental work**

### **6.4.1 Aims and methods**

The purpose of this experiment is to find out whether it is possible to use a speaker recognition technique to establish the identity of the user on a mobile phone. If so, the researcher will calculate the false rejection rate and the false acceptance rate of the system. In addition, through a set of experiments, the researcher will find out whether any potential factors which will affect the usability and accuracy of system exist. In the experimental work, the researcher has found a total of 20 participants to test the system. The followings are the steps:

- (1) Registration: when a user uses the system for the first time, they are required to choose a user name and speak a phrase five times to register.
- (2) The second step is validation; the researcher will ask each participant to

identify themselves and speak a paragraph to login. If the login attempts fails, then that means false rejection happened; otherwise, false rejection did not happened. This experiment is used to find the false rejection rate (FRR) of the system.

(3) In the last step, the researcher will ask each participant to speak another phrase and upload it again. The upload voice file will be compared with the other 19 participants' patterns in the database. If the web server return an "accept" result, that means false acceptance happened; otherwise, it did not happened. This experiment is aimed to test the false acceptance rate (FAR) of the system.

#### **6.4.2 Results**

In the set of experiments, the registration process takes about 30 to 60 seconds and the verification process takes 10 seconds to complete. There are 10 participants performed the experiment in a quiet place like the lab or home; and the other 10 participants performed in a noisy environment like outdoor or the hall of the University. By comparing the result gained from these two different groups, we can find out whether the system is sensitive to background noise or not.

(1) Experiment one:

After all the users have registered on the system, there are 100 voice files were recorded in database. In this step, each participant tried to login and claim the user name which they just registered. When the web server received the access

request, it will process the upload file and return an authentication result. The experimental interfaces are shown in Figure 6.4:

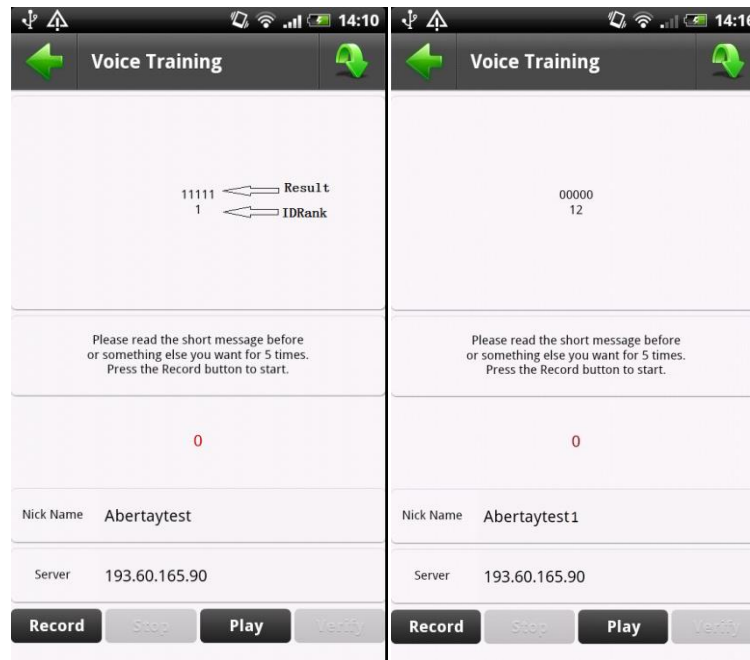


Figure 6.4: Experimental interfaces

The recognition result involves five numbers ('1' or '0'); each of the "1" means a pass for the process, and a "0" means a fail for the process. For example, in Figure 6.4, the first user "Abertaytest" gained an "11111" result which indicates that the user passed five times and the second user "Abertaytest1" gained a "00000" result which means that the user failed five times.

## (2) Experiment two:

In this experiment, each participant uploads a voice file again and the researcher compares it with the other user's patterns (each participant's pattern

contains five speech files). If five “0” recognition results are returned, it means no false acceptance happened; if any “1” exist in the recognition result, it means false acceptance happened. The experimental results are shown in Table 6.3.

	Experiment 1 result	Experiment 2 result	Length of speech	Noisy
User 1	00100	00000	1 sec	No
User 2	01101	00000	2 sec	No
User 3	11111	00000	4 sec	No
User 4	11011	00000	3 sec	No
User 5	11110	00000	5 sec	No
User 6	00101	00000	2 sec	No
User 7	11111	00000	4 sec	No
User 8	00111	00000	3 sec	No
User 9	11110	00000	4 sec	No
User 10	11001	00000	6 sec	No
User 11	01011	00000	3 sec	Yes
User 12	01100	00010	1 sec	Yes
User 13	00011	00000	5 sec	Yes
User 14	01101	00000	3 sec	Yes



User 15	10110	00000	4 sec	Yes
User 16	10001	00000	4 sec	Yes
User 17	10111	00000	7 sec	Yes
User 18	10001	00000	3 sec	Yes
User 19	11101	00000	6 sec	Yes
User 20	00000	00000	2 sec	Yes

Table 6.3: The experimental results

In Table 6.3, 200 results were gained. False rejection happened 41 times in experiment 1, the FRR is 41%. False acceptance happened once in experiment 2 and the FAR is 1%. In order to find out whether there is any potential factor which can affect the performance of the system, the speech length and environmental conditions (quiet or noisy) were recorded in Table 6.3.

#### **6.4.3 Result summary**

Comparing the result gained in Table 6.3 separately, it can be seen that in terms of the first 10 participants in group one who tested the system in a quiet environment, within these 100 recognition results, false rejection happened 16 times, the FRR is 32% and false acceptance never happened. The experimental results in group two were gained in a noisy environment. The false rejection happened 25 times and the FRR increase to 50%. False acceptance happened

once, the FAR is 2%. On the other side, it can be found that there are 18 users speak a phrase longer than or equal to 2 seconds, the false rejection happened 34 times and the FRR is  $\frac{34}{90} \times 100\% = 37.8\%$  and FAR is 0%. 15 users speak a phrase longer than or equal to 3 seconds, the false rejection happened 24 times and the FRR reduced to  $\frac{24}{75} \times 100\% = 32\%$  and FAR is 0%. Other 10 users speak a phrase longer than or equal to 4 seconds, the false rejection happened 14 times and the FRR reduced to  $\frac{14}{50} \times 100\% = 28\%$  and FAR is 0%. The details of the experimental results are shown in Table 6.4.

	Result overall	Noisy	Quiet	Voice files $\geq 2$ seconds	Voice files $\geq 3$ seconds	Voice files $\geq 4$ seconds
FRR	41%	50%	32%	37.8%	32%	28%
FAR	1%	2%	0%	0%	0%	0%

Table 6.4: The list table of experimental works

The results in Table 6.4 illustrate that the speaker recognition system will be affected by the background noise and the length of speech file. From this table, it can be found that when users register and login in a noisy environment, the FRR of the system is 50% and FAR is 2%; and when the experiment performed in a quiet place, the FRR reduce to 32% and FAR is 0%. When the length of

user's voice file longer than or equal to 2 seconds, the system FRR is 37.8%; the FRR reduced to 32% when the length of voice file is longer than or equal to 3 seconds; and the FRR is 28% when the length of voice file is longer than or equal to 4 seconds. This result demonstrates that the length of the voice file is an important factor which can affect the system accuracy. Overall, the results in Table 6.4 demonstrate that environment and the length of the voice file are two important factors which can affect the system accuracy. Quiet environment or a long sentence utterance can help to improve the system accuracy.

In the speaker recognition system, the research has setup a recognition mechanism: 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.

According to the above mechanism and experimental result, if we set the accept threshold as when the result contains three or more "1"s, there are 8 participants' recognition result contains three or more "1"s in group 1, that means, two correct users will be rejected by the speaker recognition system, and the FRR is  $\frac{2}{10} \times 100\% = 20\%$ . False acceptance did not happened in group

1. Similarly, there are 5 participants' recognition result contains more than 3 "0"s in group 2 which means the false rejection happened 5 times in quiet

environment, and the FRR is  $\frac{5}{10} \times 100\% = 50\%$  and false acceptance did not happened. When we change the threshold in the system, the details of changes of FRR and FAR are shown in Table 6.5.

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 6.5: Results summary

The result in Table 6.5 shows that the FRR and FAR of the system in group 1 are lower than in group 2. The comparison illustrates that the speaker recognition system has better performance in quiet environment than in noisy environment. Overview of the experimental results, if the system accept a user when the recognition result contains 3 or more “1”s, the FRR is 35% and false acceptance did not happened. When the accept threshold changes 2 or more

“1”s, the FRR reduced to 10% and false acceptance still not happened. The FRR are equal to the FAR when the system accept a user if the recognition result contains 1 or more “1”. Therefore, if we set the accept threshold in the system as 1 or more “1”,  $FAR = FRR$  which means the system can achieve an ERR of 5%.

## **6.5 Discussion**

Speaker's identity recognition can be regarded as a type of organism recognition technology, which belongs to the scope of pattern recognition. Compared with other biometric techniques, the text-independent speaker recognition system is easy to use and does not need any special hardware. This chapter discussed a speaker recognition system based on a mobile phone to establish the identity of the user. According to the result gained from experimental work, the speaker recognition system can achieve a low FAR and a low FRR in quiet environment. But the experimental results also indicated that noise and the length of speech are two factors which can affect the system accuracy. Therefore, the speaker recognition method is better to be used in poor light but quiet environment which is not suitable to use typing or face recognition. Overall, the mobile speaker recognition system developed in this chapter can achieve an EER of 5%; it is an important part of the multi-modal authentication system. The next chapter will focus on design a multi-modal biometric authentication system on mobile phones.

## Chapter 7

# The multi-modal biometric authentication system

In the previous chapters, a model to support the authentication of mobile business was presented; subsequently, three independent biometric authentication techniques were used to support the model. In this chapter, the researcher combines the multi-level authentication model with the three biometric authentication techniques, and presents a multi-modal biometric authentication system based on a mobile phone. This chapter will test the system, and then discuss its performance when it is used in mobile commerce.

### **7.1 Overview of the multi-modal authentication system**

The experimental work of Chapters 4, 5 and 6 demonstrated that three biometric authentication systems have the ability to confirm user's identity on a mobile

phone, each individual biometric authentication system can achieve acceptable recognition rate independently: the EER of the typing behaviour recognition system is 7.5% when  $\alpha$  value is set as 3.8; If the face recognition system accept a user when the recognition result is greater than or equal to 44 points, the EER of the system is 4%; if the speaker recognition system accept a user when the recognition result contains 1 or more “1”s, the system EER is 5%. The details of the results are shown in Table 7.1.

Techniques	Acceptance standard	EER
Typing behaviour recognition	$\alpha = 3.8$	7.5%
Face recognition	Accept a user when the result is greater than or equal to 44 points.	4%
Speaker recognition	Accept a user when the result contains 1 or more “1”s.	5%

Table 7.1: The experimental results gained from Chapter 4, 5 and 6

The biometric authentication systems which were developed in previous chapters are used independently. In this chapter, the researcher builds a system to use the security model proposed in Chapter 3, and combines typing behaviour recognition, face recognition and speaker’s identity recognition. The next section will discuss the test results in a simulated m-commerce environment.

### 7.1.1 The registration process

The registration process includes four steps: enter 4-digit PIN code, enter user name and password, and then upload a face image and speak a random phrase to complete the registration. The screenshots of registration process are shown in Figure 7.1.

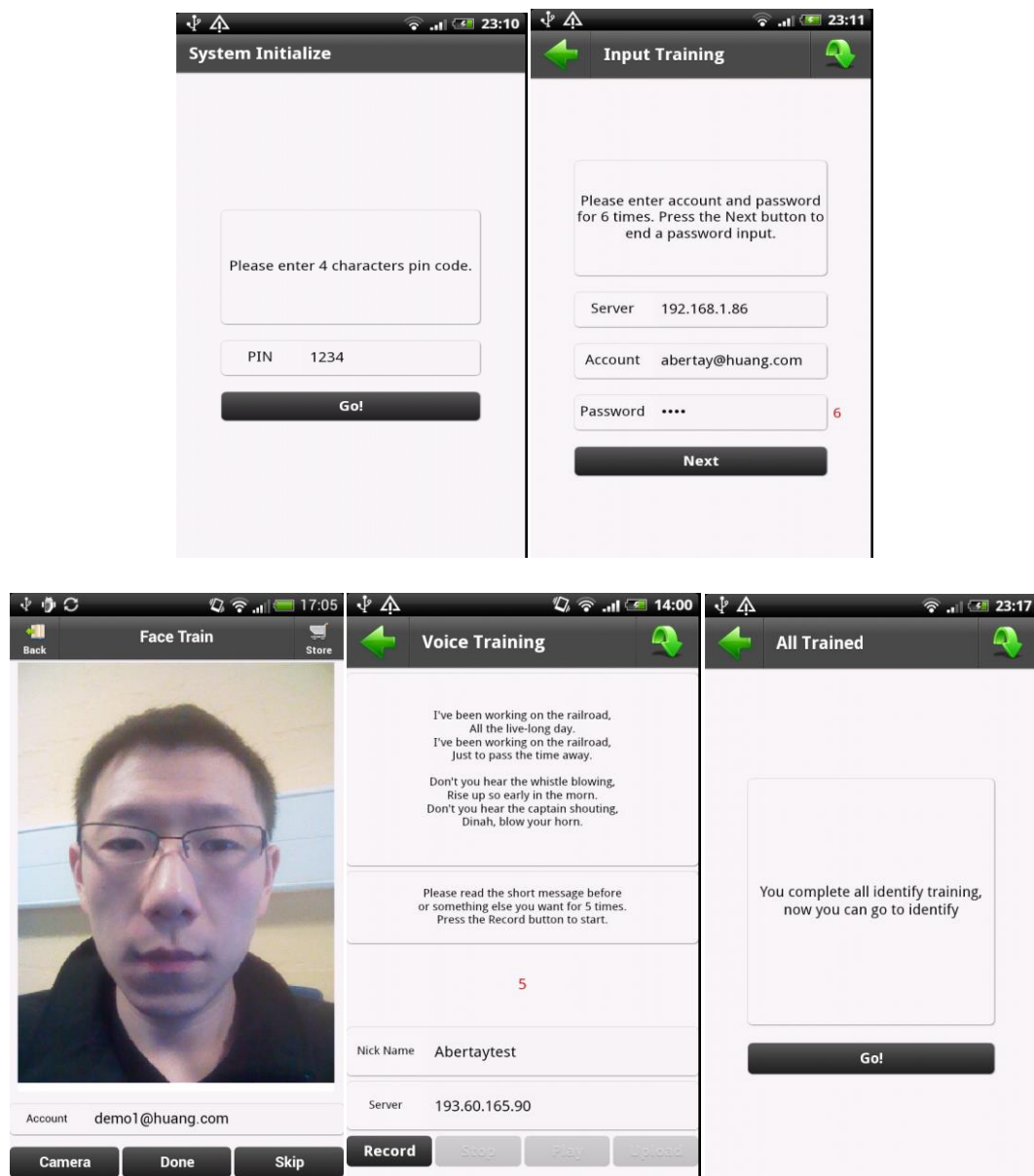


Figure 7.1: The training interfaces of multi-modal system



When a user is successful registered, all captured data will be stored in a system database. After that, every time a user starts the application, they can directly access the identify process.

### **7.1.2 The authentication process**

#### **7.1.2.1 A mobile-commerce model**

The simplest authentication model requires the user to identify themselves via a password for every transaction. This repeated entering of a password is annoying to the user. At the other extreme, if an application used a single password on start-up, this would leave the user open to a significant loss if they were to lose their phone. The smart authentication model proposed here provides a balance between repeated biometric input and single biometric input whilst adhering to the principle of higher value transactions requiring more security. Within this model, two security mechanisms have implemented:

1. The transaction value determines different authentication levels.
2. Each authentication levels corresponding to different biometric authentication mechanism.

Figure 7.2 describes the working flow of a mobile-commerce system:

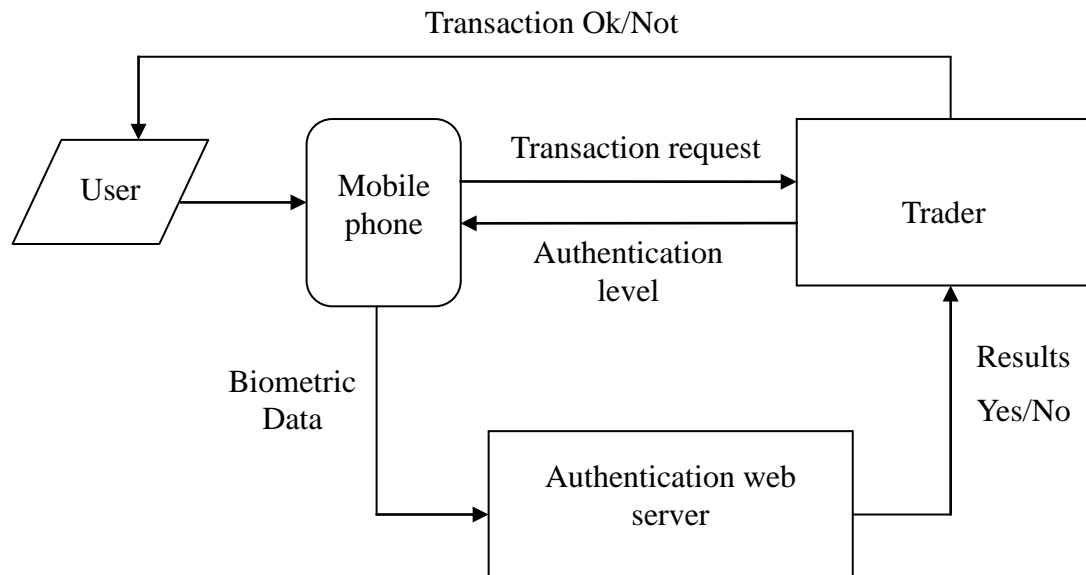


Figure 7.2: A mobile-commerce model

When the trader receives the user's transaction request, they can determine the authentication level according to the transaction value. Subsequently, the authentication web server will choose one or more suitable authentication techniques and ask the user to provide biometric data. After receiving the authentication result returned from web server, the trader can notify user whether the transaction is ok or not.

### 7.1.2.2 Authentication levels determination

According to the model proposed in Chapter 3, transaction risk is determined by the value of transaction. Table 7.2 below shows the maximum value of transactions at each authentication level.

Authentication level (AL)	Maximum Value (v)	Maximum Time (t)	Authentication techniques	Maximum number of transactions (n)
0	£15	No limit	None	30
1	£50	180	PIN	10
2	£100	60	One biometric	5
3	£250	10	Two biometrics	2
4	Restricted by payment limit	0	Three biometrics	1

Table 7.2 Potential parameters for inclusion into the multi-level authentication model

According to the mechanism set up in Table 7.2, when a user starts the phone, the starting point is  $AL=0$  and they can stay there as long as they have the phone. This allows the user to request very low level transactions before they have to authenticate. If a user requires higher value transaction, the system will use authentication mechanisms to identify the user's identity. Note that the Figures given in Table 7.2 allow for a maximum risk of a  $£500 = \text{Maximum Value (v)} \times \text{Maximum number of transactions (n)}$  loss within the given time limit. The maximum value of transactions that can be carried out before re-authentication is  $£500 (= v \times n)$ . At each of the authentication levels a user can carry out a maximum number of transactions within a fixed time scale each up to a maximum value.

### 7.1.2.3 Authentication interfaces

Each phone has a unique PIN which is set up when the user is registered; an individual can try at most three times to log in. If the PIN is correct, it has access to AL=1; the user can stay in this level for 180 seconds, the interfaces are shown in Figure 7.3

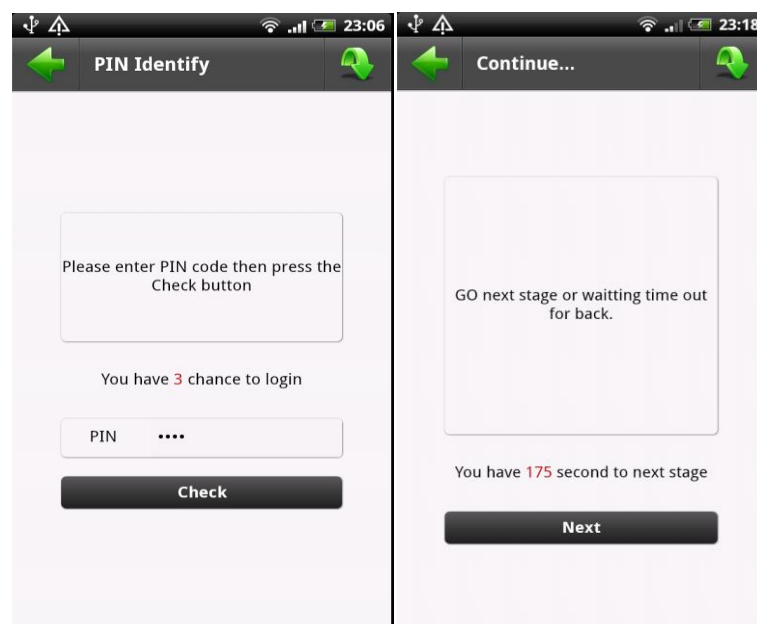


Figure 7.3: Level 1 vilified interfaces

At any level, if users request a transaction of greater value than the maximum value for the authentication level they are asked to authenticate. If this is successful the user's authentication level is increased and the transaction approved, if the user fails to authenticate the authentication level will return to previous level until the application is locked. The Figure 7.4 shows when a user request access to level 2; they have to enter username and password to login.

The authentication mechanism in this stage will check the user's account information and the keystroke data as well, if the details match, the user log in successful and access to AL= 3. The interfaces are shown in Figure 7.4.

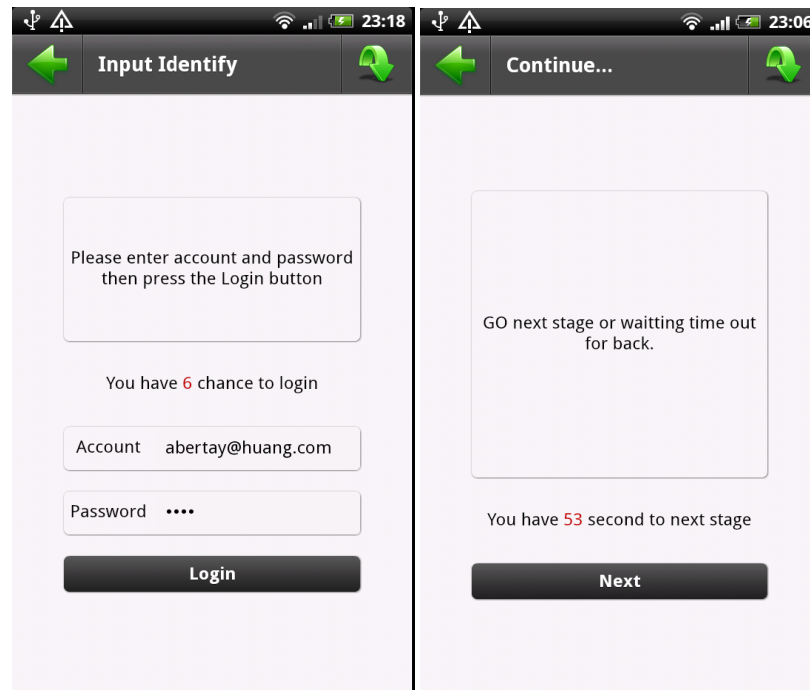


Figure 7.4: Level 2 vilified interfaces

If the user has been on a given level for a time greater than the maximum permitted, or they request more than the maximum number of transactions at that level, they are put into a lower authentication level.

If the user requests a transaction of greater value than that allowable at AL=3, then they are asked to authenticate and if successful the transaction is approved but user is returned to AL= 3.

Similar to the previous authentication mechanism, if a user wants access to

level 3 and 4, they need provide face photo or speak a random sentence to complete the recognition process. The interfaces are shown in Figure 7.5:

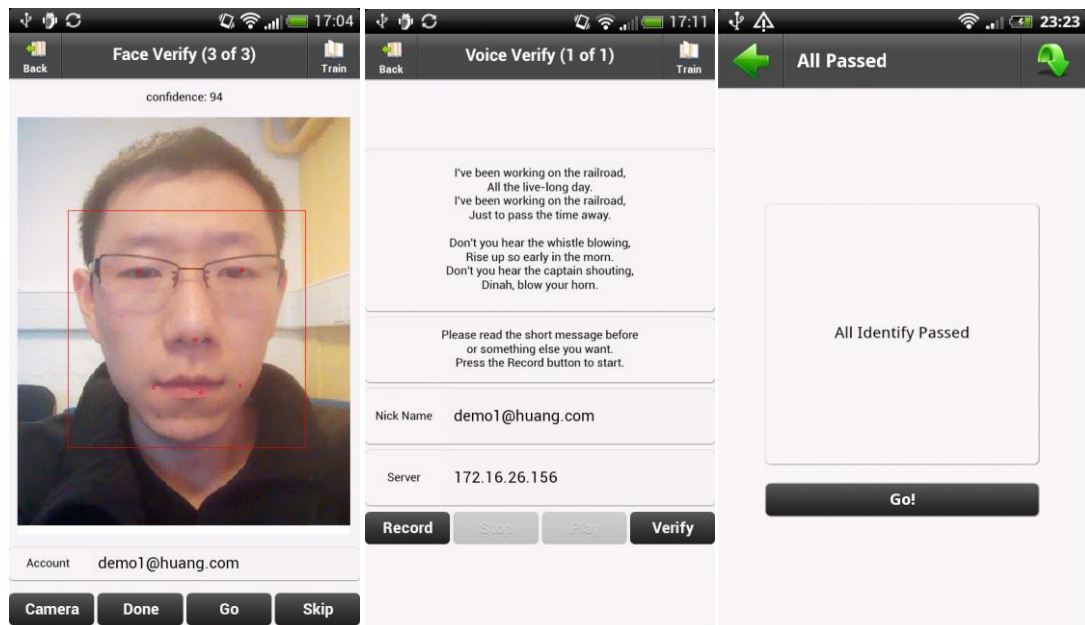


Figure 7.5: Level 3 and 4 vilified interfaces

## 7.2 Evaluation

The main purpose of the multi-modal biometric system is to investigate mobile security. In this context, the developed authentication system can provide convenient and fast authentication for low level transactions, and also provide accurate and secure authentication for high level transactions. But the Table 7.2 illustrated that the authentication level, maximum value and authentication mechanism are fixed in the system. A review of the experimental results gained in previous chapters, the respective EER of single biometric authentication systems are 7.5%, 4%, and 5%. As this composite mechanism involves multiple

authentication techniques it is necessary to calculate the FRR and FAR at each authentication level. At authentication level 3 and 4, two and three biometric authentication techniques are used. The FAR can be calculated by using the process algorithm:

$$\text{Level 3 FAR} = \text{Typing FAR} \times \text{Face FAR}$$

$$= 7.5\% \times 4\%$$

$$= 0.3\%$$

$$\text{Level 4 FAR} = \text{Typing FAR} \times \text{Face FAR} \times \text{Voice FAR}$$

$$= 7.5\% \times 4\% \times 5\%$$

$$= 0.015\%$$

On the other hand, the FRR at authentication level 3 and level 4 can be calculated by using the Genuine Acceptance Rate (GAR) of a single biometric system. GAR is a probability of an authorised user correctly being accepted, it is calculated by the formula:  $\text{GAR} = 1 - \text{FRR}$  (Awang and Yusof, 2011). The GAR of typing behaviour recognition system (FRR 7.5%) is:  $1 - 7.5\% = 92.5\%$  and the GAR of face recognition system (FRR 4%) is:  $1 - 4\% = 96\%$ . Therefore, at authentication level 3, the GAR of composite system is:  $92.5\% \times 96\% = 88.8\%$ , that means level 3 has a  $\text{FRR} = 1 - 88.8\% = 11.2\%$ .

$$\text{Level 3 FRR} = 1 - \text{Typing GAR} \times \text{Face GAR}$$

$$= 1 - 88.8\%$$

$$= 11.2\%$$

Similarly, the FRR at level 4 can be calculated by using the process algorithm:

Level 4 FRR =  $1 - \text{Typing GAR} \times \text{Face GAR} \times \text{Voice GAR}$

=  $1 - 84.4\%$

=  $15.6\%$

The details of recognition results of multi-modal biometric authentication system are shown in Table 7.3.





Authentication levels (AL)	Techniques	FRR	FAR
0	None		
1	PIN		
2	Keystroke recognition	7.5%	7.5%
3	Keystroke + Face recognition	11.2%	0.3%
4	Keystroke + Face + Speaker's identity recognition	15.6%	0.015%

Table 7.3: The recognition rate of a deterministic authentication system

From Table 7.3, it can be seen that the multi-modal biometric authentication system is more convenient to process the low level transaction and more secure to process the high level transaction. For a low value transaction, the authentication process is simple and the system can achieve a low FRR. At the



other extreme, the use of multiple biometric authentication techniques will make the high value transaction become more secure. For example, the FAR is 0.3% at  $AL=3$ , which means if a thief steals the phone and even steal the PIN and password, the criminal only has 0.3% chance to break into the system. However, the repeated use of biometric authentication will make the FRR of the system greatly reduced into an unacceptable range (over 15.6%); in addition to this, environment is another fact which could affect the recognition result of the system. Therefore, a better solution will be required.

### **7.3 Discussion**

The multi-modal biometric authentication system developed in this project has been shown to have the ability to establish the identity of the user on a mobile phone, and to achieve a low FAR. In order to test the system performance in mobile commerce, a shopping model was designed in the system. It simulates some different shopping environments and the prototype was used by a number of users to test out the model. In the experimental work, the participants were asked to go through some scenarios giving typical purchasing experiences, and their comments were recorded by the researcher. The experience of low value transaction provided a fast shopping experience for the user: Users use the phone to pay and receive an electronic receipt which could be used to prove to the merchant that they had paid. There is a psychological barrier, in that users expressed some concern about the use in a “real shop”; it is not natural to pick up an item and walk out of the shop. The ability to store all receipts would give

the users further re-assurance if they were challenged when leaving a shop. For larger and more expensive items the users expect to have to enter some form of authentication. Using a password was seen by some as insure, because it is easy to steal. Utilising some other identity management scheme, such as tying behaviour recognition, face recognition and speaker's identity recognition that have been provide would match the overall design of the system better.

There are many other researches based on multi-modal biometric authentication in recent years. Table 7.4 gives a comparison of four multi-modal biometric authentication systems.

	Koreman et al. (2006)	Clarke and Furnell (2007 <sub>a</sub> )	Zhu and Zhang (2010)	This work
Mobile phone	Yes	Yes	No	Yes
Biometrics	Voice Face Signature	Keystroke Face Voice	Finger geometry, Knuckle print Palm print	Keystroke Face Voice
Authentication levels	No	4	3	5
Accuracy rate	EER: 0.83%	FRR: 0.001-0.4(%) FAR: 0.000001-0.00 002 (%)	FRR:16% FAR: 0.000252%	FRR:15.6% FAR: 0.015%

Table 7.4: Performance comparison of related works

Table 7.4 shows that the developed multi-modal biometric system in this research is quiet promising. Compared with single biometric authentication system, the multi-modal system has a lower FRR at low authentication level and also a lower FAR at high authentication levels, which means it is easier and faster for the user to process low value transaction and at the same time, the low FAR can ensure that the system has the ability to identify unauthenticated user when they claim a high value transaction. At the other extreme, similar to other research work (Zhu and Zhang, 2010. Clarke and Furnell 2007<sub>a</sub>), some issues such as high FRR and the affect from environment affect results in this chapter. The next chapter will focus on looking for a better solution.

## Chapter 8

# A smart model in mobile-commerce system

When using a password-based authentication model to guard against hacking or fraudster break-in the system will ask users to enter a password to identify themselves each time a transaction is performed. Obviously, the repeat use of security measures is annoying to a user. In this research, the primary challenge is to develop a secure and smart authentication mechanism. The previous chapters in this thesis gave an overview of a multi-modal biometric authentication system which uses three biometric techniques instead of a password. This biometric system can achieve a low false acceptance rate, but the process is inflexible and it is easy to reject the valid user. In order to solve these issues, a new fuzzy logic model has been proposed in this chapter, and then it is used to support the decision making in mobile commerce.

### **8.1 A smart authentication mechanism**

In the deterministic models which were proposed in chapter 3 and chapter 7, risk is synonymous with value of the transaction; and the decision of whether to accept or reject a user is determined by each single biometric recognition result. These models are easy to achieve but not smart and flexible. However, a fuzzy inference mechanism which combines with the deterministic models has been proposed in this chapter. Generally, a fuzzy logic method uses an imprecise but very descriptive language to deal with input data more like a human operator (Kaehler, 1993). In this research, the fuzzy model can process multiple input data items and provide approximate solutions to the usability problem that deterministic methods find hard to solve. Within this model, two security mechanisms have been implemented:

1. The transaction value, distance from last transaction location and time interval will determine the transaction risk (TR).
2. Biometric authentication results determine the recognition rate (RR).

The work flow of a smart authentication model is shown in Figure 8.1:

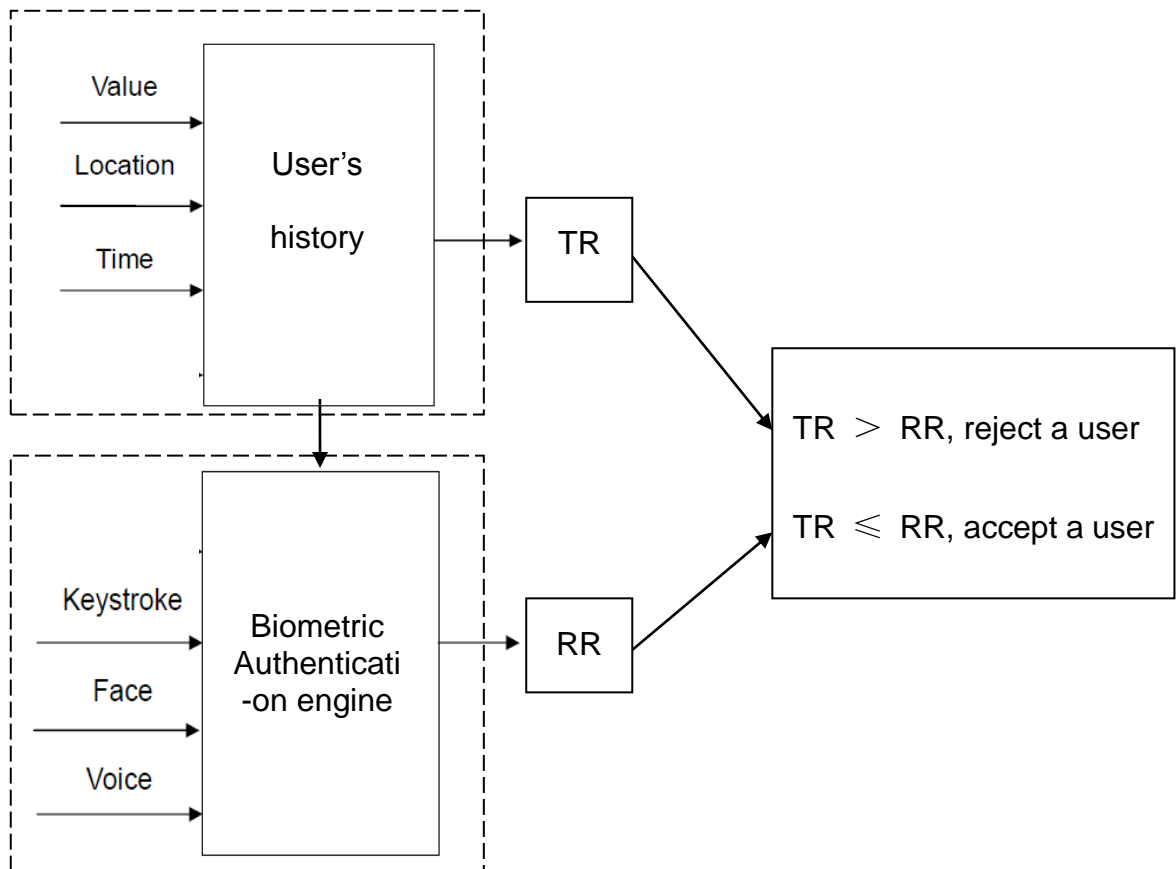


Figure 8.1: The decision tree of a smart m-commerce model

In this proposed model, when a transaction request is received, the transaction risk is determined by the transaction value, the distance from last transaction location and time interval between the last transactions. Any abnormal transaction will increase the transaction risk. For example, if a user purchased an item at location L1, after a short interval ( $t_1$  time) another transaction happened at location L2, and location L2 is far away from location L1, then the transaction risk will increase. By using a fuzzy inference model, the limitation of interval  $t_1$  and the distance between L1 and L2 is flexible; it can be easily readjusted by the trader or merchant in mobile commerce.

As shown in Figure 8.1, the recognition rate is determined by the authentication engine, when  $TR > RR$ , the user's transaction request will be rejected. If  $TR \leq RR$ , the transaction is successful.

## **8.2 A Fuzzy logic model used in m-commerce**

### **8.2.1 Why we need Fuzzy logic?**

In Chapter 3, a deterministic authentication model to support mobile commerce has been proposed. In this model, the transaction level is only determined by the transaction value, and the authentication process is always the same for each user. On the other hand, from the experimental results gained in Table 7.1, it can be found that when three biometric techniques are combined together the false rejection rate of the system could increase to an unacceptable range. The Table 7.3 illustrated that the FRR is 15.6% when users need to access authentication level 4. That means the system is likely to reject the correct user when they need access to the high transaction levels. In general, the model developed in previous chapter has three disadvantages:

1. The transaction risk is difficult to measure.
2. The accuracy rate of a biometric authentication system is dependent upon the environmental condition (such as lighting condition and background noise). The recognition sequence in this model is fixed, if the transaction happens in a poor lighting and a noisy place, it is hard for a user to pass the face recognition

and speaker recognition process.

3. The FRR is 15.6% at authentication level 4; the high FRR can seriously influence the usability of the system.

In order to solve these issues, a new mobile commerce model using fuzzy logic is proposed in this section. Fuzzy systems combine the high level flexibility and knowledge representation of conventional decision support and expert systems with the power and analytical depth of natural computing paradigms (Cox, 2005). Since Mamdani first used the fuzzy model to achieve an automatic control strategy in 1975 (Mamdani and Assilian, 1975), many more researchers (Roychowdhury and Wang, 1996; Jiang and Li, 1996; Sakly and Benrejeb, 2003) began to design and create fuzzy systems. Compared with a general control model, the fuzzy models are much more compact, less prone to error, and work well with missing some decision points (Cox, 2005). In this chapter, the main task of the proposed fuzzy model is to make the system have a high level of flexibility when using the biometric authentication techniques together.

## **8.2.2 Introduction of the algorithm**

### **8.2.2.1 Fuzzy subsets and membership functions**

The first step when building a fuzzy model is the fuzzy sets definition. In this section,  $x$  is an input value, and  $y$  is an output value. Each input and output value has a range. For example, in face recognition, the recognition result is in



the range of  $[0, 100\%]$ , every output value in this range constitute a universe of discourse  $X$ . A number of fuzzy subsets can be defined in the universe of discourse. As defined by Zadeh (Zadeh, 1965), a fuzzy subset of a set  $X$  is a map  $\mu_A: X \rightarrow [0,1]$  from  $X$  into the domain  $[0,1]$ .  $A$  is a fuzzy subset of  $X$ , and  $\mu_A$  is a membership function of subset  $A$ .

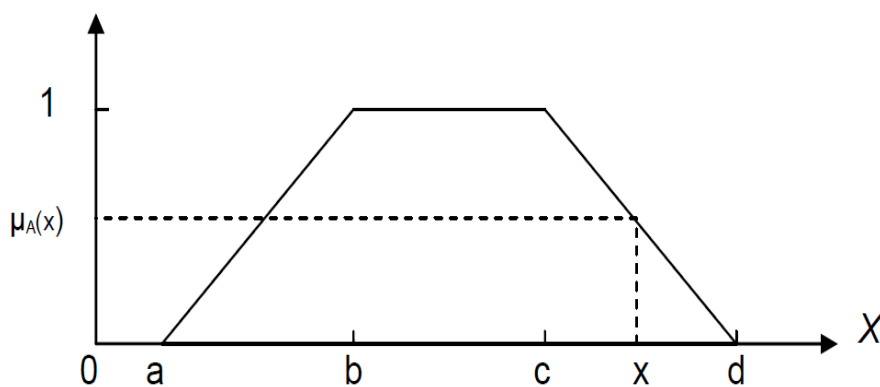


Figure 8.2: Fuzzy subsets and their membership functions

In order to define a number of fuzzy subsets in firstly, the universe of discourse  $X$  has to be divided into  $n$  intervals, each interval corresponds to a fuzzy subset. As shown in Figure 8.2, a fuzzy set  $A$  was defined, for any input value  $x$  there is a membership function  $\mu_A(x)$  which can characterise the degree of membership of  $x$ . It can use the following Equation to calculate the value of membership function.

$$\mu_A(x) = \begin{cases} \frac{x-a}{b-a} & \text{When } a < x < b \\ 1 & \text{When } b \leq x \leq c \\ \frac{d-x}{d-c} & \text{When } c < x < d \\ 0 & \text{Otherwise} \end{cases} \quad (1)$$

In Equation 1, when  $x$  is in an interval  $[b, c]$ , the value of membership function of  $x$  is 1 which means  $x$  is fully belongs to the fuzzy number  $A$ ; conversely, if the membership value is 0 that means  $x$  does not belong to  $A$ . When  $x$  is in the intervals  $(a, b)$  and  $(c, d)$  that means  $x$  partly belongs to  $A$ , and its membership can be calculated by using Equation 1.

#### **8.2.2.2. Control rules**

The fuzzy inference rule specifies a fuzzy relationship. It is an important part of a fuzzy model. The rules always use an “IF condition-THEN action” form. The collection of “if-then” rules that link a string input of linguistic variables (for example: the temperature is high) to an output value (for example: speed up the fan) (Chiu, 1997). Basically, the collection of rules can be divided into two different types: the first are conditional rules, which are executed only when the premise of the rule is true (Cox, 2005). For example, when the face recognition result is 94% similar rate, then the rule “If the face recognition result is high confidence, then accepts the user” is a conditional rule. Conversely, if the premise of the rule is false (for example: “If the face recognition result is low confidence, then reject the user”), it will be considered as an unconditional rule.

In a single output system, if there are 'k' input variables and 'n' rules, then

$$\text{Rule } j: \text{ IF } x_1 \in A_{1j} \text{ and, } \dots, \text{ and } x_k \in A_{kj} \text{ THEN } y \in B_j, \quad (j=1, \dots, n) \quad (2)$$

$A_{ij}$  is the fuzzy subset of universe of discourse  $X_i$ ,  $B_j$  is the fuzzy subset of universe of discourse  $Y$ . Each rule indicates a relationship between  $A_j$  and  $B_j$ , the rule  $j$  is:

$$R_j = A_j \cap B_j, \quad (3)$$

where  $A_j = A_{1j} \cap \dots \cap A_{kj}$ . According to the MAX-MIN fuzzy inference synthesis method which was proposed by Mamdani in the late 1970s (Mamdani and Assilian, 1975), when the rule premise contains multiple fuzzy propositions, they are combined with 'And' and 'Or' operators (Cox, 2005). An 'And' operator means take the minimum value of the degrees of membership propositions; and a 'Or' operator means take the maximum value of the degrees of membership propositions. Therefore, the membership function ' $\mu$ ' of rule  $j$  ( $R_j$ ) is:

$$\mu_{R_j}(x,y) = \min(\beta_j, \mu_{B_j}(y)), \quad (4)$$

In Equation (4),  $x = [x_1, x_2, \dots, x_k]$ ,  $\beta_j = \min[\mu_{A_{1j}}(x_1), \mu_{A_{2j}}(x_2), \dots, \mu_{A_{kj}}(x_k)]$  where  $\mu_{A_{ij}}(x_i)$  is the membership function value of  $x_i$  that belongs to a fuzzy subset  $A_{ij}$ .  $\mu_{B_j}(y)$  is a membership function of  $y$  that belongs to  $B_j$ . On the other hand, if there is a 'Or' relationship between these 'n' rules, therefore, the final fuzzy control rule is:

$$R = R_1 \cup R_2 \cup \dots \cup R_n \quad (5)$$

Using the 'Or' operator, the membership function of the final rule is:

$$\mu_{R_j}(x,y) = \max [\mu_{R_1}(x,y), \dots, \mu_{R_n}(x,y)]. \quad (6)$$

For any determined input value  $x_0$ , the membership function of  $y$  is:

$$\mu_{B'}(y) = \mu_{R(x_0,y)} \quad (7)$$

$B'$  in Equation (7) is a collection of fuzzy sets of  $y$  which can satisfy the conditional rules in Equation (5). The next step is to find out the matching rules for any input values and then use a defuzzification method to calculate an output value.

### **8.2.2.3. Defuzzification**

Defuzzification is actually a reduction process, which can produce a final result from the output fuzzy sets. There are a number of methods can be used to achieve the defuzzification, such as center of gravity, also called centroid (McGill and Ayyub, 2007; Broekhoven and Baets, 2006; Huang and Shen, 2003; Koczy and Hirola, 1993; Vass et al., 1992), Weighted average (Lee and Lim, 2008), Influence value defuzzification method (Madau, 1996), mean of maxima (Klein and Rio, 2005). The centroid method is the most prevalent and physically appealing of all the defuzzification methods (Sugenon, 1985), because it can make the most use of all the information that is contained in the final fuzzy sets (Cox, 2005). Mathematically, this method can be expressed as:

$$x = \frac{\sum_{i=1}^n d_i \times \mu_{d_i}}{\sum_{i=1}^n \mu_{d_i}} \quad (8)$$

In Equation (8),  $d_i$  is a domain value and  $\mu_{d_i}$  is its membership function. Using this defuzzification method, the fuzzy model can get a non-fuzzy value that best represents the possibility distribution of an inferred fuzzy control action (McGill and Ayyub, 2007).

### **8.2.3 Methodology**

#### **8.2.3.1 The fuzzy inference engine**

The fuzzy inference model described in this chapter is combined with two security mechanisms which were used in mobile commerce (see Figure 8.1). The main purpose of this model is to analyse the transaction risk and biometric authentication results, and then give a final decision at last. The details of a fuzzy inference engine are shown in Figure 8.3:

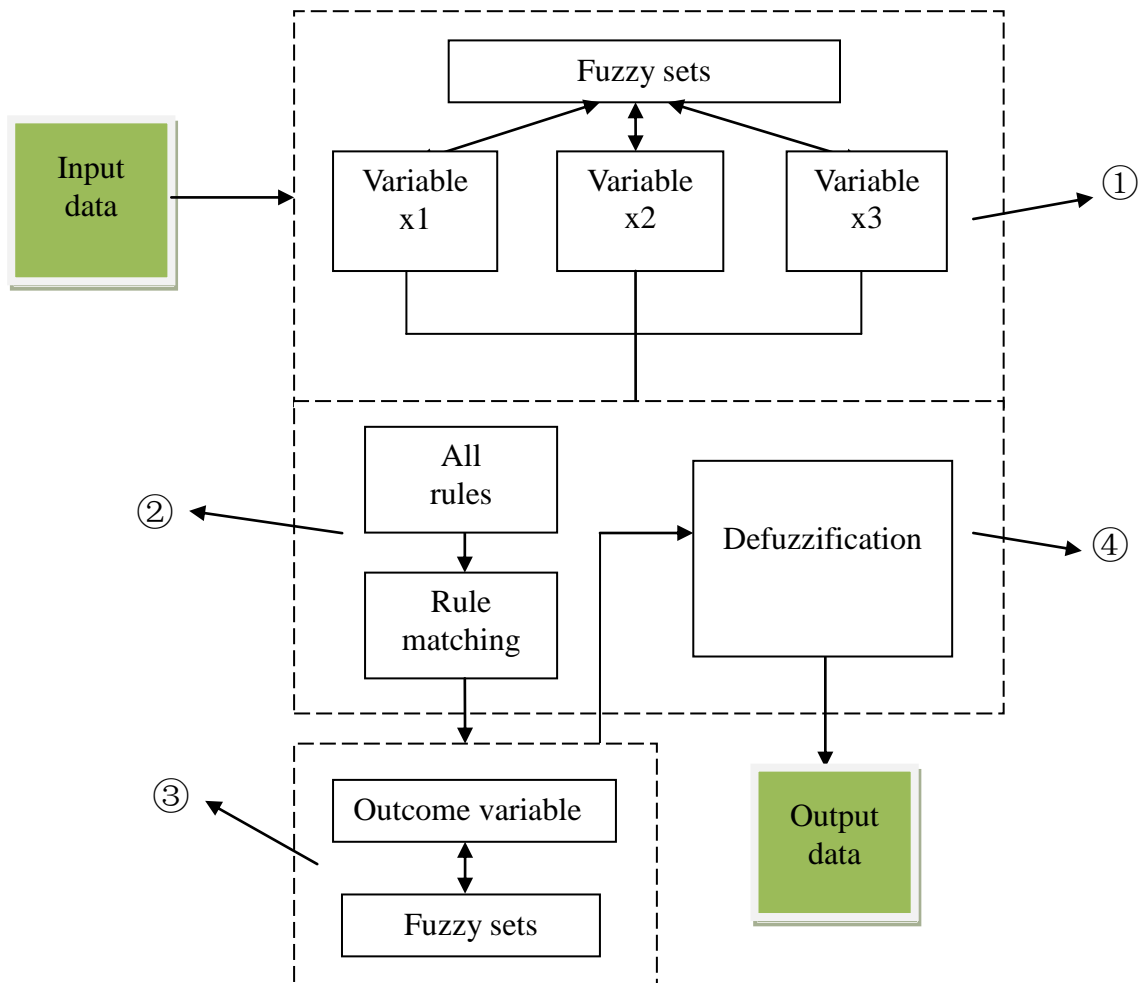


Figure 8.3: The fuzzy inference engine methods

As Figure 8.3 illustrates, a number of tasks have been completed:

- ① Fuzzification: defines a number of fuzzy sets in the input variables, and use the Fuzzification process to find out the membership value of the fuzzy sets.
- ② Set up a set of rules to specify a fuzzy relationship, like “the transaction value is low” or “the recognition result is low confidence.” According to the input values find out the conditional rules.

- ③ Obtain output fuzzy set and variables.
- ④ Defuzzifier the outcome fuzzy sets and generates an accurate output value.

### **8.2.3.2 The definition of input/output fuzzy subset**

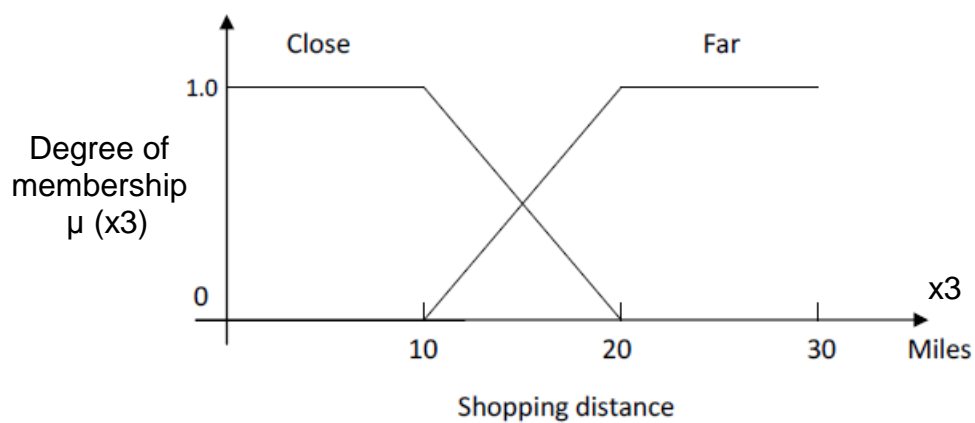
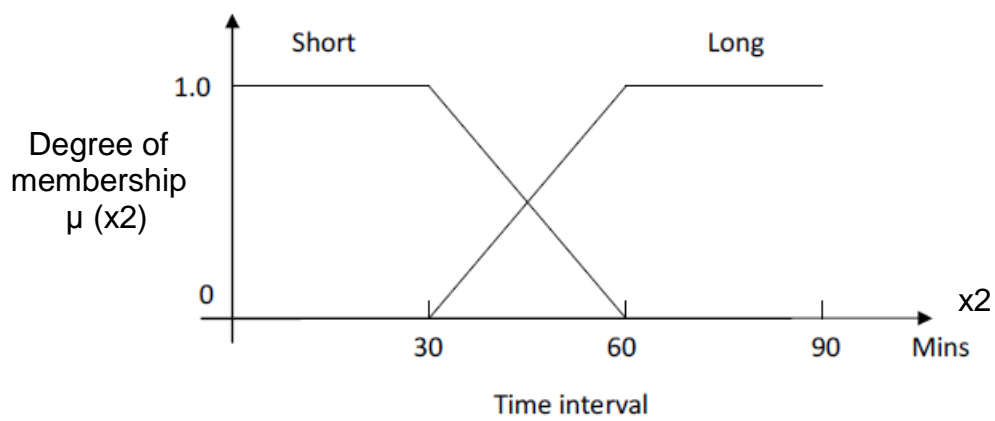
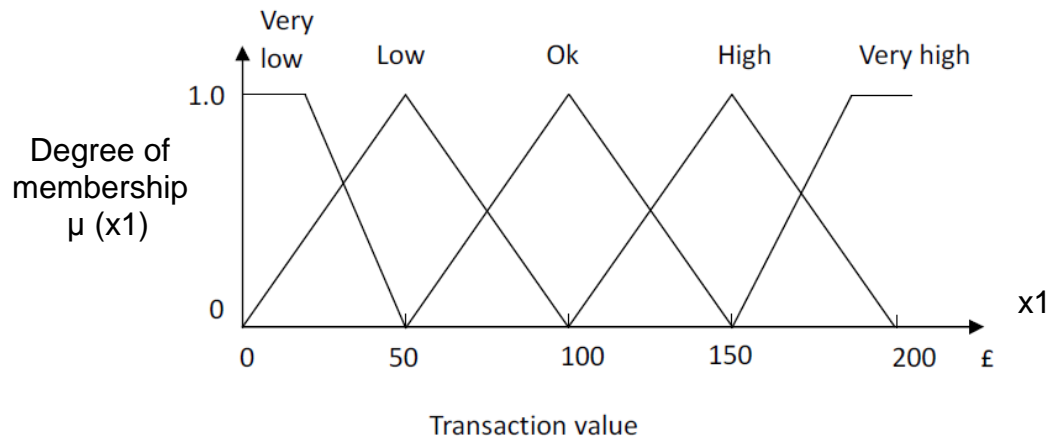
There are three input variables and one output variable in transaction risk determined mechanism for the mobile commerce model. The input variables are: transaction value, time interval from last transaction and distance from last transaction. The output variable is transaction risk which is expressed as a percentage. The fuzzy sets can be defined as shown in Table 8.1 and Figure 8.4.

Universe of discourse	Number of fuzzy subsets	Subsets name	Subsets definition
x1	5	Very low, low, ok, high, very high	[0, £50], [0, £100], [£50, £150], [£100, £200], [£150, £200],
x2	2	Short, Long	[0, 60mins], [30mins, 90mins]
x3	2	Close, Far	[0, 20miles], [10miles, 30 miles]
y	5	Very low, low, ok, high, very high	[0, 25%], [0, 50%], [25%, 75%], [50%, 100%], [75%, 100%]

Table 8.1: The details of fuzzy sets (transaction risk)

As Table 8.1 shows that the input variable x1 indicates the transaction value, x2

indicates the time interval and  $x_3$  indicates the distance from last shopping location. The output variable 'y' indicates the transaction risk.





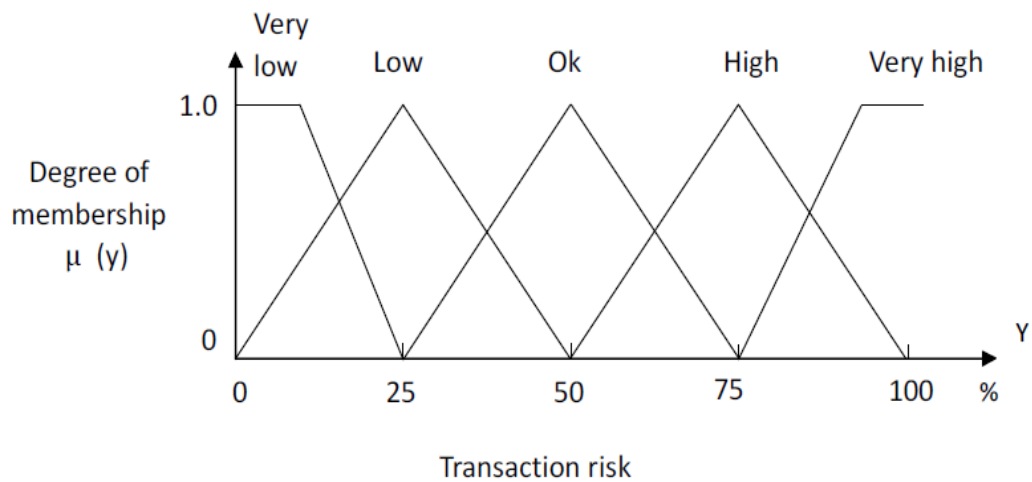


Figure 8.4: The definition of fuzzy sets (transaction risk)

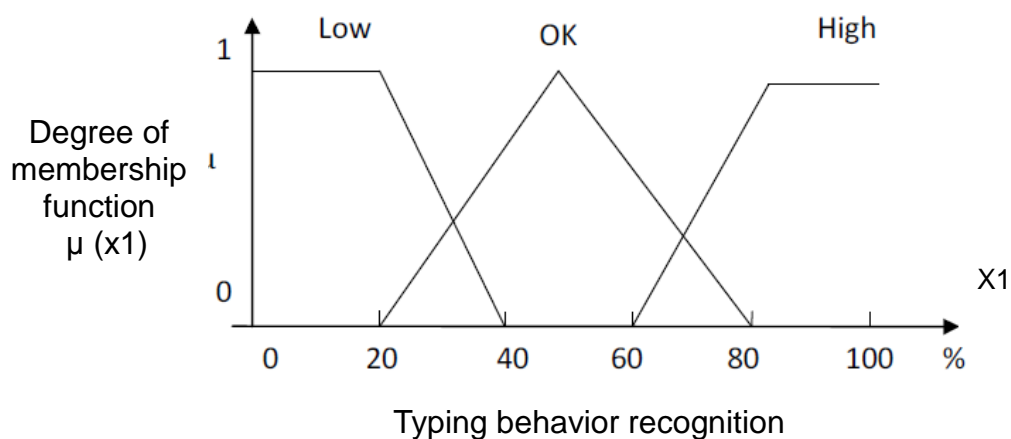
As shown in Figure 8.4, the membership functions for each of the input variable can be calculated by using Equation 1. The calculation details are given in Appendix V (6.1). In a fuzzy system, the type of the membership function can be context dependent and it is generally chosen arbitrarily according to the user experience (Mendel, 1995). In this research, the fuzzy sets are defined according to researcher's experience. In practice, the subsets definition are flexible, and it can be simply modified by the merchant or dealer.

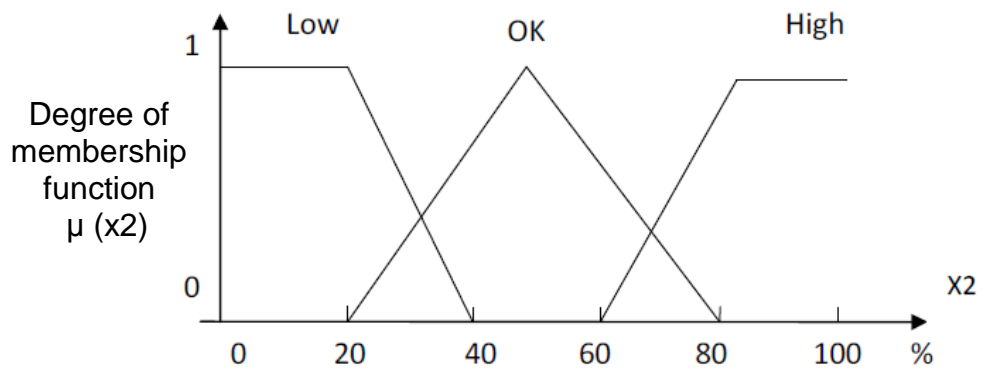
The biometric authentication mechanism also has three input variables and one output variable. The input variables are typing behaviour, face and speaker recognition results; and the output variable is recognition rate. Each of these input variables can be divided into three intervals; called: low confidence (low), medium confidence (ok) and high confidence (high). The definition method of fuzzy subset is shown as Table 8.2 and Figure 8.5:

Universe of discourse	Number of fuzzy subsets	Subsets name	Subsets definition
x1	3	low, ok, high	[0, 40%], [20%, 80%], [60%, 100%]
x2	3	low, ok, high	[0, 40%], [20%, 80%], [60%, 100%]
x3	3	low, ok, high	[0, 40%], [20%, 80%], [60%, 100%]
y	5	Very low, low, ok, high, very high	[0, 25%], [0, 50%], [25%, 75%], [50%, 100%], [75%, 100%]

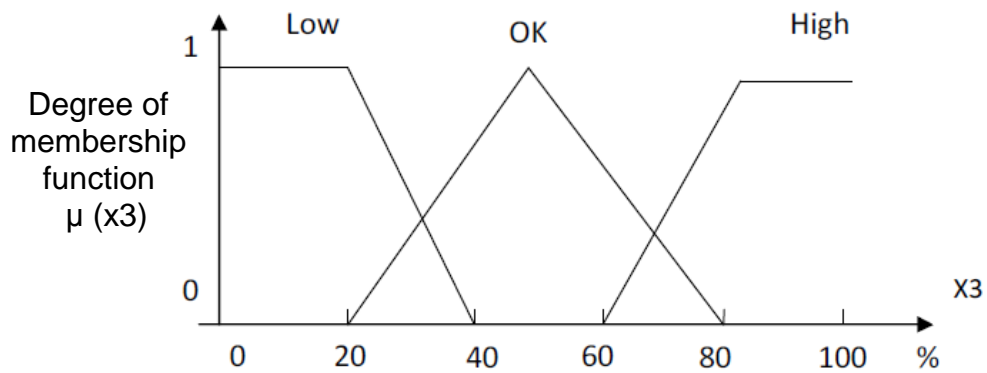
Table 8.2: The details of fuzzy sets (Recognition result)

Table 8.2, x1 indicates the typing behaviour recognition result, x2 indicates face recognition result and x3 indicates the speaker recognition result. Output 'y' indicates the recognition rate.

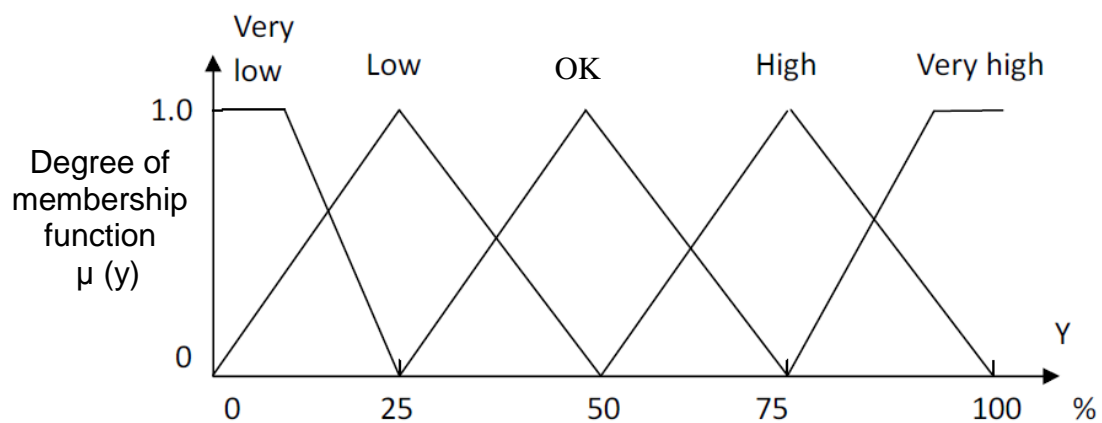




Face recognition



Speaker recognition



Recognition rate

Figure 8.5: The definition of fuzzy sets (Recognition rate)

The membership functions for each of the input variable and output result can be calculated by using Equation 1. The calculation details are given in Appendix V (6.2). As shown in Figure 8.5, three fuzzy sets were defined in each of the input universe of discourses. Particularly, in the multi-modal biometric authentication system, only face recognition mechanism can return a percentage recognition result. In this section, two different methods have been used to calculate an accuracy recognition result.

In the typing behaviour recognition system, it can use a maximum method to calculate the keystroke deviation, also considered as the ‘ $\alpha$ ’ value. For example, if a user claims to be someone and the input password involves ‘ $m$ ’ characters, there are ‘ $m$ ’ attempt duration data ( $AD_1, AD_2, \dots, AD_m$ ) and ‘ $m-1$ ’ attempt interval data ( $AI_1, AI_2, \dots, AI_{m-1}$ ) in the keystroke data. At the same time, there are ‘ $m$ ’ pattern duration data ( $PD_1, PD_2, \dots, PD_m$ ) and ‘ $m-1$ ’ pattern interval data ( $PI_1, PI_2, \dots, PI_{m-1}$ ) in the database. It can calculate the value of duration deviation ‘DD’ and interval deviation ‘ID’ by using these data:

$$\begin{aligned} &\text{When } AD_i > PD_i, \quad DD = \frac{AD_i}{PD_i} \\ &\text{Else, } DD = \frac{PD_i}{AD_i} \quad (\text{Where } 1 \leq i \leq m) \end{aligned}$$

Similarly, it can calculate the ‘ID’ value by comparing the interval data:

$$\begin{aligned} &\text{When } AI_j > PI_j, ID = \frac{AI_j}{PI_j} \\ &\text{Else, } ID = \frac{PI_j}{AI_j} \quad (\text{Where } 1 \leq j \leq m-1) \end{aligned}$$

The maximum value of ‘DD’ and ‘ID’ can be considered as the ‘ $\alpha$ ’ value of the input attempt.

$$\begin{aligned} &\alpha = \text{Max} [DD, ID] \\ &(\text{Where } 1 \leq i \leq m \text{ and } 1 \leq j \leq m-1) \end{aligned}$$

In the fuzzy inference model, the ‘ $\alpha$ ’ value will be normalised to a range of 0 to 100. For example, the range of ‘ $\alpha$ ’ value in this model is set as [6, 1], which means if the returned ‘ $\alpha$ ’ value is greater or equal to 6, the recognition result is 0 points; on the other hand, when the ‘ $\alpha$ ’ value is 1, that means the attempt keystroke data is a perfect match with the claimed user’s registered pattern, and the recognition result is 100 points.

In the speaker recognition system, according to the gained experimental results in Chapter 6, it can set up a scored mechanism: if the recognition result contains three or more “1”s, the system is high confidence to accept the user. Therefore, the result will be considered as similar rate 100%. Using the same principle, if result contains two “1”, the output value is 66%; if result contains one “1”, the input value is 33%; and the output value is 0 when no “1” exist in the recognition

result.

### **8.2.3.3 Fuzzy rules**

In the transaction risk determination mechanism, there are three input variables and each of the variables contains 5, 2 and 2 fuzzy sets. Therefore total  $5 \times 2 \times 2 = 20$  fuzzy rules are required to cover all the fuzzy relationships in this model. These rules can be called as a fuzzy associative memory (FAM) (Kong and Kosko, 1992) and are shown in Table 8.3.

Rule 1: If  $x_1$  = very low and  $x_2$  = short and  $x_3$  = close, then  $y$  = very low.

Rule 2: If  $x_1$  = very low and  $x_2$  = short and  $x_3$  = far, then  $y$  = low.

Rule 3: If  $x_1$  = very low and  $x_2$  = long and  $x_3$  = close, then  $y$  = very low.

Rule 4: If  $x_1$  = very low and  $x_2$  = long and  $x_3$  = far, then  $y$  = very low.

Rule 5: If  $x_1$  = low and  $x_2$  = short and  $x_3$  = close, then  $y$  = low.

Rule 6: If  $x_1$  = low and  $x_2$  = short and  $x_3$  = far, then  $y$  = ok.

Rule 7: If  $x_1$  = low and  $x_2$  = long and  $x_3$  = close, then  $y$  = low.

Rule 8: If  $x_1$  = low and  $x_2$  = long and  $x_3$  = far, then  $y$  = low.

Rule 9: If  $x_1$  = ok and  $x_2$  = short and  $x_3$  = close, then  $y$  = ok.

Rule 10: If  $x_1$  = ok and  $x_2$  = short and  $x_3$  = far, then  $y$  = high.

Rule 11: If  $x_1$  = ok and  $x_2$  = long and  $x_3$  = close, then  $y$  = ok.

Rule 12: If  $x_1$  = ok and  $x_2$  = long and  $x_3$  = far, then  $y$  = ok.

Rule 13: If  $x_1$  = high and  $x_2$  = short and  $x_3$  = close, then  $y$  = high.

Rule 14: If  $x_1$  = high and  $x_2$  = short and  $x_3$  = far, then  $y$  = very high.

Rule 15: If  $x_1$  = high and  $x_2$  = long and  $x_3$  = close, then  $y$  = high.

Rule 16: If  $x_1$  = high and  $x_2$  = long and  $x_3$  = far, then  $y$  = high.

Rule 17: If  $x_1$  = very high and  $x_2$  = short and  $x_3$  = close, then  $y$  = very high.

Rule 18: If  $x_1$  = very high and  $x_2$  = short and  $x_3$  = far, then  $y$  = very high.

Rule 19: If  $x_1$  = very high and  $x_2$  = long and  $x_3$  = close, then  $y$ = very high.

Rule 20: If  $x_1$  = very high and  $x_2$  = long and  $x_3$  = far, then  $y$ = very high.

Table 8.3: The fuzzy rules (Transaction risk)

In the biometric authentication mechanism, there are three input variables and all of the variables have 3 fuzzy sets. Therefore, there are total  $3 \times 3 \times 3 = 27$  fuzzy rules shown in Table 8.4:

Rule 1: If  $x_1$  = low and  $x_2$  = low and  $x_3$  = low then  $y$ = very low.

Rule 2: If  $x_1$  = low and  $x_2$  = low and  $x_3$  = ok then  $y$ = very low.

Rule 3: If  $x_1$  = low and  $x_2$  = low and  $x_3$  = high then  $y$ = low.

Rule 4: If  $x_1$  = low and  $x_2$  = ok and  $x_3$  = low then  $y$ = very low.

Rule 5: If  $x_1$  = low and  $x_2$  = ok and  $x_3$  = ok then  $y$ = ok.

Rule 6: If  $x_1$  = low and  $x_2$  = ok and  $x_3$  = high then  $y$ = high.

Rule 7: If  $x_1$  = low and  $x_2$  = high and  $x_3$  = low then  $y$ = low.

Rule 8: If  $x_1$  = low and  $x_2$  = high and  $x_3$  = ok then  $y$ = high.

Rule 9: If  $x_1$  = low and  $x_2$  = high and  $x_3$  = high then  $y$ = high.

Rule 10: If  $x_1$  = ok and  $x_2$  = low and  $x_3$  = low then  $y$ = very low.

Rule 11: If  $x_1$  = ok and  $x_2$  = low and  $x_3$  = ok then  $y$ = ok.

Rule 12: If  $x_1$  = ok and  $x_2$  = low and  $x_3$  = high then  $y$ = high.

Rule 13: If  $x_1$  = ok and  $x_2$  = ok and  $x_3$  = low then  $y$ = ok.

Rule 14: If  $x_1$  = ok and  $x_2$  = ok and  $x_3$  = ok then  $y$ = ok.

Rule 15: If  $x_1$  = ok and  $x_2$  = ok and  $x_3$  = high then  $y$ = high.

Rule 16: If  $x_1$  = ok and  $x_2$  = high and  $x_3$  = low then  $y$ = ok.

Rule 17: If  $x_1$  = ok and  $x_2$  = high and  $x_3$  = ok then  $y$ = high.

Rule 18: If  $x_1$  = ok and  $x_2$  = high and  $x_3$  = high then  $y$ = very high.

Rule 19: If  $x_1$  = high and  $x_2$  = low and  $x_3$  = low then  $y$ = low.

- Rule 20: If  $x_1 = \text{high}$  and  $x_2 = \text{low}$  and  $x_3 = \text{ok}$  then  $y = \text{high}$ .
- Rule 21: If  $x_1 = \text{high}$  and  $x_2 = \text{low}$  and  $x_3 = \text{high}$  then  $y = \text{high}$ .
- Rule 22: If  $x_1 = \text{high}$  and  $x_2 = \text{ok}$  and  $x_3 = \text{low}$  then  $y = \text{high}$ .
- Rule 23: If  $x_1 = \text{high}$  and  $x_2 = \text{ok}$  and  $x_3 = \text{ok}$  then  $y = \text{high}$ .
- Rule 24: If  $x_1 = \text{high}$  and  $x_2 = \text{ok}$  and  $x_3 = \text{high}$  then  $y = \text{very high}$ .
- Rule 25: If  $x_1 = \text{high}$  and  $x_2 = \text{high}$  and  $x_3 = \text{low}$  then  $y = \text{high}$ .
- Rule 26: If  $x_1 = \text{high}$  and  $x_2 = \text{high}$  and  $x_3 = \text{ok}$  then  $y = \text{very high}$ .
- Rule 27: If  $x_1 = \text{high}$  and  $x_2 = \text{high}$  and  $x_3 = \text{high}$  then  $y = \text{very high}$ .

Table 8.4: The fuzzy rules (Recognition result)

Generally, the membership functions and fuzzy rules in a fuzzy system are usually built by human experts or experienced users (Hong and Lee, 1996). In this chapter, a 'Fuzzy Logic Controller' application has been developed and the membership functions and fuzzy rules are predefined by the researcher. However, according to the principle of fuzzy logic, if the membership functions and fuzzy rules are not accurately defined or the fuzzy system cannot perform well, administrator can modify the 'Variables' and 'Rules' documents according to actual demand in mobile commerce. This work can be achieved by using the definition function in the application (The 'Fuzzylogic controller' application can be found in Appendices III ).

#### **8.2.4 Example tests**

In order to test the performance of the fuzzy inference model, some transaction values and recognition results have been assumed. In the first example, the



transaction details are shown in Table 8.5.

Input variables	Transaction risk	Recognition rate
X1	£80	$\alpha = 2.5$ (70)
X2	5 mins	94% (94)
X3	30 miles	One "1" (33)

Table 8.5: Input values

According to the model proposed in Figure 8.1, there are two steps in this example:

### **Step 1: Transaction risk determination**

According to the input values and FAM, there are two true (conditional) rules are applied for this set of input values in the transaction risk determined mechanism:

Rule 6:  $x_1 = \text{low}$ ,  $x_2 = \text{short}$ ,  $x_3 = \text{far}$ , then  $y = \text{ok}$ .

Rule 10:  $x_1 = \text{ok}$ ,  $x_2 = \text{short}$ ,  $x_3 = \text{far}$ , then  $y = \text{high}$ .

Using the calculation methods which are given in Appendix V (6.1) and (6.2), it can calculate the membership of each input value and output result. For example, when  $x_1 = 80$ , the membership function of  $x_1$  can be calculated by using the following Equation:

$$\mu_{R6}(x1) = \begin{cases} \frac{x1-0}{50-0} & \text{When } 0 < x1 < 50 \\ 1 & \text{When } x1=50 \\ \frac{100-x1}{100-50} & \text{When } 50 < x1 < 100 \\ 0 & \text{Otherwise} \end{cases}$$

When  $x1=80$ ,  $\mu_{R6}(x1) = \frac{100-80}{100-50} = 0.4$ . Similarly, the membership functions

of other input values can be calculated by using the Equation which can be found in Appendix V (6.1) and (6.2).

Rules		X1=80	X2=5	X3=30	Y
Rule 6	Description	Value is low	Time interval is short	Distance is far	Transaction risk is ok
	$\mu$	[0.4]	[1.0]	[1.0]	[0.4]
Rule 10	Description	Value is ok	Time interval is short	Distance is far	Transaction risk is high
	$\mu$	[0.6]	[1.0]	[1.0]	[0.6]

Table 8.6: The output fuzzy sets after conditional rules are executed

Using the Min-Max inference method, see Equation (4) and (6), it can get the outcome fuzzy sets after executing Rule 6 and Rule 10. According to the Equation (4), the membership of output fuzzy sets can be calculated by taking

the minimum of three truth membership values of the input fuzzy sets.

$$\begin{aligned}\mu_{R6}(Y) &= \min [ \mu_{R6}(x1), \mu_{R6}(x2), \mu_{R6}(x3) ] \\ &= 0.4\end{aligned}$$

Therefore, the membership value of Y for rule 6 is 0.4. The details of inference processes are shown in Figure 8.6.

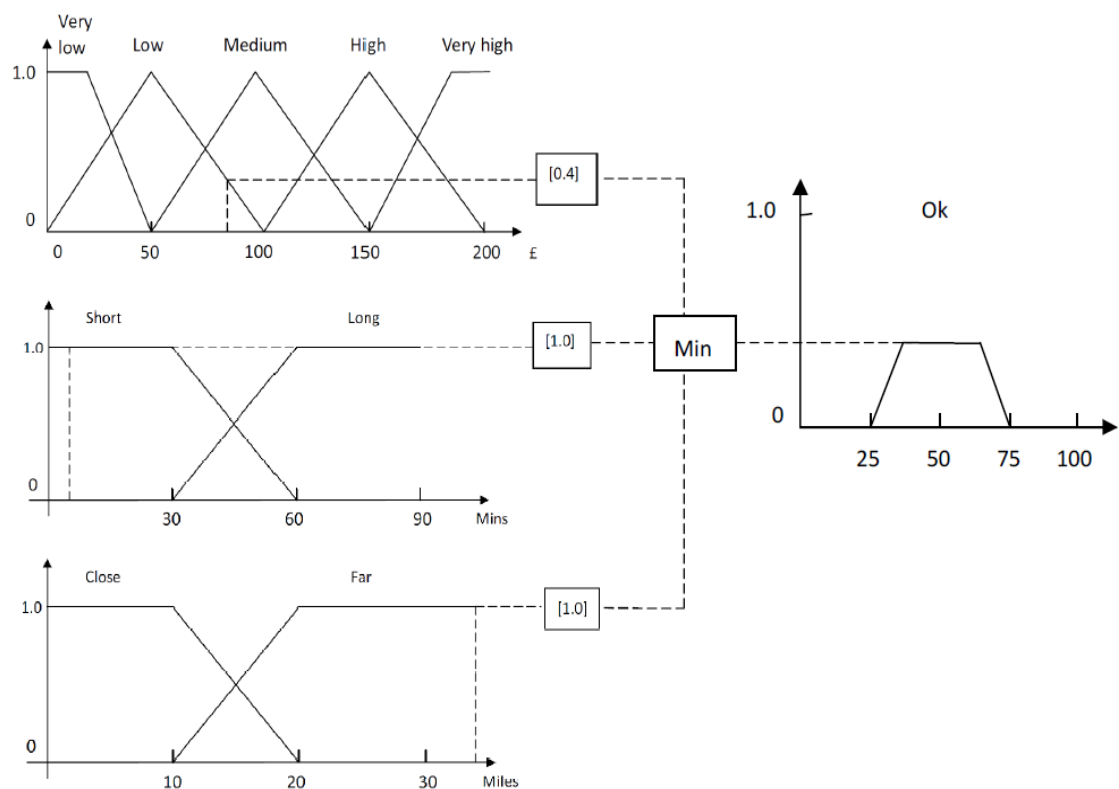


Figure 8.6: The gained outcome fuzzy set after execute Rule 6

Similarly, the membership value of Y for rule 10 can be calculated by the following process.

$$\begin{aligned}\mu_{R10}(Y) &= \min [ \mu_{R10}(x1), \mu_{R10}(x2), \mu_{R10}(x3) ] \\ &= 0.6\end{aligned}$$

The details of inference processes are shown in Figure 8.7.

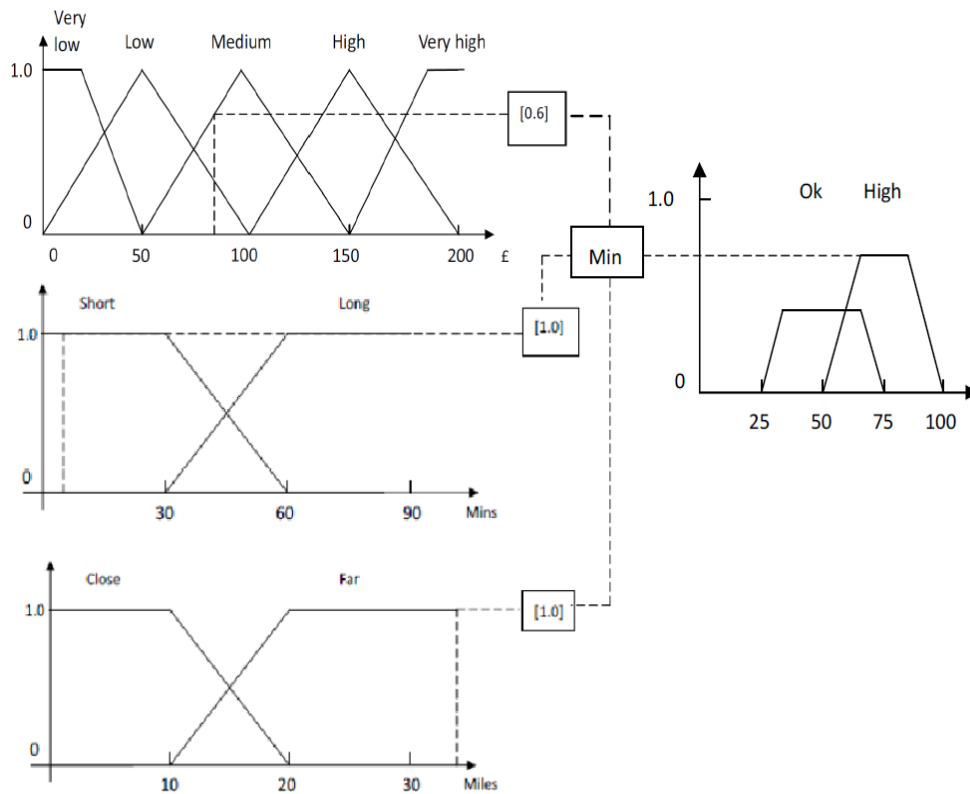


Figure 8.7: The gained outcome fuzzy set after execute Rule 10

As Figure 8.7 shows, the final output fuzzy sets can be gained by use a union operation, see Equation (6). Therefore,

$$\mu_{R}(x,y) = \max [ \mu_{R6}(x,y), \mu_{R10}(x,y) ]$$

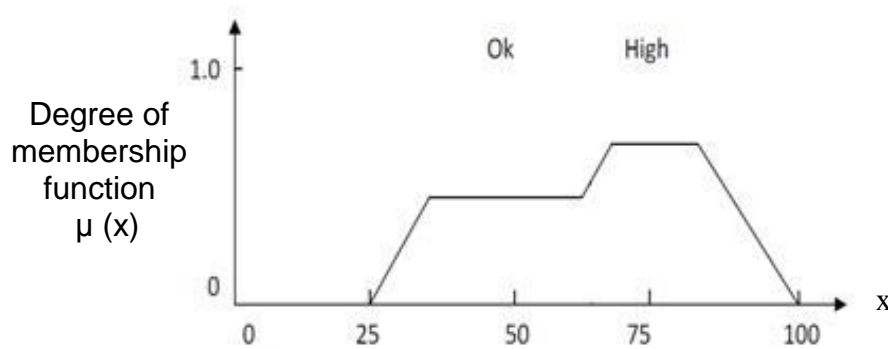


Figure 8.8: The output result of Step 1

Subsequently, it can use the center of gravity method (see Equation (8)) to calculate the defuzzified output result.

$$\begin{aligned}
 Y1 &= \frac{\sum_{i=25}^{100} di \times \mu di}{\sum_{i=25}^{100} \mu di} \\
 &= \frac{25 \times \mu_{25} + 26 \times \mu_{26} + \dots + 100 \times \mu_{100}}{\mu_{25} + \mu_{26} + \dots + \mu_{100}} \\
 &= 64.2
 \end{aligned}$$

The output result from the inference engine is 64.2, which means the risk of this transaction is 64.2%. The calculation code and application are given in Appendix III. The implement of the model on computer side is shown in Figure 8.9:

The screenshot shows a software interface for a Fuzzy Logic Controller. It has four tabs: Configuration, Variables, Rules, and Results. The Results tab is active. The interface is divided into several sections:

- Inputs:** A text box contains the values "80, 5, 30". An "OK" button is next to it.
- Output:** A text box displays "Y1 : 64.2241379310345". A "Clear" button is next to it.
- Report:** A table-like structure showing the following data:
 

Input values	Fuzzy Inputs	Conditional rules	Fuzzy Output
X1 : 80	X1		<b>Y1</b>
X2 : 5	Low:0.4	Rule :6	OK : 0.4
X3 : 30	OK:0.6	Rule :10	High : 0.6
	X2		
	Short:1		
	X3		
	Far:1		

Figure 8.9: The Fuzzy Logic Controller Interface

## Step 2: Recognition rate determination

Similar with the transaction risk determined mechanism, the biometric authentication input values and their membership are shown in Table 8.7:

	Input values	Degree of membership		
		Low	Ok	High
X1	$\alpha = 2.5$	/	0.33	0.5
X2	94%	/	/	1
X3	33%	0.35	0.4	/

Table 8.7: Input values and their membership

Examining the FAM in recognition result determined model, there are four true (conditional) rules:

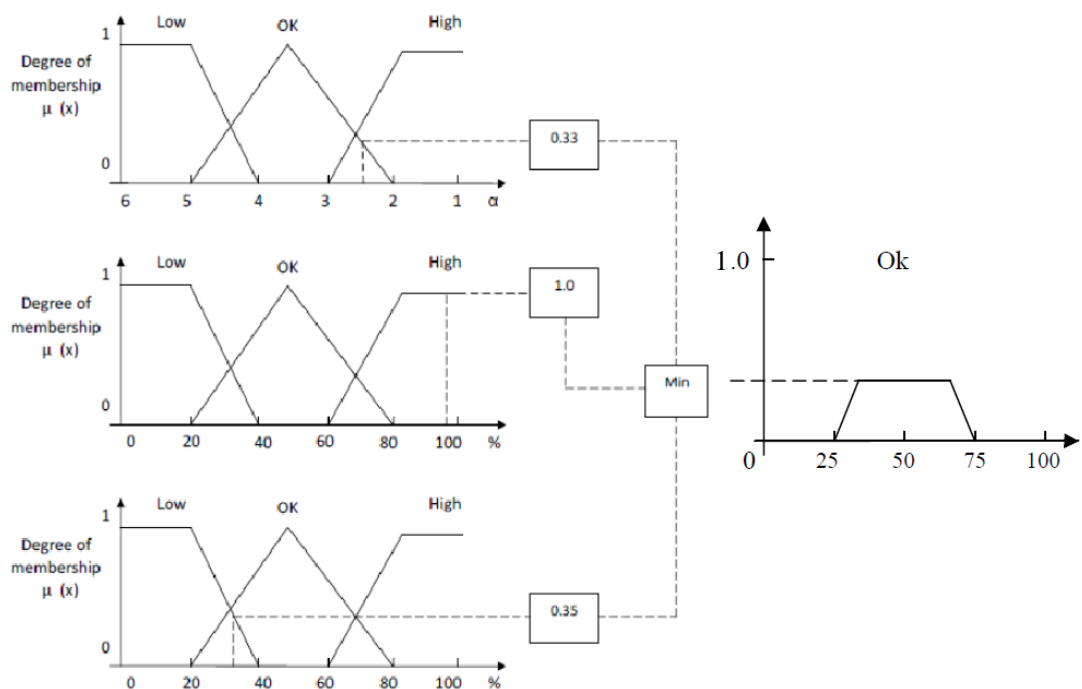
R16:  $x_1=ok$ ,  $x_2=high$  and  $x_3=low$ , then  $Y=ok$

R17:  $x_1=ok$ ,  $x_2=high$  and  $x_3=ok$ , then  $Y= high$

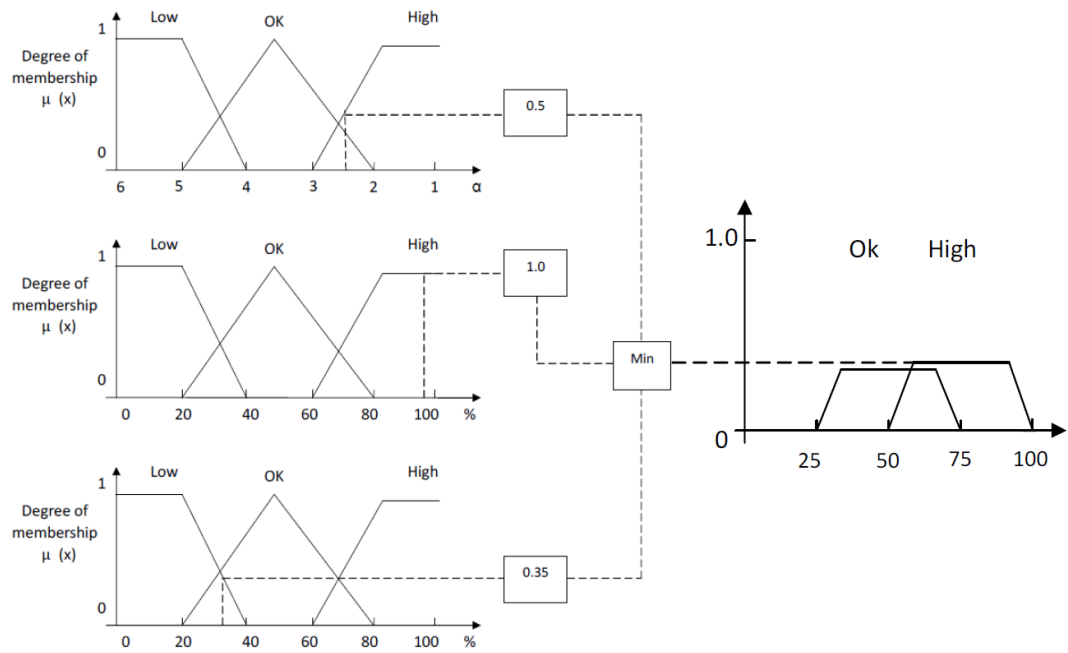
R25:  $x_1= high$ ,  $x_2=high$  and  $x_3=low$ , then  $Y= high$

R26:  $x_1= high$ ,  $x_2=high$  and  $x_3=ok$ , then  $Y=very high$

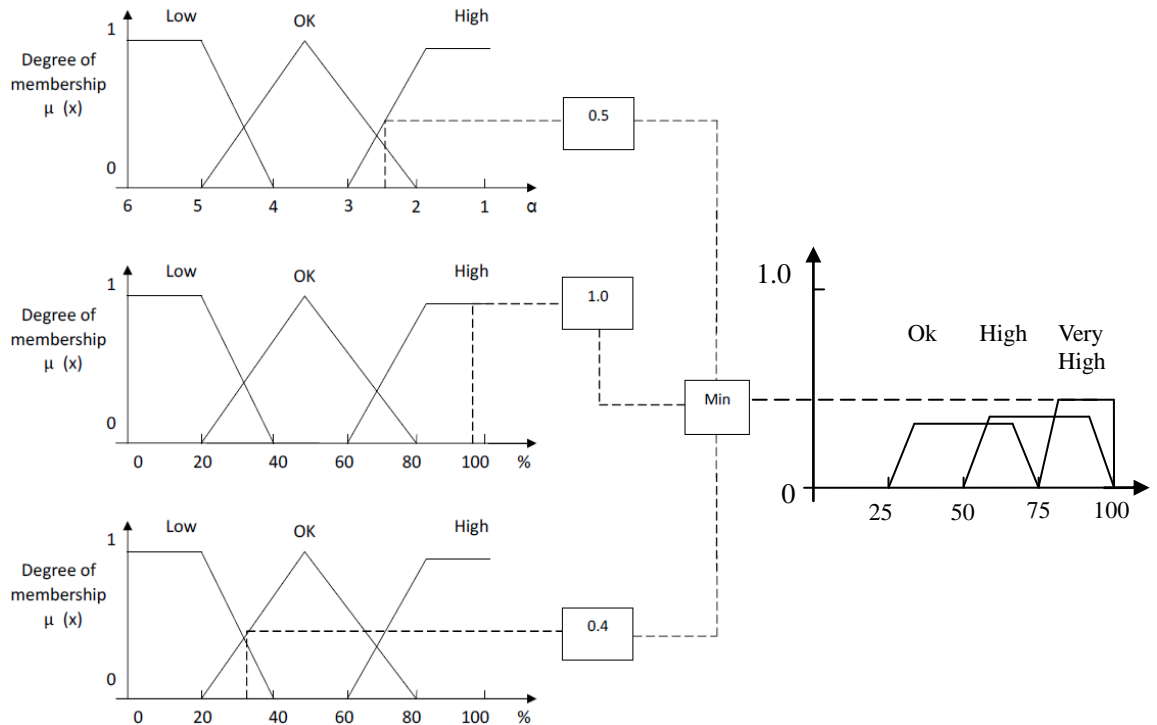
The outcome fuzzy sets can be gained after executing these four conditional rules, and the processes are shown in Figure 8.10.



First conditional rule (R16)



Second conditional rule (R17, R25)



Fourth conditional rule (R26)

Figure 8.10: The final outcome fuzzy set



In conditional rules 17 and 25, both of the output fuzzy set is 'high'. When  $\mu_{R17}=0.33$ , and  $\mu_{R25}=0.35$ , according to the Equation (6),

$$\mu_R(x,y) = \max [ \mu_{R16}(x,y), \mu_{R17}(x,y), \mu_{R25}(x,y), \mu_{R26}(x,y) ]$$

Therefore, the output fuzzy membership of Second conditional rule is 0.35 which was shown as in Figure 8.10. And the final output result for Step 2 is shown in Figure 8.11.

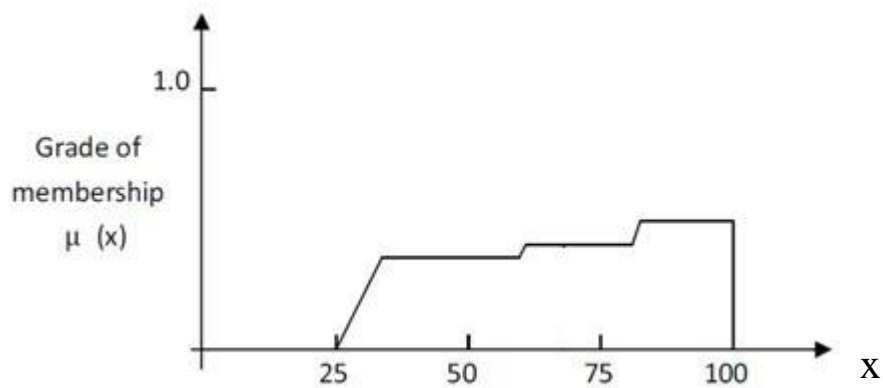


Figure 8.11: The output result of Step 2

Using the center of gravity method; it can calculate the defuzzified output result as follow:

$$\begin{aligned} Y1 &= \frac{\sum_{i=25}^{100} di \times \mu di}{\sum_{i=25}^{100} \mu di} \\ &= \frac{25 \times \mu_{25} + 26 \times \mu_{26} + \dots + 100 \times \mu_{100}}{\mu_{25} + \mu_{26} + \dots + \mu_{100}} \\ &= 68.4 \end{aligned}$$

The calculation code is given in Appendix III. The interface of fuzzy inference model is shown in Figure 8.12:

The screenshot shows a software window titled "Fuzzy Logic Controller" with a menu bar (File, Predefined Tests) and a tabbed interface (Configuration, Variables, Rules, Results). The "Results" tab is active, displaying the following information:

**Inputs:** A text box contains "70,94,33". An "OK" button is next to it.

**Output:** A text box displays "Y1 : 68.3673469387755". A "Clear" button is next to it.

**Report:** A table-like structure showing the inference process:

Input values	Fuzzy Inputs	Conditional rules	Fuzzy Output
X1 : 70	X1		<b>Y1</b>
X2 : 94	OK:0.3333333333333333	Rule :16	OK : 0.3333333333333333
X3 : 33	High:0.5	Rule :17	High : 0.35
	X2	Rule :25	Very High :
	High:1	Rule :26	0.4333333333333333
	X3		
	Low:0.35		
	OK:0.4333333333333333		

Figure 8.12: The Fuzzy Logic Controller Interface

According to the security mechanism which was set in Figure 8.1, the final decision is:

If Recognition rate (68.4%) > Transaction risk (64.2%),  
then the transaction is successful.

## **8.3 Experimental work**

### **8.3.1 Aim and objectives of the experiments**

There are two aims of the experiments: experiment 1 aims to test the developed fuzzy logic software. Experiment 2 aims to compare the fuzzy logic based model with the deterministic model which was discussed in Chapter 7. The objectives of experiment 1 are to evaluate and test the software written to implement the fuzzy system. Experiment 2 is designed to find out the accuracy rate of the developed fuzzy logic based multi-modal system, and also to ascertain whether the fuzzy logic based multi-modal system can reduce the influence of environment on the authentication performance.

### **8.3.2 Methods**

A fuzzy logic inference application has been developed for the experiments. There are three functions of this application: (1) define fuzzy sets and membership function, (2) define the control rules, and (3) calculate the output result. The interfaces are shown in Figure 8.13:

ConfigurationVariablesRulesResults

### 1. Input/Output Variables

X1  
X2  
X3  
Outputs

### 2. Set up Rules

IF

X1 is Low
X2 is Low

Then

Y1 is Very Low

### 3. Existing Rules

IF X1 is Low And X2 is Low And X3 is Low Then Y1 is Very Low  
IF X1 is Low And X2 is Low And X3 is OK Then Y1 is Low  
IF X1 is Low And X2 is Low And X3 is High Then Y1 is OK  
IF X1 is Low And X2 is OK And X3 is Low Then Y1 is Low  
IF X1 is Low And X2 is OK And X3 is OK Then Y1 is OK  
IF X1 is Low And X2 is OK And X3 is High Then Y1 is High  
IF X1 is Low And X2 is High And X3 is Low Then Y1 is OK

### 1. Variable details

Variable Type  
Input

Variable Name  
X1

Range  
0, 100

### 2. List of membership function

Low OK High

### 3. Membership function details

Name  
Low

Type  
Trapmf

Parameters  
0, 0, 20, 40

Change Save

x1: Typing, x2: Face, x3: Voice

Inputs

84,94,33

OK

Output

Y1 : 80.70162863569

Clear

### Report

Input values	Fuzzy Inputs	Conditional rules	Fuzzy Output
X1 : 84	X1	Rule :25	Y1
X2 : 94	High:1	Rule :26	High : 0.35
X3 : 33	X2		Very High : 0.4333333333333333
	High:1		
	X3		
	Low:0.35		
	OK:0.4333333333333333		

Figure 8.13: Fuzzy inference application interfaces

As shown in Figure 8.13, the fuzzy sets, membership functions and control rules in the fuzzy logic system can be modified through the software. In this section, all the experimental results are gained from the fuzzy inference application.

### (1) Experiment 1

The task of experiment 1 is to find out the relationship between input variables and the output results from fuzzy inference engine. There are three input variables:  $x_1$  indicates typing behaviour recognition result,  $x_2$  indicates face recognition result, and  $x_3$  indicates face recognition result. In this experiment, two constant input values ( $x_1$  and  $x_3$ ) and one variable input value ( $x_2$ ) are used to test the developed software, to do so; a figure can be used to display the relationship between input variables and the output results.

The experiment is carried out in the following way: 33 groups of biometric recognition results were input to the fuzzy inference engine. The first 11 groups of data involve two randomly chosen high recognition results:  $x_1 = 80$ ,  $x_3 = 100$  and other 11 face recognition results  $x_2 = 0, 10, 20, \dots, 90, 100$ . The blue line in Figure 8.14 shows the output results returned from the fuzzy inference engine. A second 11 groups' data preset two medium recognition results ( $x_1 = 60$ ,  $x_3 = 66$ ) and 11 face recognition results. The Red line shows the output results. The rest 11 groups' data preset two low recognition results ( $x_1 = 10$ ,  $x_3 = 33$ ) and 11 face recognition results. The green line shows the output results. The details of input variables are shown in Table 8.8 and output results are

shown in Figure 8.14.

Input variables			Output result
x1 (Typing behaviour recognition result)	x2 (face recognition result)	x3 (speaker recognition result)	
80 (High)	0 -- 100	100 (High)	Blue line
60 (Medium)	0 -- 100	66 (Medium)	Red line
10 (Low)	0 -- 100	33 (Low)	Green line

Table 8.8: Input variables

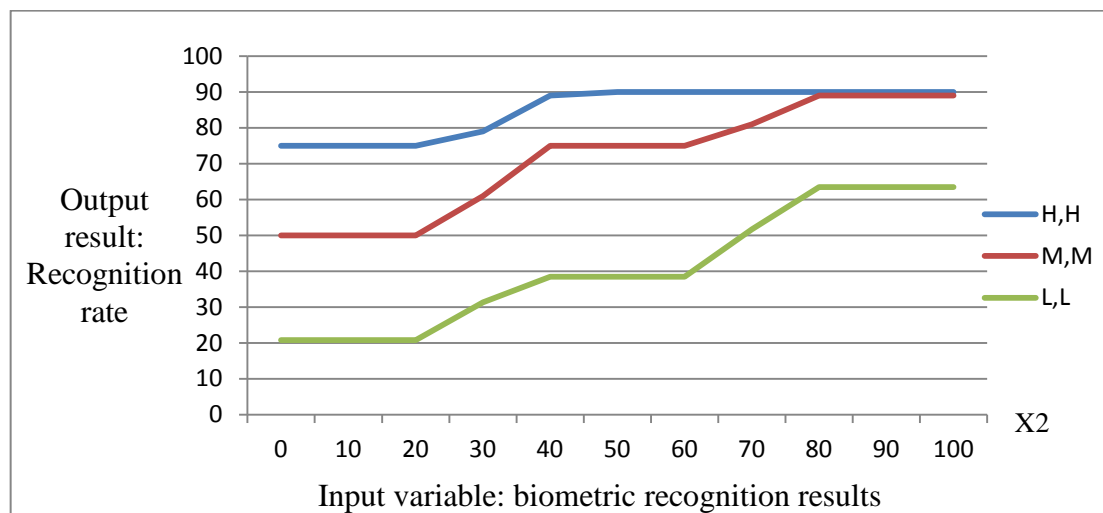


Figure 8.14: Output results after using fuzzy logic method in multi-modal biometric authentication system

Figure 8.14 displays the relationship between input variables and output results. Firstly, as the figure shows, whether the input variables are high, medium or low, the fuzzy inference engine can analysis all three biometric authentication results, and makes a final decision by using the reasonable result. The authentication

results of the multi-modal biometric system are truly reflected by the fuzzy logic based model. Secondly, when one input recognition rate is 0, the fuzzy inference engine can return a valuable output result. That means the multi-modal biometric system works well even with missing some decision points. The software written gives an accurate implementation of the fuzzy system, and by using the fuzzy logic method in biometric authentication system, the authentication mechanism is becoming more robust, and the output results are reasonable.

## (2) Experiment 2

The first experiment demonstrated that the implementation of the fuzzy inference model gives robust results processing the input data and then calculating a final decision. Within the second experiment, in order to evaluate the authentication performance of fuzzy logic based smart system, a simulation test was arranged. In this experiment: 6 groups of biometric authentication results were randomly selected and input to the fuzzy logic inference software developed. Each set of data contains 10 recognition results. The experimental interface is shown in Figure 8.15 and the details of input variables are shown in Table 8.9.

X1

0,0,0,0,7,15,16,20,22,26

X2

0,0,0,0,0,1,2,6,11,21

X3

0,0,0,0,0,0,0,0,0,0

Input Variables

26,21,0

OK

Output

Y1 : 18.5078050766933

Clear

Counting left: 0

Result details

Inputs

X1 : 26

X2 : 21

X3 : 1E-07

Fuzzy Inputs

X1

Low:0.7

OK:0.2

X2

Low:0.95

OK:0.0333333333333333

Conditional rules

Triggered Rules

Rule :1

Rule :4

Rule :10

Rule :13

Fuzzy Output

Y1

Very Low : 0.7

Low : 0.2

OK : 0.0333333333333333

Summary:

Recognition rate<17: 990 times, 17 <= Recognition rate < 50: 10 times, 50 <= Recognition rate < 75: 0 times, Recognition rate >= 75: 0 times

Figure 8.15: Fuzzy inference application interface

Unauthorised users	Group 1	Typing recognition results (x1)	0, 0, 0, 0, 7, 15, 16, 20, 22, 26
	Group 2	Face recognition results (x2)	0, 0, 0, 0, 0, 1, 2, 6, 11, 21
	Group 3	Speaker recognition results (x3)	0, 0, 0, 0, 0, 0, 0, 0, 0, 0
Authorised users	Group 4	Typing recognition results (x1)	0, 9, 68, 77, 80, 84, 84, 85, 86, 88
	Group 5	Face recognition results (x2)	29, 77, 80, 80, 88, 94, 94, 94, 94, 94
	Group 6	Speaker recognition results (x3)	0, 33, 66, 66, 66, 66, 66, 100, 100, 100

Table 8.9: The details of experimental results



As shown in Table 8.9, the first 3 groups of biometric recognition results were gained from 10 unauthorised users, each group involves 10 typing behaviour recognition results, 10 face recognition results, and 10 speaker recognition results. Other three groups of results were gained from 10 authorised users; each group also involves 10 recognition results. When the recognition results are input to the fuzzy inference software, the first three groups of input variables have  $10 \times 10 \times 10 = 1000$  combinations. The software gives us 1000 recognition rates for unauthorised users. Similarly, the software gives other 1000 recognition rates for authorised users. In practice, the accuracy rate of a fuzzy logic based security system is generally difficult and expensive to measure, often requiring significant time and analytical resources to make defensible quantitative statements about security (McGill and Ayyub, 2007). Therefore, three transactions have been simulated in this experiment:

Transaction 1, the user purchases a low value item (worth £20) in Dundee, the authentication level (AL) in a deterministic model is 1, and the transaction risk calculated by the fuzzy inference engine is 17.

In transaction 2, the user purchases a high value item (worth £100) at the same place in a short time interval, the authentication level (AL) in a deterministic model is 3, and the transaction risk is 50.

At last, the user purchases a very high value item (worth £150) in transaction 3, the authentication level (AL) is 4, and the transaction risk is 75.

In these three simulated transactions, the  $AL=1, 3, 4$  in a deterministic model corresponds to transaction risk = 17, 50, 75 in a fuzzy logic based model. Comparing the 2000 recognition rates returned from the fuzzy inference engine against the transaction risks, if any recognition rates of unauthorised users are equal to or greater than the transaction risk that means a false acceptance has occurred. Conversely, if any recognition rates of authorised users are less than the transaction risk, this means a false rejection has occurred. The experimental results are summarised in Table 8.10.

	Low Transaction risk (TR=17)	High Transaction risk (TR=50)	Very high Transaction risk (TR=75)
How many unauthorised user's $RR \geq TR$	10	0	0
FAR	1%	0%	0%
How many authorised user's $RR < TR$	0	17	119
FRR	0%	1.7%	11.9%

Table 8.10: The comparison of results which were gained from fuzzy

As shown in Table 8.10, when the recognition rates of unauthorised user compared against (1) low transaction risk (TR=17), (2) medium transaction risk (TR=50) and (3) high transaction risk (TR=75), the respective FARs are 1%, 0% and 0%. When the recognition rates of authorised users are compared against low, medium and high transaction risks, the respective FRRs are 0%, 1.7% and

11.9%. The details of FAR and FRR of the fuzzy logic based authentication system can be shown in Figure 8.16.

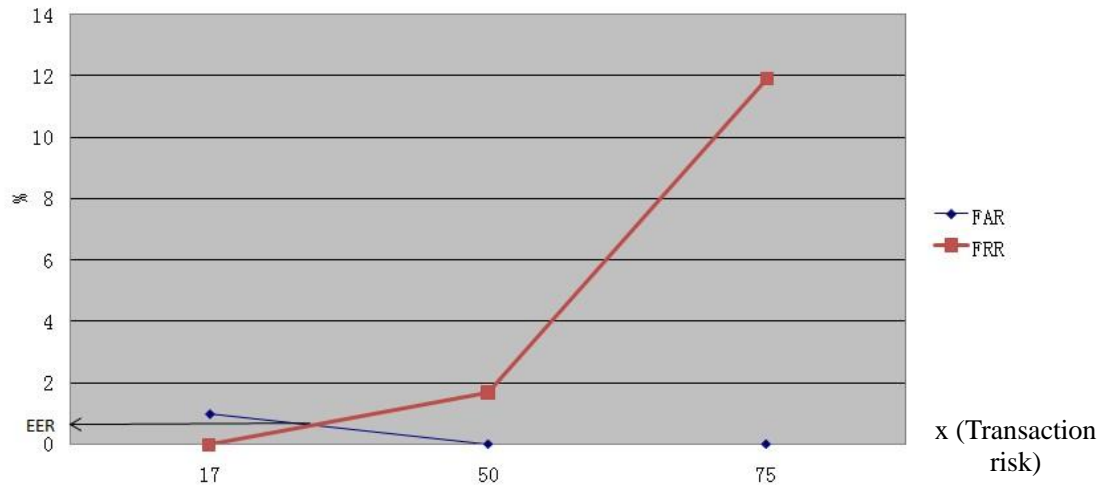


Figure 8.16: EER of the fuzzy logic based authentication system

As shown in Figure 8.16, the blue line indicates FAR, the red line indicates FRR, and x indicated the transaction risk. The blue line and red line crossed when the transaction risk in the interval [17, 50]. To calculate the EER (the cross over point) where FAR = FRR:

$$FAR = \frac{50-x}{50-17} \times 1\%$$

$$FRR = \frac{x-17}{50-17} \times 1.7\%$$

$$EER = \frac{50-x}{50-17} \times 1\% = \frac{x-17}{50-17} \times 1.7\% \text{ giving the cross over point } x = 29.2. \text{ The}$$

$$EER \text{ of the fuzzy logic based authentication system is } \frac{50-29.2}{50-17} \times 1\% = 0.63\%.$$

Using the results from Table 7.3, a comparison can be made of the fuzzy logic based model with the deterministic model discussed in Chapter 7. The comparison result is given in Table 8.11.

	Low value transaction (£20)	High value transaction (£100)	Very high value transaction (£150)
Deterministic model	Authentication level (AL=1)	Authentication level (AL=3)	Authentication level (AL=4)
	FAR: 0% FRR: 0%	FAR: 0.3% FRR: 11.2%	FAR: 0.015% FRR: 15.6%
Fuzzy logic based model	Transaction risk = 17	Transaction risk = 50	Transaction risk = 75
	FAR: 1% FRR: 0%	FAR: 0% FRR: 1.7%	FAR: 0% FRR: 11.9%

Table 8.11: The difference between the two authentication models

The results in Table 8.11 show that, for a low value transaction, the FAR of the fuzzy logic based model is low (1%) and false rejection did not happen in the experiment. For a high value transaction, the FRR of the deterministic model at AL=3 is 11.2%, the fuzzy logic based model can achieve a reduction of 9.5% ( $11.2\% - 1.7\% = 9.5\%$ ) to 1.7% for the FRR. For a very high value transaction, the FRR of the deterministic model at AL=4 is 15.6%, the fuzzy logic based model can achieve a further reduction of 3.7% ( $15.6\% - 11.9\% = 3.7\%$ ) for the

FRR. From these comparison results, it is clear that the fuzzy logic based model is highly effective in reducing the FRR and more accuracy (which corresponds to an EER of 0.63%) than a deterministic model.

### **8.3.3 Result summary**

The calculation results in Chapter 7 indicated that, when the multi-modal system is used in some particular environments like noisy or poor lightning place, the biometric authentication systems are difficult to achieve a high accuracy rate. The deterministic model is likely to reject the right user because this model only considers the result from a single authentication process. If users were rejected by any one of the biometric authentication processes, it is hard to access high authentication level in a deterministic model. However, the experimental results in this chapter indicated that the fuzzy logic based multi-modal system can perform all three biometric authentication processes, and enables the system to compensate for potential weaknesses of one biometric by using the strength of the others. From the comparison results gained in Table 8.11, it can be seen that the developed fuzzy logic based multi-modal system can achieve further FRR reduction of 9.5% for a high value transaction and 3.7% reduction for a very high value transaction. Furthermore, through a set of simulation tests, the results have proven the fuzzy logic based model can achieve an EER of 0.63%.

## **8.4 Discussion**

### **I. The fuzzy logic based model VS the deterministic model**

The smart model proposed in this chapter involves two security mechanisms: transaction risk assessment and recognition rate evaluation. A fuzzy inference model has been used in these two mechanisms to improve the usability and security of the system. Reviewing the deterministic model proposed in Chapter 7, it can be seen that the transaction level in the deterministic model is fixed by the transaction value, and the multi-modal authentication mechanism is also fixed. If a user failed in one recognition process, the system cannot continue to identify the user by using the other two. This is an important reason that leads to a high false rejection rate. The experimental results in this chapter show that, by using the fuzzy inference software we developed, the standard to accept or reject a user in mobile commerce is not fixed or determined by the system developer. The standard can be changed by modify the fuzzy set or membership functions in the fuzzy inference engine. In terms of accuracy rate, compared with the deterministic authentication system, the fuzzy logic based multi-modal authentication system is efficient to reduce the false rejection rate, and can achieve a low EER of 0.63%. Therefore, the fuzzy logic based multi-modal system is more robust and more accuracy than a deterministic authentication system.

**II. The fuzzy logic based model VS other related works**

The gained experimental results in this chapter show that the fuzzy logic based model can effectively resolve the issues that exist in the deterministic model.

The comparisons of the developed system and related studies are shown in Table 8.12.

	Lau et al., 2004	Alsaade, 2010	Abdolahi et al., 2013	This work
System model	Fuzzy logic based Multi-modal biometrics	Fuzzy logic based Multi-modal biometrics	Fuzzy logic based Multi-modal biometrics	Fuzzy logic based Mobile commerce and Multi-modal biometrics
Techniques	Face Speech Fingerprint	Face Voice	Face Fingerprint Iris	Typing behaviour Face Voice
Platform	Desktop	Desktop	Desktop	Mobile phone
Mechanism	Fixed	Fixed	Fixed	Flexible
Accuracy rate	EER: 0.5 – 0.84%	EER: 0 – 27.88%	EER: 1.7%	EER: 0.63%

Table 8.12: Comparison of related works

From Table 8.12, it is clear that there are three benefits of this research: firstly, the developed system in this research is not only for multi-modal biometrics authentication but also designed to support mobile commerce. Within this model, the transaction risk which determined by the transaction value and user's last

transaction detail is no longer fixed by the transaction value. Any unusual transaction behaviour increases the transaction level. Secondly, in other related studies in Table 8.11, the authentication mechanism is fixed, whether to accept or reject a user is only determined by the recognition result. In this research, the authentication mechanism is more flexible. The system will make a final decision after compare the recognition result against the transaction risk in mobile commerce. Finally, in mobile commerce, if the bank or merchants think the transaction risk is too high or too low, they can adjust the risk at anytime by modified the membership functions of variables and control rules within the fuzzy model. That means the fuzzy logic model developed in this chapter features convenient adjustment and is highly flexible.

Furthermore, the biometric authentication results used in the simulation test are randomly selected, some of the results were gained in particular environment such as noisy and poor lightning condition place. The simulation test results show that, the fuzzy logic based model is highly effective in reducing the FRR and improving the authentication performance. In addition, this research proposes the use of fuzzy logic decision fusion which can achieve a lower EER than other related works. Overall, the developed fuzzy logic based model increases the usability and security of the multi-modal biometric authentication system while it is been used in mobile commerce.



## Chapter 9

# Conclusion and future work

### 9.1 Conclusion

Research on fuzzy logic based multi-modal biometric authentication system has been presented in the thesis. There are three contributions to knowledge coming from this research: firstly, a model to support the authentication of mobile commerce was proposed. Secondly, three biometric authentication techniques which involve typing behaviour recognition, face recognition and speaker recognition were used to instead of password. Finally, the major contribution of this thesis is the use of fuzzy logic technique to improve the usability and performance of the multi-modal biometric authentication system. In this final chapter, the concept of mobile security and smart system is evaluated based on the findings of authentication model, multi-modal biometric authentication and fuzzy logic inference engine.

The first two introductory chapters (Chapter 1 and 2) provided a review of the

mobile authentication and mobile commerce history. Through analysing the deficiency of existing models, this thesis proposes a new model based on biometric authentication and smart mobile commerce. The subsequent study implemented in Chapter 3 built a multi-level authentication model to support mobile security. Based on this model, a multi-modal biometric authentication system was developed to establish user's identity on a mobile phone. The experimental results gained in Chapters 4, 5 and 6 show that though the security system it is possible to achieve user authentication with a good accuracy rate on mobile phones. However, the results also revealed that the biometric authentication performance was affected by the external environment condition. Examining the results from Chapter 7, the use of a deterministic authentication model will also reduce the usability of the system. To solve the issues, Chapter 8 presented a fuzzy inference model which can be used to determine the transaction risk in mobile commerce and the biometric recognition rate. The results in Chapter 8 indicated that the fuzzy logic based multi-modal biometric authentication system can reduce the affect of external environment conditions and make the authentication mechanism become more flexible.

#### **9.1.1 A model to support the authentication on mobile phones**

Chapter 3 has put forward an authentication model for use within mobile commerce applications. The model has been implemented, as a prototype, within an NFC based mobile shopping application using PIN and password as the authentication method. Analysis of the implementation shows that the model

has a minimal requirement for the user to authenticate themselves, whilst keeping the risks following phone loss to an acceptable level. The purpose of this research is to check the validity of the model. The experimental results in Chapter 3 show that the five levels authentication model is more secure than a single authentication model, and the evidence does show that the model is workable and acceptable to users.

### **9.1.2 Development of the multi-modal biometric authentication system**

The Chapters 4, 5 and 6 presented three independent biometric authentication mechanisms. The application developed can run on most mobile phones, and the experimental results show that it is possible to use these biometric techniques for detecting an authorised or unauthorised user on a mobile phone. By using the commerce model proposed in Chapter 3, users can simply process low value transaction just by typing in a correct PIN. For high risk transactions, the combined biometric techniques can achieve a higher accuracy rate than many individual authentication techniques alone. From the calculation results in Chapter 7, the system can achieve 0.015% or less FAR at the top authentication level. However, the FRR at authentication level 3 and level 4 are unacceptably high (11.2% at level 3 and 15.6% at level 4). The experimental results also show that the system is secure but still has some shortcomings such as: inflexible authentication mechanism and the accuracy rate may be influenced by the environment. To addresses these issues, a smart model was developed in Chapter 8.

### **9.1.3 Development of a smart m-commerce model**

In Chapter 8, a fuzzy logic method was used in the smart model. Within this model, the transaction risk is no longer fixed by the transaction value. The fuzzy inference engine can determine the risk according to transaction value, location distance and time interval. On the other hand, the multi-modal biometric authentication mechanism is more flexible. In a deterministic authentication system, the authentication process is fixed. When a user is failed in the first biometric recognition process, the system cannot continue to identify the user by using other two biometric techniques. When facing a high risk transaction, the smart model can perform all three biometric authentication processes and then give a final decision. Though the experimental work present in Chapter 8, it has been seen that the smart model is able to improve the performance of the multi-modal biometric authentication system and also make the authentication mechanism in mobile commerce become more accurate and more robust. Overall, the smart multi-modal biometric authentication system successfully achieve the authentication on a mobile phone, it has the ability to allow users use their mobile phone as a new payment tool and identification process in future.

## **9.2 A holistic interpretation of the research**

In reviewing the findings of the research, it is clear that this research had successfully contributed new knowledge to the mobile commerce research

domain. The design and development of multi-modal biometric authentication system which is helped to overcome the issues of single model authentication system (e.g. Campisi et al., 2009; Dave et al., 2010; Kinnunen and Li, 2010) and to corroborate existing predictions (e.g. Koreman et al., 2006; Clarke and Furnell, 2007<sub>a</sub>). Moreover, this research proposes the use of fuzzy logic decision fusion, in order to account for external environment conditions that affect the authentication performance. The comparison table (Table 2.2) in Chapter 2 had introduced other related works, and a new comparison table which involves our work is given in Table 9.1:

	Campisi et al. (2009)	Dave et al. (2010)	Kinnunen and Li (2010)	Koreman et al. (2006)	Clarke and Furnell (2007 <sub>a</sub> )	This work
Mobile phone	Yes	Yes	No	Yes	Yes	Yes
Biometrics	Keystroke	Face	Voice	Voice Face Signature	Keystroke Face Voice	Keystroke Face Voice
Mechanism	Deterministic	Deterministic	Deterministic	Deterministic	Deterministic	Fuzzy logic
Model	Single biometric	Single biometric	Single biometric	Multimodal biometric	Multimodal biometric	Multimodal biometric/ smart model for mobile commerce
Accuracy rate	EER: 16%	EER: 25%	EER: 2.49%	EER: 0.83 – 2.39%	FRR: 0.001-0.4(%) FAR: 0.000001-0.0002(%)	EER:0.63%

Table 9.1: Comparison of related work

In Koreman et al. (2006) and Clarke and Furnell (2007<sub>a</sub>)'s work, they have presented a multi-modal biometric authentication system that combines a number of biometric techniques. From the comparison result in Table 9.1, it is clear that the multi-modal biometric system can achieve a higher accuracy rates than any single biometric system. But in the related work, they also point out that the affect from environment is a problem which is hard to solve. As discussed in Chapter 8, the investigation has proven that the developed mobile security and smart system in this research is highly effective in reducing the influence of environment on the authentication performance, and can achieve a multi-modal biometric authentication with low EER of 0.63%. Moreover, a new smart model is designed for mobile commerce. Within this model, whether to accept or reject a user is not only determined by the authentication result, but also determined by the transaction risk. For instance, the experimental result in Chapter 8 shows that only good recognition results can achieve a high recognition rate to against the transaction risk. Addition to this, another benefit of the fuzzy logic based authentication system is: in practice, the fuzzy sets and control rules can be adjusted by the bank or merchant. Overall, the conclusion in this chapter showed that the initial aim had been successfully addressed by the research, and that the developed system could be of practical application in future mobile commerce projects.

### **9.3 Implications and limitations of the research**

As discussed in Chapter 2, the research into mobile security is primarily rooted

in the studies of single biometric authentication such as typing behaviour recognition (e.g. Clarke and Furnell, 2007<sub>b</sub>; Campisi et al., 2009; Zahid et al., 2009), face recognition (e.g. Lanitis et al., 2002; Tremblais and Augereau, 2004; Li and Prince, 2009) and speaker recognition (e.g. Shriberg et al., 2005; Campbell et al., 2006; Kinnunen and Li, 2010). These studies have shown that biometric techniques can be used instead of passwords in mobile security. However, the current understanding of biometric authentication is itself limited by the environmental influence. Other related studies such as (Koreman et al., 2006; Clarke and Furnell, 2007<sub>a</sub>; Zhu and Zhang, 2010) have proposed the use of multi-modal biometric authentication mechanism to improve the authentication performance. The use of multiple authentication techniques enables the system to compensate for potential weaknesses of one biometric technique by using the strengths of others. These studies were found to be informative but lacking with either high false rejection rate (FRR) or inflexible authentication mechanism. The research presented in this thesis not only contains a multi-modal biometric authentication model, but also proposes a fuzzy logic based smart model which can be used in mobile commerce. There are two implications of this research. Firstly, the implication of the research on the improvement of multi-modal biometric authentication system is clear. Evidenced by the results of Chapter 8, the combination of fuzzy logic method and multi-modal authentication mechanism can have a positive effect on mobile authentication. The fuzzy logic based model has potential for use in multi-modal authentication in place of a deterministic model. Secondly, in practice, the

proposed smart model is clearly distinct from other existing models because, by using the smart model, the decision in mobile commerce is no longer determined by the recognition results. The fuzzy logic based model will make a decision after analysis both transaction risk and recognition result. This proposed model could provide an ideal for new directions in the research of mobile commerce. Therefore, the findings of the fuzzy logic based mobile authentication research will have implications for the future research into multi-modal biometric authentication and mobile commerce transaction model.

In terms of limitations, it must be re-iterated that the fuzzy sets and control rules in the fuzzy logic system is defined according to the researcher's experience. This thesis is not arguing that these particular fuzzy sets or rules are defined in the best way. However, as discussed in Chapter 8, a set of simulation tests were arranged in the experimental work and the results have proven that the use of fuzzy logic based model increases the usability and security of the multi-modal biometric authentication system in mobile commerce. Furthermore, the fuzzy sets and control rules in the fuzzy logic based system is not fixed. Further work is required to set the parameters of any fuzzy logic based systems. This can be done by the system administrator to reflect the risk policy of the organisation. Further research will seek to establish the relationship between these parameters and the FAR/FRR.



## **9.4 Future work**

At the beginning of this research, the study question is whether the mobile security and smart system can be used in mobile commerce to establish a user's identity and make the transaction more reliable. In the conclusion sections, it is clear that the developed system has high performance and the research is valuable. In future, the next step work will focus on three parts:

(1) More biometric authentication techniques for mobile phone.

In this research, three biometric authentication techniques have been used to establish a mobile user's identity. With the development of mobile phone, maybe more accurate biometric authentication techniques can be used in a multi-modal biometric authentication system to increase the recognition rate and improve the system performance.

(2) Study the feasibility of building a mobile commerce model for disabled users.

The multi-modal biometric authentication system can be used by disabled users to achieve the identification work. Using the model presented in this research, it is possible for some disabled user to pass one or two recognition process and access to a low authentication level. For example, voice prompt can be used for the visually impaired user; and the speaker recognition process will never appeared if a user indicated they are speech impairment when registering. If more functions and more services can be provided, the mobile commerce will

become easier and more convenience for the disabled user.

(3) The improvement of the smart model

The smart model developed in this project can achieve smart control of the transaction risk and identification rate determination. In the future, if the mobile phone can automatically choose a biometric method according to the environment (like the light or background noisy); the system could be even “smarter”.

If the three parts of work can be achieved in future, it has great potential to be used to improve the usability and security of the mobile commerce. Perhaps few years later, more mobile service can be provided and more people will chose mobile-commerce. By then, we can face such a scene: the password-based technology has been completely eliminated, speaker recognition, face recognition or another biometric technology become a global common standards, personal identity recognition will be convenient and secure, and more and more people can prove their identity or make a payment through their mobile phone. If so, such a mobile commerce system can be widely used in other respects like: medical, government and Council Services, government military/Police, vehicle security, time and attendance and airport Security.

# Appendices

## **I. Mobile application**

The mobile application code is included in the Appendix I folder on the accompanying CD. The “PocketIDroid.fxp” file is the project file, which can be opened by Adobe Flash Builder 4.5 or above. And “PocketIDroid.apk” is an Android application, which is suitable for any mobile phones with Android 2.3 or above operating system.

## **II. Web server**

The web service source code is included in the Appendix II folder on the accompanying CD. The project files can be opened by Microsoft Visual Studio 2010 or above. The web server contains typing recognition and speaker recognition authentication engines.

## **III. Fuzzy inference application**

The developed “Fuzzy logic controller” application is included in the Appendix III folder. The project “FuzzyLogicUI” can be opened by Microsoft Visual Studio 2008 or above. A window forms user Interface is built for this fuzzy logic controller. The predefined test 1 and 2 are used to determine the transaction risk and recognition results which were discussed in chapter 8. In addition, it can

simply add or change the input variables, membership functions, and rules within this model.

#### **IV. The deterministic model proposed in Chapter 7**

The source code of the deterministic model proposed in Chapter 7 is included in the Appendix IV folder. These data involves the web service source code and an Android application. The details of this model were discussed in Chapter 7.

#### **V. The code used in the thesis**

The source codes discussed in this thesis are given in this Appendix V. Section 8.2.3.2: The membership functions for each of the input variable are given in Appendix V (6.1 and 6.2).

#### **VI. The demo test videos**

Four videos were involved in this folder. Video 1 shows the process of purchase a low value item; transaction is successes when user enters the correct PIN.

Video 2 shows the user successful purchase a normal value item after typing the password, and chose skip the face and speaker recognition process. Transaction risk is automatically calculated by the fuzzy inference engine, and transaction is successes when recognition rate is higher than transaction risk.

Video 3 shows the user successful purchase a high value item by complete the

typing behaviour, face and speaker recognition process.

Video 4 shows a participant try to use the researcher's phone to purchase an item. Transaction is failed when transaction risk is higher than the recognition rate.

## **VII. Published papers**

Xuan Huang, Geoffrey Lund, Victor Bassilious and Andrew Sapeluk (2011) "A model to support the authentication of mobile business" the paper was published at E-Business and E-Government (ICEE), 2011 International Conference in Shanghai, on May 2011.

Xuan Huang, Geoffrey Lund, and Andrew Sapeluk (2012) "Development of a typing behaviour recognition mechanism on Android", this paper was published at The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. (TrustCom 2012) in Liverpool, on June 2012.

These two papers are included in the Appendix VI folder on the accompanying CD.

## Reference

Abdollahi, M., Mohamadi, M. and Jafari, M. (2013) *Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic*. Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic, Volume 2, Issue 6, January 2013, pp. 504–510.

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

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

Animetrics (2008) “*Biometrics and Facial Recognition*”. Animetrics. Accessed at 7<sup>th</sup> Jan 2013: <http://www.animetrics.com/technology/frapplications.html>

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

Araujo, L., L. S., Lizarraga, M. L., Ling, L. and YabuUti, J.B. (2005) *User Authentication Through Typing Biometrics Features*. IEEE Transactions on Signal Processing, vol. 53, Issue 2, Part 2, pp. 851–855.

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

Bai, Y., Zhao Z.D., Qi Y.C., Wang, B. and Guo, J.Y. (2006) *Research on*

*Text-Independent Speaker Recognition Methods Using Wavelet Neural Network*. Chinese Journal of Electronics & Information Technology, Vol.28, No.6, 1036–1039

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

Bartlett, M.S., Movellan, J.R. and Sejnowski, T.J. (2002) *Face recognition by independent component analysis*. *IEEE Trans. Neural Networks*, vol. 13, no. 6, pp. 1450–1464.

Barnes, S.J. and Corbitt, B. (2003) *Mobile banking: concept and potential*, *International Journal of Mobile Communications*, 2003 Volume 1, Number 3/2003, pp. 273-288.

BBC news (2010) “*Government calls for action on mobile phone crime*”. Technology correspondent,  
<http://news.bbc.co.uk/1/hi/technology/8509299.stm>.

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

Blanz, V., Romdhani, S. and Vetter, T. (2002) *Face identification across different poses and illuminations with a 3D morphable model*. Proc. IEEE International Conference on Automatic Face and Gesture Recognition, pp. 202–207.

Blender, S. and Postley, H. (2007) *Key sequence rhythm recognition system and method*. Patent No. 7 206 938, U.S. Patent and Trademark Office.

Borde, D. (2007) *Selecting a two-factor authentication system*. Network Security, 2007,

Volume 2007, Issue 7, July 2007, pp.17-20.

Broekhoven, E.V. and Baets, B.D. (2006) *Fast and accurate center of gravity defuzzification of fuzzy system outputs defined on trapezoidal fuzzy partitions*. Fuzzy Sets and Systems 157, pp. 904 – 918.

Büyüközkan, G. and Feyzioğlu, O. (2004) *A fuzzy-logic-based decision-making approach for new product development*. International Journal of Production Economics, Volume 90, Issue 1, 8 July 2004, Pages 27–45.

Campbell, W., Sturim, D., and Reynolds, D. (2006). *Support vector machines using GMM supervectors for speaker verification*. IEEE Signal Process. Lett. 13 (5), pp. 308–311.

Campisi, P., Maiorana, E., Bosco, M. L. and Neri, A. (2009) *User Authentication Using Keystroke Dynamics for Cellular Phones*. IET Signal Processing - Special Issue on Biometric Recognition, vol. 3, no. 4, pp.333–341.

Carney, W. and Solomon, Y. (2002) *The future of wireless LANs will be multimode*. Texas Instruments White Paper SPLA001 (Nov. 2002);  
[focus.ti.com/pdfs/vf/bband/80211\\_wp\\_multimode.pdf](http://focus.ti.com/pdfs/vf/bband/80211_wp_multimode.pdf).

CBS News. (2010) *"Number of Cell Phones Worldwide Hits 4.6B"*. 15 February 2010.

Cellular-news.com, (2009) *"Vodafone Sees Loss of UK Market Share and Lower ARPUs"*. Cellular-news.com. 2009-04-23.

Chen, S. Zhang, T. Zhang, C. and Cheng, Y. (2010) *A real-time face detection and recognition system for a mobile robot in a complex background*. Artificial Life and Robotics. Volume 15, Number 4 (2010), pp. 439 – 443.



Chiu, S. L. (1997). *Extracting Fuzzy Rules from Data for Function Approximation and Pattern Classification*. In Dubois, D., Prade, H., and Yager, R. eds. *Fuzzy Information Engineering: A Guided Tour of Applications*. Wiley & Sons, NY, pp.149 – 162.

Clarke, N.L., Furnell, S.M., Lines, B., Reynolds, P.L. (2002) *Subscriber authentication for mobile phones using keystroke dynamics*. In: *Proceedings of the Third International Network Conference (INC 2002)*, Plymouth, UK, pp. 347–355

Clarke, N.L. and Furnell, S.M. (2007 a) *Advanced user authentication for mobile devices*. *Journal of Computer & Security* 26, pp.109-119.

Clarke, N.L. and Furnell, S.M. (2007 b) *Authenticating mobile phone users using keystroke analysis*. *International journal of information security*. Vol.6, pp.1-14.

Clark. S (2010) *Mobile wallet solutions are our top priority’ says PayPal boss*. *NFC world.com*  
<http://www.nfcworld.com/2010/08/17/34314/mobile-wallet-solutions-are-our-top-priority-says-paypal-boss/>

Cox, E. (2005) *Fuzzy modeling and genetic algorithms for data mining and exploration*. Book, published by Morgan Kaufmann Publishers.

Crawford, H. (2010) *Keystroke Dynamics: Characteristics and Opportunities*. 2010 Eighth annual international conference on privacy, security and trust. 2010 IEEE, pp.205-213.

Crisman, P.A. (1965) *CTSS Programmer’s guide, 2nd Ed.*, MIT Press, Cambridge, Mass., 1965.

Curtin, M., Tappert, C., Villani, M., Ngo, G., Simone, J., Fort, H. St. and Cha S.-H (2006) *Keystroke Biometric Recognition on Long-Text Input: A Feasibility Study*. In

Proceedings of Student/Faculty Research Day, CSIS, Pace University, May 5th, 2006

Dave, G., Chao, X., and Sriadibhatla, K. (2010) *Face Recognition in Mobile Phones*, Department of Electrical Engineering, Stanford University.

Denning, D. (1999) *Information warfare & security*. US: ACM Press.

"Facial Recognition Applications". Animetrics. Retrieved 2008-06-04.

Face.com (2012) Accessed at 10<sup>th</sup> Aug 2012: [www.face.com](http://www.face.com)

Figliola, P.M. (2006) *Wireless Privacy and Spam: Issues for Congress*, CRS Report for congress. Order Code RL31636.

Finan, R.A., Damper, R.I, and Sapeluk, A.T. (2001) *Improved Data Modeling for Text-Dependent Speaker Recognition Using Sub-Band Processing*. International Journal of Speech Technology, Volume 4, Number 1, March 2001, pp. 45-62(18).

Finan, R.A., Sapeluk, A.T. and Damper, R.I. (1997) *Impostor Cohort Selection for Score Normalisation in Speaker Verification*, Pattern Recognition Letters, 1997, Vol. 18 pp 881-888.

findBIOMETRICS.com. (2001) *Biometrics: The Anatomy Lesson*.  
<http://www.findbiometrics.com/pages/feature%20articles/anatomy.html> .

Garcia, J. (1986) *Personal identification apparatus*. Patent No. 4 621 334, U.S. Patent and Trademark Office.

Griaule Biometrics (2008) *Book-Understanding Biometrics*, copy right by Griaule Biometrics.

Haidar, S., Abbas, A. and Zaidi, A. (2000) *A Multi-Technique Approach for User Identification through Keystroke Dynamics*. in the 2000 IEEE International Conference on Systems, Man, and Cybernetics, vol. 2. Nashville, Tennessee, USA: IEEE, 2000, pp. 1336–1341.

Hatch, D. (2008) *Mobile Business Intelligence: Best-in-Class Secrets to Success*, news Information Week.com, Aberdeen Group.  
<http://www.informationweek.com/news/212300110>

Heeks, R. (2008) "Meet Marty Cooper – the inventor of the mobile phone". BBC 41 (6):pp. 26–33.doi:10.1109/MC.2008.192.

Hong, J.G. and Yu, Y.B. (2009) *Design and Realization of Embedded Speaker Recognition System Based on DSP*, Modern Electronics Technique, 32(22), 2009.

Hong, L. and Jain, A. (1998) *Htegrating faces and fingerprints for personal identification*, IEEE Trans. on Poitern Analysis and Machine Intelligence, Val. 20, No 12, pp.1295-1307, 1998.

Hong, T.P. and Lee, C.H (1996) *Induction of fuzzy rules and membership functions from training examples*. Fuzzy Sets and Systems, Val. 84, No.1, pp.33 -47.

Höppner, H., Klawonn, F., Kruse, R., and Runkler, T. (1999). *Fuzzy cluster analysis: methods for classification, data analysis and image recognition*. New York: John Wiley. ISBN 0-471-98864-2.

Huang, J.M. (2004) *Design and implementation of speaker's identity recognition system*, computer engineering, Vol.30 Supplementary Issue, Dec 2004

Huang, Z.H., and Shen, Q. (2003) *A New Fuzzy Interpolative Reasoning Method Based on Center of Gravity*, In Proc. of the International Conference on Fuzzy Systems,

volume 1, pp 25–30.

Huang, X., Lund, G. and Sapeluk, A. (2012) *Development of a typing behaviour recognition mechanism on Android*, IEEE International Conference on Trust Security and privacy in Computing and Communications, Liverpool June 2012.

IBG. (2007) *Global Biometric Market - New Opportunities (2007-2010)* International Biometric Group  
[www.biometricgroup.com/reports/public/market\\_report.html](http://www.biometricgroup.com/reports/public/market_report.html).

Internet Retailing. (2011) *UK mobile retail access via smartphone grew 163% in past year*, finds ComScore, August.

Intersperience. (2011) *Phone users concerned about possible data theft*. Online resource. [http://www.intersperience.com/knowledge\\_more.asp?know\\_id=57](http://www.intersperience.com/knowledge_more.asp?know_id=57)

Itavisen. (1999) *The World's first WAP Bank is Norwegian*. Itavisen.no. 1999-09-24. <http://www.itavisen.no/237581/verdens-forste-wap-bank-fra-norge>

Jahanshahi, A.A., Mirzaie and Amin Asadollahi, A. (2011) Mobile commerce beyond electronic commerce: issue and challenges. *Asian Journal of Business and Management Sciences* (2011) Vol. 1 No. 2, pp.119-129.

Jain, A., Bolle, R. and Pankanti, S. (1999). *Biometrics: Personal Identification in Networked Society*, Kluwer Academic Publishers, Dordrecht, 1999.

Jain, A., Hong, L., & Pankanti, S. (2000). *"Biometric Identification"*. *Communications of the ACM*, 2000, Vol. 43(2), pp. 91-98.

Jain, A. (2004) *An introduction to biometric recognition*. IEEE Transactions on Circuits

and Systems for Video Technology, Vol. 14, No. 1, 2004.

Jiang, T. and Li, Y. (1996) *Generalized defuzzification strategies and their parameter learning procedures*, IEEE Trans. Fuzzy Systems, 1996, vol.4, pp.64–71.

Kaehler, S.D (1993) *Fuzzy logic – an introduction Part 4*, Available on <http://123seminaronly.com/Seminar-Reports/014/7270869-Fuzzy-Logic.pdf>

Karatzouni, S. and Clarke, N.L. (2007) *Keystroke Analysis for Thumb-based Keyboards on Mobile Devices*. IFIP International Federation for Information Processing, Volume 232/2007, pp. 253-263.

Kinnunen, T. and Li, H.Z. (2010) *An overview of text-independent speaker recognition: From features to supervectors*, Speech Communication 52, pp.12–40.

Kirby, M. and Sirovich, L. (1990) *Application of the karhunen-loeve procedure for the characterization of human faces*. IEEE Pattern Analysis and Machine Intelligence, vol. 12, no. 1, pp. 103-108, 1990.

Klein, T. and Rio, E. (2005) *Concentration around the mean for maxima of empirical processes*. The Annals of Probability 2005, Vol. 33, No. 3, 1060–1077

Koczy, L. T., and Hirota, K. (1993) *Interpolative reasoning with insufficient evidence in sparse fuzzy rule bases*. Inform. Sci., vol. 71, pp. 169-201.

Komninos, N., Vergados, D. and Douligieris, C. (2006) *Layered security design for mobile ad hoc networks*, computers & security, 25, pp. 121-130.

Kong, S.G. and Kosko, B. (1992) *Adaptive fuzzy systems for backing up a truck-and-trailer*. IEEE Transactions on Neural Networks, Vol. 3, 2 (Mar. 1992), pp. 211–223.

Koreman, J., Morris, A.C., Wu, D., Jassim, S. and Sellahewa, H. (2006) *Multi-modal biometric authentication on the SecurePhone PDA*, 2nd Int. Workshop on Multi-modal User Authentication, 2006.

Lanitis, A., Taylor, C. J., and Cootes, T. F. (2002) *Towards automatic simulation of ageing effects on face images*. IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 4, pp. 442–455, 2002.

Lau, C.W., Ma, B., Meng, H.M., Moon, Y.S. and Yam, Y. (2004) *Fuzzy Logic Decision Fusion in a Multimodal Biometric System*, 8th International Conference on Spoken Language Processing, Jeju Island, Korea, October 4-8, 2004.

Lawton, G. (1998) *Biometrics: a new era in security*, Computer, Volume 31, Issue 8, 1998, pp. 16–18.

Lee, H. (2009) *A voice trigger system using keyword and speaker recognition for mobile devices*. Consumer Electronics, 2009, Volume 55, Issue 4, pp. 2377–2384.

Lee, S.H. and Lim J.S. (2008) *Kospi time series analysis using neural network with weighted fuzzy membership functions*. Agent and Multi-Agent Systems: Technologies and Applications Lecture Notes in Computer Science, Volume 4953, 2008, pp 53-62.

Li, P. and Prince, S. J. D. (2009) *Joint and Implicit Registration for Face Recognition*, (Former: "Registration-Free Face Recognition"), CVPR 2009, Miami, USA, June 20-25.

Lin Hong. (1998) *"Automatic Personal Identification Using Fingerprints"*, Ph.D. Thesis, 1998.

Lin, L.C and Chang, C.C. (2009) *A countable and time-bound password-based user*

*authentication scheme for the applications of electronic commerce*. Information Sciences 179 (2009) pp.1269–1277

Lin, S.H. (2000) *An introduction to face recognition technology*. Informing science special issue on multimedia informing technologies – Part 2, Volume 3, No 1, pp. 1- 7.

Madau, D.P. (1996) *Influence value defuzzification method*, in *Fuzzy Systems*, Proceedings of the Fifth IEEE International Conference on 8-11 Sep 1996, vol.3, Page 1819 – 1824.

Mamdani, E.H. and Assilian, S. (1975) *An experiment in linguistic synthesis with a fuzzy logic controller*. Int. J. Man-Machine studies, vol. 7, pp. 1-13.

McGill, W.L. and Ayyub, B.M. (2007) *Multicriteria Security System Performance Assessment Using Fuzzy Logic*. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, October 2007, vol. 4, no. 4, pp. 356-376.

Mendel, J. (1995) *Fuzzy logic systems for engineering: a tutorial*. Proceedings of the IEEE. Vol.83, no.3, pp.345-377, Mar 1995.

Miller, B. (1994) *Vital signs of identity*, IEEE Spectrum, Volume 32, Issue 2, 1994, pp. 22–30.

MMA, (2010) *Mobile Consumer Briefing – 2010*. May 2010 U.S. <http://www.mmaglobal.com/node/2816>

Mobile commerce – white paper, (2010) *Mobile commerce – The future is here*, 2010, <http://www.3dcart.com/whitepapers/Mobile-Commerce-White-Paper.pdf>

Mobile Data Association. *UK text messaging total tops 20 billion for 2003*. Mobile Data Association. Available from:

<http://www.text.it/mediacentre/default.asp?intPageId%4617>.

Monrose, F. and Rubin, A.D. (2000) *Keystroke Dynamics as a Biometric for Authentication*, Future generation computer systems, Volume 16, Issue 4, February 2000, pp. 351–359.

Morris, R. and Thompson, K. (1979) *Password security: a case history*. Communications of the ACM, Volume 22, Issue 11, November 1979, pp. 594-597.

Moskovitch, R.. (2009) *Identity Theft, Computers and Behavioral Biometrics*, IEEE Intelligence and Security Informatics 2009, Dallas, USA.

Mulpuru, S. (2010) *The State Of Retailing Online 2010: Marketing, Social Commerce, And Mobile*, July 2010, Forrester Research, Inc.

[http://www.cfs.purdue.edu/richardfeinberg/csr%20406%20e-retailing%20fall%202010/affiliate%20marketing/state\\_of\\_retailing\\_online\\_2010\\_marketing\\_social.pdf](http://www.cfs.purdue.edu/richardfeinberg/csr%20406%20e-retailing%20fall%202010/affiliate%20marketing/state_of_retailing_online_2010_marketing_social.pdf)

Nanavati, S., Thieme, M., and Nanavati, R. (2002) *Biometrics. Identity verification in a networked world*. John Wiley & Sons.

Napier, R., Lavery, W., Mahar, D., Henderson, R., Hiron, M., and Wagner M. (1995) *Keyboard user verification: toward an accurate, efficient and ecologically valid algorithm*. International Journal of Human–Computer Studies 1995; 43, pp. 213–222.

Novák, V. and Perfilieva, I. (1999) *Evaluating linguistic expressions and functional fuzzy theories in fuzzy logic*, in: L.A. Zadeh, J. Kacprzyk (Eds.), *Computing with Words in Information and Intelligent Systems 1*. Springer-Verlag, Heidelberg, 1999, pp. 383–406.

Obaidat, M. and Sadoun, B. (1997) *Verification of computer uses using keystroke dynamics*. IEEE Transactions on Systems, Man, and Cybernetics: Part B – Cybernetics



1997; 27(2):261–269.

Ofcom News. (2011) *A nation addicted to smartphones*, August 4, 2011  
<http://media.ofcom.org.uk/2011/08/04/a-nation-addicted-to-smartphones/>

Patel, A.V. and Mohan, B.M. (2002) *Some numerical aspects of center of area defuzzification method*. Journal Fuzzy sets and systems, Volume 132 Issue 3, December 2002, Pages 401 - 409

Pankanti, S. Bolle, R.M. and Jain, A. (2000) *Biometrics: The future of identification*. Computer, Volume 33, Issue 2, Feb 2000, pp. 46-49.

Pentland, A., Moghaddam, B. and Starner, T. (1994) *View-based and modular eigenspaces for face recognition*, in Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Jun. 1994, pp. 84–91.

Post Note, Mobile telephone crime, UK Parliament report, June 1995.

Ramakrishnan, B. (2008) *Mobile Business Intelligence for Intelligent Businesses*, information-management.com, published on July 2008.

[http://www.information-management.com/specialreports/2008\\_89/10001705-1.html?zkPrintable=1&nopagination=1](http://www.information-management.com/specialreports/2008_89/10001705-1.html?zkPrintable=1&nopagination=1)

Realwire.com. (2011) *10 million UK consumers using mobile commerce but 83% have experienced problems*.

<http://www.realwire.com/releases/10-million-UK-consumers-using-mobile-commerce-but-83-have-experienced-problems>

Reynolds, D.A. and Rose, R.C. (1995) *Robust Text-independent speaker identification. Using Gaussian mixture speaker models*. IEEE Speech and Audio, 1995, 3 (1), pp. 72–83.

Ricci. R, Chollet. G, Crispino. M. V, Jassim. S, Koreman. J.C, Morris. A.C, Olivar-Dimas. M, Garcia-Salicetti. S, and Soria-Rodriguez. P (2006): *The "SECUREPHONE" - A Mobile Phone with Biometric Authentication and e-Signature Support for Dealing Secure Transactions on the Fly*. SECRYPT 2006: pp. 9-16.

Richards, L. (2011) *Mobile commerce in the UK: stats round up*. Online resource. Nov 2011.

<http://econsultancy.com/uk/blog/8226-mobile-commerce-in-the-uk-stats-round-up>

Rogers, W. (2010) *"Frictionless mobile commerce"*,

<http://www.bakercommunications.com/CBS/Frictionless-Mobile-Commerce.htm>

Ross, B., Jackson, C., Miyake, N., Boneh, D., and Mitchell, J. (2005) *Stronger password authentication using browser extensions*. 14th Usenix Security Symp.; July 31–August 5; Baltimore, MD. USENIX Association; 2005. pp. 17-32.

Roychowdhury, S. and Wang, B.-H. (1996) *Cooperative neighbors in defuzzification*, Fuzzy Sets and Systems, 1996, vol.78, pp.37–49.

Sakly, A. and Benrejeb, M. (2003) *Activation of trapezoidal fuzzy subsets with different inference methods*, in: T. Bilgic, B. De Baets, O. Kaynak (Eds.), Fuzzy Sets and Systems—Proc. IFSA 2003, Lecture Notes in Artificial Intelligence, vol. 2715, Springer, Berlin, 2003, pp. 450–457.

Samal, A. and Iyengar, P.A. (1992) *Automatic recognition and analysis of human faces and facial expressions: a survey*. Pattern Recognition, Volume 25, Issue 1, January 1992, Pages 65–77.

Saquib, Z., Salam, N., Nair, R. and Pandey, N. (2011) *Voiceprint Recognition Systems for Remote Authentication-A Survey*, International Journal of Hybrid Information

Technology Vol. 4, No. 2, April, 2011.

Scheffer, N., Lei, Y. and Ferrer, L. (2011) *Factor analysis back ends for MLLR transforms in speaker recognition*, 12th Annual Conference of the International Speech Communication Association, August 2011, Florence, Italy.

Shaw, K. (2004) *Data on PDAs mostly unprotected*. Network World Fusion. Available from: <http://www.nwfusion.com/>.

Shepherd, L. (2011) *Determining identity on mobile phones using keystroke analysis*. Master dissertation, School of Computing and Engineering Systems, University of Abertay Dundee.

Shriberg, E., Ferrer, L., Kajarekar, S., Venkataraman, A., and Stolcke, A., (2005) *Modeling prosodic feature sequences for speaker recognition*. Speech Comm. 46 (3–4), pp. 455–472.

Song, Y.H., Wang, G.S., Wang, P.Y. and Johns, A.T. (1997) *Environmental/economic dispatch using fuzzy logic controlled genetic algorithms*. Generation, Transmission and Distribution, IEE Proceedings, 1997, Volume 144, pp. 377-382.

Spillane, R. (1975) *Keyboard apparatus for personal identification*. IBM Technical Disclosure Bulletin 1975; Tech. Rep. 17:3346.

Sugenon, M. (1985) *An Introductory survey of fuzzy control*. Information sciences 1985, Vol.36, pp. 59-79

Sukumar, S. (2011) *The Future of Cell Phones*, [buzzle.com](http://www.buzzle.com/articles/the-future-of-cell-phones.html),  
<http://www.buzzle.com/articles/the-future-of-cell-phones.html>

Szymkowiak, A., Dowman, M.C., and Ball, L.D. (2009) *A biometric security method*,

*system and computer program*, US Patent App. 12/555,429, 2009.

Tremblais, B. and Augereau, B. (2004) *A fast multi-scale edge detection algorithm*, Pattern Recognition Letters 25, pp. 603–618.

U.S. Smartphone Market: Who's the Most Wanted?

<http://blog.nielsen.com/nielsenwire/?p=27418>

Uludag, U., Pankanti, S., Prabhakar, S. and Jain, A.K. (2004) *Biometric cryptosystems: issues and challenges*. Proceedings of the IEEE Volume: 92, Issue: 6, pp. 948-960.

Vass, G., Kalmar, L. and Koczy, L. T. (1992) *Extension of the fuzzy rule interpolation method*. In Proc. 11. Conf. Fuzzy Sets Theory Applications, Liptovsky, Czech Republic, Jan.

Visiongain (2013) *The Biometrics Market 2012-2022 report*. Available on <http://www.visiongain.com/Report/898/The-Biometrics-Market-2012-2022>

Wang, Y., Hu, J. and Philips, D. (2007) *A Fingerprint Orientation Model Based on 2D Fourier Expansion (FOMFE) and its Application to Singular-Point Detection and Fingerprint Indexing*. Pattern Analysis and Machine Intelligence, 2007, Volume 29, Issue 4, pp. 573-585

Weinstein, E., Ho, P., Heisele, B., Poggio, T., Steele, K. and Agarwal, A. (2002) *Handheld face identification technology in a pervasive computing environment*. In Pervasive 2002, pages 48–54, Zurich, Switzerland.

Wikipedia, (2010) Near Field Communication,

[http://en.wikipedia.org/wiki/Near\\_field\\_communication](http://en.wikipedia.org/wiki/Near_field_communication)

World Health Organization (WHO) Library Cataloguing-in-Publication Data, World

report on disability 2011.

Xi, K., Ahmad, T., Han, F. and Hu, J. (2011) *A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment*. Security and Communication Networks, volume 4, Issue 5, pages 487–499.

Yang, J.H. and Chang, C.C. (2009) *An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem*, computers & security, 2009, pp. 1–6

Yang, M.H. (2002) “*Kernel eigenfaces vs. kernel fisherfaces: Face recognition using kernel methods*,” in *Proc. IEEE International Conference on Automatic Face and Gesture Recognition*, Washington D. C., May 2002, pp. 215–220.

Zadeh, L.A. (1965) *Fuzzy sets*. Information and Control. Volume 8, Issue 3, pp.338–353.

Zahid, S., Shahzad, M., Khayam, S.A. and Farooq, M. (2009) *Keystroke-Based User Identification on Smart Phones*. RAID '09 Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection Springer-Verlag Berlin, Heidelberg.

Zhao, W., Chellappa, R., Phillips, P. J. and Rosenfeld, A. (2003) *Face Recognition: A Literature Survey*, Journal ACM Computing Surveys (CSUR) Volume 35 Issue 4.

Zhang, C.P., and Su, G.D. (2000) *Human Face Recognition: A Survey*, Journal of image and graphics, 5(A), No.11, pp885-894.

Zhang, D. (2000) *Automated Biometrics—Technologies and Systems*, Kluwer Academic Publishers, Dordrecht, Hingham, MA, 2000.

Zhu, L.Q. and Zhang, S.Y. (2010) *Multimodal biometric identification system based on finger geometry, knuckle print and palm print*, Pattern Recognition Letters, Volume.31 (2010), pp.1641-1649.