FEATURES EXTRACTION SCHEME FOR BEHAVIORAL BIOMETRIC AUTHENTICATION IN TOUCHSCREEN MOBILE DEVICES

ALA ABDULHAKIM ABDULAZIZ

UNIVERSITI TEKNOLOGI MALAYSIA

FEATURES EXTRACTION SCHEME FOR BEHAVIORAL BIOMETRIC AUTHENTICATION IN TOUCHSCREEN MOBILE DEVICES

ALA ABDULHAKIM ABDULAZIZ

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

Advanced Informatics School
Universiti Teknologi Malaysia

FEBRUARY 2016

DEDICATION

A special feeling of gratitude to my loving parents, Abdulhakim and Asmran whose words of encouragement and push for tenacity ring in my ears. My brothers and sister have never left my side and are very special to me.

I also dedicate this thesis to my many friends and my other family members who have supported me throughout the process. I will always appreciate all they have done to me, especially my uncle Jamil Alariki for helping me to get scholarship and financial support.

I also dedicate this work and give special thanks to my lovely wife Sarah Ahmed and my wonderful son Mohammed Ala for being there for me throughout the entire doctorate program. Both of you have been my best cheerleaders.

ACKNOWLEDGEMENT

In the Name of Allah, Most Gracious, Most Merciful, all praises and thanks are due to Allah, peace and blessings be upon His Messenger. I express my appreciation to Allah for giving me the strength, patience, courage, and determination in completing this work.

I would like to express my most sincere appreciation to my supervisor Prof.Dr. Azizah Abdul Manaf for the continuous support in my Ph.D. program, for her patience, motivation, enthusiasm, and immense knowledge. She has been extremely helpful and offered me all the necessary support needed to succeed in every stage of my thesis, as such; I owe her a duty to be appreciative. Her guidance helped me all the time of my research and writing of this thesis. I could not have imagined having a better supervisor and mentor for my Ph.D. study.

My heartfelt gratitude goes to my parents Abdulhakim and Asmran for bearing with me for my weakness upon weakness from cradle to date. I am also grateful to my beloved wife Sarah Ahmed because of her uninterrupted support and encouragement during my study. I am also grateful to all my family members and friends. Last but not least, my thanks go to everyone who has helped in the development and final fruition of this work. I also would like to thank my country Yemen for funding my research and study.

ABSTRACT

Common authentication mechanisms in mobile devices such as passwords and Personal Identification Number have failed to keep up with the rapid pace of challenges associated with the use of ubiquitous devices over the Internet, since they can easily be lost or stolen. Thus, it is important to develop authentication mechanisms that can be adapted to such an environment. Biometric-based person recognition is a good alternative to overcome the difficulties of password and token approaches, since biometrics cannot be easily stolen or forgotten. An important characteristic of biometric authentication is that there is an explicit connection with the user's identity, since biometrics rely entirely on behavioral and physiological characteristics of human being. There are a variety of biometric authentication options that have emerged so far, all of which can be used on a mobile phone. These options include but are not limited to, face recognition via camera, fingerprint, voice recognition, keystroke and gesture recognition via touch screen. Touch gesture behavioural biometrics are commonly used as an alternative solution to existing traditional biometric mechanism. However, current touch gesture authentication schemes are fraught with authentication accuracy problems. In fact, the extracted features used in some researches on touch gesture schemes are limited to speed, time, position, finger size and finger pressure. However, extracting a few touch features from individual touches is not enough to accurately distinguish various users. In this research, behavioural features are extracted from recorded touch screen data and a discriminative classifier is trained on these extracted features for authentication. While the user performs the gesture, the touch screen sensor is leveraged on and twelve of the user’s finger touch features are extracted. Eighty four different users participated in this research work, each user drew six gesture with a total of 504 instances. The extracted touch gesture features are normalised by scaling the values so that they fall within a small specified range. Thereafter, five different Feature Selection Algorithm were used to choose the most significant features subset. Six different machine learning classifiers were used to classify each instance in the data set into one of the predefined set of classes. Results from experiments conducted in the proposed touch gesture behavioral biometrics scheme achieved an average False Reject Rate (FRR) of 7.84%, average False Accept Rate (FAR) of 1%, average Equal Error Rate (EER) of 4.02% and authentication accuracy of 91.67%,. The comparative results showed that the proposed scheme outperforms other existing touch gesture authentication schemes in terms of FAR, EER and authentication accuracy by 1.67%, 6.74% and 4.65% respectively. The results of this research affirm that user authentication through gestures is promising, highly viable and can be used for mobile devices.

ABSTRAK

Mekanisme pengesahan lazim untuk peranti mudah alih seperti kata laluan dan Nombor Pengenalan Peribadi gagal untuk bersaing dengan sentakan cabaran disebabkan penggunaan merata peranti internet kerana ia mudah hilang atau senang dicuri. Oleh itu, pembangunan mekanisme pengesahan yang boleh di adaptasi kepada persekitaran sedemikian amat penting. Pengecaman perseorangan berasaskan biometrik adalah alternatif terbaik untuk mengatasi kesukaran yang dihadapi pendekatan penggunaan katalaluan dan token, kerana biometrik tidak mudah dicuri atau dilupai. Ciri penting pengesahan secara biometrik adalah perhubungan tersurat dengan identiti pengguna, kerana biometrik bergantung sepenuhnya kepada ciri perlakuan dan fisiologi manusia. Terdapat beberapa pilihan pengecaman biometrik yang wujud sejak kebelakangan ini, dan kesemuanya boleh digunakan untuk telefon mudah alih. Pilihan ini termasuk tetapi tidak terhad kepada pengecaman muka melalui kamera, cap jari, pengecaman suara, ketukan kekunci, dan pengecaman gerak isyarat melalui skrin sentuh. Perlakuan biometrik gerak isyarat sentuhan lazimnya digunakan sebagai penyelesaian alternatif kepada mekanisme biometrik tradisional sedia ada. Walau bagaimanapun skema pengesahan gerak isyarat sentuhan dipenuh dengan masalah ketepatan pengesahan. Dalam beberapa kajian skema gerak isyarat sentuhan, ciri yang diekstrak hanya terhad kepada komponen kelajuan, masa, kedudukan, saiz jari dan tekanan jari. Walau bagaimanapun, pengekstrakan beberapa ciri daripada sentuhan individu adalah tidak memadai dalam membezakan pengguna secara tepat. Dalam kajian ini, ciri tingkah laku diekstrak dari data skrin sentuh yang telah direkodkan. Pengkelas diskriminatif difokuskan kepada ciri tersebut bagi tujuan pengesahan. Semasa pengguna melakukan gerak isyarat, skrin sentuh akan diumpil dan dua belas daripada ciri sentuhan jari pengguna diekstrak. Lapan puluh empat pengguna berbeza mengambil bahagian dalam kajian ini; setiap pengguna melakarkan enam gerak isyarat yang berbeza dengan 504 jumlah tika. Ciri gerak isyarat sentuhan yang diekstrak dinormalisasikan melalui penskalaan nilai supaya ia tergolong dalam julat kecil tertentu. Seterusnya lima Algoritma Pemilihan Ciri berlainan digunakan untuk memperolehi ciri subset yang paling bererti. Enam pengkelas pembelajaran mesin berbeza telah digunakan untuk mengkelas setiap tika dalam set data kepada salah satu daripada set kelas yang tertakrif. Hasil ujikaji yang dilaksanakan dalam skema biometrik tingkah laku ini mencapai ketepatan purata FRR (Kadar Pendakan Palsu) sebanyak 7.84%, purata FAR (Kadar Penerimaan Palsu) sebanyak 1%, purata EER (Kadar Ralat Sama) sebanyak 4.02% dan ketepatan pengesahan sebanyak 91.67%. Perbandingan hasil kajian menunjukkan skim yang dicadangkan mengatasi skim pengesahan gerak isyarat sentuhan sedia ada dari segi keupayaan FRR, FAR dan EER masing-masing sebanyak 1.67%, 6.74%, dan 4.65%. Hasil kajian ini mengesahkan bahawa pengesahan pengguna menggunakan gerak isyarat adalah sangat menggalakkan, berdaya maju, dan boleh digunakan untuk peranti mudah alih.

TABLE OF CONTENTS

CHAPTER	TITLE		PAGE
	DEDICATION		iii
	ACKNOWLEDGEMENT		iv
	ABSTRACT		v
	ABSTRAK		vi
	TABLE OF CONTENTS		vii
	LIST OF TABLES		xiv
	LIST OF FIGURES		xvi
	LIST OF ABBREVIATIONS		xx
	LIST OF APPENDICES		xxii
1	**INTRODUCTION**		**1**
	1.1	Research Overview	1
	1.2	Research Background	3
	1.3	Problem Statement	9
	1.4	Research Questions	10
	1.5	Research Objectives	11
	1.6	Scope of Study	11
	1.7	Significance of the Study	12
	1.8	Thesis Organization	13
	1.9	Summary	14
2	**LITERATURE REVIEW**		**15**
	2.1	Introduction	15
	2.2	Prevalence of Mobile Devices	15
	2.3	Mobile Devices in Society	18

2.4 Mobile Devices Security Threats and Controls 20
2.5 Authentication 21
2.5.1 Something in Your Possession (Token, ATM card) 22
2.5.2 Something You Know (password) 23
2.5.3 Something of Who You Are (Biometrics) 23
2.6 An Overview of Biometrics 25
2.6.1 Biometrics Types 27
2.6.1.1 Physical Biometrics 28
2.6.1.2 Behavioral Biometrics 29
2.7 General Scheme of Biometric 29
2.7.1 Enrolment Process 29
2.7.2 Authentication process 30
2.8 Evaluation of Biometrics Scheme 32
2.8.1 False Rejection Rate (FRR) 33
2.8.2 False Acceptance Rate (FAR) 34
2.8.3 Equal Error Rate (EER) 34
2.8.4 Accuracy 35
2.8.5 ROC Curve 35
2.9 Overview of Touch Screen and Its Features 36
2.9.1 Touch Features based Gesture Behavioral Biometric 38
2.9.2 Types of Touch Gesture 40
2.9.2.1 Zoom 40
2.9.2.2 Dwell 40
2.9.2.3 Rotate 41
2.9.2.4 Scroll 41
2.9.3 Advantages of Touch Features based Gesture Behavioral Biometric 42
2.10 Feature Normalization 43
2.10.1 Min-max normalization 43
2.10.2 Z-score normalization 44
2.10.3 Decimal scaling 44

2.11 Features Selection Approach 45
2.11.1 Filter Approach 46
2.11.2 Wrapper Approach 48
2.11.3 Embedded Approach 49
2.11.4 Feature Selection Comparison 50
2.12 Classification Algorithm 52
2.12.1 Decision Trees Classification 53
2.12.2 Rule-based Classification 54
2.12.3 Probabilistic methods Classification 55
2.12.4 Instance-based Classification 56
2.12.5 Support Vector Machine Classification 58
2.12.6 Neural Networks Classification 61
2.13 Related Work on Touch Gesture Biometric Authentication Scheme 62
2.14 Discussion on Touch Gesture Biometric Authentication Scheme 70

3 RESEARCH METHODOLOGY 73
3.1 Introduction 73
3.2 Research Procedure 73
3.3 Operational Framework 74
3.4 Methodology Phases 75
3.4.1 Literature Review Phase 77
3.4.2 Data Collection Phase 78
3.4.2.1 Design and Implementation 80
3. SQLite Database 85
3.4.2.2 Data Acquisition 86
3.4.3 Enrollment Phase 86
3.4.3.1 Feature Extraction 87
3.4.3.2 Data Preparation 88
3.4.3.3 Features Normalization 88
3.4.3.4 Features Selection 89
3.4.4 Authentication 90
3.4.4.1 Classification 91

3.4.4.2 Weka Tool 91
3.4.5 Evaluation of the Proposed Touch Gesture Authentication Scheme 92
3.5 Software and Hardware Requirements 92
3.6 Summary 93

4 FEATURES IDENTIFICATION, EXTRACTION AND NORMALIZATION 94
4.1 Introduction 94
4.2 Feature Identification 94
4.3 Finger Touch Features 97
4.4 The Feature Extraction Algorithms 100
4.4.1.1 Position 102
4.4.1.2 Touch Minor Up 102
4.4.1.3 Touch Minor Down 104
4.4.1.4 Time 104
4.4.1.5 Finger Pressure Up 105
4.4.1.6 Finger Pressure Down 106
4.4.1.7 Acceleration 106
4.4.1.8 Distance 107
4.4.1.9 Finger Size Up 109
4.4.1.10 Finger Size Down 109
4.4.1.11 Speed 110
4.4.1.12 Touch Major Up 111
4.4.1.13 Touch Major Down 112
4.5 Extracted Features Discussion 113
4.6 Feature Normalization 116
4.6.1 Time Normalization 118
4.6.2 Distance Normalization 118
4.6.3 Speed Normalization 119
4.6.4 Acceleration 120
4.7 Summary 121

5 FEATURES SELECTION AND CLASSIFICATION ALGORITHMS 122

5.1 Introduction 122

5.2 Features Selection Algorithms 122

5.2.1 Attribute Evaluator 123

5.2.2 Search Method 125

5.2.2.1 Best First Search Algorithm 126

5.2.2.2 Genetic Algorithm 126

5.2.2.3 Greedy Stepwise Search Algorithm 128

5.2.2.4 Random Search Algorithm 129

5.2.2.5 Forward Selection Algorithm 130

5.3 Classification Algorithms 132

5.3.1 Bayesian Classifier 133

5.3.1.1 Naïve Bayes Classifier 133

5.3.1.2 Bayes Net Classifier 135

5.3.2 Lazy Classifier 136

5.3.2.1 K-Star Classifier 136

5.3.3 Meta Classifier 137

5.3.3.1 Bagging Classifier 137

5.3.4 Trees Classifier 138

5.3.4.1 J48 Classifier 139

5.3.4.2 Random Forest Classifier 140

5.4 Performance Evaluation 141

5.4.1 Confusion Matrix 141

5.4.2 Receiver Operating Curves 143

5.5 Summary 145

6 RESULTS, ANALYSIS AND DISCUSSIONS 146

6.1 Introduction 146

6.2 Implementation Procedure 146

6.3 Features Extraction Implementation 147

6.4 Features Normalization Analysis 150

6.5 Features Selection Analysis 152

6.5.1 Best First Features Selection Analysis 152

6.5.2 Genetic Algorithm Features Selection Analysis 153
6.5.3 Greedy Stepwise Features Selection Analysis 155
6.5.4 Random Search Algorithm Feature Selection Analysis 156
6.5.5 Forward Feature Selection Analysis 158
6.6 Features Selection Result Discussion 160
6.7 Classification Analysis 162
6.7.1 Naïve Bayes Analysis 163
6.7.2 Bayesian Network Analysis 164
6.7.3 K-Star Analysis 166
6.7.4 Bagging Analysis 167
6.7.5 J48 Analysis 169
6.7.6 Random Forest Analysis 170
6.8 Summary of Classification Results 172
6.9 Analysis on the Proposed Touch Gesture Biometric Scheme 176
6.9.1 False Rejection Rate 179
6.9.2 False Accept Rate 179
6.9.3 Equal Error Rate 180
6.9.4 Accuracy 181
6.10 ROC Curve Analysis 182
6.11 Comparative Study 183
6.12 Summary 189

7 CONCLUSION 190
7.1 Introduction 190
7.2 Conclusion 190
7.2.1 Identify and Extract Finger Touch Features 191
7.2.2 Develop Features Selection and Classification Algorithms 192
7.2.3 Develop Touch Gesture-Based Behavioral Biometrics Scheme 193

7.3	Research Contribution	194
7.4	Recommendations for Future Research	196
7.5	Limitation	197
REFERENCES		**198**
Appendices A-H		215-257

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	World smart phone and client PC shipments in 2010 and 2011	17
2.2	Authentication Classes	24
2.3	Comparing Physical and Behavioral Biometrics	27
2.4	Confusion Matrix for Two-class Problem	33
2.5	Comparison Types of Mobile Touch	37
2.6	Feature Selection Compassion	51
2.7	Touch Gesture Behavioral Biometrics Related work Comparison	71
3.1	Operational Research Framework	74
3.2	Data Collection Details	79
3.3	Features Extraction	87
4.1	Mapping between the feature extraction references of the PSs	99
4.2	Comparison between Previous studies and proposed scheme	114
4.3	Proposed Scheme Feature Extraction Contribution	115
4.4	Time Normalization	118
4.5	Distance Normalization	119
4.6	Speed Normalization	119
4.7	Acceleration Normalization	120
5.1	Confusion Matrix	142
6.1	Normalized Features for Four users	151
6.3	Selected Features with Best First Algorithm	152
6.4	Selected Features with Genetic Algorithm	154
6.5	Selected Features with Greedy Stepwise Algorithm	155

6.6	Selected Features with Random Search Algorithm	157
6.7	Selected Features with Forward selection Algorithm	158
6.8	Feature Selection user Profile Dataset	162
6.9	Feature Selection Dataset with Naïve Bayes Classification Accuracy	163
6.10	Feature Selection Dataset with Bayesian Classification Accuracy	165
6.11	Feature Selection Dataset with K-Star Classification Accuracy	166
6.12	Feature Selection Dataset with Bagging Classification Accuracy	168
6.13	Feature Selection Dataset with J48 Classification Accuracy	169
6.14	Feature Selection Dataset with Random Forest Classification Accuracy	171
6.15	Summary of Dataset Accuracy per Classification Algorithm	173
6.16	Performance Measurement Result	177
6.17	Touch Gesture Biometrics Related work Result Comparison	188

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Mobile Subscriber Base-Worldwide	16
2.2	Mobile Penetration by Regional	16
2.3	Consumer Mobile Activities	19
2.4	Security Problems	21
2.5	User Authentication	22
2.6	Biometric Traits	26
2.7	Types of Biometric	28
2.8	General Framework of Biometrics System	31
2.9	The EER (25.99%) point	34
2.10	Diagram of Touch Screen Working	36
2.11	Touch Gestures	39
2.12	Zoom Gestures	40
2.13	Dwell Gestures	40
2.14	Rotate Gestures	41
2.15	Scroll Gestures	41
2.16	Feature Selection Algorithm	45
2.17	(a) framework (b) Algorithm	47
2.18	Wrapper Approach	48
2.19	Wrapper Approach Algorithm	49
2.20	Embedded Algorithm	50
2.21	Embedded Approach Algorithm	52
2.22	Decision Trees	53
2.23	Instance-based	57
2.24	K-nearest Neighbor	57
2.25	Support Vector Machine	59
2.26	Neural Networks	61

2.27	Touch Fingertip Movement	63
2.28	The Proposed Architecture	64
2.29	The Proposed architecture	65
2.30	Gesture authentication Architecture	66
2.31	Touch-dynamics-based authentication	67
3.1	Research Procedure	74
3.2	Research Methodology Flowchart	76
3.3	Implementation Procedure	80
3.4	Eclipse Android Emulator SDK Platform	81
3.5	Application Screenshot	82
3.6	Creating SQLite Database	83
3.7	Create Table	84
3.8	Feature Selection	89
3.9	Overview Authentication process	90
4.1	Finger Touch Event	95
4.2	Feature Component	96
4.3	Number of extracted features by previous studies	100
4.4	Minor Axis	103
4.5	Touch Minor Up Algorithm	103
4. 6	Touch Minor Down Algorithm	104
4.7	Finger Pressure up Algorithm	105
4.8	Finger Pressure down Algorithm	106
4.9	Distance Historical points.	108
4.10	Distance Algorithm	108
4.11	Finger Size up Algorithm	109
4.12	Finger Size down Algorithm	110
4.13	Major Axis	111
4.14	Touch Major up Algorithm	112
4.15	Touch Major down Algorithm	112
4.16	Percentage for each features used among the previous studies	113
5.1	Feature Selection in Weka	123
5.2	Wrapper approach for feature selection	125
5.3	Genetic Search Algorithm	127

5.4	Forward Selection Search Iteration	130
5.5	Classification Algorithms	132
5.6	Bayes Net applied in Classification	135
5.7	Bagging Classification	138
5.8	Decision Tree Classification	138
5.9	J48 Tree Classification	139
5.10	Random Forest Classifier	140
5.11	ROC curves: (a) regions of a ROC graph (b)	144
6.1	Enrolment Screen	147
6.2	Features Extraction Screen	148
6.3	Screen Shot of Enrolled Touch Gestures	149
6.4	Screen Shot of Touch Gesture Data Set	150
6.5	Comparison between Date Set before and after Normalization	151
6.6	Best First Algorithm Accuracy	153
6.7	Genetic Algorithm Accuracy	154
6.8	Greedy Stepwise Algorithm Accuracy	156
6.9	Random Search Algorithm Accuracy	157
6.10	Forward selection Search Algorithm Accuracy	159
6.11	Naïve Bayes Classification Analysis (a) A comparison between	164
6.12	Bayes Net (a) A comparison between correctly and incorrectly	165
6.13	K-Star (a) A comparison between correctly and incorrectly classified	167
6.14	Bagging (a) A comparison between correctly and incorrectly classified	168
6.15	J48 (a) Compare between correctly and incorrectly classified instances	170
6.16	Random Forest (a) A comparison between correctly and incorrectly	171
6.17	A comparison of classification accuracy amongst classifiers.	172
6.18	Visualization of Classification Errors in Weka	178

6.19	Equal Error Rate for user number three from ROC Curve in Weka	181
6.20	Classification Accuracy in Weka	182
6.21	Regions of a ROC Graph	183
6.22	A comparison of the proposed scheme in terms of accuracy	185
6.23	A comparison of the proposed scheme in terms of Equal Error Rate	186
6.24	A comparison of the proposed scheme in terms of FAR and FRR	187

LIST OF ABBREVIATIONS

AC	-	Accuracy
API	-	Application Program Interface
ATM	-	Automated Teller Machine
BPNN	-	Back-Propagation Neural Networks
CER	-	Cross-over Error Rate
DAG	-	Directed Acyclic Graphs
DTW	-	Dynamic Time Warping
EER	-	Equal Error Rate
FAR	-	False Acceptance Rate
FN	-	False Negatives
FP	-	False Positives
FRR	-	False Rejection Rate
IDE	-	Integrated Development Environment
JDK	-	Java Development Kit
JRE	-	Java Runtime Environment
K-NN	-	K-Nearest Neighbor
LCD	-	Liquid Crystal Display
MAX		Maximum
MEMS	-	Micro-Electro-Mechanical Systems
MIN	-	Minimum
NIST	-	National Institute of Standards and Technology

NN	-	Neural Networks
NSF	-	National Science Foundation
PAN	-	Personal Area Network
PIN	-	Personal Identification Number
RBFN	-	Radial Basis Function Network
ROC	-	Receiver Operating Characteristic
SAW	-	Surface Acoustic Wave
SMS	-	Short Message Service
SQL	-	Structured Query Language
SVM	-	Support Vector Machine
TN	-	True Negatives
TNR	-	True Negative Rate
TP	-	True Positives
TPR	-	True Positive Rate
UI	-	User Interfaces
Weka	-	Waikato Environment for Knowledge Analysis
Wi-Fi	-	Wireless Fidelity

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Source Code of the Proposed Scheme	215
B	Data Collection Guidelines Form	227
C	Touch Gesture Database	229
D	Experimental Result for Features Selection Algorithms	234
E	Experimental Result for Classification Algorithms	239
F	Confusion Matrix	254
G	Features Visualization	256

CHAPTER 1

INTRODUCTION

In this chapter, the research problem background and statement are stated, and then followed by research objectives, which used to handle and treat these problems. Furthermore, other aspects such as research scope, and significance of the research are determined. Finally, the chapter concluded with thesis organization and summary.

1.1 Research Overview

Mobile phones and to be specific the smartphone have largely permeated in almost all our daily lives, currently they are part and particle of our daily lives be it at work, in schools, generally in all spheres of our lives today. This has been largely due to the wide range of services the smartphone provides such as keeping track of appointments, meetings, providing multimedia storage, access to social media and email, among others making it a very fundamental device in human life today. This has made its demand to soar up in terms of number of its users, according to Seo et al (2012), there were 326.5 million smartphone users in 2010 globally, this was an increase of roughly 15 times in comparison to the number of users in 2005; they forecast by 2012 the number of users would reach 766.1 million. Most mobile phone services are provided via the internet making it ubiquitous, with a potential of unauthorized users getting unlimited access to the device. This may lead to data that is private and sensitive to the owner be stolen or abused (Guse and Müller, 2011). To help deter such, it is necessary to develop authentication mechanisms that are reliable and secure enough for mobile phones.

Currently common mobile authentication mechanisms such as passwords, PINs have failed to keep up with the pace of challenges presented with use of ubiquitous devices over the internet, since they can easily be lost or stolen (Crawford, 2010). Thus, it is important to develop authentication mechanisms that can be adapted to such environment. Biometric-based person recognition is a good alternative to overcomes the difficulties of password and token approaches (El-Abed et al, 2010; Jain and Kumar, 2010; Shanmugapriya and Padmavathi, 2011). In addition unlike PINs, passwords, tokens, biometrics cannot be easily stolen or forgotten.

An important characteristic of biometric authentication is that there is an explicit connection with the user's identity, since biometrics rely entirely on behavioral and physiological characteristics of the human being. Thus, require the physical presence of the human being in question to explicitly provide the required biometric authentication actions for the device authenticate. Derawi et al, 2010 mentioned that there are a variety of biometric authentication options that have so far emerged which can be used on a mobile phone. These options include but not limited to, face recognition through the camera, fingerprint, voice recognition, keystroke and gesture recognition via touch screen or camera.

Android mobile devices recently brought face recognition to the masses by enabling user authentication through the front-facing camera. Even though intuitive and fast, this type of authentication suffers from typical computer vision limitations. According to Wang et al (2015) face recognition performance degrades under poor or different lighting conditions than the ones used during training. Given that mobile devices constantly follow their users, such fluctuations on the environmental conditions are common.

More recently, iPhone mobile devices enabled users to easily and securely unlock their devices by embedding a fingerprint sensor in the home button. Even though this approach addresses both the usability and security requirements of the authentication process, it is fundamentally limited to devices with large physical buttons on the front, such as the home button on iPhone, where such a sensor can be

fitted. However, as phone manufacturers push for devices with large edge-to-edge displays, physical buttons are quickly replaced by capacitive buttons that can be easily embedded into the touch screen, eliminating the real-estate required by a fingerprint sensor. Embedding fingerprint sensors into touch screens behind gorilla glass is challenging, and has not been demonstrated.

This research focuses one of the mentioned biometric authentication methods, namely touch gesture recognition. According to Zhang et al (2015) most of the latest mobile phones have embedded sensors which can be used for touch gesture mobile biometric authentication. Touch gestures, as a kind of behavioural biometric, are basically the way users swipe their fingers on the screen of their mobile devices. They have been used to authenticate users while users perform basic operations on the phone. In these methods, a behavioural feature is extracted from the recorded screen touch data and a discriminative classifier is trained on these extracted features for authentication.

While the user performs the gesture, it leverages the touch screen sensor to extract touch user's finger features (size, pressure, timing and distance). When combined, the information from touch sensors provides ides a detailed view into how the individual user performs the gesture, and, as it shows in this research, it can be used as a sensor finger touch to authenticate the user. Attackers willing to bypass this authentication mechanism, face a much harder task as they have to simultaneously reproduce the timing, placement, size, and pressure of each finger touch. This thesis presents a mechanism of user authentication in mobile devices based on gestures as the behavioral biometrics. Results from experiments conducted in this research work affirm that user authentication through gestures is promising, viable and can be used in mobile devices.

1.2 Research Background

When a mobile phone in particular a smartphone is stolen, a lot of private and sensitive data can be compromised and be exploited for malicious activities, as such

users of such phones usually are concerned about their sensitive data stored in the phone than the phone itself (Kuhn and Johnson, 2013). In essence, when a smartphone is lost, the consequences that come with it are dire, they include privacy intrusion, user impersonation, and sometimes severe financial loss. As a first defense step, user authentication is essential to protect a system (Crawford, 2010). Currently, user authentication systems for mobile phones are mainly based on three techniques: passwords, physiological biometrics and behavioral biometrics (Meng et al, 2013).

Password authentication has well-known drawbacks, for instance, passwords can often easily be guessed and stolen through "shoulder surfing" (Meng et al, 2013). Ross et al (2008), have come up with a list of attacks such as password guessing, shoulder surfing and password log-in mobile applications among others; in most cases these attacks are easily launched to compromise password based authentication systems. Furthermore, even the best password can be stolen by dictionary and brute force attacks (Karnan et al, 2011). Moreover, password authentication method bring insufficient security level because writing them down, using simple passwords, or reusing passwords make them easy to break.

In order to alleviate these pitfalls that are associated with password authentication, ongoing research is focused on biometric authentication mechanisms that can be used with mobile phones. Previous studies (Sesa-Nogueras and Faundez-Zanuy, 2012; El-Abed et al, 2010; Jain and Kumar, 2010; Shanmugapriya and Padmavathi, 2011; Karnan et al, 2011) have reported that biometric-based person recognition is a good alternative to overcome the difficulties of password authentication. Biometric authentication is an authentication mechanism that uses human behavioral or physiological characteristics that are measurable, to define and represent the identity of a user.

Human physiological biometrics are the physical human body characteristics that uniquely identify a person, these include fingerprints, retina and human face (Bours, 2012). Such biometrics are known to offer a consistent performance, however, they are also known to have a common disadvantage of being non-standardized and costly (Ngugi et al, 2011). In addition physical biometrics are

difficult and intrusive for collectability, Low degree of user acceptability (Jain and Kumar, 2010). Banerjee and Woodard (2012), reported that the use of biometrics such as face, fingerprints and signature requires additional tools to acquire the biometric which leads to an increase in costs.

In contrast, behavioral biometrics authentication rely upon a person's actions or habits to uniquely identify that person. Behavioral biometrics authentication may include signature recognition, mouse dynamics, touch gesture and keystroke dynamics. Behavioral biometrics can be an alternative to physical biometrics, therefore address some of the earlier pitfalls of physical biometrics. In addition, behavioral biometrics are easily implementable since they can be implemented at the software level (Yampolskiy and Govindaraju, 2010). These biometrics can be unobtrusive and easily collected, without the user's knowledge (Bours, 2012). In addition, collection of data about the behavioral biometrics does not often require any special hardware and therefore it is cost effective (Jamil and Khan, 2011).

Traditional biometric methods include fingerprints, face or voice recognition have been used in mobile devices for user authentication. However, face or voice recognition have an issue not very well suited in every situation. The authentication method must be able to cope with very different environments for example relatively dark or noisy. In addition, Fingerprints rely on specific scanners which are not available on every smartphones today. Furthermore, embedding fingerprint sensors into touch screens behind gorilla glass is challenging, and has not been demonstrated (Wang et al, 2015). In the other hand, another traditional biometric method is keystroke authentication. keystroke authentication used traditional keyboards could only provide temporal information for example time interval between keystroke and time interval of a key being pressed (Trojahn and Ortmeier, 2013).

Touch screen like most popular input devices like the keyboard and mouse, can easily be used to recognize a person by extracting the features and use them through analyzing input patterns. In as such much as touch screen based devices use the touch screen as the basic input platform that facilitates interaction between the device and the user, there is very little knowledge about how this interaction can be

related to a specific user. Trojahn and Ortmeier (2013) said that touch screen mobile devices can provide very specific data of finger pressure, finger size or (relative) position where a touch has been hit. In addition, some features from the touch screen authentication method can be used because of the capacitive display.

With the increased popularity of touchscreen mobile phones, touch gesture behavior is increasingly becoming important in comparison to its counterpart the keystroke behavior, since almost all smartphones use the touch screen as the main input method (Meng et al, 2013). A gesture based authentication system would make it more difficult for a shoulder surfer to replay the password, even if he observes the entire gesture. Subtleties like force, speed, flexibility, pressure, and individual anatomical differences would prevent the casual observer of the password (Niu and Chen, 2012).

Many touch gesture behavioral biometrics authentication schemes have been produced for smartphones authentication. Burgbacher et al (2014), proposed authentication scheme for smartphones and other touch screen-based devices that combine behavioral biometrics from the fingertip movement on touch screens. They developed an android application which collects behavior features from the touch screen such as a sequence of x and y positions representing the location of the finger touch, and a timestamp for each location. The proposed authentication scheme and recognition algorithms are assessed by 42 users with 90% accuracy. The weakness of their proposed authentication scheme is concerning the small session number in which the data was collected. Because the data from a single subject was obtained in only one session may have influenced the performance of the system. In addition, one way to improve the proposed scheme could be to involve more features such as the fingertip pressure and finger size.

Veniamin Ginodman et al (2014) presented an authentication scheme based on behavioural biometric, consisting of two gesture touch screen related features such as speed and time. They implemented an extraction application system for these features using a touch screen mobile phone, running Android operating system of a Google/HTC Nexus One phone. In their evaluation, they used three classifiers

algorithms to classify their touch data namely Naive Bayes (NBayes), decision tree and k-nearest neighbour (IBK). However, the WEKA platform tool was used for data extraction to avoid any implementation bias. The evaluation was conducted using 50 participants with Android phones. Their study evaluation results show that their proposed authentication mechanism positively affects the performance of authentication by having good authentication accuracy with an average FAR of 7.74% and an average FRR of 6.65%. The accuracy of authentication can further be improved by adding more appropriate classifiers, such as bagging classifier or random forest classifier and also consider other touch gesture related features like the touch distance.

Xu et al (2014) suggested a touch-based authentication framework to authenticate user. The authentication proceeds in a passive way while the user performs her normal touch operations. As a first attempt, they investigated the underlying fundamentals of touch operations as biometrics. In other words, they evaluated whether the data features are distinctive among various users and they manage to achieve 8.67% average equal error rate. They have conducted a real-world experiment involving over 30 users. They collected four types of touch features which are x and y coordinates, time, size, pressure, and saves their touch data sequences for further analysis. There is a quite implementation issue of their touch-based authentication framework. Examples design a user-friendly mechanism to obtain data samples for training purpose rather than runs silently as a smartphone background service.

Li et al (2013) proposed gesture biometric-based system to achieve authentication for smartphones using users' finger movements. They carried out all our data collections and experiments on Motorola Droid phones involving 75 users. The data collections will gather the four types of touch features which position, pressure, distance, time and saves their touch data sequences for further analysis. Experiments show that their system is efficient on smartphones and achieves good 79.74% accuracy. In order to improve the accuracy result, more touch features could be extracted.

Wolff (2013) looked at the different sensors provided by mobile phones, and show that data collected from these sensors can distinguish mobile users by analyzing the user's interaction with the device. He extracted additional features, inducing the direction of a gesture, the end point, the distance between the beginning and end of a gesture, the gesture speed, and the lateral variance on a gesture. He was able to correctly identify the user with 83% accuracy. The weakness of his work is having small number of user to test and evaluate the scheme. A larger scale study incorporating more users is needed in order to realize a more accurate authentication mechanism that can identify them based on data of their touch gesture biometric.

Meng et al (2013) utilized accurate user authentication mechanism which a behavioral feature set that is related to touch dynamics. Results from this experiment show that the neural network classifier is accurate enough to authenticate a variety of users; however, there was an error rate of 7.8% on the selected features used in that experiment. They suggested that using other classifiers, involving more participants and also gather more data on touch gesture biometrics, may help in even getting a more accurate and efficient mechanism.

In their behavioural biometrics touch screen study, Kolly et al (2012) investigated whether they could differentiate users based on their behaviour on the touch screen. To accomplish that objective, they collected data on touch events for 5 users; and realized that they could identify a user with an accuracy of 80% there about. The data collected was on basic touch properties like pressure, time and position. The weakness of his work is having a small number of users to test and evaluate the scheme. As such, a large scale study that incorporates more users is preferred such that more data can be collected, hence realize a more accurate mechanism to identify users based on data from their touch gesture behavior biometric.

Although, several researches have been conducted on touch gesture behavioral biometrics authentication, there are still some issues that can be highlighted. The main issue is to enhance authentication accuracy (Burgbacher et al, 2014; Li et al, 2013; Wolff, 2013; Kolly et al, 2012). In order to enhance the

authentication accuracy, using more several known machine learning algorithms (e.g., Naive Bayes, decision tree) for classification and features selection algorithm. The second issue is extracting few touch features from individual touches, such as touch duration and touch direction which is not enough to distinctive among various users (Sitova et al, 2015; Xu et al, 2014; Meng et al, 2013; Trojahn and Ortmeier, 2013). It can extract all possible touch gesture features, such as fingertip pressure and finger size to distinctive among various users. Finally, conducted experiment with small number of user to test and evaluate the authentication scheme (Angulo and Wästlund, 2012; De Luca et al, 2012; Kolly et al, 2012; Wolff, 2013).

The aim of touch gesture is to develop scheme that enhance the authentication accuracy and performance of determination users based on their touch gesture behavioral biometrics. From the existing works, scheme (Angulo and Wästlund, 2012; De Luca et al, 2012; Kolly et al, 2012; Wolff, 2013) collected and tested their methods in small group of users and advice to include more users and larger sample size in order to make a more robust determination on the ability to identify users. This research develop a scheme to extract and study more touch gesture features and tested in large group of user by using multiple classification techniques, hence this will increase the accuracy with good performance authentication.

1.3 Problem Statement

Many biometric methods exist today and finding the best suitable one for access control on mobile phones is not easy. Touch gesture behavioural biometrics used as an alternative solution to existing traditional biometric mechanism that utilize fingerprints, facial impressions, keystroke dynamics authentication or voice recognition which present several pitfalls as earlier discussed. Several schemes namely : (Meng and wong, 2014), (Burgbacher et al, 2014), (Veniamin Ginodman et al, 2014), (Xu et al, 2014), (Li et al, 2013), (Min, 2014), (Murmuria et al, 2015), (Shih et al, 2015), (Buduru and Yau, 2015), (Feng et al, 2014) and (Qiao et al, 2015) have been proposed in recent years on touch gesture behavioral biometrics

authentication. While these touch gesture features they used in their schemes have shown potential and provided promising results, there is still space for extracting and analyzing new touch features from individual touches to substantially improve authentication accuracy.

In fact, the touch gesture features used in their schemes are speed, time, position, and finger size and finger pressure. However, extracting few touch features from individual touches is not enough to distinctive among various users accurately. Therefore, in order to secure mobile devices and protect users' data, it is very crucial to enhance user authentication scheme for mobile phones. One fundamental mobile security problem is user authentication, and if not executed correctly, leaves the mobile user vulnerable to harm like impersonation or unauthorized access.

The key idea is to combine the features that can be extracted from mobile sensors when human finger touch mobile screen with an extended features by preforming mathematics calculations. The best features subset choosed based on performing different feature selection algorithms which aims to speed classification algorithms and enhance authentication accuracy. Several machine learning classifier used to authenticate users this is due to the fact that the performance of a classifier may be fluctuant in terms of different training datasets. For instance, an algorithm may achieve a very good authentication result regarding a set of user inputs, but its performance may drop quickly for another set of user inputs (Veniamin Ginodman et al,2014). This strategy is crucial to perform high-accuracy user authentication, outperforming all the prior touch gesture behavioral biometric authentication sachems for mobile devices.

1.4 Research Questions

This research aims to determine whether it can distinguish users based on their touch dynamics using a behavioural feature set related to those dynamics to help realize an accurate user authentication mechanism on mobile devices. In order to achieve that aim, the following research questions were addressed:

i. What are the current user authentication systems and schemes for touch gesture-based behavioral biometrics that are used on mobile phones?

ii. What are the touch features have been used in previous studies and how the previous studies extract the features?

iii. How can the touch gesture-based behavioral biometrics schemes be improved to distinguish users based on their touch dynamics and also obtain enhanced authentication accuracy?

1.5 Research Objectives

In order to answer the research questions stated above, the research objectives were identified as follows:

i. To identify and extract finger touch features for touch gesture-based behavioral biometrics authentications scheme on mobile phones.

ii. To develop five different features selection algorithms and six different classification algorithm based on the extracted features.

iii. To develop touch gesture-based behavioral biometrics scheme and determine its authentication accuracy on user's touch dynamics.

1.6 Scope of Study

The main aim of this research is to design and develop a touch gesture-based behavioral biometrics scheme, which helps to enhance user authentication required for mobile devices. Therefore, this study was limited to the following research scope:

i. The study was delimited to the data acquisition, feature extracting, features selection and classification process of behavioral biometrics. There were four biometrics performance requirements (false reject rate, false accept rate, equal error rate and accuracy) used to evaluate and target the enhancement of behavioral biometrics authentication.

ii. The proposed scheme controls the user activities by providing a guideline during the data collection process in such way the features will be extracted. The extracted features were normalized by scaling its values using the Min-Max normalization technique, to that they are within a certain specified range.

iii. The touch-gesture behavioral biometric authentication data was collected from students and staff of the Universiti Teknologi Malaysia and were duly informed about the purpose of this work.

iv. The implementation of feature extraction and the graphical user interface are done using Java Eclipse with an Android phone. SQLite database was used to store data for the extracted features. Testing, data analysis and evaluation were done using WEKA machine learning toolkit (WEKA tool).

1.7 Significance of the Study

The outcomes of this research would greatly contribute to behavioural biometric authentication schemes for mobile devices. The significance of this research are:

i. It established scheme based on touch gestures authentication in order to secure against shoulder surfers, even those with video cameras, because it is hard to estimate the force and timing of gestures correctly solely with brute force.

ii. Touch gestures authentication scheme helps to improve the security of password-based authentication. Touch gestures authentication scheme

confirm the authorized user based on his finger touch features, which is providing an additional security level of verification. Even if the touch gesture is revealed by unauthorized user, the difficulty of breaking the authentication is increased.

iii. It identifies and understands the extracted features from finger contacted the touch screen, it started to record and save the trace by recording raw touch finger movement features.

iv. Another important implication of this scheme extend beyond touch gesture authentication; it might be applied to any biometric source such as keystroke dynamics, signature or gait.

v. Touch gestures authentication scheme introduce dataset captured from 84 subjects over six sessions. This dataset will be available to researchers to facilitate progress in this field.

vi. The implication of this scheme is that unlike the existing schemes, our scheme used five different feature selection algorithms to choose the most significant feature subset. This was a process to speed classification algorithms, enhance prediction accuracy and comprehensibility.

1.8 Thesis Organization

This thesis is divided into seven chapters. Chapter one introduces the problem area which is problem background and problem statement. From the problem statement, the objectives of this research specified to be achieved. Furthermore, the research scope is stated and determined. Chapter two begins by reviewing the popularity of mobile device along with the increasing reliance upon them establish in the security of the mobile device. It is also presenting a generic biometric schemes, the performance measurement and evaluation. Touch gesture behavioral biometrics

were chosen due to their various advantages that can provide protection security. It concluded with a review of the existing touch gesture behavioral biometrics.

Chapter three describes research procedures and research phases (literature review phase, data collection phase, enrolment phase, and authentication phase). Chapter four presents the systematic literature review for feature identification and extraction. It also provides a brief review of previous studies for touch features used in their schemes. Chapter five elaborates the five different features selection algorithms and six different classification algorithms. It illustrates technical and practical performance evaluation of the proposed scheme.

Chapter six provides the analysis and discussion of the results. A number of experimental studies into the analyzing and testing linguistic features using a pattern classification method based upon six different classification algorithms. Furthermore, a comparative study between the algorithm proposed in this research and other touch gesture behavioral biometrics techniques for authentication is also presented and discussed. Chapter seven presents review and the main conclusions from the research. It identifies the main methods used and discusses their implications in the research. It discusses the contributions of this research as well the recommendation and future works.

1.9 Summary

This chapter firstly has discussed the problem background in order to demonstrate the current state of knowledge in the field, and identify the gap in the concerned study. Then, the problem statement has been formulated based on the gap that has figured out. After that, the chapter had covered relevant research questions, which needed to be answered in this research. Afterward, research objectives, research scope and research significance have determined. Finally, the chapter concluded with research significance and thesis organization. The next chapter will investigate, study and analyze the related works in the same field of this research are.

REFERENCES

ABI (2012). Smart, the Next Wave of Bluetooth. *ABl research*. Retrieved March 2, 2015, from http://www.abiresearch.com/research/product/1013429-smart-the-next-wave-ofbluetooth/.

Ade, R., and Deshmukh, P. (2014). Instance-based vs Batch-based Incremental Learning Approach for Students Classification. *International Journal of Computer Applications*, 106(3), 37-41.

Aggarwal, C. C. (2014). Data Classification: Algorithms and Applications. Data Mining and Knowledge Discovery Series. *CRC Press*.

Aha, D. W. and Bankert, R. L. (1996). A comparative evaluation of sequential feature selection algorithms. *Proceedings of the Fifth International Workshop on Artificial Intelligence and Statistics*. Springer New York, 199-206.

Al Shalabi, L., and Shaaban, Z. (2006). Normalization as a preprocessing engine for data mining and the approach of preference matrix. *Proceedings of the International Conference on Dependability of Computer Systems*, Szklarska Poreba 207-214.

Ali, H. and Salami, M. (2009). Keystroke pressure based typing biometrics authentication system by combining ANN and ANFIS-based classifiers. *5th International Colloquium on Signal Processing & Its Applications (CSPA)*, Kuala Lumpur, 198-203.

Ali, J., Khan, R., Ahmad, N., & Maqsood, I. (2012). Random forests and decision trees. *International Journal of Computer Science Issues (IJCSI)*, *9*(5), 272-278.

Angulo, J. and Wästlund, E. (2012). Exploring touch-screen biometrics for user identification on smart phones. *Advances in Information and Communication Technology*. Springer Berlin Heidelberg, 130-143.

Araujo, L. C., Sucupira Jr, L. H., Lizarraga, M. G., Ling, L. L. and Yabu-Uti, J. B. (2005). User authentication through typing biometrics features. *IEEE Transactions on Signal Processing*, 53(2), 851-855.

Arthi, K.,. Nandhitha, N.M. and Roslin, S (2013). A Study and Evaluation of Different Authentication Methods and Protocols. *International Journal of Computer Science and Management Research*, 2(1), 549-555.

Aruna, S., Rajagopalan, S. and Nandakishore, L. (2011). An Empirical Comparison of Supervised Learning Algorithms in Disease Detection. *International Journal of Information Technology Convergence and Services–IJITCS*. 1(4), 81-92.

Aung, W. T. and Hla, K. H. M. S. (2009). Random forest classifier for multi-category classification of web pages. *Services Computing Conference, APSCC 2009*. IEEE Asia-Pacific. Singapore, 372-376.

Ashbourn, J. (2004). Practical Biometrics: From Aspiration to Implementation. London: *Springer.*

Banerjee, S. P. and Woodard, D. L. (2012). Biometric Authentication and Identification using Keystroke Dynamics*:* A Survey. *Journal of Pattern Recognition Research,*7(1), 116-139.

Battles, M. D. Gartner identifies the top 10 strategic technology trends for 2013. *Gartner Symposium*. Retrieved 23-Oct-2013, from http://www.gartner.com/newsroom/id/2209615

Berg Insight (2011). Mobile Money in Emerging Markets. *Berg Insight's VAS research series.* Retrieved February 20, 2012, from http://www.berginsight.com/ReportPDF/ProductSheet/bi-mm1-ps.pdf.

Bhalla, M. R. and Bhalla, A. V. (2010). Comparative Study of Various Touchscreen Technologies. *International Journal of Computer Applications IJCA*. 6(8), 12-18.

Bimbot, F., Bonastre, J.-F., Fredouille, C., Gravier, G., Magrin-Chagnolleau, I., Meignier, S., Merlin, T., Ortega-García, J., Petrovska-Delacrétaz, D. and Reynolds, D. A. (2004). A tutorial on text-independent speaker verification. *EURASIP journal on applied signal processing*, 4 , 30-451.

Bolón-Canedo, V., Sánchez-Maroño, N. and Alonso-Betanzos, A. (2013). A review of feature selection methods on synthetic data. *Knowledge and information systems.* 34(3), 483-519.

Bonastre, J.-F., Bimbot, F., Boë, L.-J., Campbell, J., Reynolds, D., and Magrin-Chagnolleau, I. Person authentication by voice: a need for caution. *The Proceeding of 8th European Conference on Speech Communication and Technology*, Geneva, Switzerland, 33–36.

Bonev, B. (2010). Feature selection based on information theory. *Universidad de Alicante. Kochi University of Technology*, Spain, PhD Thesis.

Bours, P. (2012). Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report*, ELSEVIER, 17(1-2), 36-43.

Bragdon, A., Nelson, E., Li, Y. and Hinckley, K. (2011). Experimental analysis of touch-screen gesture designs in mobile environments. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York, 403-412.

Buchoux, A. and Clarke, N. L. (2008). Deployment of keystroke analysis on a smartphone. *Proceedings of the 6th Australian Information Security Management Conference*, Western Australia, 7-48.

Burgbacher, U., Pratorius, M., and Hinrichs, K. (2014). A behavioral biometric challenge and response approach to user authentication on smartphones. *Proceedings of the International Conference on Systems, Man and Cybernetics (SMC)*, San Diego California, 3328-3335.

Burr, W. E., Dodson, D. F., Newton, E. M., Perlner, R. A., Polk, W. T., Gupta, S. and Nabbus, E. A. (2011). Electronic Authentication Guideline. *National Institute of Standards and Technology*, NIST Special Report 800–63-1.

Cai, Z., Shen, C., Wang, M., Song, Y. and Wang, J. (2013). Mobile authentication through touch-behavior features. *Lecture Notes in Computer Science, Biometric Recognition*, Springer International Publishing, 386-393.

Caruana, R. and Freitag, D. (1994). Greedy Attribute Selection. *The Proceedings of 11 International Conference on Machine Learning*, Morgan Kaufmann, 28-36.

Cateni, S., Vannucci, M., Vannocci, M. and Colla, V. (2012). Variable Selection and Feature Extraction through Artificial Intelligence Techniques. *Multivariate Analysis in Management, Engineering and the Science*. 103-118.

Chauhan, S., Arora, A. and Kaul, A. (2010). A survey of emerging biometric modalities. *Procedia Computer Science*, 2, 213-218.

Cheng, J., Grainer, G., Kelly, J., Bell, D. and Lius, W. (2002). Learning bayesian networks from data: An information-theory based approach. University of Alberta, Canada, PhD Thesis.

Chong, A. Y.-L., Chan, F. T. and Ooi, K.-B. (2012). Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia. *Decision Support Systems*, 53(1), 34-43.

Chouaib, H., Terrades, O. R., Tabbone, S., Cloppet, F. and Vincent, N. (2008). Feature selection combining genetic algorithm and adaboost classifiers. *19th International Conference on Pattern Recognition (ICPR)*. Tampa Florida, 1-4

Cisco, I. (2009). Data Leakage Worldwide: Common Risks and Mistakes Employees Make. *Cisco Systems*. Retrieved September 2 2012, from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-499060.pdf

Clarke, N. L. and Furnell, S. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*. 6(1), 1-14.

Clarke, N. L., Furnell, S. M. and Reynolds, P. L. (2002). Biometric authentication for mobile devices. *Proceeding of 3rd Australian Information Warfare and Security Conference*, Perth, Australia, 61-69.

Cooper, D. (2012). Canalys: More smartphones than PCs shipped in 2011. *Canalys survey*. Retrieved April 4 2013, from http://www.engadget.com/2012/02/03/canalys-more-smartphones-than-pcs-shipped-in-2011/.

Crawford, H. (2010). Keystroke dynamics: Characteristics and opportunities. *Eighth Annual International Conference on Privacy, Security and Trust*, Ottawa, Canada, 205-212.

Crawford, H. A. (2012). A framework for continuous, transparent authentication on mobile devices. University of Glasgow, United Kingdom, PhD Thesis.

Cufoglu, A., Lohi, M. and Madani, K. (2009). A comparative study of selected classifiers with classification accuracy in user profiling. *World Congress on Computer Science and Information Engineering*, Los Angeles, California 708-712.

De Luca, A., Hang, A., Brudy, F., Lindner, C. and Hussmann, H. (2012). Touch me once and i know it's you!: implicit authentication based on touch screen patterns. *SIGCHI Conference on Human Factors in Computing Systems*, Vancouver, Canada, 987-996.

Derawi, M. O., Nickel, C., Bours, P. and Busch, C. (2010). Unobtrusive user-authentication on mobile phones using biometric gait recognition. *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*. Darmstadt, Germany, 306-311.

Devasena, C. L. (2014). Adeptness Comparison between Instance Based and K Star Classifiers for Credit Risk Scrutiny. *International Journal of Innovative Research in Computer and Communication Engineering*. 2(1), 20-28.

Devijver, P. A. and Kittler, J. (1982). Pattern recognition: A statistical approach. *Prentice-Hall London.*

do Nascimento, M. V., Batista, L. V. and Cavalcanti, N. (2014). Comparative study of learning algorithms for recognition by hand geometry. *IEEE International Conference on Systems, Man and Cybernetics (SMC)*, San Diego California, 423-428.

Du, P., Xia, J., Zhang, W., Tan, K., Liu, Y. and Liu, S. (2012). Multiple classifier system for remote sensing image classification: a review. *Sensors*, 12(4), 4764-4792.

El-Abed, M., Giot, R., Hemery, B. and Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. *IEEE International Carnahan Conference on Security Technology (ICCST)*, San Jose California, 170-178.

EN 50133 (1997). Alarm systems. Access control systems for use in security applications. System requirements. *BSI*.

Feizi-Derakhshi, M.-R. and Ghaemi, M. (2014). Classifying Different Feature Selection Algorithms Based on the Search Strategies. *International Conference on Machine Learning, Electrical and Mechanical Engineering (ICMLEME)*. Dubai, United Arab Emirates, 8-9.

Feng, T., Liu, Z., Kwon, K.-A., Shi, W., Carbunar, B., Jiang, Y. and Nguyen, N. (2012). Continuous Mobile Authentication using Touchscreen Gestures. *IEEE Conference on Technologies for Homeland Security (HST)*, Waltham,United States, 451-456.

Fierrez-Aguilar, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J. and Bigun, J. (2005). Discriminative multimodal biometric authentication based on quality measures. *Pattern Recognition*. 38(5), 777-779.

Frank, M., Biedert, R., Ma, E., Martinovic, I. and Song, D. (2013). Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. Information Forensics and Security, *IEEE Transaction on Information Forensics and Security*, 8(1), 136-148.

Gafurov, D., Snekkenes, E. and Buvarp, T. E. (2006). Robustness of biometric gait authentication against impersonation attack. *Proceedings of the First International Workshop on Information Security ((IS'06)*, Montpellier, France, 51-59.

Grenga, A. J. (2014). Android Based Behavioral Biometric Authentication via Multi-Modal Fusion. *Graduate School of Engineering and Management, Air Force Institute of Technology, Air University: DTIC Document*.

Gupta, S., Kumar, D. and Sharma, A. (2011). Data mining classification techniques applied for breast cancer diagnosis and prognosis. *Indian Journal of Computer Science and Engineering (IJCSE)*. 2(2), 188-195.

Guse, D. (2011). Gesture-based User Authentication for Mobile Devices. Technischen Universität Berlin, Germany, Master Thesis.

Hamzaçebi, C. and Kutay, F. (2007). Continuous functions minimization by dynamic random search technique. *Applied Mathematical Modelling*. 31(10), 2189-2198.

Henry, P. and Luo, H. (2002). WiFi: what's next?. IEEE *Communications Magazine*, 40(12), 66-72.

Holmes, J. H. (1999). Quantitative methods for evaluating learning classifier system performance in forced two-choice decision tasks. *Proceedings of Second International Workshop on Learning Classifier Systems*, Orlando Florida, 250-257.

Hoogsteder, V. (2010). Our presentation from Mobile World Congress 2010–Mobile application stores state of play. *Accessed (07.11. 14)*

Horning, N. (2010). Random Forests: An algorithm for image classification and generation of continuous fields data sets. *Proceeding of the 5th International Conference on Geoinformatics for Spatial-Infrastructure Development in Earth and Allied Sciences (GIS-IDEAS)*, Hanoi, Vietnam, 93–98.

Hossain, M. R., Oo, A. M. T. and Ali, A. S. (2013). The combined effect of applying feature selection and parameter optimization on machine learning techniques for solar Power prediction. *American Journal of Energy Research*. 1(1), 7-16.

IBG (2010). How is biometric defined?. *International Biometric Group*. Retrieved December 5, 2012, from http://www.biometricgroup.com/reports/biometric_definition.html97.

Jain, A., Bolle, R. and Pankanti, S. (2002). Introduction to biometrics. *In Biometrics Personal Identification in Networked Society,* Norwell, Kluwer, 1, 1-41.

Jain, A. K. and Kumar, A. (2010). Biometrics of next generation: An overview. Second Generation Biometrics. *Springer Berlin*, Germany.

Jain, A. K., Ross, A. and Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology,* 14(1), *4-20.*

Jamil, D. and Khan, M. N. A. (2011). Keystroke Pattern Recognition Preventing Online Fraud. *International Journal of Engineering Science and Technology (IJEST)*, 3(3), 1953-1958.

Jeon, S., Bang, J., Byun, K. and Lee, S. (2012). A recovery method of deleted record for SQLite database. *Personal and Ubiquitous Computing.* 16(6), 707-715.

Jie, Y. L., Yi, Z. X., Da, C. and Siting, Z. (2012). Development and implementation of Eclipse-based file transfer for Android Smartphone. *7th International Conference on Computer Science & Education (ICCSE 2012)*, Melbourne, Australia, 568-571.

Jo, H.-H., Karsai, M., Kertész, J. and Kaski, K. (2012). Circadian pattern and burstiness in mobile phone communication. *New Journal of Physics*. 14(1), 1-17.

Kalyani, G. and Lakshmi, A. J. (2012). Performance assessment of different classification techniques for intrusion detection. *Journal of Computer Engineering (IOSRJCE)*, 7(5), 25-29.

Karnan, M., Akila, M. and Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*. 11(2), 1565-1573.

Kaspersky. (2012). Perception and knowledge of IT threats: the consumer's point of view. *Kaspersky survey lab*, Retrieved March- 2, 2012, from https://www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf

Kenny, P., Ouellet, P., Dehak, N., Gupta, V. and Dumouchel, P. (2008). A study of interspeaker variability in speaker verification. *IEEE Transactions on Audio, Speech, and Language Processing*, 16(5), 980-988.

Kesavaraj, G. and Sukumaran, S. (2013). A study on classification techniques in data mining. *4th IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT)*, Tiruchengode, India, 1-7.

Kitchenham, B. and Charters, S (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering, *Keele University and University of Durham*, UK, EBSE Technical Report, Version 2.3.

Kohavi, R. and John, G. H. (1997). Wrappers for feature subset selection. *Artificial intelligence*. 97(1), 273-324.

Kolly, S. M., Wattenhofer, R., & Welten, S. (2012, November). A personal touch: Recognizing users based on touch screen behavior. *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones.* New York, USA, 1-5.

Komatineni, S and MacLean, D. (2012). Pro Android 4 (Vol. 1). *New York: Apress*.

Koreman, J., Morris, A., Wu, D., Jassim, S., Sellahewa, H., Ehlers, J., Chollet, G., Aversano, G., Bredin, H. and Garcia-Salicetti, S. (2006). *Multi-modal* biometric authentication on the SecurePhone PDA. *Second Workshop on Multimodal User Authentication*, Toulouse, France,1-8.

Kotsiantis, S., Kanellopoulos, D. and Pintelas, P. (2006). Data preprocessing for supervised leaning. *International Journal of Computer Science*. 1(2), 111-117.

Kuhn, M. and Johnson, K. (2013). Applied predictive modeling. *Springer*, London, Limited Document, 4.1.

Kumar, R. and Verma, R. (2012). Classification algorithms for data mining: A survey. *International Journal of Innovations in Engineering and Technology* (IJIET). 1(2), 7-14.

Kumar, V. and Minz, S. (2014). Feature Selection: A literature review. *Smart Computing Review*, 4(3), 211–229.

Lavesson, N. (2003). Evaluation of classifier performance and the impact of learning algorithm parameters. *Master's thesis, Department of Software Engineering and Computer Science*, Blekinge Institute of Technology, Sweden.

Lee, S. (2012). Creating and Using Databases for Android Applications. *International Journal of Database Theory & Application*. 5(2), 99-106.

Li, L., Zhao, X. and Xue, G. (2013). Unobservable Re-authentication for Smartphones. *Proceedings of the 20th Network and Distributed System Security Symp (NDSS)*. San Diego, United States, 1-16

Ling, C. X., Huang, J. and Zhang, H. (2003). AUC: a statistically consistent and more discriminating measure than accuracy. *Proceedings of the 18th International Joint Conferences on Artificial Intelligence (IJCAI)*, San Francisco, USA, 329-341

Liu, H. and Yu, L. (2005). Toward integrating feature selection algorithms for classification and clustering. , *IEEE Transactions on Knowledge and Data Engineering*. 17(4), 491-502.

Marcano-Cedeño, A., Quintanilla-Domínguez, J., Cortina-Januchs, M. and Andina, D. (2010). Feature selection using sequential forward selection and classification applying artificial metaplasticity neural network. *36th Annual Conference on IEEE Industrial Electronics Society (IECON)*, Glendale, United States, 2845-2850.

Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.-M. and Ailisto, H. (2005). Identifying users of portable devices from gait pattern with accelerometers. *IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, Montreal, Canada, 2, ii/973 – ii/976.

Meng, Y. and Wong, D. S. (2014). Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones. *Proceedings of 29th Annual ACM Symposium on Applied Computing*, Gyeongju, Korea, 1680-1687.

Meng, Y., Wong, D. S. and Schlegel, R. (2013). Touch Gestures Based Biometric Authentication Scheme for Touchscreen Mobile Phones. *Information Security and Cryptology*. Springer, 331-350.

Metropolitan Police Service (2011). Safeguarding your mobile phone. *Metropolitan police*. Retrieved March 1, 2015, from http://www.met.police.uk/crimeprevention/phone.htm.

Monaco, J. V., Bakelman, N., Cha, S.-H. and Tappert, C. C. (2012). Developing a Keystroke Biometric System for Continual Authentication of Computer Users. *European Intelligence and Security Informatics Conference (EISIC)*, Odense, Denmark, 210-216.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Lohlein, B., Heister, U., Moller, S. and Rokach, L. (2009). Identity theft, computers and behavioral biometrics. *IEEE International Conference on Intelligence and Security Informatics (ISI'09)*, Dallas Texas, United States, 155-160.

Murphy, K. P. (2007*)*. Performance evaluation of binary classifiers, *University of British Columbia*, Technical Report. Springer.

Ngugi, B., Kahn, B. K. and Tremaine, M. (2011a). Typing Biometrics: Impact of Human Learning on Performance Quality. *Journal of Data and Information Quality (JDIQ).* 2(2), 1-21.

Ngugi, B., Tremaine, M. and Tarasewich, P. (2011b). Biometric keypads: Improving accuracy through optimal PIN selection. *Decision Support Systems*. 50(4), 769-776.

Niu, Y. and Chen, H. (2012). Gesture authentication with touch input for mobile devices. *Security and Privacy in Mobile Information and Communication Systems.* Springer Berlin Heidelberg, 94, 13-24.

Nookala, G. K. M., Pottumuthu, B. K., Orsu, N. and Mudunuri, S. B. (2013). Performance analysis and evaluation of different data mining algorithms used for cancer classification. *International Journal of Advanced Research in Artificial Intelligence* (IJARAI). 2(5), 49-55.

Pappa, G. L. and Freitas, A. A. (2010). Automating the Design of Data Mining Algorithms: An Evolutionary Computation Approach. *Natural Computing*. NewYork, Springer.

Patel, V. R. and Mehta, R. G. (2011). Impact of Outlier Removal and Normalization Approach in Modified k-Means Clustering Algorithm. *International Journal of Computer Science Issues* (IJCSI). 8(5).

Patil, T. R. and Sherekar, M. S. (2013). Performance Analysis of Naive Bayes and J48 Classification Algorithm for Data Classification. *International Journal of Computer Science and Applications*. 6(2), 331-336.

Pettey, C. and Goasduff, L. (2013). Gartner Says Worldwide Mobile Application Store Revenue Forecast to Surpass $15 Billion in 2011. *Gartner survey*. Retrieved March 9, 2013, from http://www.gartner.com/it/page.jsp?id=1529214.

Phyu, T. N. (2009).Survey of classification techniques in data mining. *Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS)*, Kowloon, Hong Kong, 18-20.

Portio Research (2012). Portio Research Mobile Factbook 2012. *Portio Research*. Retrieved March 18, 2014, from http://www.portioresearch.com/media/1797/Mobile%20Factbook%202012.pdf.

Pratama, S. F., Muda, A. K., Choo, Y.-H. and Muda, N. A. (2011). Computationally Inexpensive Sequential Forward Floating Selection for Acquiring Significant Features for Authorship Invarianceness in Writer Identification. *International Journal of New Computer Architectures and their Applications (IJNCAA)*. 1(3), 581-598.

Portmann, D. Z. M. and Indulska, A.-H. T. J. (2009). Ubiquitous Intelligence and Computing. *6th International Conference on Ubiquitous Intelligence and Computing*, Brisbane, Australia, 193-203.

Pylvänäinen, T. (2005). Accelerometer based gesture recognition using continuous HMMs. *Pattern Recognition and Image Analysis*. 413-430.

Qi, Y. (2012). Random forest for bioinformatics. Ensemble machine learning. *Springer*. New York, USA.

Qin, Z. (2006). Naive Bayes classification given probability estimation trees. Machine Learning and Applications, 2006. *Proceedings of 5th International Conference on Machine Learning and Applications (ICMLA'06)*, Orlando Florida, 34-42.

Rejer, I. and Lorenz, K. (2013). Genetic algorithm and forward method for feature selection in EEG feature space. *Journal of Theoretical and Applied Computer Science*. 7(2), 72-82.

Ren, X. and Wu, X.-W. (2012). A novel dynamic user authentication scheme. *International Symposium on Communications and Information Technologies (ISCIT)*, Queensland, Australia, 713-717.

Rokach, L. and Maimon, O. (2010). Data Mining and Knowledge Discovery. *Springer Science+ Business Media*. Handbook, Second edition, 167-192.

Ross, A., Nandakumar, K. and Jain, A. K. (2008). Introduction to multibiometrics. *Springer*. Handbook of Biometrics, 271-292.

Sae-Bae, N., Ahmed, K., Isbister, K. and Memon, N. (2012). Biometric-rich gestures: a novel approach to authentication on multi-touch devices. *Proceedings of t2012 ACM annual conference on Human Factors in Computing Systems*. Austin Texas, United States, 977-986.

Saevanee, H. (2014). Continuous User Authentication Using Multi-Modal Biometrics. , *School of Computing and Mathematics, Plymouth University*, England, PhD Thesis.

Saeys, Y., Inza, I. and Larrañaga, P. (2007). A review of feature selection techniques in bioinformatics. *bioinformatics*. 23(19), 2507-2517.

Sandberg, R. and Rollins, M. (2013). A Brief Introduction to Android Development. The Business of Android Apps Development. *Springer*. Handbook, Second edition, 39-50.

Sandnes, F. E. and Zhang, X. (2012). User Identification Based on Touch Dynamics. *9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing*, Fukuoka, Japan, 256-263.

Santra, A. and Christy, C. J. (2012). Genetic Algorithm and Confusion Matrix for Document Clustering. *International Journal of Computer Science Issues (IJCSI)*. 9, 322-328.

Saravanan, P., Clarke, S., Chau, D. H. P. and Zha, H. (2014). LatentGesture: active user authentication through background touch analysis. *Proceedings of Second International Symposium of Chinese CHI*. Ontario, Canada, 110-113.

Sae-Bae, N., Memon, N. and Isbister, K. (2012).Investigating multi-touch gestures as a novel biometric modality. *IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, Virginia, 156-161.

Sae-Bae, N., Memon, N., Isbister, K. and Ahmed, K. (2014). Multitouch gesture-based authentication. *IEEE Transactions on Information Forensics and Security*, 9(4), 568-582.

Saeys, Y., Inza, I. and Larrañaga, P. (2007). A review of feature selection techniques in bioinformatics. *bioinformatic*s. 23(19), 2507-2517.

Seo, H., Kim, E. and Kim, H. K. (2012). A Novel Biometric Identification Based on a User's Input Pattern Analysis for Intelligent Mobile Devices. *International Journal of Advanced Robotic Systems.* 9, 1-10.

Sesa-Nogueras, E. and Faundez-Zanuy, M. (2012). Biometric recognition using online uppercase handwritten text. *Pattern Recognition*. 45(1), 128-144.

Singh, N. and Khan, R. (2014). Equal Error Rate and Audio Digitization and Sampling Rate for Speaker Recognition System. *Advanced Science Letters.* 20(5-6), 1085-1088.

Shahzad, M., Liu, A. X. and Samuel, A. (2013). Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it. *19th annual international conference on Mobile computing & networking*. New York, United States, 39-50.

Shanmugapriya, D. and Padmavathi, G. (2009). A survey of biometric keystroke dynamics: Approaches, security and challenges. *International Journal of Computer Science and Information Security*. 5, 115-119.

Shanmugapriya, D. and Padmavathi, G. (2011). An Efficient Feature Selection Technique for User Authentication using Keystroke Dynamics. *International Journal of Computer Science and Network Security (IJCSNS)*. 11(10), 191-195.

Shanmugapriya, V. and Padmavathi, G. (2010). Keystroke Dynamics Authentication Using Neural Network Approaches. *Information and Communication Technologies*. 101(3), 686-690.

Sherly, K. (2012). A Comparative Assessment of Supervised Data Mining Techniques for Fraud Prevention. *International journal of soft computing and engineering*, 1. 1-6.

Shi, E., Niu, Y., Jakobsson, M. and Chow, R. (2011). Implicit authentication through learning user behavior. *Springer, Information security*.6531, 99-113.

Shi, W., Yang, J., Jiang, Y., Yang, F. and Xiong, Y. (2011).Senguard: Passive user identification on smartphones using multiple sensors. *IEEE 7th International*

Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Wuhan, China, 141-148.

Singh, N. and Khan, R. (2014). Equal Error Rate and Audio Digitization and Sampling Rate for Speaker Recognition System. *Advanced Science Letters*. 20(5-6), 1085-1088.

Sitova, Z., Sedenka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P. and Balagani, K. (2015). HMOG: A New Biometric Modality for Continuous Authentication of Smartphone Users. *IEEE Transactions on Information Forensics and Security*. 3(1), *1-17*.

Sridhar, V. (2012). Image Based Password Authentication for Illiterates with Touchscreen. *International Journal of Science, Engineering and Technology Research.* 1(3), 18-25.

Syed, Z., Helmick, J., Banerjee, S. and Cukic, B. (2015). Effect of User Posture and Device Size on the Performance of Touch-Based Authentication Systems. *IEEE 16th International Symposium on High Assurance Systems Engineering (HASE)*, Daytona Beach Shores, Florida, United States, 10-17.

Symantec (2012). State of Mobility Survey. *Symantec commissioned ReReZ research*, Retrieved June-2, 2013, from http://www.symantec.com/content/en/us/about/media/pdfs/bstate_of_mobility_survey_2012.en-us.pdf.

Tan, P.-N., Steinbach, M. and Kumar, V. (2006). Classification: basic concepts, decision trees, and model evaluation. *Introduction to Data Mining*. 1, 145-205.

Tasia, C. J., Chang, T. Y., Cheng, P. C. and Lin, J. H. (2014). Two novel biometric features in keystroke dynamics authentication systems for touch screen devices. *Security and Communication Networks*. 7(4), 750-758.

Teh, P. S., Teoh, A. B. J., Tee, C. and Ong, T. S. (2010). Keystroke dynamics in password authentication enhancement. *Expert Systems with Applications*. 37(12), 8618-8627.

TNS (2012). Mobile Life 2012. *TNS*. Retrieved May 2, 2014, from http://www.tnsglobal.be/sites/default/files/whitepaper/tns_mobile_life_2012.pdf.

Toh, K.-A., Kim, J. and Lee, S. (2008). Biometric scores fusion based on total error rate minimization. *Pattern Recognition.* 41(3), 1066-1082.

Tripathi, K. (2011). A Comparative Study of Biometric Technologies with Reference to Human Interface. *International Journal of Computer Applications*. 14(5).

Trojahn, M. and Ortmeier, F. (2013). Toward mobile authentication with keystroke dynamics on mobile phones and tablets. *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA*), Barcelona Spain, 697-702.

Tu, H. (2012). Designing Touch-based Gesture Interactions. Information Systems Engineering, Kochi University of Technology, German, PhD Thesis.

Veniamin Ginodman, M. N. O., Mr Ram Herkanaidu, Mr, Meng, W., S. Wong, D. and Kwok, L.-F. (2014). The effect of adaptive mechanism on behavioural biometric based mobile phone authentication. *Information Management & Computer Security*. 22(2), 155-166.

Vijayarani, S. and Muthulakshmi, M. (2013). Comparative Analysis of Bayes and Lazy Classification Algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*. 2(8), 3118-3124.

Vohra, R. (2014). Prediction of Diabetes Using Bayesian Network. *International Journal of Computer Science & Information Technologies.* 5(4), 5174-5178.

Wahbeh, A. H. and Al-Kabi, M. (2012). Comparative Assessment of the Performance of Three WEKA Text Classifiers Applied to Arabic Text. *Journal of Abhath Al-Yarmouk Basic Science and Engineering*, *21*(1), 15-28.

Wald, R., Khoshgoftaar, T. and Napolitano, A. (2013). Filter-and wrapper-based feature selection for predicting user interaction with Twitter bots. *IEEE 14th International Conference on Information Reuse and Integration (IRI)*, San Francisco, California, 416-423.

Wang, H., Lymberopoulos, D. and Liu, J. (2015). Sensor-Based User Authentication. *European Conference on Wireless Sensor Networks (EWSN)*. Porto, Portugal, 168-185.

Warwick, A. (2010). Millions downloaded suspicious Android wallpaper. *Warwick*. Retrieved August 2, 2012, from Computer Weekly: http://www. computerweekly.com/news/1280093401/Millions-download-suspicious Android-wallpaper.

Watanabe, Y. and Fujita, T. (2013). Toward Introduction of Immunity-based Model to Continuous Behavior-based User Authentication on Smart Phone. *Procedia Computer Science*. 22, 1319-1327.

Wayman, J., Jain, A., Maltoni, D. and Maio, D. (2005). An introduction to biometric authentication systems: Technology, Design and Performance Evaluation. *New York, Springer*, 1-20.

Westfeld, A. (2007). ROC curves for steganalysts. *Proceedings of the 3rd WAVILA Challenge (WaCha)*, Saint Malo, France, 39-45.

Wiedenbeck, S., Waters, J., Birget, J.-C., Brodskiy, A. and Memon, N. (2005). PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*. 63(1), 102-127.

Wilson, C., Hicklin, A. R., Bone, M., Korves, H. and Grother, P. B. (2004). Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report. *National Institute of Standards and Technology*. Technical Report NISTIR 7123, Nat'l Inst. Standards and Technology.

Witten, I. H. and Frank, E. (2005). Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations. *Morgan Kaufmann.*

Wolff, M. (2013). Behavioral Biometric Identification on Mobile Devices. *15th International Conference on Human-Computer Interaction (HCI)*, Las Vegas, United States, 783-791.

Xhemali, D., Hinde, C. J. and Stone, R. G. (2009). Naive Bayes vs. decision trees vs. neural networks in the classification of training web pages. *International Journal of Computer Science Issues (IJCSI)*. 4(1), 16-23.

Xu, H., Zhou, Y. and Lyu, M. R. (2014). Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones. *Proceedings of the Tenth Symposium on Usable Privacy and Security (SOUPS 2014)*, Menlo Park Caltrain, United States, 187-198.

Yan, P. (2006). Ear biometrics in human identification. University of Notre Dame, United States, PhD Thesis.

Yampolskiy, R. V. and Govindaraju, V. (2010). Taxonomy of behavioural biometrics. *Behavioral Biometrics for Human Identification*. 1-43.

Zhai, S., Kristensson, P. O., Appert, C., Anderson, T. H. and Cao, X. (2011). Foundational Issues in Touch-Surface Stroke Gesture Design—An Integrative Review. *Human–Computer Interaction*. 5(2), 97-205.

Zhang, H., Patel, V. M., Fathy, M. and Chellappa, R. (2015).Touch Gesture-Based Active User Authentication Using Dictionaries. *IEEE Winter Conference on Applications of Computer Vision*, Waikoloa Hawai‘i, United States, 207-214.

Zhang, X. (2011). Finger Movements Based on Biometric Authentication for Touch Devices. *Department of Informatics, Oslo University*, Norway, Master Thesis.

Zhao, Y. and Zhang, Y. (2008). Comparison of decision tree methods for finding active objects. *Advances in Space Research*. 41(12), 1955-1959.

Zheng, N., Bai, K., Huang, H. and Wang, H. (2012). You Are How You Touch: User Verification on Smartphones via Tapping Behaviors. *IEEE 22nd International Conference on Network Protocols*, Raleigh, Carolina, United States, 221 – 232.