



05-4506832



pustaka.upsi.edu.my



Perpustakaan Tuanku Bainun  
Kampus Sultan Abdul Jalil Shah



PustakaTBainun



ptbupsi

# DESIGN AND EVALUATION OF NEW SENSORS- BASED SMARTPHONE AUTHENTICATION TECHNIQUES

MOCEHEB LAZAM SHUWANDY ALRUFAYE



05-4506832



pustaka.upsi.edu.my



Perpustakaan Tuanku Bainun  
Kampus Sultan Abdul Jalil Shah



PustakaTBainun



ptbupsi

SULTAN IDRIS EDUCATION UNIVERSITY

2019



05-4506832



pustaka.upsi.edu.my



Perpustakaan Tuanku Bainun  
Kampus Sultan Abdul Jalil Shah



PustakaTBainun



ptbupsi



05-4506832



pustaka.upsi.edu.my



Perpustakaan Tuanku Bainun  
Kampus Sultan Abdul Jalil Shah



PustakaTBainun



ptbupsi

# DESIGN AND EVALUATION OF NEW SENSORS-BASED SMARTPHONE AUTHENTICATION TECHNIQUES

MOCEHEB LAZAM SHUWANDY ALRUFAYE



05-4506832



pustaka.upsi.edu.my



Perpustakaan Tuanku Bainun  
Kampus Sultan Abdul Jalil Shah



PustakaTBainun



ptbupsi

THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENT FOR THE  
DEGREE OF DOCTOR OF PHILOSOPHY

FACULTY OF ART, COMPUTING AND CREATIVE INDUSTRIES  
SULTAN IDRIS EDUCATION UNIVERSITY

2019



05-4506832



pustaka.upsi.edu.my



Perpustakaan Tuanku Bainun  
Kampus Sultan Abdul Jalil Shah



PustakaTBainun



ptbupsi



UPSI/IPS-3/BO 32  
Pind: 00 m/s: 1/1

## INSTITUTE OF GRADUATE STUDIES DECLARATION OF ORIGINAL WORK2

Please tick ( ✓ )

Project Paper

Masters by Research

Masters by Mix Mode

Ph.D.

✓

This declaration is made on the 12/11/2019

### i- Student's Declaration:

I Moceheb Lazam Shuwandy Alrufaye-P20161000220-Faculty of Art, Computing, and Creative Industry hereby declares that the dissertation /thesis for Doctor of Philosophy titled "Design and Evaluation of New Sensors-Based Smartphone Authentication Techniques" is my original work. I have not plagiarized from any other scholar's work and any sources that contain copyright had been cited properly for the permitted meanings. Any quotations, excerpt, reference or re-publication from or any works that have copyright had been clearly and well cited.

Signature of the student

### ii- Supervisor's Declaration:

I Dr. Bilal Bahaa Zaidan hereby certify that the work entitled, "Design and Evaluation of New Sensors-Based Smartphone Authentication Techniques" was prepared by the above-named student, and was submitted to the Institute of Graduate Studies as a partial / full fulfillment for the conferment of the requirements for Doctor of Philosophy (By Research), and the aforementioned work, to the best of my knowledge, is the said student's work.

Date

Signature of the Supervisor

**INSTITUT PENGAJIAN SISWAZAH /  
INSTITUTE OF GRADUATE STUDIES****BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK  
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM**

Tajuk / Title: **Design and Evaluation of New Sensors-Based Smartphone Authentication Techniques**

No. Matrik / Matric No.: **P20161000220**

Saya / I: **Moceheb Lazam Shuwandy Alrufaye**

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)\* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-

*acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-*

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.  
*The thesis is the property of Universiti Pendidikan Sultan Idris*
2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.  
*Tuanku Bainun Library has the right to make copies for the purpose of reference and research.*
3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.  
*The Library has the right to make copies of the thesis for academic exchange.*
4. Sila tandakan ( ✓ ) bagi pilihan kategori di bawah / Please tick ( ✓ ) from the categories below:-

☐**SULIT/CONFIDENTIAL**

Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / *Contains confidential information under the Official Secret Act 1972*

☐**TERHAD/RESTRICTED**

Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restricted information as specified by the organization where research was done.*

☐**TIDAK TERHAD / OPEN ACCESS**

(Tandatangan Pelajar/ Signature)

(Tandatangan Penyelia / Signature of Supervisor)

&amp; (Nama &amp; Cop Rasmi / Name &amp; Official Stamp)

Tarikh: \_\_\_\_\_

Catatan: Jika Tesis/Disertasi ini **SULIT @ TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

*Notes: If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the related authority/organization mentioning the period of confidentiality and reasons for the said confidentiality or restriction.*





## ACKNOWLEDGMENT



First of all, I want to thank Allah to help me to complete this thesis.



Foremost, I would like to express my sincere gratitude to my supervisor Dr. Bilal Baha, for the continuous support of my Ph.D. study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. He supported me through the whole writing process from the start to end. He has given me advice and kept me on the right path.



I would also like to thank my family, my father, my wife and my children who supports me.



Special thanks to Dr. Aws Allaa to help me to collect the participants. I'd like to thanks the staff of Lab in the new campus of UPSI who has helped me to use the lab in order to complete the development apps of this thesis. Most thank my friends who help me Mussab Allaa, Khalid Ibrahim, and Ahmed Marwan to help me to complete the experiments. Lastly, I want to thank all of our participants, who gave me their time, not once but multi-times. Special thanks to my brother Abdullah Al-Moodi to help me by his advices. Finally Most thanks to FSKIK's staff to help me through my Ph.D. study.

Moceheb Lazam Shuwandy,





## ABSTRACT

This study aims to design, develop, and test new sensor-based smartphone authentication techniques with the use of new sensors, namely 3D-touch and microphone sensors, with the former being used to simulate the hardware of the 3D-touch sensor of iPhone. Essentially, a 3D-touch sensor converts the authentication pattern of Android devices into a multi-layer pattern. For the microphone sensor, an authentication method based on a silent air-blowing technique was proposed and developed. The proposed authentication schemes were tested, evaluated, and validated based on several scenarios. Two experimental settings, namely controlled and uncontrolled, were used to test the usability (i.e., the remember rate) of the authentication schemes with a sample size of 92 participants, consisting of 60 males and 32 females. False Reject Rate (FRR) and False Accept Rate (FAR) were utilized to analyze the security performance of such schemes by exposing each authentication pattern to various measures of FRR and FAR. Finally, a comparison of groups was performed to compare the analysis that helped provide greater insight into such usability measures. The results showed that the remember rates of the 3D-touch and microphone sensors were 26.25% and 8.22%, respectively, under the uncontrolled setting. In contrast, under the controlled setting, the remember rates of the 3D-touch and microphone sensors were 40.51% and 42.30%, respectively. Also, the FRR and FAR measures of the 3D-touch sensor were 66.73% and 0.15%, respectively. For the microphone sensor, the FRR and FAR measures were 58.04% and 39.17%, respectively. Also, the average results of the 3-Dimension Touchscreen Pattern Test (3DTPT) and Blowing-Voiceless Password (BVP) for both genders were 34.78% and 22.36%, respectively. In conclusion, the research findings were promising despite stringent experimental restrictions. The implication of this study is that the improvement of current sensor-based authentication techniques can be achieved based on the usability of such techniques.





## REKA BENTUK DAN PENGUJIAN TEKNIK-TEKNIK PENGESAHAN TELEFON PINTAR BERASASKAN PENDERIA BAHARU

### ABSTRAK

Kajian ini bertujuan untuk mereka bentuk, membangun, dan menguji beberapa teknik pengesahan telefon pintar berasaskan penderia pintar baharu, iaitu penderia sentuhan 3D dan penderia mikrofon, di mana penderia kedua digunakan untuk mensimulasikan peranti penderia sentuhan 3D iPhone. Secara asasnya, penderia sentuhan 3D menukar corak pengesahan peranti *Android* ke corak sentuhan 3D pelbagai lapisan. Untuk penderia mikrofon, kaedah pengesahan berdasarkan teknik tiupan senyap dicadangkan dan dibangunkan. Skema pengesahan yang dicadangkan telah diuji, dinilai, dan disahkan berdasarkan beberapa senario. Dua set eksperimen, iaitu dikawal dan tidak dikawal, digunakan untuk ujian kebolegunaan (i.e., kadar ingatan) skema berkenaan dengan saiz sampel yang terdiri daripada 92 peserta yang melibatkan 60 lelaki dan 32 wanita. *False Reject Rate* (FRR) dan *False Accept Rate* (FAR) digunakan untuk menganalisis prestasi keselamatan skema berkenaan dengan mendedahkan setiap corak pengesahan kepada beberapa ukuran FRR dan FAR. Akhir sekali, satu analisis perbandingan dijalankan untuk menonjolkan kebolehan skema berkenaan. Dapatan menunjukkan kadar ingatan penderia sentuhan 3D dan penderia mikrofon dalam tetapan tidak dikawal adalah 26.25% dan 8.22%, masing-masing. Dalam tetapan dikawal pula, kadar ingatan penderia sentuhan 3D dan penderia mikrofon adalah 40.51% dan 42.30%, masing-masing. Tambahan pula, ukuran FRR dan FAR bagi penderia sentuhan 3D adalah 66.73% dan 0.15%, masing-masing. Untuk penderia mikrofon, ukuran FFR dan FAR adalah 58.04% dan 39.17%, masing-masing. Dapatan purata untuk *3-Dimension Touchscreen Pattern Test* (3DTPT) dan *Blowing-Voiceless Password* (BVP) bagi kedua-dua kumpulan jantina adalah 34.78% dan 22.36%, masing-masing. Sebagai kesimpulan, dapatan kajian adalah memberangsangkan dengan mengambil kira kekangan eksperimen yang ketat dalam kajian ini. Implikasi kajian ini menunjukkan peningkatan dalam teknik-teknik pengesahan berasaskan penderia semasa dapat dicapai berdasarkan kebolegunaan teknik-teknik berkenaan.



## CONTENTS

	Page
<b>DECLARATION OF ORIGINAL WORK</b>	<b>ii</b>
<b>DECLARATION OF THESIS</b>	<b>iii</b>
<b>ACKNOWLEDGMENT</b>	<b>iv</b>
<b>ABSTRACT</b>	<b>v</b>
<b>ABSTRAK</b>	<b>vi</b>
<b>CONTENTS</b>	<b>vii</b>
<b>LIST OF TABLES</b>	<b>xi</b>
<b>LIST OF FIGURES</b>	<b>xviii</b>
<b>LIST OF ABBREVIATIONS</b>	<b>xxv</b>
<b>LIST OF GLOSSARIES</b>	<b>xxvi</b>
<b>LIST OF APPENDICES</b>	<b>xxvii</b>
<b>CHAPTER 1 INTRODUCTION</b>	
1.1 Introduction	1
1.2 Research Background	2
1.3 Challenges Inherited from the Academic Literature to this Research	4
1.4 Problem Statement	8
1.5 Research Objectives	10
1.6 Research Questions	10
1.7 Research Scope	11
1.8 Research Flow	12
1.9 Operations and Definitions	15
1.10 Thesis Outlines	16
<b>CHAPTER 2 LITERATURE REVIEW</b>	
2.1 Introduction	19
2.2 Systematic Review Method	19
2.2.1 Information Sources	20
2.2.2 Study Selection	21



2.2.3	Search Scenario	21
2.2.4	Eligibility Criteria	23
2.2.5	Data Collection Process	23
2.3	Taxonomy of Research Literature	24
2.3.1	Defense Articles	28
2.3.2	Attack Articles	34
2.3.3	Others Articles	35
2.4	Motivations, Challenges and Recommendations	35
2.4.1	Articles's Motivations	36
2.4.2	Articles's Challenges	47
2.4.3	Articles's Recommendations	57
2.5	Methodology Aspects of Previous Researches	62
2.5.1	Sample Size	63
2.5.2	Age Group	64
2.5.3	Gender Group	65
2.5.4	Frequency of Attempts Iteration and Time Interval	66
2.5.5	Equipment Types	69
2.5.6	Performance Analysis	70
2.5.7	Sensors Utilized in the Previous Studies	71
2.6	Literature Synthesis	72
2.7	Methods and Materials	75
2.8	Chapter Summary	81

### CHAPTER 3 RESEARCH METHODOLOGY

3.1	Introduction	83
3.2	Research Methodology Phases	84
3.2.1	Phase One: Systematic Review	87
3.2.2	Phase Two: Design New Sensor Based Smartphone	88
3.2.3	Phase Three: Development and Data Collection	105
3.2.4	Phase Four: Usability Testing	114
3.3	Chapter Summary	124

### CHAPTER 4 DEVELOPMENT AND TESTING OF 3D TOUCHSCREEN SENSOR

4.1	Introduction	126
4.2	Sensor and Authentication Approach Development	128

4.2.1	Android Studio	129
4.2.2	Activities and Layouts	130
4.2.3	3D Touch Screen Sensor	143
4.3	3DTPT App Testing	152
4.4	3DTPT App Validation	158
4.4.1	Validate the Pattern Value in Database	160
4.4.2	Oily Residues on Touchscreen	163
4.5	Chapter Summary	165

## CHAPTER 5 DEVELOPMENT AND TESTING OF MICROPHONE SENSOR

5.1	Introduction	166
5.2	Sensor and Authentication Approach Development	168
5.2.1	Android Studio	169
5.2.2	Activities and Layouts	170
5.2.3	Permissions	178
5.2.4	Microphone Sensor	182
5.3	BVP App Testing	185
5.4	BVP App Validation	191
5.4.1	Validate the BVP Pattern Value in Database	191
5.4.2	Validation Avoid the Problem of Voice Detection	193
5.5	Chapter Summary	194

## CHAPTER 6 UNCONTROLLED AND CONTROLLED EXPERIMENTS

6.1	Introduction	195
6.2	Sensors Dataset	197
6.3	Uncontrolled Experiment	199
6.3.1	3D Touchscreen Sensor (TPT)	202
6.3.2	Microphone Sensor (BVP)	211
6.4	Controlled Experiment	219
6.4.1	3D Touchscreen Sensor (TPT)	220
6.4.2	Microphone Sensor (BVP)	231
6.5	Result Finding	241
6.5.1	3D Touchscreen Finding	241
6.5.2	Microphone Finding	243
6.6	Chapter Summary	245

## CHAPTER 7 USABILITY TESTING BY FAR, FRR, GENDER AND AGE

7.1	Introduction	247
7.2	FAR and FRR	248
	7.2.1 Multi-Attempts per Participant of TPT	248
	7.2.2 Multi-Attempts per Participant of BVP	253
7.3	Gender and Age Groups	257
	7.3.1 Male Participants	257
	7.3.2 Female Participants	273
7.4	Result Finding	291
	7.4.1 FAR and FRR	291
	7.4.2 Gender and Age Groups	291
7.5	Chapter Summary	293

## CHAPTER 8 CONCLUSION

8.1	Introduction	295
8.2	Discussion and Highlight Points	295
8.3	How Research Objectives were Achieved	298
8.4	Research Limitations	299
8.5	Conclusion	300
8.6	Future Work	301

<b>REFERENCES</b>	302
-------------------	-----

<b>APPENDICES</b>	312
-------------------	-----

## LIST OF TABLES

Table No.	Page
2.1 Age Groups Distribution	64
2.2 Gender distribution	65
2.3 Frequency of Iteration Attempts	67
2.4 Detail the List Different Time Interval System and Time Used	68
3.1 Sample of Analysis Table Used in the Literature Analysis	87
3.2 3D Touchscreen Requirement and Solution	92
3.3 Microphone Sensor Requirement and Solution	94
3.4 Android Version Distribution	97
3.5 Unique Patterns with Respect to the Length of Pattern	107
3.6 Proposed Time Interval Configuration for our Experiment	112
4.1 The Purpose of Each Layout	139
4.2 The User Interface Element of Pattern_Screen with XML View	141
4.3 Sign up Decision Table of Black box testing	154
4.4 The Information from the Database of MySql and ORIGINAL Pass	155
4.5 Sign in Decision Table of Black box testing	156

4.6	3DTPT Attempts Decision Table	157
4.7	The Information from the Database of Mysql	157
4.8	Example of Developer's attempts	161
4.9	Validation Avoid the Problem of Oily Effects using Imposters Guesses	164
5.1	The Purpose of Each Layout	176
5.2	The User Interface Element of Record_screen with XML View	177
5.3	The API of each Sensor	182
5.4	Examples of count pulses by BVP pattern	185
5.5	BVP Sign up Decision Table of Black box testing	185
5.6	The Information from the Database of MySql and Pass ORIGINAL	187
5.7	Sign in Decision Table of Black box testing of BVP	188
5.8	BVP Attempts Decision Table of BVP	189
5.9	Information from the Database of MySql	190
5.10	Two Examples from the Dataset of BVP	191
6.1	Dataset of all Participants in Controlled and Uncontrolled Experiments	199
6.2	Records of all Participants in the Registration	200
6.3	Results of all Participants in 1 <sup>st</sup> and 2 <sup>nd</sup> Attempt Through Three Days	201
6.4	A Dataset Sample of the 1 <sup>st</sup> Attempt with Results Uncontrolled Experiment	204



6.5	Remember Rate of TPT for (73) Participants in 1 <sup>st</sup> attempt	207
6.6	Dataset of Participants in Second Attempts	208
6.7	Remember Rate of TPT for (3) Participants in 2 <sup>nd</sup> Attempt	211
6.8	Some Dataset of One Attempt with Results	213
6.9	Remember Rate of BVP for (73) Participants in 1 <sup>st</sup> Attempt	215
6.10	Dataset of Participants in Two Times Attempts	216
6.11	Remember Rate of BVP for (73) Participants in 2 <sup>nd</sup> Attempt	218
6.12	Dataset of Controlled Experiments of TPT for all Participants	220
6.13	Number of Participants According Attempts	221
6.14	Remember of 1 <sup>st</sup> Attempt of all Participants	222
6.15	Remember of 2 <sup>nd</sup> Attempt of (P1-P15) Participants	223
6.16	Remember of 3 <sup>rd</sup> Attempt of all Participants	224
6.17	Remember of 4 <sup>th</sup> Attempt of all Participants	225
6.18	Remember rate of 5 <sup>th</sup> Attempt of all Participants	226
6.19	Remember of 6 <sup>th</sup> Attempt of all Participants	227
6.20	Remember of 7 <sup>th</sup> Attempt of all Participants	228
6.21	Remember of 8 <sup>th</sup> Attempt of four Participants	229
6.22	Remember of 9 <sup>th</sup> Attempt of (P1-P3) Participants	230





6.23	Dataset of Controlled Experiments of BVP for all Participants	231
6.24	Number of Participants According Attempts of BVP	232
6.25	Remember Rate in 1 <sup>st</sup> Attempt to all Participants	232
6.26	Remember Rate in 2 <sup>nd</sup> Attempt to all Participants of BVP	234
6.27	Remember Rate in 3 <sup>rd</sup> Attempt to (n=8) Participants	235
6.28	Remember Rate in 4 <sup>th</sup> Attempt of all Participants	236
6.29	Remember Rate in 5 <sup>th</sup> Attempt to Six Participants	236
6.30	Remember Rate in 6 <sup>th</sup> Attempt to Five Participants	237
6.31	Remember of 7 <sup>th</sup> Attempt of all Participants	238
6.32	Remember of 8 <sup>th</sup> Attempt of all Participants	239
6.33	Remember of 9 <sup>th</sup> Attempt of (P1 and P2) Participants	240
6.34	The Finding Result of Uncontrolled Experiment	242
6.35	The Finding Result of Controlled Experiment	243
6.36	The Finding Result of Uncontrolled Experiment	244
6.37	The Finding Result of Controlled Experiment	245
7.1	Attempts Result of all Genuine Participants	249
7.2	Attempts P1 Imposter to Other Participants	249
7.3	Attempts P2 Imposter to Other Participants	250



7.4	Individuals Genuine and Imposter Results of P1-P10 Participants	251
7.5	Individuals Genuine and Imposter Results of P11-P19 Participants	252
7.6	Evaluation the Usability by FAR and FRR from (P1-P10)	252
7.7	Evaluation the Usability by FAR and FRR from (P11-P19)	252
7.8	Attempts Result of all Genuine Participants	253
7.9	Attempts P1 Imposter to Other Participants	254
7.10	Attempts P2 Imposter to Other Participants	255
7.11	Individuals Genuine and Imposter Results of P1-P10 Participants	255
7.12	Individuals Genuine and Imposter Results of P11-P15 Participants	256
7.13	Evaluation the Usability by FAR and FRR from (P1-P10)	256
7.14	Evaluation the Usability by FAR and FRR (P11-P15)	256
7.15	The Number of Male Participants According to Dates in all Age Groups	258
7.16	Some Dataset of Attempt	259
7.17	Male Participants of (1-9) Attempts in TPT Experiment	260
7.18	TPT Results of Male Participants in each Login Attempts	262
7.19	Male Participants of (1-9) Attempts in BVP Experiment	263
7.20	BVP Attempts of Male Participants	264
7.21	Number of Male Participants 18-35 Through Five Days	265



7.22	Male Participants of (1-9) Attempts in TPT Experiment in 18-35 Years	265
7.23	TPT Attempts of Male Participants 18-35 Years	266
7.24	Male Participants of (1-8) Attempts in BVP Experiment in 18-35 Years	267
7.25	BVP Attempts of Male Participants 18-35 Years	268
7.26	Number of Male Participants 36-55 through Five Days	269
7.27	Male Participants of (1-9) Attempts in TPT Experiment in 36-55 Years	270
7.28	TPT Attempts of Male Participants 36-55 Years	271
7.29	Male Participants of (1-9) Attempts in BVP Experiment in 36-55 Years	272
7.30	BVP Attempts of Male Participants 36-55 Years	272
7.31	Number of Male Participants Older than 55 Years Old Through Five Days	273
7.32	TPT Attempts of Male Participants Older than 55 Years	274
7.33	BVP Attempts of Male Participants Older than 55 Years	274
7.34	The Number of Female Participants According to Dates in all Age Groups	275
7.35	The Number of Female Participants According to Dates	277
7.36	Female Participants of (1-3) Attempts in TPT Experiment for all Female	278
7.37	TPT Attempts of Female Participants	279
7.38	Female Participants of (1-3) Attempts in BVP Experiment in All Female	280
7.39	BVP Attempts of Female Participants	280



7.40	Number of Female Participants Less than 18 through Five Days	281
7.41	Number of Female Participants 18-35 through Five Days	282
7.42	Female Participants of (1-3) Attempts in TPT Experiment in 18-35 Years	283
7.43	TPT Attempts of Female Participants 18-35 Years	284
7.44	Female Participants of (1-3) Attempts in BVP Experiment in 18-35 Years	285
7.45	BVP Attempts of Female Participants 18-35 Years	286
7.46	Number of Female Participants 36-55 through Five Days	287
7.47	Female Participants of (1-3) Attempts in TPT Experiment in 36-55 Years	288
7.48	TPT Attempts of Female Participants 36-55 Years	289
7.49	Female Participants of (1-3) Attempts in BVP Experiment in 36-55 Years	289
7.50	BVP Attempts of Female Participants 36-55 Years	290
7.51	The Finding Result of Usability Test According the Gender and Age	293



## LIST OF FIGURES

Figure No.	Page
1.1 Challenges and Issues Categories	8
1.2 Research Flow	14
2.1 Flow Chart of Study Selection, Including the Search Query and Inclusion	22
2.2 Number the Articles According to Index Source and Type	24
2.3 (A) Sensors, (B) Axes, (C) Position of Phone During Gait Recognition	25
2.4 Total Articles According the Countries	26
2.5 A Taxonomy of Research Literature on Authentication of Smartphone Based	27
2.6 Number of Included Articles in Different Categories by Years of Publication	28
2.7 Using a Magnet to Perform 3D Magnetic Signature in the Space a Round	31
2.8 The Behavior Authentication Pattern in (a) and (b)	32
2.9 Gait Recognition by Gait Cycle (Hoang et al., 2013)	32
2.10 Benefits Categories for Smartphone Authentication Based Sensor	37
2.11 Challenges Categories for Smartphone Authentication Based Sensor	48
2.12 Recommendations Categories for Smartphone Authentication Based Sensor	59

2.13	Methodological Aspects Illustrated from Previous Studies	62
2.14	Number of Samples According to Academic Articles	63
2.15	Visualization of Gender Distribution	66
2.16	Different Time Interval System, A (Sec.), B (Min.), C (Day), D (Week)	68
2.17	Devices Used in the Previous Studies and the Frequency of Usage	70
2.18	Low FRR and High FAR, more Usability (Feng, Zhao, et al., 2013)	71
2.19	Sensors Utilized in the Academic Literature	72
3.1	Relation Between Methodology Phases, Research Objectives	85
3.2	Research Methodology Phases	86
3.3	Toptic Engine in 3D Touchscreen Sensor in the iPhone	89
3.4	A. The 3D Touchscreen Sensor Layer B. Transport from Level 1 to Level 2	91
3.5	The Apps mic.apk for Recording Voice	94
3.6	Android System Architecture	96
3.7	Android Version Distribution Pie-chart	98
3.8	Use Case Diagram of Checking and Register New User	99
3.9	Sequence Diagram of Signup Scenario for New Participant	100
3.10	Login Scenario for Checking Username and Password in Database	102



3.11 Sequence Diagram of Sign in Scenario for Participant	103
3.12 Update Scenario for Store Data of Sensor in Database	104
3.13 Sequence Diagram of Update Scenario for Participant	105
3.14 Air Blowing Technique	106
3.15 Proposed 3D Touch Based Authentications	108
3.16 Sample Size, Gender and Age of Participants	110
3.17 Usability Criteria	115
3.18 The First Attempt for Using Process of Authentication	116
3.19 The Usability Testing Relation between Criteria and Remember	117
3.20 Using Participant Attempts as Impostor Attempts to Other Genuine	119
3.21 Using Participant Attempts as Genuine Attempts to Other Genuine	120
3.22 Group Comparisons	122
3.23 Example of Levenshtein distance metric	124
4.1 Chapter Content Structure	128
4.2 Huawei Tablet T1-701u device Apply 3D TPT	129
4.3 Android Studio User Interface	130
4.4 The Activity and Layout Files	131



4.5	Life Cycle of Activity	133
4.6	The Main Activity Contents	134
4.7	The Code of the Main Activity	135
4.8	Pseudo Code: Check the Signup information in the class	136
4.9	Flowchart to Checking the Username Before Signup Operation	137
4.10	Left: The Layout Design and Right: XML Code of this Design	139
4.11	Left: The Layout Design of main2 activity. Right: XML Code	140
4.12	Left: The Layout Design of Pattern_Screen. Right: XML Code	141
4.13	Left: The Layout of Signup Activity. Right: XML Code of This Design	142
4.14	Psuedo Code to Determine the pressure in three levels	144
4.15	The Pressure Force Value of Activity_3DTPT	145
4.16	Touchscreen Sensor 6x6 Pixels	146
4.17	Force Pressure on Touchscreen in Level One 2x2 Pixels, Black Pixels	147
4.18	Force Pressure on Touchscreen in Level Two 4x4 Pixels	148
4.19	Force Pressure on Touchscreen in Level Three 6x6 Pixels	149
4.20	The Number Sequence of the Pattern Nodes and Direction	150
4.21	The Patterns Nodes Direction in Each Level	151



4.22 A. Choose Sign up B. Registration C. Set Pattern	154
4.23 A. Choose Sign in. B. Try 3dTPT	157
4.24 Validate Example on TPT Data Validator	159
4.25 Validate the Value of TPT and the Direction for Three Levels to Example	162
4.26 Sample pattern and its Smudge showing a direction of edges	164
5.1 The Structure Flow of the Chapter	168
5.2 Huawei Tablet T1-701u Device Apply BVP	169
5.3 Android Studio User Interface	170
5.4 The Activity and Layout Files	171
5.5 Life Cycle of Activity	172
5.6 The Procedure of “ActivitySignup”	174
5.7 Checking the Username before Signup Operation	174
5.8 The Activity_BVP Class Contents	175
5.9 Left: the Layout Design of Record Screen and Right: XML Code	176
5.10 The Permission Follow between Apps and Kernel Approval	179
5.11 Permission Request of Record Audio in Low Versions	180
5.12 Permission Request of Record Audio in High Versions	181





5.13	Microphone sensing by Pulse Last Level value recording	183
5.14	Psuedo Code Show Recording Listener	184
5.15	A. Choose Sign up, B. Registration, C. Try BVP by Record	187
5.16	Left: Choose Sign in, Right: Try BVP	189
5.17	Validate the Value of BVP and the Graph View with Blow Voiceless	192
6.1	View the Number of Participants and the Number of Records in Dataset	198
6.2	The Ratio of Male to Female in Uncontrolled Experiment	201
6.3	Compare Between the Results of Password and TPT of First Attempt	205
6.4	The TPT Remember Rate of all Participants	206
6.5	The TPT Remember Rate of all Participants in Two Attempts	209
6.6	Use Rate of TPT of all Participants in 2 <sup>nd</sup> Attempt	210
6.7	The Results of BVP in Two Times Attempts	213
6.8	The BVP Remember Rate of all Participants	214
6.9	The Results of BVP in two Times Attempts	217
6.10	The BVP Remember Rate of all Participants in 2 <sup>nd</sup> Attempt	218
7.1	Male Participants and the Age Groups Ratio	258
7.2	Number of Male Participants in Five Days	260





7.3	Female Participants and the Age Groups Ratio	276
7.4	Number of Participants Female in Five Days	277
7.5	The Number of Female Participants in Five Days 18-35 Years	283
7.6	The Number of Female Participants in Five Days 36-55 Years	287



## LIST OF ABBREVIATIONS

3D	3 Dimension
3DTPT	3 Dimension Touchscreen Pattern Test
App	Application
BVP	Blowing Voice Password
CLIP	Continuous Location Integrity and Provenance
FAR	The False Accept Rate
FRR	The False Reject Rate
IEEE	Institute of Electrical and Electronics Engineers
PC	Personal Computer
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PHP	Programming Hypertext Preprocessor
S	Successful
SD	Science Direct
U	Unsuccessful
WISDM	Wireless Sensor Data Mining
WoS	Web of Science





## LIST OF GLOSSARIES

Terms	Definition
Smartphone, smart phone, cell phone or mobile	It represents intelligent handphone. These four terms give the same meaning, and thus, the three alternatives used in the main body of this report.
Sensor or sensing	It is detectors that can measure some physical quality that is happening and able to convert the measurement into a signal. Both keywords used in the body of this thesis.
Participant, volunteer, subject and client	He/she is the person who does the experiment according to the app in this thesis.
Genuine or legitimate	He/she is the person who made the original password.
Imposter or illegitimate	He/she is a person who pretends to be a genuine person (i.e. Fake owner).
App or Application	An application, especially as downloaded by a user to a mobile device.
Last Level or LL	The last level when find absolute of the division of Levels Summation (SL) by Buffer Read Result (BRR)
Oily residues, or smudges	Smudges on the touch screen surface, are one side effect of touches from which frequently used patterns such as a graphical password might be inferred.



## LIST OF APPENDICES

A Literature View Tables

B Experiments Tables

C Development Tables



## CHAPTER 1

### INTRODUCTION



#### 1.1 Introduction

This chapter introduces the direction of our work, a brief background about the research, the state of the problem, the ambitions and motivation of this research, and the research objectives.

In Section 1.2, a brief background of the research components presented. In Section 1.3, the state of the problem on which the direction of the research has identified and introduced. In Section 1.4, Section 1.5 and Section 1.6, research objectives, research questions and the scope of the study reported respectively. In Section 1.7, the research flow reported. While, in Section 1.8, the operations and definitions reported, outline the main structure of the thesis briefly reported in section 1.9. Finally, In Section 1.10, chapter summary.





## 1.2 Research Background

The exploration of the literature reveals several research articles in the areas of sensors based smartphones authentication. A few years ago, several methods and technologies were developed to recognise genuine access to the smartphone. The scope of this study, discussed the usage of smartphone sensors, in particular, Orientation sensor (Accelerometer, Gyroscope and Magnetic sensors), finger sensor, camera sensor and touch screen sensor. The main focus of these studies related to usability and security (H. Wang, Lymberopoulos, & Liu, 2015). Authentication solutions based on biometrics are promising techniques to replace traditional authentication mechanisms where traditional techniques relying on personal identification numbers or passwords, which are often perceived as inconvenient by users (Fantana, Ramachandran, Schunck, & Talamo, 2016). Biometrics is inherently more reliable and more capable in differentiating between an authorised person and imposter than traditional methods. This can be done by verifying the owner's identity rather than merely confirming the user's knowledge or possession of a particular secret. The biometric approach has two types; behavioural and physiological. The biometric approach can efficiently prevent identity theft and unauthorised access to mobile terminal resources (Corpus, Gonzales, Morada, & Vea, 2016; Fantana et al., 2016; Sun & Wang, 2015)

In 2016 Ling stated, Residue-based attacks exploit oily or heat residues on the touch screen, computer vision-based attacks analyse the hand movement on a keyboard, and sensor-based attacks measure a device's motion difference via motion sensors as different keys are tapped (Ling et al., 2016). The use of sensors has varied, and new ways of protecting smart devices have developed. User recognition methods without





requiring identification made by detecting the user's fingertip (Ali, Payton, & Sritapan, 2016), gesture (S. Lee, Song, & Choi, 2012; Liu, Wang, Zhao, Yan, & Ding, 2016; Sun & Wang, 2015) or gait (Muaaz & Mayrhofer, 2013; Nickel, Brandt, & Busch, 2011). Some of these studies based on the user's behaviour, and therefore the authentication was divided into four sections: Continuous Authentication (Crouse, Chandra, & Barbello, 2013; Roy, Halevi, & Memon, 2015), Implicit Authentication (Dandachi, Hassan, & Hussein, 2013; Feng et al., 2014), Mechanism Authentication (Laghari & Memon, 2016; Shih, Lu, & Shih, 2015) and hybrid tracking (Feng et al., 2014).

With this development on both smartphone sensor-based defence and attack, researchers developed methods so users can easily use that, and it happens through specific criteria (Goethem(B), Scheepers, Preuveneers, & Joosen, 2016; Lin, Chang, Liang, & Yang, 2012; Nguyen, Nguyen, Hoang, Choi, & Nguyen, 2016). In 2014, Rybnicek reported the lack of databases of available user samples containing stored data from the accelerometer, gyroscope, touch screen, keyboard, and terrestrial magnetic sensors, therefore, researchers are required to acquiring data prior the exploration of new authentication technique (Rybnicek, Lang-Muhr, & Haslinger, 2014). Nevertheless, several researchers used ready-made dataset (Pisani, Lorena, & De Carvalho, 2017).

Exploring the literature via a systematic review classified articles based on the patterns founded into two categories, articles related to the usage of smartphone sensors on attacking phones 4.93% ( $n=4/81$ ) articles and articles developed new smartphone sensors authentication techniques to defend the smartphones from attackers 86.41% ( $n=70/81$ ) articles. Rather than that, there are few research articles related to





smartphone sensor-based security are utilized more than one sensor type sensors for evaluation, data acquisitions and/or another related topic 8.64% ( $n=7/81$ ) articles. These articles are listed in a dedicated category named as others. Further analysis can be found in chapter two section 2.3.

Therefore, research in this area opens a new era of smartphone authentication application which required long investigation and exploration to develop a mutual sensor-based authentication approaches.

### 1.3 Challenges Inherited from the Academic Literature to this Research

In the age of technology, smartphones are not only a device to make phone calls but also, banking transaction, e-wallet, health monitoring device, browsing internet, social activities, and several other functions. Thanks to sensors and sophisticated electronic gadgets attached to the smartphone devices made the smartphone the most ever used devices with estimation of 62.5% of the worldwide population owned smartphone in 2016. However, comfortability increased alongside with security vulnerability. Therefore, smartphone required a high level of protection to ensure users' privacy and guarantee genuine access to the smartphone. Sensor-based authentication considers as one of the latest security technologies started in the second decade of 21 century. An intensive review on the academic literature suggested several challenges and barriers when developing new sensor-based authentication. The relevant challenges to this research would be categorized into six main groups associated with several aspects per category. The first concern is related to concern on data protection, where reliable







authentication technique is required (Dandachi et al., 2013; Feng et al., 2014; Nixon, Chen, Mao, Chen, & Li, 2013; Rahman, Gani, Ahsan, & Ahamed, 2014; Sanzziri, Nandugudi, Upadhyaya, & Qiao, 2013; Zhu, Wu, Wang, & Zhang, 2013). In addition to that, the new method should avoid leaving any security vulnerabilities sources such as oil on screen in the case of patterns drawing or lips movement with voice recognition. Both vulnerabilities can be decoded into the authentication code (Aviv, Sapp, Blaze, & Smith, 2012; Hussain et al., 2016; S. Lee et al., 2012; Ling et al., 2016; H. Yang et al., 2015; Zheng, Bai, Huang, & Wang, 2014). The second concern is related to the applicability of the new authentication technique. This challenge involves several technical aspects such view behavior (i.e. ensure the correct pattern made) (Pisani, Lorena, & De Carvalho, 2017), access to sensors permissions which is mostly relies on API's of the android (Feng et al., 2014; Hussain et al., 2016; W.-H. L. and R. B. Lee & Princeton, 2015; Owusu, Han, Das, Perrig, & Zhang, 2012). This feature can limit the choice of the developers or developers are required to produce multi-versions of a particular app. The other aspect in this challenge is by having multiple android versions which have different development strategy (Chen, S., Pande, A., and Mohapatra, 2014; Hoang, Nguyen, Luong, Do, & Choi, 2013; Witte, Rathgeb, & Busch, 2013) while the last aspect is related to activity recognition in which, features of a particular sensor data needs a flexible mechanism of recognition (Bajrami, Derawi, & Bours, 2011; Islam, Naeem, & Amin, 2017; W.-H. L. and R. B. Lee & Princeton, 2015). The set of aspects in this challenge can be handled during the development. However, it would limit the participants during the controlled experiment and focused groups. It would also limited the number of participants if the experiment design is an uncontrolled group.





The third concern is related to the sensor's availability (i.e. sensors are available with a device rather than other devices, e.g. iPhone and Android devices etc.). Unlike, the devices operated by Android, 3D touch sensor is available with iPhone LCD's in hardware, therefore, when developers planning to develop apps of such sensor with Android devices, they need to simulate the 3D touch sensor with different scenarios. Similarly, other sensors are required to be implemented in a simulated environment (Laghari & Memon, 2016; Sun & Wang, 2015). Nonetheless, user behavior (i.e. the way of using the simulated or hardware sensor) should be considered during the development (Shen, Li, Chen, Guan, & Maxion, 2017). Several examples of user behavior are explained in chapter two. Sensors such as fingerprint, gyroscope, accelerometer and other sensors are developed and utilised in several apps. Thus, public datasets are available per sensor to study that particular sensor without developing a data collection approach. New sensors are required data collection which considers as a challenging task (Hussain et al., 2016). Dataset availability considers as the fourth challenge discussed in this thesis. Aspects such as different devices (Feng et al., 2014; Haque, Zawood, & Hasan, 2013; Hoang et al., 2013; Islam et al., 2017) and different software (Chen, S., Pande, A., and Mohapatra, 2014; Hoang et al., 2013; Witte et al., 2013) are always creating barriers towards developing new sensors-based authentication. Figure 1.1.

Datasets for such authentication scenarios and quality of the collected data are yet another challenge to study new authentication techniques (Ali et al., 2016; Shih et al., 2015; Sun & Wang, 2015). Traditional authentication such as pin and password require explicit interaction and thus is time-consuming and not very user-friendly (Nickel & Busch, 2013).





The other challenge identified in the literature is the usability. Insufficient security might lead serious security and privacy issues (Derawi, Bours, & Holien, 2010). Therefore, the development of strong authentication technique is an urgent need (Bajrami et al., 2011; Derawi, Bours, et al., 2010). However, there is a tradeoff between authentication technique and usability (Chen, S., Pande, A., and Mohapatra, 2014; Crouse et al., 2013; Feng, Zhao, Carbunar, & Shi, 2013; S. Lee et al., 2012; Nguyen, Nguyen, Hoang, Choi, & Nguyen, 2016; Nguyen Ngoc Diep, Cuong Pham, 2015; H. Wang et al., 2015; H. Yang et al., 2015; Zheng et al., 2014). Sensor-based authentication is a newly identified authentication approach. This approach can play a great role in the future of smartphone authentication. However, such approaches produced a none standard patterns in the sense of pattern layout (Nguyen et al., 2016; Zhong, Deng, & Meltzner, 2015) if imposters are incapable of copying these patterns. An imposter is a person or machine that are attacking smartphone by fake authentication codes. Imposters consider as one of the important usability aspect (Abate, Nappi, & Ricciardi, 2017; Guerra-Casanova, J., Sanchez-Avila, C., Bailador Del Pozo, G., & De Santos-Sierra, 2013; Guerra-Casanova, Sánchez-Ávila, Bailador, & de Santos Sierra, 2012; Pisani, Lorena, & De Carvalho, 2014; Pisani et al., 2017; Shila, Srivastava, O'Neill, Reddy, & Sritapan, 2016; H. Wang et al., 2015).

The last concern is related to cost which can be considered of upgrading hardware (Feng, Prakash, & Shi, 2013; Lyu et al., 2015; Muaaz M.; Mayrhofer R., 2015; Nguyen et al., 2016; Nickel, Brandt, et al., 2011; Nixon et al., 2013; Roshandel, Haji-Abolhassani, & Ketabdar, 2015), power (Feng, Prakash, et al., 2013; Lyu et al., 2015) and time (Chen, S., Pande, A., and Mohapatra, 2014; Zheng et al., 2014).







or at least within the scope of this systematic review. Therefore, to develop a new sensor-based authentication technique, the researcher should consider the above authentication challenges. Apart from the mentioned challenges, there are articles discussed techniques that are capable of reading the people lips movement (unconnected to the internet) over walls (Adib et al., 2014; Wei et al., 2015; G. Wang et al., 2016; Cheng, Bagci & Yan, 2018). Such capacity of attackers leaves no choice for developers but to develop a silent voice, no face changes (including lips movement) and leave no sign of usage on the smartphone (Aviv, Sapp, Blaze, & Smith, 2012; Hussain et al., 2016; S. Lee et al., 2012; Ling et al., 2016; H. Yang et al., 2015; Zheng, Bai, Huang, & Wang, 2014). Therefore, this research is an attempt to develop new sensors-based authentication techniques for smartphones. The new proposed authentication suggested utilizing unexplored sensors namely microphone sensor and the 3D touchscreen sensor.



Looking at the previous section, there are several challenges need to be addressed in order to develop new sensor-based authentication. These challenges inherited to this thesis; in particular, dataset availability for the proposed sensors are not available or at least within the scope of this research (Haque et al., 2013; Muaaz M.; Mayrhofer R., 2015; Sun & Wang, 2015; Nickel et al., 2012). The other challenge is related to user behavior to modulating the user behavior required understanding the parameters and set rules in order to perform the authentication approach. Nonetheless, simulating sensors if the sensors are not available in hardware form (Sun & Wang, 2015; Laghari & Memon, 2016; Ketabdar et al., 2012; Roshandel et al., 2015; Zhong et al., 2015; Nguyen et al., 2016; Shila, Srivastava, O'Neill, Reddy, & Sritapan, 2016). Not to mention the security vulnerabilities resulted from the new authentication





approach. To handle these challenges, a new authentication application implemented to collect the data. These authentication approaches required modulating users' behavior via new sensor-based authentication techniques. The new authentication techniques are planned to be tested in house and evaluated against different type imposters.

### 1.5 Research Objectives

This study aimed to design, develop and evaluate the usability for two newly proposed sensors based smartphone authentication techniques. Towards this end the below objectives are set to be achieved:

- i. To investigate academic literature related to smartphone sensor based authentication via systematic review
- ii. To design new sensors based authentication approach using 3D-Touch sensor and microphone sensor
- iii. To develop the new authentication concepts in objective 2
- iv. To perform usability testing experiment for the develop authentication approach in objective 3

### 1.6 Research Questions

This research tries to answer the below research questions:

- i. What are the available research articles related to sensor-based smartphone authentication techniques?





- ii. What are the unexplored sensors in the area of sensor-based smartphone authentication?
- iii. Is 3D Touch sensor in smartphone suitable for authentication? If yes, How to employ 3D-Touch sensor in smartphone authentication?
- iv. Is microphone sensor in smartphone suitable for authentication techniques? If yes, How to employ microphone sensor in smartphone authentication techniques?
- v. Is 3D Touch sensor useable authentication techniques for users? To what extend?
- vi. Is Microphone sensor useable authentication techniques for users? To what extend?



## 1.7 Research Scope

With regard to the scope of this research, it is important to note the following:

- i. This research focuses primarily on the development of new authentication style and usability measurement standards. Therefore, the security measurement method is not the main issue; the type of smartphone protection approach in place does not matter.
- ii. The status of the selected study was developed on the basis of the authentication approach. Thus, the literature of the study case covers the techniques of usability utilized in the selected studies (the systematic review selected set).





- iii. This research focuses on the development of authentication in the smartphone using two sensors in its structure and assessment based on the degree of usability. In other words, assessments are the level of authentication and protection of those methods is not the subject of our research.
- iv. This research designed to answer the following questions, is it applicable to use this particular sensor (i.e. Microphone or 3D Touch)? If yes, is it usable?

## 1.8 Research Flow

The sources utilized in this thesis were carefully screened from the literature sources (i.e. used search databases). Ten years span was relied on for this thesis, it started from 2007 until 2017. Articles were screened and filtered to exclude duplicates and those unrelated to the topic. Subsequently, a full-text reading was conducted to analyses all the articles in details.

One of the major contributions of this thesis is to develop a new sensor based smartphone authentication. Another contribution of this research was by investigating unexplored new sensors-based smartphone authentication within ten years period (i.e. 2007-2017). Authentication technologies with respect to sensor based ones are scattered across the literature, not to mention its restrictions. Therefore, the systematic literature analysis (i.e. SLR) approach served a very significant purpose of exploring trends and gaps and provide valuable insights into this line of research. Related articles were acquired by building a comprehensive search query, filtering the articles and classifying





them into various categories. There are several generic outputs of this thesis explained below point and visualized in Figure 1.2.

1. Systematic literature is constructed from four database resources to comprehensively cover the topic of this thesis.
2. Investigating two unexplored sensors on the authentication based smartphone after analyzing all sensors in the academic literature.
3. The Microphone sensor is available in all devices under the android platform.
4. 3DTouchscreen sensor development was accomplished by simulating the sensor on android platform according to iOS authentication system and development (i.e. 3DTPT). BVP is developed based on the Microphone sensor (i.e. recording sensing) and recognizing the participants' behavior in two apps.
5. The testing process is completed by following the apps procedures for both 3DTPT and BVP, which they operate successfully without errors.

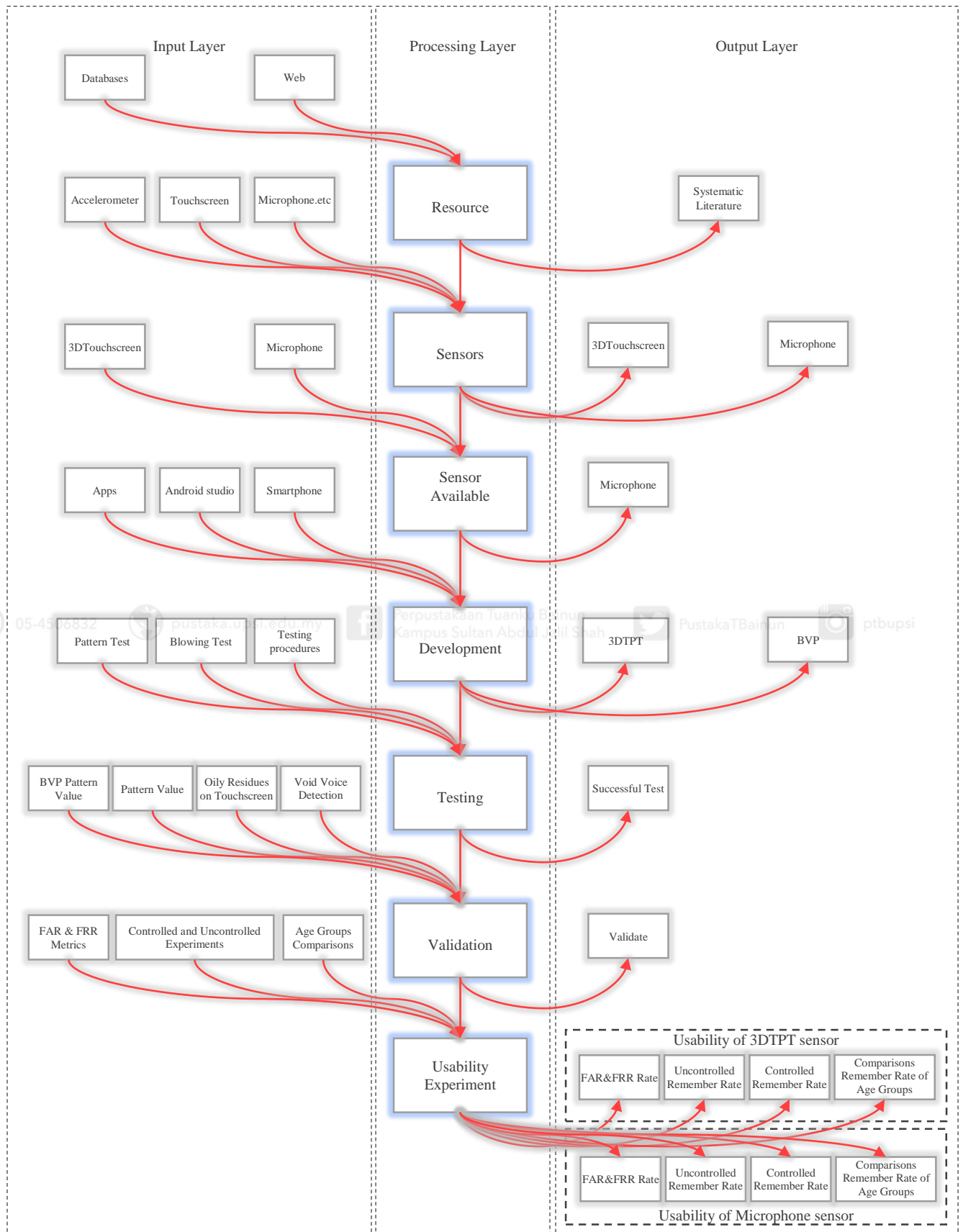


Figure 1.2. Research Flow



6. The apps validate output when acquiring getting the proper right inputs. Apps Validation was to avoid oily screen and avoid voice Detection through the experiment operations.

7. Four methods were used through the usability experiment of the two sensors.

8. FAR&FRR metrics, Controlled and Uncontrolled mode, and comparison of age groups, were used in this research towards finding the usability rate for each sensor.

## 1.9 Operations and Definitions

The following definition of the operations that using in this thesis:

1- Genuine operation (i.e.legitimate): the owner participant whom create the original pattern.

2- Imposter operation (i.e. illegitimate): the fake owner whom trying guessing to matching the original pattern of genuine.

3- Uncontrolled experiment: This operation is represent serially experiment one by one using one device. Since the experiment makes personally and individual without care about time. Therefore it is called controlled experiment.

4- Controlled experiment: This operation is represented procedure experiment, each participant makes their own nine attempts individual, they using their own smartphones in particular period time.

5- False Acceptance Rate (FAR): It is a unit used to measure the average number of false acceptances within a security system. It measures and evaluates the efficiency and accuracy of a system by determining the rate at which unauthorized or illegitimate users are verified on a particular system. It is



calculated by dividing the number of false acceptances by the number of identification attempts

- 6- False Rejection Rate (FRR): It is a unit used to measure the average number of false rejections within a usability system. It measures and evaluates the efficiency and accuracy of a system by determining the rate at which authorized or legitimate users are verified on a particular system. It is calculated by dividing the number of false rejections by the number of identification attempts.
- 7- Groups Comparison: It is the operation compare between the results of the Male group and Female group, then compare the result between age group of each gender.
- 8- Touch pressure listening: It is the function used to get the data value from the touchscreen sensor, the value is depend on the area of finger on the screen.
- 9- App system: It consists of a user interface, and a database of some sort.
- 10- Smartphone sensor: A number of different types of sensing devices installed on a user's phone to gather data for various user purposes, often in conjunction with a mobile app.
- 11- Smartphone Authentication: the verification of a user's identity through the use a mobile device and one or more authentication methods for secure access.

### 1.10 Thesis Outlines

This thesis consists of seven chapters; Chapter One provided background about the usability of authentication problem, research objective, scope, and research questions, and the rest of the thesis is organized as follows:



**Chapter Two:** In Chapter Two, A systematic review protocol is developed for literature review to grouping articles and making the taxonomy, analyses motivations, challenges and recommendations then methodology aspect include the main criteria and features.

**Chapter Three:** In Chapter Three, research methodology: Propose and evaluate usability, experiments design, explain remember, group comparisons and performance. Explain the features: Number of participants, Ages & Gender, Equipment and Time interval. Explain the experiment of 3D Touchscreen and BVP usability. Then the data collection and evaluation.

**Chapter Four:** In Chapter Four, development and data collection 3D Touchscreen sensor: Sensor and authentication approach development: using the environment of Android studio, explain activities and layouts, and explain the 3D Touchscreen sensor coding build. Explain the TPT app and data testing using sample. Then explain a validation of data by using application to prove it.

**Chapter Five:** In Chapter Five, development and data collection Microphone sensor: Sensor and authentication approach development: using the environment of Android studio, explain activities and layouts, and explain the microphone sensor coding build and permissions issue to get the approval. Explain the BVP app and data testing using sample. Then explain a validation of data by using application to prove it.

**Chapter Six:** In Chapter Six, Explain the dataset content. Discussion the Uncontrolled experiment results: remember rate of 3D Touchscreen sensor (TPT) patterns in the 1<sup>st</sup> attempt and the 2<sup>nd</sup> attempt and remember rate of Microphone sensor (BVP) patterns in a 1<sup>st</sup> attempt and a 2<sup>nd</sup> attempt. Discussion the Controlled experiment results: remember





rate of 3D Touchscreen sensor (TPT) patterns from a 1<sup>st</sup> attempt to a 9<sup>th</sup> attempt and remember rate of Microphone sensor (BVP) patterns from a 1<sup>st</sup> attempt to a 9<sup>th</sup> attempt. Discussion the finding results of usability testing of the two sensors in uncontrolled and controlled mode.

**Chapter Seven:** In Chapter Seven, Explain the FAR and FRR metrics results: the usability of multi-attempt per participants in TPT and in BVP. Discussion the results of gender and age groups: male participants with four age groups and female participants with four age groups. Discussion the finding results of comparing groups of each gender to find best group yield result of usability.

**Chapter Eight:** In Chapter Eight, Explain research achievement, how research objectives were achieved and research limitations. Finally, explain briefly the conclusion including the future works.

