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

MOCEHEB LAZAM SHUWANDY ALRUFAYE

SULTAN IDRIS EDUCATION UNIVERSITY

2019

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

MOCEHEB LAZAM SHUWANDY ALRUFAYE

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

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

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

**Please tick ( ✓ )**

Project Paper □

Masters by Research □

Masters by Mix Mode □

Ph.D. ☑

## INSTITUTE OF GRADUATE STUDIES
## *DECLARATION OF ORIGINAL WORK2*

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

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

UPSI/IPS-3/BO 31
Pind.: 01 m/s:1/1

**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*)
& (Nama & Cop Rasmi / *Name & 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 CONFIDENTAL or RESTRICTED, please attach with the letter from the related authority/organization mentioning the period of confidentiality and reasons for tphe 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 kebolehgunaan (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 kebolehgunaan teknik-teknik berkenaan.

# CONTENTS

Page

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

**CHAPTER 8 CONCLUSION**

# LIST OF TABLES

# LIST OF FIGURES

**Figure No.** **Page**

## 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

# 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, & Husseini, 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 lock 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 relays 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, Zawoad, & 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).

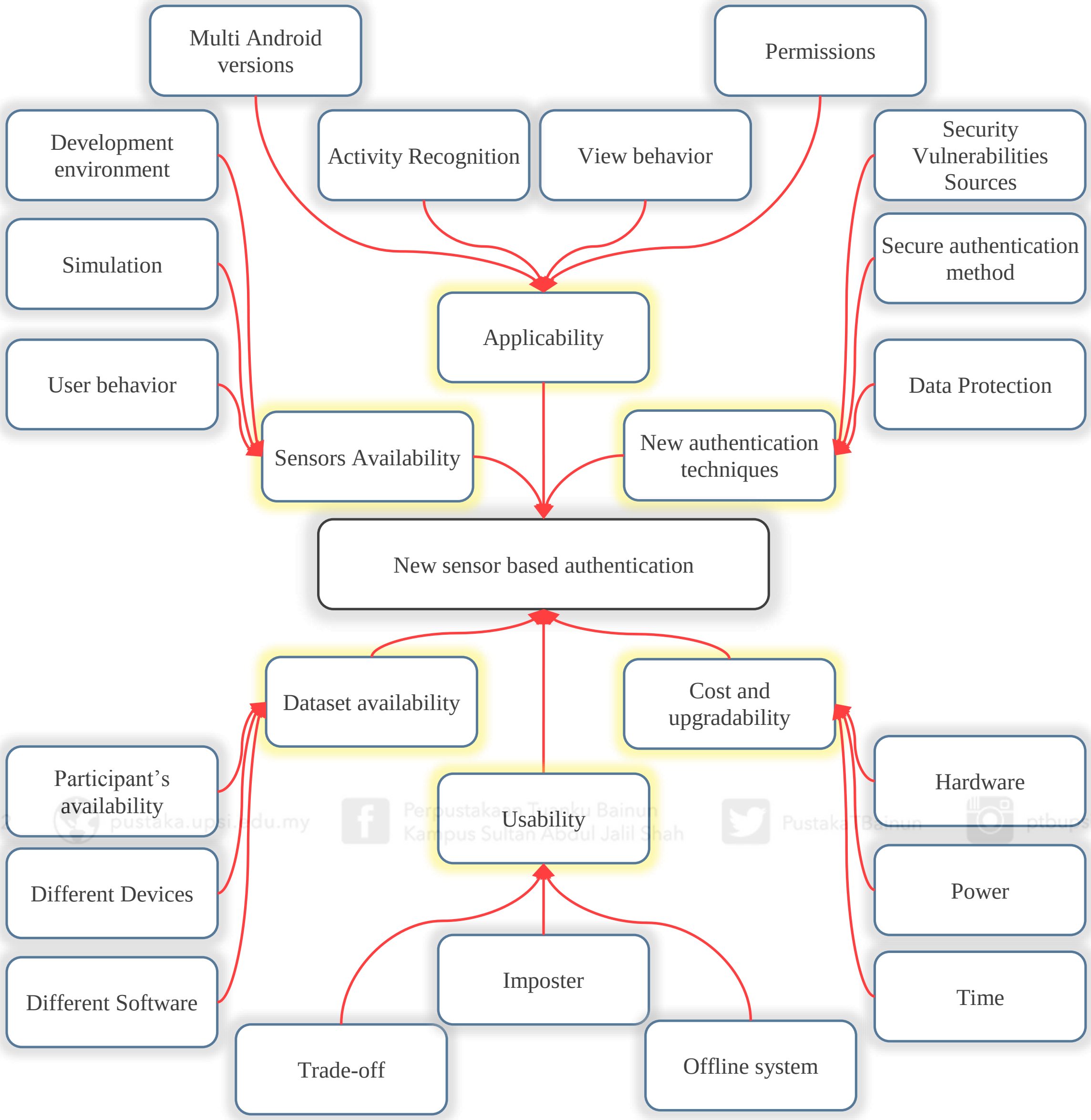

*Figure 1.1.* Challenges and Issues Categories

## 1.4 Problem Statements

There are several sensors utilized in the previous studies such as gyroscope sensor, accelerometer sensor, magnetic sensor, camera, fingerprint, and touchscreen (H. Wang, Lymberopoulos, & Liu, 2015). However, there are other sensors is yet to be explored 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 employ3D-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.

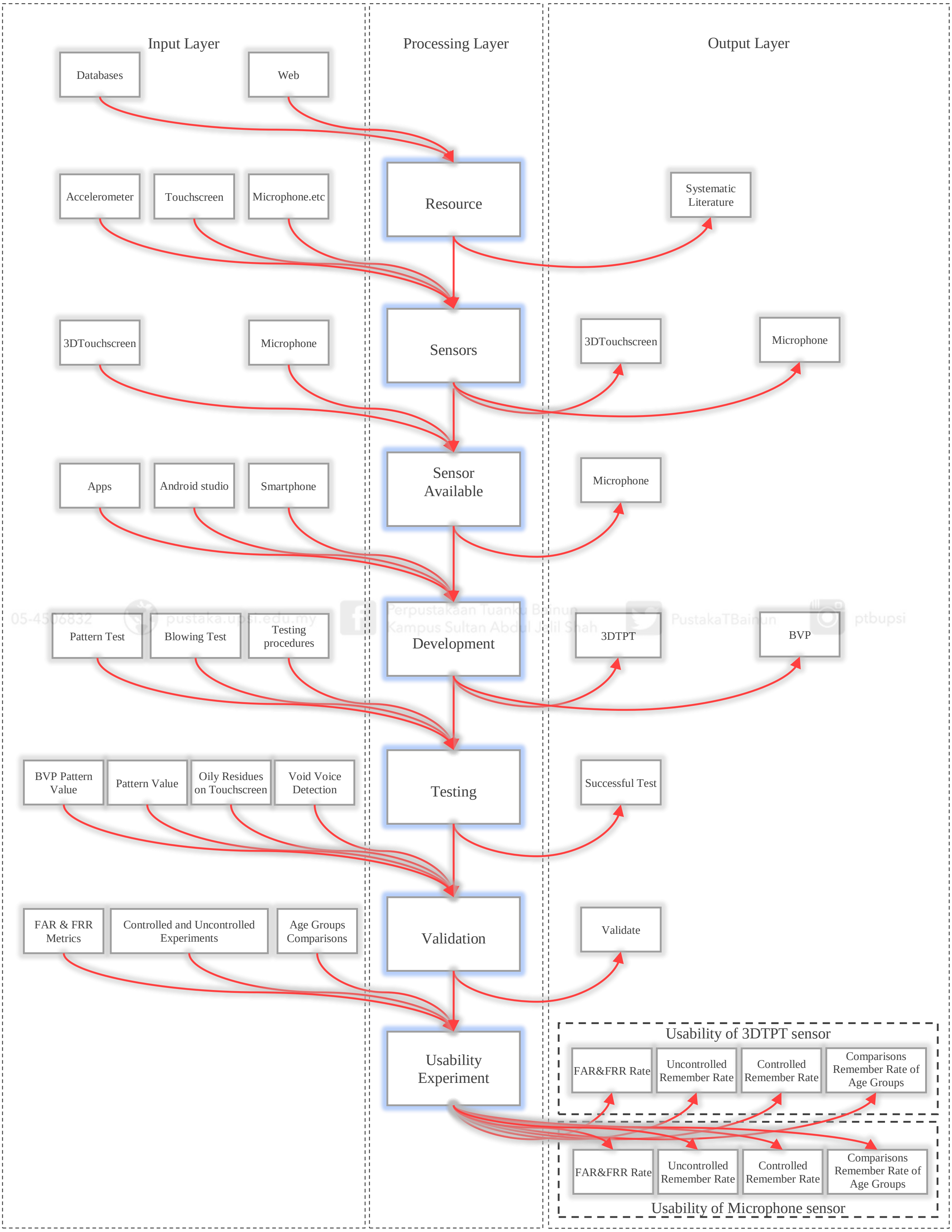

*Figure 1.2*. Research Flow

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 1st attempt and the 2nd attempt and remember rate of Microphone sensor (BVP) patterns in a 1st attempt and a 2nd attempt. Discussion the Controlled experiment results: remember rate of 3D Touchscreen sensor (TPT) patterns from a 1st attempt to a 9th attempt and remember rate of Microphone sensor (BVP) patterns from a 1st attempt to a 9th 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.