

**PIN Authentication Using Multi-Model Anomaly  
Detection in Keystroke Dynamics on Mobile Devices**

التحقق من الرقم الشخصي باستخدام نموذج متعدد لكشف التباين في  
اسلوب الكتابة على المفاتيح على الاجهزة المحمولة

By

**Ghofran Mahmood Khalaf**

**Supervisor**

**Dr. Mudhafar Al-Jarrah**

**A Thesis Submitted in Partial Fulfillment of the Requirements  
for the Master Degree in Computer Science**

**Department of Computer Science**

**Faculty of Information Technology**

**Middle East University**

**Jan. 2019**

## Authorization

I, **Ghofran Mahmood Khalaf**, hereby authorize Middle East University to supply copies of my thesis to libraries, organizations or individuals when required.

Name: Ghofran Mahmood Khalaf

Date: 26 / 01 / 2019.

Signature: 

## Thesis Committee Decision

This thesis titled “**Pin Authentication Using Multi-Model Anomaly Detection in Keystroke Dynamics on Mobile Devices**”.

Was successfully defended and approved on 26 / 01 / 2019.

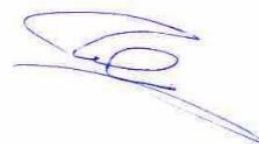
### Thesis Committee Members

### Signature

*(Supervisor)*

Dr. Mudhafar Al-Jarrah

Middle East University

A handwritten signature in blue ink, consisting of a stylized 'M' followed by a horizontal line and a small flourish.

*(Head of the Committee and Internal Examiner)*

Dr. Hesham Abusaimh

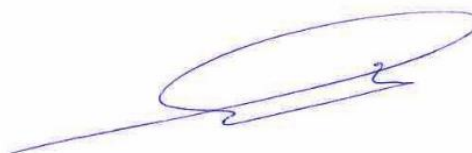
Middle East University

A handwritten signature in blue ink, featuring a large, stylized 'H' followed by a series of loops and a long horizontal stroke.

*(External Examiner)*

Dr. Mohammed Shakoukani

Applied Science University

A handwritten signature in blue ink, showing a large, stylized 'M' followed by a horizontal line and a small flourish.

## Acknowledgement

( اللهم ربنا لك الحمد، مِلءَ السَّمَوَاتِ وَمِلءَ الأرضِ، وَمِلءَ ما شِئْتَ مِنْ شَيْءٍ بَعْدَ )

First and above all, I give special thanks, praise and glory to Almighty Allah for his mercy, and reconcile and for granting me knowledge, confidence, patience to pass this Master thesis successfully.

I would like to express my profound thank to my thesis advisor. **Dr. Muthafar Al-Jarrah** for suggesting this field of research work and continue working with full enthusiasm. I gratefully acknowledge his kindness, patience, encouragement, for the complete guidance throughout the thesis stages, and for the critical assistance in designing and proceeding the methodology of my research. In addition, I would like to express my deepest gratitude to all the respectable lecturers at the Faculty of Information Technology, Middle East University. I also appreciate the effort and time that the professors of the committee spend in reading and discussing the thesis.

**The Researcher**  
**Ghofran Mahmood**

بسم الله الرحمن الرحيم

"وقل ربي زدني علما"

## Dedication

This thesis dedicated to my whole family;

**Especial thanks to my one and only my mother**, who always proud of me and supported me in every step of my life, no words can describe what you have done for me, thank you for your endless love.

**My Father**, who taught me to work hard for the things that I aspire to achieve.

**My Sisters and brother**, who are one part of my life.

**My aunts**, who support and love me.

**My best friends**, who always been there for me during difficult and stressful times, particularly, **Renad Al-Manaseer**.

**My friends Fatima and Russel**, who support me with their precious words and love me, and I thank Allah for their presence in my life.

**My friends**, who supported me with their nice words, who were the cause of my happiness during my last days at university, and who loved them and will stay in my heart.

## Table of Contents

Title .....	I
Authorization .....	II
Thesis Committee Decision .....	III
Acknowledgement .....	IV
Dedication .....	V
Table of Contents .....	VI
List of Abbreviations .....	VIII
List of Tables .....	IX
List of Figures .....	X
English Abstract.....	XI
Arabic Abstract .....	XII
Chapter One .....	1
Introduction.....	1
1.1 Research Context .....	1
1.2 Background of the Study.....	1
1.3. Problem Statement .....	2
1.4 Scope of Work.....	2
1.5 Limitations of the Research Work .....	2
1.6 Goal and Objectives .....	2
1.7 Motivation .....	3
1.8 Significance of Work .....	3
1.9 Research Questions .....	4
1.10 Thesis Organization .....	4
Chapter Two .....	6
Background and Literature Review .....	6
2.1 Background .....	6
2.2 Classification Methods .....	7
2.3.1 Binary Classification (two-class classification) .....	7
2.4 Biometric Technologies .....	9
2.5 PIN Technology .....	10
2.6 Keystroke Dynamics Technology .....	10
2.7 Ensemble Models Concept.....	11
2.7.1 Simple Ensemble Techniques.....	11
2.7.2 Advanced Ensemble Techniques.....	12

2.8 Related Work .....	13
2.9 Summary of Related Work.....	20
Chapter Three .....	23
Methodology and the Proposed Model .....	23
3.1 Methodology Approach .....	23
3.2 Outline of the Proposed Model .....	23
3.3 The Proposed Work .....	23
3.3.1 Feature Selection .....	24
3.4 Anomaly Detector Models .....	26
3.4.1 Single Anomaly Detection Models .....	27
3.4.2 Multi-Model Anomaly Detectors .....	28
3.4.3 Template Calculation of the Single Anomaly Detectors .....	29
3.4.4 Score Calculation and Outcome of the Typed PIN .....	30
3.5 Evaluation Metrics .....	31
3.6 The Data Collection System.....	31
Chapter Four .....	34
Experimental Results and Discussion.....	34
4.1 Introduction .....	34
4.2 Objectives of the Experimental Work.....	34
4.3 Feature Sets Selection .....	34
4.4 The Proposed (PIN Dynamics) System.....	36
4.5 Screen Shots of the Proposed (PIN Dynamics) System.....	36
4.6 EER Analysis Steps.....	40
4.7 Data Collection Using the Proposed (PIN Dynamics) System .....	42
4.8 Results and Discussion.....	42
4.9 Comparison with EER Results of the MOBIKEY data set.....	46
Chapter Five.....	48
Conclusion and Future Work.....	48
5.1 Conclusion.....	48
5.2 Suggestion for Future Work.....	49
Appendix A.....	55
Appendix B .....	57

## List of Abbreviations

Abbreviations	Meaning
<b>AAD</b>	Average Absolute Deviation
<b>CSV</b>	Comma Separated Values
<b>EER</b>	Equal-Error-Rate
<b>FAR</b>	False-Acceptance-Rate
<b>FRR</b>	False-Rejection-Rate
<b>KSD</b>	Keystroke Dynamics
<b>MAD</b>	Median Absolute Deviation
<b>PIN</b>	Personal Identification Number
<b>STD</b>	Standard Deviation

## List of Tables

<b>Chapter No. Table No.</b>	<b>Contents</b>	<b>Page No.</b>
<b>2.1</b>	Summary of the Review of Related Study	20
<b>4.1</b>	List of Primary and Secondary Feature Sets	35
<b>4.2</b>	EER Analysis Results Using Primary Features	43
<b>4.3</b>	EER Analysis Results Using Secondary Features	44
<b>4.4</b>	EER Analysis Results Using a Reduced Imposter Set	45
<b>4.5</b>	Summary of EER Results of the MOBKEY Data set	47

### List of Figures

<b>Chapter No. Figure No.</b>	<b>Contents</b>	<b>Page No.</b>
<b>3.1</b>	Registration Module	32
<b>3.2</b>	Training Module	33
<b>4.1</b>	Program Background	37
<b>4.2</b>	Account Creation	38
<b>4.3</b>	Enter PIN Code Enrollment Screen	39

# **PIN Authentication Using Multi-Model Anomaly Detection in Keystroke Dynamics on Mobile Devices**

**By: Ghofran Mahmood Khalaf**

**Supervisor: Dr. Mudhafar Al-Jarrah**

## **Abstract**

The use of behavioral biometrics in user authentication has recently moved to new security application areas, one of which is verifying the Personal Identification Number (PIN). This thesis investigates the design of anomaly detectors and feature sets for PIN authentication on touch mobile devices. The work involved a selection of raw data feature sets that are extracted from modern mobile devices, such as finger area, pressure, and timestamp. A set of primary and secondary authentication features have been formulated, which are calculated from the raw data features. The proposed anomaly detectors are based on the outlier concept, where an input PIN's calculated feature element is classified as imposter value if it is outside an acceptable zone from a central value such as the mean or median of a set of training values. The Z-Score method is used as the distance function of the anomaly detectors, and three versions are investigated; the standard deviation-based Z-Score, the modified Z-Score which uses the Median-Absolute-Deviation (MAD) and the Average-Absolute-Deviation (AAD) Z-Score function. Also, the three single models are combined into ensemble models. The proposed feature sets are implemented as a data collection system on a Nexus-9 Android tablet. Experimental work resulted in collecting a PIN dataset (PIN Dynamics) from 70 subjects, where the data included genuine and imposter PIN data. The raw data features data from the new dataset were converted to the proposed authentication primary and secondary features.

The authentication features dataset was analyzed by utilizing the three single anomaly detectors and the three ensemble anomaly detectors, using the Equal-Error-Rate (EER) metric. The results showed that the AAD Z-Score anomaly detector produced the lowest error rate among the single models, while the merged AAD and MAD ensemble model achieved the lowest overall error rate. The thesis ends with a conclusion and suggestion for future work.

**Keywords: PIN; Anomaly Detector; Z-Score; EER; MAD; AAD; Feature Set; Ensemble Model.**

## التحقق من الرقم الشخصي باستخدام نموذج متعدد لكشف التباين في أسلوب الكتابة

### على المفاتيح على الأجهزة المحمولة

اعداد: غفران محمود خلف

اشراف: الدكتور مظفر الجراح

### الملخص

انتقل استخدام القياسات الحيوية السلوكية في مصادقة المستخدم مؤخرًا إلى مناطق تطبيق أمان جديدة، أحدها يتحقق من رقم التعريف الشخصي (PIN). تبحث هذه الأطروحة في تصميم أجهزة الكشف عن الشذوذ والمجموعات المميزة لمصادقة PIN على الأجهزة المحمولة التي تعمل باللمس. تضمن العمل مجموعة مختارة من مجموعات بيانات البيانات الأولية التي يتم استخراجها من الأجهزة المحمولة الحديثة، مثل منطقة الإصبع والضغط والطابع الزمني. تمت صياغة مجموعة من ميزات التوثيق الأساسية والثانوية، والتي يتم حسابها من ميزات البيانات الأولية. ويستند كاشف الشذوذ المقترح إلى المفهوم الغريب، حيث يتم تصنيف عنصر العنصر المحسوب لـ PIN المدخلات كمسجل إذا كان خارج منطقة مقبولة من قيمة مركزية مثل متوسط أو متوسط مجموعة من قيم التدريب. يتم استخدام طريقة Z-Score كوظيفة المسافة للكشف عن الشذوذ، ويتم التحقيق في ثلاثة إصدارات؛ مقياس Z-Score المعتمد على الانحراف المعياري، المعدل Z-Score الذي يستخدم الانحراف المطلق (MAD) ودالة Z-Score للامتداد المطلق (AAD). أيضًا، يتم دمج النماذج الثلاثة الفردية في نماذج المجموعة. يتم تطبيق مجموعات الميزات المقترحة كنظام لجمع البيانات على جهاز Nexus-9 Android اللوحي. نتج عن العمل التجريبي جمع مجموعة بيانات (PIN Dynamics) PIN من 70 موضوعًا، حيث تضمنت البيانات بيانات PIN حقيقية ونامية. تم تحويل بيانات ميزات البيانات الأولية من مجموعة البيانات الجديدة إلى ميزات التوثيق الأساسية والثانوية المقترحة. تم تحليل مجموعة بيانات ميزات المصادقة من خلال استخدام أجهزة الكشف الشاذة الأحادية الثلاثة والكاشفات الشاذة الثلاثة للمجموعة، باستخدام مقياس معدل الخطأ المتساوي (EER). وأظهرت النتائج أن كاشف الشاذة AAD Z-Score أنتج أدنى معدل للخطأ بين النماذج المفردة، في حين حقق نموذج AAD وMAD المدمج أدنى معدل للخطأ الكلي. تنتهي الرسالة باستنتاج واقتراح للعمل المستقبلي.

الكلمات المفتاحية: رقم التعريف الشخصي، كاشف الشذوذ، نتيجة Z، معدل الخطأ المتساوي، مجموعة الميزات، متوسط الانحراف المطلق، الانحراف المطلق المتوسط.

# **Chapter One**

## **Introduction**

### **1.1 Research Context**

This thesis deals with the problem of user authentication on mobile devices, using keystroke dynamics behavioral biometrics of the user on touch screens, through anomaly detection models and features to support the verification of Personal Identification Number (PIN) codes.

### **1.2 Background of the Study**

The research explores different behavioral biometric approaches to increase the authentication security on mobile devices, using available sensor data on modern tablets and smartphones (mobile devices). Several studies have addressed the issue of user authentication using the keystroke dynamics modality, based on various anomaly detection models and feature sets (Killourhy, 2012; Aljarrah2013; Al-Obaidi2016). Most of the reported experimental work utilized a common 12-character password that was proposed by Kilorhy and Maxon (2009), while Antal and Lehel Nemes (2016) considered alternative strong and easy passwords. The use of short passcodes such as the PIN code in security systems has been investigated due to the wide-spread utilization of 4-digit PIN codes in banks' ATM and credit cards, on mobile devices, and in buildings access control systems.

### **1.3. Problem Statement**

The problem addressed in this study is the strengthening of user authentication on mobile devices where an intruder has captured the PIN code. The research investigates the use of the keystroke dynamics modality features on mobile devices, combined multi-model anomaly detection models, to improve the detection accuracy of the short 4-digit PIN code.

### **1.4 Scope of Work**

The research proposes to examine anomaly detection models and features that can be utilized to enhance user authentication on touch / mobile devices, using a short numeric passcode, based on the keystroke dynamics approach. Alternative single models and ensemble models will be investigated, using alternative feature sets derived from PIN typing data.

### **1.5 Limitations of the Research Work**

The main limitation of this research is that the proposed model and experimental work will be based on the Android platform. Further work will be needed for implementation on other mobile platforms such as IOS.

### **1.6 Goal and Objectives**

The aim of this research is to improve the authentication of users on touch mobile devices using a short password approach, the 4-digit Personal Identification Number (PIN) and the keystroke dynamics approach.

The following objectives are taken into consideration:

1. Investigation of the set of biometric features that will be used in the user authentication process.

2. Selection of alternative single anomaly detection models and model ensembles to enhance authentication.
3. Implementation of the raw features data collection system as a tool on the Android operating system.
4. Experimental work to collect the raw features data.
5. Evaluation of the proposed anomaly detection models and feature sets using the new datasets.

## **1.7 Motivation**

The need for better authentication of users on technological systems such as mobile devices, banks ATM terminals, and buildings access control panels, continue to require higher dependability methods to prevent illegal access by impostors. Traditional PIN or password-based approaches have the limitation that secret codes can be elicited by various methods such as shoulder-surfing or video recording, therefore additional traits of a user are needed to be included in the authentication process.

## **1.8 Significance of Work**

The expected significance of this work is in enhancing the security of mobile devices, and similar touch devices, by adopting new anomaly detection models and features, and utilizing available sensor data, without the need to add any special hardware.

## **1.9 Research Questions**

1. What are the single and multi-model anomaly detectors that will be used in the authentication process?
2. What are the new authentication features that will be used?
3. Will increasing the number of biometric features result in better authentication?
4. Will combining several anomaly detectors as an ensemble result in better authentication?
5. What will be the error metrics that will be measured in the experimental study and what are the achieved error rates?

## **1.10 Thesis Organization**

This thesis is divided into five chapters:

Chapter one: contains general concepts of this thesis which include the topic, background of the study, problem statement, scope of work, limitation of the proposed work, goal and objectives, motivation, the significance of work and questions to be answered.

Chapter two: presents the literature review, concepts, and definitions which introduced the introduction, classification methods, biometric technologies, and related work.

Chapter three: presents the methodology and the proposed model, which introduced the methodology approach, the outline of the proposed model, methodology steps, features selection, the anomaly detector, the proposed system and error metrics.

Chapter four: presents experimental results and discussion, which introduced the introduction, objectives of the experimental work, EER analysis steps, feature sets selection, analysis of the (PIN Dynamics) dataset, the proposed system, data collection the proposed system and discussion of results.

Chapter five: contains conclusions and future work.

## **Chapter Two**

### **Background and Literature Review**

#### **2.1 Background**

The last decades have witnessed an explosion of computing (i.e., mobile devices, the applications running on them, and the underlying infrastructure). Mobile computing is a prime target of authentication fraud because the level of security in mobile devices is, in general, kept to the minimum not only by design but sometimes for the convenience of the users. While numerous protection schemes are available on these devices, many users view these protections as hindrances and tend to disable or bypass them. In most cases, the maximum-security level enabled and used on these devices consists of a Personal Identification Number (PIN) or a password (Alshanketi, Traoré, & Awad, 2018).

A PIN is a secret sequence of digits widely used to authenticate a user while unlocking a phone as well as in many financial and mobile applications. Typically, a user enters her PIN into a system by pressing or tapping buttons corresponding to the digits in sequential order. A user is then authenticated only if the sequence of digits entered matches the one stored in the system during enrollment. That is, a traditional PIN authentication system only verifies knowledge of the PIN and utilizes no other user characteristic (Nguyen, Sae-Bae, & Memon, 2015).

In recent years there has been a growing interest in using password based on behavioral biometrics such as keystroke dynamics (KD) for mobile authentication as this biometric can be collected transparently without the need for any special purpose sensor or any special requirement from the user (Alshanketi, Traoré, & Awad, 2018).

Most behavioral biometrics on mobile devices do not require special hardware, apart from the available built-in features and sensors (Bubeck & Sanchez, 2003).

## **2.2 Classification Methods**

In the authentication work, users who are attempting to access a computer resource, based on authentication features, a one-class classifier is required to be used as an anomaly detector that is trained on the positive samples from a genuine user. There are several anomaly detectors that can be used to authenticate that the input data is within the established thresholds as calculated in the training phase, e.g. the Euclidian distance (Krislock & Wolkowicz, 2012).

The classification methods that are relevant to this research can be divided into two areas, as below:

### **2.3.1 Binary Classification (two-class classification)**

In this method, we classify the data into two subsets or categories, based on the features of each category. The data in this method can be genuine or forgery, positive or negative, legitimate or imposter.

The collected data is divided into two subsets; the training subset and the testing subset. The training subset contains labeled data from both categories, while the testing subset contains unlabeled data from the two categories (Kim, Khanna, & Koyejo, 2016)

### 2.3.2 Anomaly Detection (one-class classification)

Anomaly detection is a way that is used to authenticate a person established on his genuine or correct biometric features in a real application, without having access to negative data samples. It is the case in which a security system is trained for user authentication established on the individual's profile of input, regardless the knowledge of how forgers or impostors would input their data. The only data that is available to the anomaly detector, the one-class classifier, is the extracted training data. The one-class classifier knows only characteristics of the good users, because of this, any input that does not fit the profile of the genuine user will be rejected as negative or in our case imposter, 11 and any user who doesn't resemble the good user will be rejected.

Negative and positive data are needed to assess the classifier's capability in distinguishing between genuine and impostor users to evaluate the detection performance of a one-class classifier. False rejecting a genuine person or false accepting an impostor cause the anomaly detector to make mistakes. A template of the user's profile requires be designing and tuning to avoid two error cases of detection of false acceptance and false rejection (Chandola, Banerjee, & Kumar, 2009).

This method is divided into two types as below:

1. **Supervised anomaly detection** if the training or labeled instances for normal, as well as anomaly classes, are available, the supervised approach can be found to be effective in the detection of known attack (Gogoi, Borah, & Bhattacharyya, 2010).

2. **Unsupervised anomaly detection** in case of non-availability of labeled or purely normal data, the unsupervised approach of anomaly detection can be found to be effective in the detection of known as well as unknown attack. However, the rate of false positive is more in case of this approach (Gogoi, Borah, & Bhattacharyya, 2010).

## 2.4 Biometric Technologies

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions (Kalyan, 2017).

A Biometric identification refers to the consistent identification of an individual based on his/her physiological (e.g., face, fingerprint, hand, iris, DNA) or behavioral (e.g., keystroke, signature, voice) individuality. This technique of identification offers several compensations over traditional methods involving ID cards or PIN numbers for various reasons. Biometric-based authentication applications include a workstation, network, and domain access, single sign-on, application login, data protection, remote access to resources, transaction security and Web security. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys, and digital signatures, biometrics is set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient

(nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive (Kalyan, 2017).

## **2.5 PIN Technology**

Personal Identification Numbers generally consist of four numeric digits which are generated by the user or by the authentication system. PIN technology performs various cryptographic techniques for protecting data or devices (Karnan & Krishna, 2012). The main advantage of the PIN approach is flexibility and usability; it is easy for people to remember a 4-digit code. The disadvantages of the PIN approach are that the 4-digit is easier to be picked up by a shoulder-surfing intruder, and it can be guessed by the intruder if he has knowledge about user's personal data.

## **2.6 Keystroke Dynamics Technology**

Keystroke Dynamics is defined as the typing rhythm diagnosis processing of a user's typing behavior, which is divided into two application areas: access control using passcode authentication, and continuous authentication (Bours and Mondal, 2015).

This process is based on typing time, typing errors, and the complexity of keystrokes. (Chang, Tsai, & Lin, 2012)

The main advantage of the KSD approach is that an intruder who has already obtained a passcode is unlikely to be able to mimic the typing rhythm. The main disadvantage of this approach is that the typing rhythm of a user can change due to various environmental and psychological factors, so a genuine user might get rejected even if he has entered the correct passcode.

## 2.7 Ensemble Models Concept

Ensemble models in machine learning operate on the idea that different classification models can yield interleaving results which when merged can lead to more accurate classification. They combine the decisions from multiple models to improve the overall performance. This can be achieved in various ways:

### 2.7.1 Simple Ensemble Techniques

The most powerful techniques in this category (Singh,2018) are:

- 1. Max Voting:** The max voting method is generally used for classification problems. In this technique, multiple models are used to make predictions for each data point. The predictions by each model are considered as a 'vote'. The predictions that we get from most of the models are used as the final prediction.
- 2. Averaging:** Like the max voting technique, multiple predictions are made for each data point in averaging. In this method, we take an average of predictions from all the models and use it to make the final prediction. Averaging can be used for making predictions in regression problems or while calculating probabilities for classification problems.
- 3. Weighted Averaging:** This is an extension of the averaging method. All models are assigned different weights defining the importance of each model for prediction. For instance, if two of your colleagues are critics, while others have no prior experience in this field, then the answers by these two friends are given more importance as compared to the other people.

### 2.7.2 Advanced Ensemble Techniques

The most important techniques in this category (Singh,2018) are:

1. **Stacking:** Stacking is an ensemble learning technique that uses predictions from multiple models (for example decision tree, KNN or SVM) to build a new model. This model is used for making predictions on the test set.
2. **Blending:** Blending follows the same approach as stacking but uses only a holdout (validation) set from the train set to make predictions. In other words, unlike stacking, the predictions are made on the holdout set only. The holdout set and the predictions are used to build a model which is run on the test set
3. **Bagging:** The idea behind bagging is combining the results of multiple models (for instance, all decision trees) to get a generalized result. There is a high chance that these models will give the same result since they are getting the same input. One of the techniques to solve this problem is bootstrapping. Bootstrapping is a sampling technique in which subsets of observations are created from the original dataset, with replacement. The size of the subsets is the same as the size of the original set. Bagging (or Bootstrap Aggregating) technique uses these subsets (bags) to get a fair idea of the distribution (complete set). The size of subsets created for bagging may be less than the original set.

## 2.8 Related Work

The numerous keystroke dynamics features are making this field is renewable in Mobile applications and contains the ability to find several articles present new ideas and PIN technology as well. The Mobile application also is developed day after day by applying new techniques to protect these devices. This thesis is discussing the several studies which are related to multi-modeling authentication:

1. Jay Richards Young (2018): This research evaluated the chance to use keystroke dynamics for type fingerprints to authenticate via online rating status. This research installed to set how fully key prints to recognize persons when typing under several treatment cases. The authentication could be very hard when trying to recognize correctly users, the results of this research marked that key prints to be a solid indicator of negative cases. Typing with a temporary barrier does reduce the ability of algorithms to recognize persons. This is also the case when user samples are typed under conditions different from those in which the key print baseline signature was captured. The ability to recognize persons is challenging when using small comparison samples.
2. Athanasios, et al. (2017): This research verifies the following issues: they designed Illusion PIN (IPIN) for touch screen devices. The virtual keypad of IPIN consists of two keypads with different digit orderings, mixed in a single hybrid image, they improved an approach to estimate if or not the user's keypad is visible to an observer at a given viewing position, they tested the estimated visibility of Illusion PIN through a user study of simulated shoulder-surfing attacks on smartphone devices.

Finally, they estimated the minimum distance between the camera and the user's keypad to the camera does not capture the information from the keypad.

3. Toan Van Nguyen et al. (2017): This research discussed DRAW-A-PIN, an eyes-free, two-factors, and shoulder surfing resistant PIN-based authentication system by using finger-drawn digit influence. This research presented a PIN's privacy, finger drawn digits utilized as a second factor for user authentication because they have drawing stamps that are specific to the users. This research developed an algorithm of finger-drawn digit PIN authentication that is including two models: PIN content Analyzer and drawing Behavior Analyzer to achieve the two factors of a log-in attempt. Finally, the research evaluated DRAW-A-PIN in different settings through covering and not monitored attempts. They did two studies to evaluate the performance of DRAW-A-PIN system under two attacks models where the intruder has various levels of knowledge about the user's finger drawn PIN.
4. Marian Harbach, et al. (2016): This research presented the technique of Smartphone locking and what is the procedure to do that. Also presented the mechanism of the user monitoring from login to the system until the log out from it. They also presented how the locked screen of any smartphone in a way to recognize the user's features for increasing the security and usability. This research explored that PIN is reliable than others in spending the time of unlocking smartphone devices. The results of this work provided the ability to increase usability and security.

5. Noor Al-Obaidi, (2016): This thesis studied keystroke dynamics by analyzing the experimental datasets collected on mobile devices, which included timing features as well as key-press pressure and finger area. This thesis proposed a statistical median-based binary classifier (anomaly detector) and Med-Min-Model, which utilizes the distance to the median in computing the upper and lower of feature's characteristics. The two characteristics are determined in the training phase and used later in the authentication (testing) phase to categorized feature values that result from typing during the testing phase, as genuine or cheaters. An available dataset is used to test the proposed model's EER (Equal-Error-Rate) in comparison with three verification models. The result of the EER value is 6,79% which is much lower than the EER value of the three verification models (Euclidean, Manhattan, and Mahalanobis). The proposed model is carried out as a data collection and authentication system, by using a touch tablet under the Android operating system, which measured typing timing feature, pressure, and finger area. The system is used for collecting a new dataset (MEU-Mobile) from 56 subjects where each subject typed on the tablet a unified password 51 times (34 training attempts and 17 testing attempts).
6. Toan Van Nguyen et al. (2016): This research approach adopted the Dynamic Time Warping (DTW) algorithm to calculate the variations between PIN samples. The testing of their system by using two types of attacks: PIN attack where an intruder knows the user's PIN number but did not know the number's features, and traditional attack where the intruder can access to the sequence of dynamic drawing of user's finger drawing PIN.

The results of this work which comes from 40 users and 2400 traditional samples from two attacks produced an Equal Error Rate (EER) of 6.7% and 9.9% respectively.

7. Ramzi Saifan, et al. (2016): This work presented an overall survey on research in the last two decades on keystroke dynamics authentication. The objective is to discuss, summarize and provide a comparison for the well-known methodologies used in keystroke dynamics such as statistical and neural network methodologies, offering suggestions and possible future research direction, for touch-screen and mobile devices. Keystroke dynamics provide a second authentication factor for touch screen devices, as they are rapidly increasing in their use and are replacing the classical keyboards in the markets.
8. Jayanthi N. M. C. Chandrasekar, (2016): This work focused on using multimodal biometrics user authentication by explaining their model and analysis of user behavior in social networks. The multimodal features are as the face, and fingerprint which are using for reducing the time of authentication by removing the repeated information. This work contributed representation of locative vector to save the removed features. Finally, the normalization gained through minimum and maximum (M. Indovina et al, 2003) performs a fusion template matching by applying Structural Biometric Fusion Template Matching algorithm.
9. Syed Zulkarnain Syed Idrus, (2015): This research refocused on biometric authentication and used keystroke dynamics to solve password-based authentication problems. This work contributed to enhancing the performance of keystroke dynamics systems by improving the quality metric for keystroke dynamics and by

using known soft biometrics information and combining the authentication process with soft biometric characteristics. The results are used to enhance the authentication system based on keystroke dynamics by fusion soft biometric criteria with distance score provided by the biometric authentication system when comparing with the existing dataset, and combination processes to improve the recognition approaches that is contributed to the favorable effects in the system's overall performance. This work gained the results from different combination techniques, where the best performance was with the fusion of all passwords, which gained an EER value that is 5.41%.

10. Aude Plateaux, et al. (2014): This work explored how user authentication with biometrics can be made more powerful in the online banking case by using a specific device called Off PAD. The case requires that authentication is realized by the bank and not only by the user (or by the personal device) contrary to standard banking systems. A new protocol for the generation of one-time passwords from biometric data is presented, ensuring the security and privacy of the full package. The results of this work presented performance considering with regards to false positives.
11. V. Shanmugavalli, et al. (2013): This research presented three stages and used two stages to design the authentication of the user by using fingerprint and keystroke. The three stages are a fingerprint, login to the system by username and password and the last stage is keystroke dynamic. They used additional features to increase the security level that is recording period and Verification period. This research proposed the multimodal biometric methodology to increase the security level and accurate than the previous system.

12. Debnath Bhattacharyya, et al. (2009): This research proposed many approaches to ensure that only a legal user, and not anyone else accesses the delivered services. The biometrics is possible to assure an individual's identity. This work summarized ideas about the usability of biometric authentication systems, the comparison between different techniques and their advantages and disadvantages.
  
13. The Ph.D. thesis of Killourhy (2012) and the paper by Killourhy and Maxion (2009) present an important milestone in KSD research. The work, which was carried out at the Biometrics Lab of Carnegie Mellon University (CMU), presented a comprehensive comparative study of KSD anomaly detectors, using an experimental approach in which a KSD dataset was collected and utilized in the comparison. The aim of the study was to evaluate most published anomaly detectors on a unified dataset, using the same typing text, to arrive at a fair and scientifically based comparison. The work was motivated by the fact that published results of some classifiers cannot be reproduced, so when evaluations are replicated. The results are often extremely different; one classifier's error rate jumped from 1% to 85% upon replication. Therefore, an independent evaluation is needed in which different algorithms are compared on equal grounds the work involved implementing 14 known anomaly detection algorithms, which helped to provide an unbiased implementation platform for all algorithms.
  
14. Antal (2016): This research collected data from 51 subjects typing 400 passwords each and implemented and evaluate 14 detectors from the keystroke dynamics and pattern recognition literature. The unified password that was typed by all subjects is

a complex password of mixed characters (“tie5Roanl”). The work identified which detectors have the lowest error rates on the collected data. The dataset was made available online so that other researchers can assess new detectors and report comparative results. This work conducted an important experiment for collecting a KSD dataset on touch mobile devices, using a Nexus 7 tablet and a mobile phone (LG Optimus L7II, both running the Android operating system. The measured features included timing, pressure and finger area. The collected dataset included typing records of 42 subjects where each subject made 51 typing attempts, 34 for training and 17 for testing. The study used the CMU password (“. tie5Roanl”), which has been used by several research papers for comparison purposes. In this study, EER were computed using three different distance metrics: Euclidean, Manhattan, and Mahalanobis.

15. Alshanketi, et.al (2018): This paper proposed a multimodal approach that combines fixed and variable keystroke dynamic biometric passwords, which used variable passwords or one-time passwords (OTPs). The variability of OTPs increases the level of uncertainty for the attacker and makes statistical attacks and other attacks. They studied and compared two different fusion models: matching decision fusion and feature-level fusion with new missing feature prediction model based on curve fitting. Experimental evaluation of the proposed approach over different subsets of a global data set of 100 users, yields very promising results in terms of accuracy and resistance against statistical attacks. The best performance, obtained by combining fixed and OTP features, is an EER of 5.5% for feature-level fusion model.

## 2.9 Summary of Related Work

Table (2.1) shows a summary of related work:

**Table (2.1): Summary of the Review of Related Study**

<b>Name</b>	<b>Year</b>	<b>Summary</b>
<b>Jay Richards Young</b>	2018	This research evaluated the chance to use keystroke dynamics for type fingerprints to authenticate via online rating status
<b>Athanasios</b>	2017	This research improved an approach to estimate if or not the user's keypad is visible to an observer at a given viewing position. They estimated the minimum distance between the camera and the user's keypad to the camera does not capture the information from the keypad.
<b>Toan Van Nguyen</b>	2017	This research presented a PIN's privacy; finger drawn digits utilized as a second factor for user authentication because they have drawing stamps that are specific to the users. They developed an algorithm of finger-drawn digit PIN authentication
<b>Marian Harbach</b>	2016	This research presented technique of the Smartphone locking and what is the procedure to do that. They also presented the mechanism of the user monitoring from login to the system until the log out from it. They also presented how the locked screen of any smartphone in a

		way to recognize the user's features for increasing the security and usability
<b>Noor Al-Obaidi</b>	2016	This research studied keystroke dynamics by analyzing the experimental datasets collected on mobile devices that included timing features as well as key-press pressure and finger area. The author proposed a statistical median-based binary classifier (anomaly detector) and Med-Min-Model.
<b>Toan Van Nguyen</b>	2016	This research presented approach adopted the Dynamic Time Warping (DTW) algorithm to calculate the variations between PIN samples.
<b>Ramzi Saifan</b>	2016	This research presented an overall survey on research in the last two decades on keystroke dynamics authentication.
<b>Jayanthi N. M. C. Chandrasekar</b>	2016	This research focused on using multimodal biometrics user authentication by explaining their model and analysis of user behavior in social networks.
<b>Syed Zulkarnain Syed Idrus</b>	2015	This research focused on biometric authentication and used keystroke dynamics to solve password-based authentication problems.

<b>Aude Plateaux</b>	2014	This research explored how user authentication with biometrics can be made more powerful in the online banking case by using a specific device called Off PAD.
<b>V. Shanmugavalli</b>	2013	This research presented three stages and used two stages to design the authentication of the user by using fingerprint and keystroke.
<b>Debnath Bhattacharyya</b>	2009	This research proposed many approaches to ensure that only a legal user, and not anyone else accesses the delivered services.
<b>The Ph.D. thesis of Killourhy</b>	2012	This thesis presented a comprehensive comparative study of KSD anomaly detectors, using an experimental approach in which a KSD dataset was collected and utilized in the comparison.
<b>Antal</b>	2016	This work identified which detectors have the lowest error rates on the collected data. The dataset was made available online so that other researchers can assess new detectors and report comparative results.
<b>Alshanketi, Traoré, &amp; Awad</b>	2018	This paper proposed a multimodal approach that combines fixed and variable keystroke dynamic biometric passwords which used variable passwords or one-time passwords (OTPs).

## **Chapter Three**

### **Methodology and the Proposed Model**

#### **3.1 Methodology Approach**

This thesis develops a multi-model authentication scheme, which is based on PIN verification using the keystroke dynamics modality. The proposed methodology is experimental which involves model development, data collection system implementation, and data collection and analysis. The scheme will include single model anomaly detectors and ensembles of the single models. Evaluation of authentication accuracy of the various models will be based on the EER error metric.

#### **3.2 Outline of the Proposed Model**

The proposed scheme aims to develop an integrated biometric approach using the user's PIN typing data, to achieve more accurate authentication. The proposed model will select features and anomaly detection models, implement the data collection system, and collect data and evaluate the authentication accuracy of the single and multi-model ensembles.

#### **3.3 The Proposed Work**

The proposed work involves features selection, single anomaly detection models, and multi-model ensembles, to be used in the authentication process. A typed PIN is considered as genuine if the PIN-Score is within a pre-determined Pass-Mark threshold. A Pass-Mark is determined experimentally to give the lowest EER.

### 3.3.1 Feature Selection

Mobile devices have measurable features, which are different from standard keyboards. These features include the pressure of the finger, size of finger area, velocity, and acceleration. In this work, we include some of the built-in features that are relevant to keystroke dynamics. These features are classified as in the following:

**1. Raw features:** These are measurable attributes that are collected during the typing of a PIN, using built-in functions of the Android operating system. The selected raw features for this work are:

**Timestamp:** Time in milliseconds between the start and end of the typing event of a single key.

**Pressure:** Finger pressure on the selected key.

**Finger area:** Size of the finger area of the selected key.

**2. Primary authentication features:** These features are the same as proposed in the CMU research (Killourhy, 2012) with the addition of pressure and finger area as in (Antal, 2016; Al-Obaidi, 2016), which consists of the following feature elements.

- **Hold (H):** The elapsed time during key-press, which is the difference between key-down and key-up timestamps.
- **Up-Down (UD):** The latency time between key-up of the first key in a typing sequence and key-down of the second key.

- Down-Down (DD): The elapsed time between key-down of the first key and key-down of the second key, it is a composite feature of Hold of the first key and the latency between the first and second keys.
- Pressure (P): Value of the finger pressure on the screen during the key-press duration of a key.
- Finger Area (FA): Value of the finger area on the screen during the key-press duration of a key.

**3. Secondary authentication features:** These are additional calculated features that are extracted from the primary features, to enhance the anomaly detection, which is included based on their contribution to the authentication process, including the following features:

- Down-Up (DU): This represents the total time for every pair of typed keys; it is the elapsed time between key-down of the first key and key-up of the second key, which is a composite feature of Hold of the first key, UD between first and second keys and Hold of the second key.
- Med hold: Median of the hold of the four keys and the Enter key.
- Med press: Median of the pressure the four keys and the Enter key.
- Med area: Median of the area of the four keys and the Enter key.
- Total hold: The total of the Hold time during key-press of the four keys and the Enter key.
- Total UD: The total of the latency time (UD) between key-up of the first key in the typing sequence and key-down of the second key, of all key pairs.

- Total UD / total Hold: The ratio of the total Hold and total latency (UD) during PIN typing.
- Med UD: Median of the latency (UD) during PIN typing.
- Max UD: Maximum of the latency (UD) during PIN typing.
- Max pressure: Maximum of the pressure of the four keys and the Enter key.
- Max hold: The maximum of the Hold time of the four keys and the Enter key.
- Max area: Maximum of the finger area of the four keys and the Enter key.
- Hold/area: The ratio of the median of Hold to the median of finger area.
- Hold / press: The ratio of the median of Hold to the median of pressure.

### **3.4 Anomaly Detector Models**

The selected anomaly detector models are based on the outlier concept, represented by the Z-score model; it is aimed to be used for the detection of outlier anomalous values of keystroke dynamics features of typing the PIN, to determine whether the user is genuine or an imposter.

Each feature element is compared with a central value of that feature obtained during the training phase, where the central value can be the mean or the median, depending on the chosen anomaly detection model. The following alternative anomaly detection models are used in the proposed scheme:

### 3.4.1 Single Anomaly Detection Models

- **The Average Absolute Deviation (AAD) Anomaly Detector**

This model uses a modified version of the Z-Score function (Al-Khafaji, 2017), to calculate the acceptable distance metric. This version uses the mean and the Absolute Average Deviation (AAD) to calculate the modified Z-Score for a given feature element, as below:

$$\text{AAD Z-score of } xi = \frac{|xi - \bar{x}|}{AAD(x)} \quad \dots\dots\dots(1)$$

where the AAD is calculated as below:

$$\text{AAD of } x = \text{Mean of } |xi - \text{Mean}(x)| \quad \dots\dots\dots(2)$$

A feature element value is considered genuine if it is within the threshold of the Z-score model. In this work, we will determine the threshold value experimentally that will lead to lower error rates.

- **The Median Absolute Deviation (MAD) Anomaly Detector**

This model uses a modified version of the Z-Score function, to calculate the acceptable distance metric. This version uses the median and the Median Absolute Deviation (MAD) (Rousseeuw & Croux, 1993) to calculate the modified Z-Score for a given feature element as below:

$$\text{MAD Z-Score of } xi = \frac{xi - \text{Median}(x)}{MAD(x)} \quad \dots\dots\dots (3)$$

where the MAD is calculated as below:

$$\text{MAD of } x = \text{Median of } (|x_i - \text{Median}(x)|) \quad \dots\dots\dots(4)$$

A feature element value is considered genuine if it is within the threshold of the Z-score model.

In this work we will determine the threshold value experimentally that will lead to lower error rates

- **The Standard Deviation Anomaly Detector Model**

This model uses the original version of the Z-Score function, to calculate the acceptable distance metric. This version uses the mean and the Standard Deviation (STD) to calculate the Z-Score for a given feature element, as below:

$$\text{STD Z-score of } x = \sqrt{\frac{\sum (x - \bar{x})^2}{(n-1)}} \quad \dots\dots\dots (5)$$

A feature element value is considered genuine if it is within the threshold of the Z-score model.

In this work we will determine the threshold value experimentally that will lead to lower error rates

### 3.4.2 Multi-Model Anomaly Detectors

To enhance the anomaly detection outcome, ensembles of the three single anomaly detectors are proposed, using two approaches:

- **Merged models ensemble:** in this approach, the feature scores for the single models that are part of the ensemble are combined in one feature vector, and the PIN-Score is calculated as the number of feature elements in the combined vector that have a score of 1 (genuine).
- **Voting models ensemble:** in this approach, the PIN-Score for every single model which is part of the ensemble is calculated, and then a vote is taken of the outcome of the three models. A typed PIN is considered genuine if two or three models give it a genuine outcome. This approach requires an odd number of single models, so we will have one ensemble of three single models.

The following model ensembles will be used:

- **An ensemble of the two merged models (AAD, MAD):** created by merging features of the two single models.
- **An ensemble of the three models (AAD, MAD, STD):** created by merging features of the three single models.
- **An ensemble of the three models (AAD, MAD, STD):** created by taking a vote of the three single models, where a PIN entry is considered genuine if two single models recognize it as such.

### 3.4.3 Template Calculation of the Single Anomaly Detectors

For each single anomaly detector, a template is created from features of the genuine user's PIN data, as follows:

- AAD model template, consists of

AAD vector for the PIN features.

Mean vector for the PIN features.

- MAD model template, consists of

MAD vector for the PIN features.

Median vector for the PIN features.

- STD model template, consist of

STD vector for the PIN features.

Mean vector for the PIN features.

### **3.4.4 Score Calculation and Outcome of the Typed PIN**

For every typed PIN, whether it is genuine or imposter, a PIN-Score is calculated as follows:

- Feature-Score = 1 if the feature element is within the model's threshold, otherwise it is 0.
- PIN-Score = total number of feature element of the typed PIN with a genuine (1) Feature-Score.

The typed PIN is classified as genuine if the PIN-Score is equal or above the Pass-Mark, otherwise, it is classified as an imposter. The Pass-Mark is defined as the minimum number of feature elements of a typed PIN that are marked as genuine so that the typed PIN is classified as genuine.

### **3.5 Evaluation Metrics**

Evaluation of the authentication experimental work is based on measuring the following metrics:

False Rejection Rate (FRR): The system's rate of rejecting a legitimate user's input. FRR is also known as the Type I error.

False Acceptance Rate (FAR): The system's rate of accepting an impostor input. FAR is also known as Type II error.

### **3.6 The Data Collection System**

The proposed data collection system is aimed to provide a tool for user registration and PIN data entry based on the proposed feature sets.

The system consists of two modules:

a. Registration module: to register a user with user ID and PIN, as shown in fig 3.1. In this flowchart, the user enters his user ID, and if it exists in the database, it will be rejected.

Then, the user enters his 4-digit PIN code, which will be stored in the database.

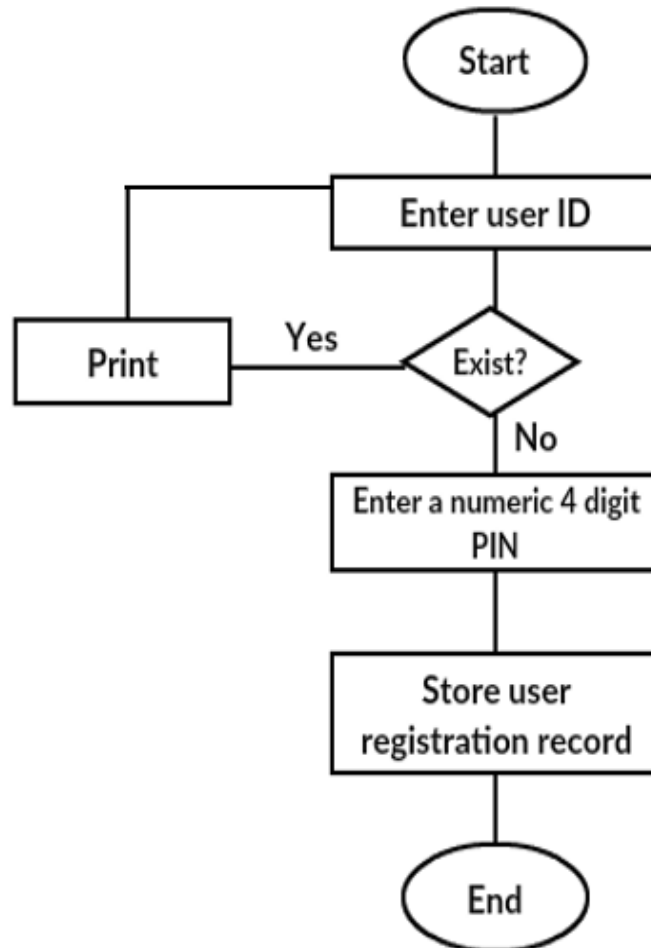


Figure 3.1 Registration Module

b. Data entry module: to collect a set of PIN typing data vectors for an individual, where each vector contains the primary authentication features, as shown in fig 3.2:

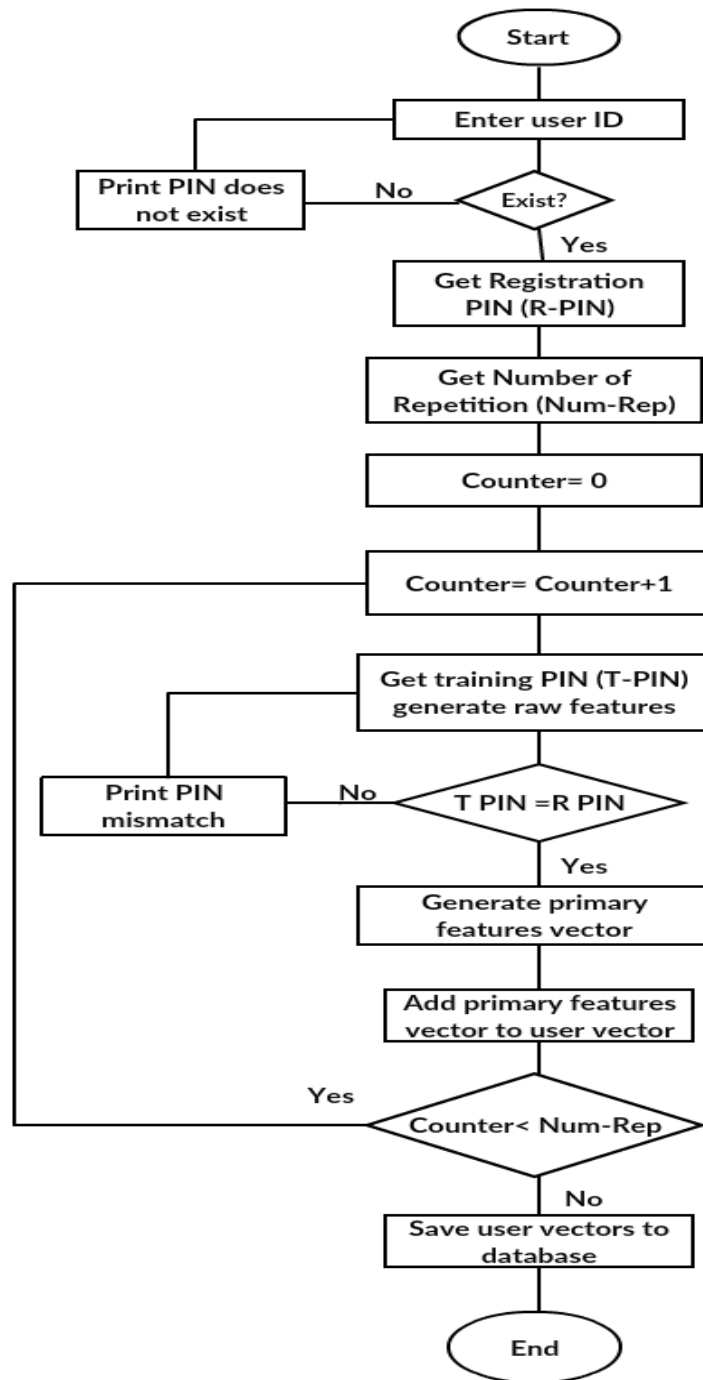


Figure 3.2 Training Module

## **Chapter Four**

### **Experimental Results and Discussion**

#### **4.1 Introduction**

The current chapter provides the practical side of the research work. It presents an implementation of the models discussed in chapter three, the data sources used in the experiments, the experimental data modules, and analysis and discussion of the results. The data sources consist of locally collected data obtained using the data collection system, from subjects in the university environment.

#### **4.2 Objectives of the Experimental Work**

The experimental work is designed to fulfill the following tasks:

1. Implementation of the proposed PIN data collection system.
2. Data collection from group users, using the data collection system.
3. Analysis of the collected data using the EER metric, for the single anomaly detectors.
4. Analysis of the collected data using the EER metric, for various ensembles of the single anomaly detectors.
5. Selecting the model with the lowest EER results

#### **4.3 Feature Sets Selection**

In chapter three, a set of 40 authentication features was proposed, to be used in the anomaly detection process. The primary and secondary authentication features are calculated from raw data features collected from the touch device during the PIN typing process.

The secondary authentication features are chosen based on their contribution in reducing error rates as observed in the experiments.

Table 4.1 shows the selected primary and secondary features.

**Table 4.1: List of Primary and Secondary Feature Sets**

<b>Feature Set</b>	<b>Number of Features</b>	<b>Calculated Feature Set Elements</b>
<b>A</b>	23	Hold1, Hold2, Hold3, Hold4, Hold-Enter UD12, UD23, UD34, UD4-Enter DD12, DD23, DD34, DD4-Enter, Pressure1, Pressure2, Pressure3, Pressure4, Pressure-Enter Finger Area1, Finger Area2, Finger Area3, <b>B</b> 17 Finger Area4, Finger Area-Enter DU12, DU23, DU34, DU4-Enter, Med Hold, Med Press, Med Area, Tot Hold, Tot UD, Tot UD/H, Med UD, MaxUD, Max Press, Max Hold, Max Area, Hold/Area, Hold/Press.

---

Set A represents the primary authentication features, where the Hold, Pressure and Finger Area are calculated for the four-digit PIN Keys plus the ‘Enter’ key, while the latency features (UD and DD) are calculated for four pairs of the PIN keys and the Enter key.

Set B represents the 17 secondary authentications feature we got this feature by experience. The complete authentication feature set is the combined set of primary and secondary features.

#### **4.4 The Proposed (PIN Dynamics) System**

The proposed data collection system implementation consists of two parts: the user registration module and the PIN data entry module, it is implemented in Java for Android. The data source consists of a locally collected data obtained by entering the PIN code by a group of users, using the developed data collection tool.

#### **4.5 Screen Shots of the Proposed (PIN Dynamics) System**

The proposed system provides the following interface screens:

1. System entry screen, as shown in Figure (4.1). Apart from registration, this screen provides settings change function, to update the number of enrollment repetitions. The screen provides options for creating an account (registration) and enrollment, and for changing the settings.

The screenshot displays the 'PIN Dynamics' application interface. At the top, the title 'PIN Dynamics' is shown in white, with 'Version 1.01' in yellow below it. The main content area is a white card titled 'NEW USER' with the instruction 'Enter your username and password'. It contains two input fields: 'User Name' with a person icon and 'Password' with an eye icon. A blue 'REGISTER' button is positioned below these fields. Below the card, there are two buttons: a green 'LOGIN' button and an orange 'USERS LIST' button. The bottom of the screen features a dark grey virtual keyboard with three rows of letters and symbols, and a black navigation bar at the very bottom with standard Android icons.

PIN Dynamics  
Version 1.01

NEW USER  
Enter your username and password

User Name

Password

REGISTER

LOGIN

USERS LIST

q w e r t y u i o p  
a s d f g h j k l  
↑ z x c v b n m  
123? SPACE ← RETURN

**Figure (4.1) System entry screen**

2. Account creation as shown in Figure (4.2). In this screen, the user enters his name and his 4-digit PIN code.

**PIN Dynamics**  
Version 1.01

**NEW USER**  
Enter your username and password

ghofran

1972

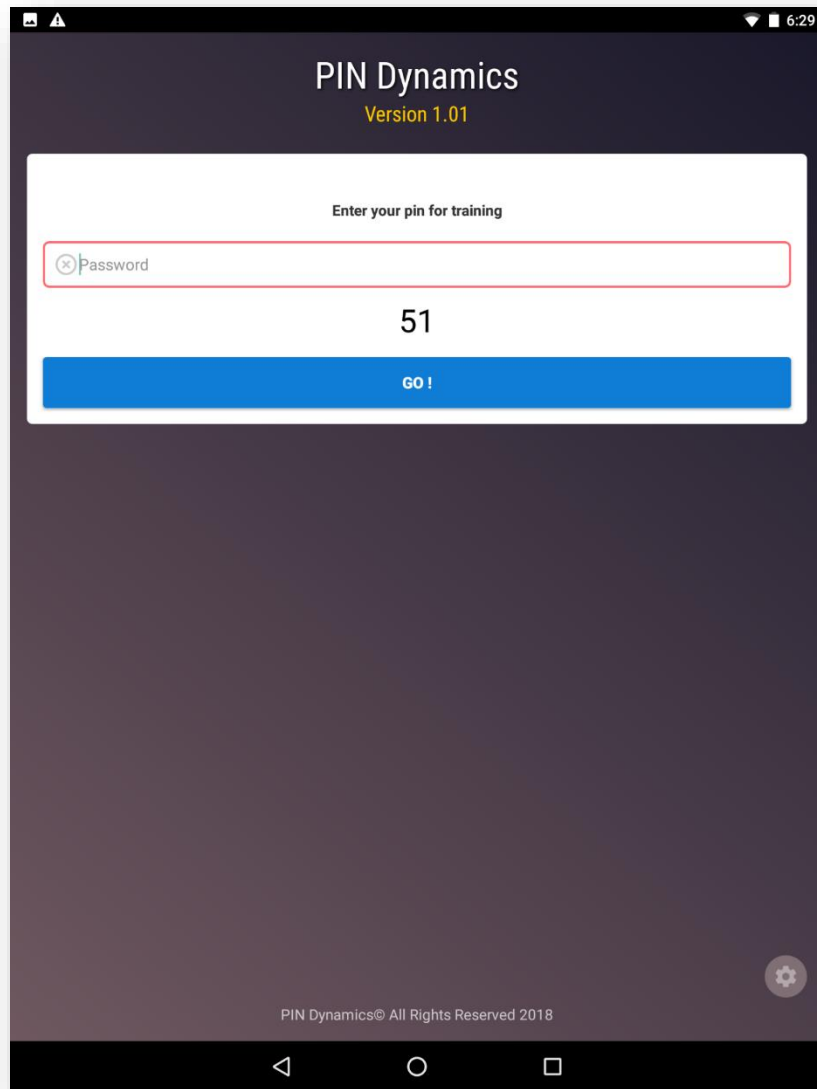
REGISTER

LOGIN USERS LIST

1 2 3  
4 5 6  
7 8 9  
← 0 RETURN

**Figure (4.2) Account Creation**

3. PIN code entry screen for enrollment as shown in Figure (4.3). The user enters his PIN several times as determined in the setting.



**Figure (4.3) PIN enrollment entry screen**

## 4.6 EER Analysis Steps

To measure the average EER value for a set of experimental PIN typing data, genuine and imposter samples, for a group of users, the average of user population EER is calculated separately using either a global pass-mark for all or a separate user pass-mark for each user. The average EER value for a set of PIN typing attempt is calculated as the average of False Acceptance Rate (FAR) and False Rejection Rate (FRR) of the PIN typing attempts. The EER analysis is performed using Excel and it consists of the following steps:

The average EER for a set of experimental PIN typing of genuine and imposter samples for a group of users is calculated in two ways:

- Global EER (EER<sub>g</sub>): The average EER of all users using a fixed pass-mark, for all.
- Users EER (EER<sub>u</sub>): The average of EER of all users where the pass-mark is selected separately for each user to give the lowest EER for the user.

**The following steps are followed to calculate the EER result:**

1. **Data partitioning:** The data rows of feature vectors of each user is divided into three subsets:
  - 20 user feature vectors data rows for training.
  - 20 user feature vectors for genuine user testing.
  - 2 rows from all other users to form the imposter testing data against each user.

2. **Templates Calculation:** The templates for the three single models (AAD), (MAD), (STD) are calculated for each user, which consists of:

The vector of Mean or Median for each feature element.

Vector of AAD, MAD, STD for each feature element.

3. **Score calculation:** Each feature element of each PIN features vector is given a Z-score value according to each model. The PIN-Score is a count of the number of feature elements that are equal higher than the Z-Score threshold. The outcome of the PIN typing attempt is considered as genuine if the PIN score is equal to or higher than the pass mark.
4. **FRR Calculation:** The false rejection rate for each user typing attempt is calculated as the ratio of the genuine user's testing vectors with the outcome of an imposter to the total number of genuine users testing vectors.
5. **FAR Calculation:** The false acceptance rate (FAR) is calculated as the ratio of the number of imposter feature vectors that have been classified as “genuine” to the total number of imposter vectors.
6. **EER Calculation:** The EER value for each user is calculated as the average of FRR and FAR of that user.

The average EER for the entire population is calculated as the average of user's EER of all users.

#### **4.7 Data Collection Using the Proposed (PIN Dynamics) System**

The proposed system is implemented on a Nexus-9 tablet under Android 7.1 to provide a data collection function for PIN authentication. The data collection module is used for collecting PIN data. In the experimental work, the PIN “1972” was used by all users where the individual digits were chosen to have different distances between them on the keyboard.

The experimental work resulted in 70 users typing data

The collected data was partitioned for training and testing as below:

- 20 records of each user for training on his typing profile
- 20 records of each user for genuine user testing
- 138 records for imposter testing (two records from each other user)

The selected authentication features were calculated, grouped into two feature sets:

- Primary Authentication Feature Set (23 feature elements)
- Secondary Authentication Feature Set (17 feature elements)

#### **4.8 Results and Discussion**

Table 4.2 shows the EER analysis results of using the 23 primary features and the five anomaly detection models (three single models and three model ensemble). We got these Threshold 3.2 By experiences.

The results were calculated for the two cases of global EER, using a fixed pass-mark, and user EER, using an individual pass-mark for each user. The AAD model has resulted in the lowest EER value for both global and user EER, for the single anomaly detectors.

For model ensembles, the two-model ensemble of AAD and MAD produced the lowest error rates for both global and user EER, among the single and multi-models. Also, the voting model ensemble has shown a lower error rate compared with the merged three-model ensemble, but it is higher than the merged two-model ensemble.

**Table 4.2: EER Analysis Results Using 23 Primary Features with Z-score Threshold 3.2**

<b>Anomaly Detection Model Code</b>	<b>Anomaly Detection Model Description</b>	<b>EERg</b>	<b>EERu</b>
<b>A</b>	Mean/AAD	10.10%	10.10%
<b>B</b>	Med/MAD	10.13%	11.86%
<b>C</b>	Mean/STD	11.56%	11.91%
<b>D</b>	2 merged models (A, B)	9.58%	8.59%
<b>E</b>	3 merged models (A, B, C)	10.27%	9.40%
<b>F</b>	3 voting models (A, B, C)	9.96%	10.08%

Table 4.3 shows the EER analysis results of using the complete feature set of primary and secondary features, using the five anomaly detection models (three single models and three model ensembles). We got these Threshold 3.2 By experience.

The results are calculated for the two cases of global EER, using a fixed pass-mark, and user EER, using an individual pass-mark for each user. In this case, the AAD model has resulted in the lowest EER value for both global and user EER, for single anomaly detectors. For model ensembles, the two-model ensemble of AAD and MAD produced the lowest error rates for both global and user EER, among the single and multi-models. Also, the merged three-model ensemble has shown a lower error rate compared with the voting three model ensemble.

**Table4.3 EER Analysis Results Using 40 Primary and Secondary Features With Z-score Threshold 3.2**

<b>Anomaly Detection Model Code</b>	<b>Anomaly Detection Model Description</b>	<b>EERg</b>	<b>EERu</b>
<b>A</b>	Mean/AAD	9.43%	8.41%
<b>B</b>	MED/MAD	9.65%	8.84%
<b>C</b>	MED/STD	11.07%	11.34%
<b>D</b>	2 Merged models (A, B)	8.32%	7.33%
<b>E</b>	3 Merged models (A, B, C)	8.58%	7.70%
<b>F</b>	3 voting models (A, B, C)	9.43%	8.84%

Table 4.4: Shows the EER analysis results after reducing the number of imposter attacks to 69, which represents one attack from each other user. The results show a decrease in the EER values in comparison with the case of two attacks from each imposter that was discussed earlier. The results show a similar pattern as in Table 4.4, with the merged two-model ensemble having the lowest EER value, the merged three-model ensemble is lower than the voting three-model ensemble, with the exception that the MAD model is slightly lower than the AAD model.

**Table 4.4: EER Analysis Results Using a Reduced Imposter Set with Z-score Threshold 3.2**

<b>Anomaly Detection Model Code</b>	<b>Anomaly Detection Model Description</b>	<b>EERg</b>	<b>EERu</b>
<b>A</b>	Mean/AAD	7.71%	7.17%
<b>B</b>	Med/MAD	7.65%	5.89%
<b>C</b>	Mean/STD	8.92%	8.27%
<b>D</b>	2 merged models (A, B)	6.46%	6.04%
<b>E</b>	3 merged models (A, B, C)	6.52%	6.07%
<b>F</b>	3 voting models (A, B, C)	7.59%	6.19%

#### **4.9 Comparison with EER Results of the MOBIKEY data set**

To compare the obtained EER results in this work using the proposed feature set and anomaly detectors with previous work, there were no available results using a short passcode of 4 digits and the keystroke dynamics approach. Therefore, the results of Antal and Nemes (2016) was selected for comparison due to the similarity in the data collection environment, despite the differences in password length and anomaly detectors. They collected data from 54 subjects who took part in the experiment; at the registration stage, they stated their experience with touchscreen devices as inexperienced, 6 – beginners, 17 – intermediate and 29 advanced touchscreen users. Data were collected in three sessions one week apart. In each session, they typed at least 60 passwords, at least 20 passwords from each type of easy, logical and strong. At the end of data collection, each user had provided at least 60 samples from each type of password (easy: 3323 samples, strong: 3303, logical strong: 3308). The data was collected using 13 identical Nexus 7 tablets. Each password had to be typed in the same way: the same keys had to be typed in the same order. EER values were computed using three different distance metrics for anomaly detection: Euclidean, Manhattan, and Mahalanobis.

Table 4.5 shows a summary of the EER results obtained in Antal’s experiment using various anomaly detection models and the strong password which was proposed by Killorhy and Maxion (2009).

**Table 4.5: Summary of EER Results of the MOBIKEY Dataset**

<b>Method</b>	<b>Average EER</b>
<b>Euclidean</b>	19.5 %
<b>Manhattan</b>	16.7 %
<b>Mahalanobis</b>	21.0 %
<b>Outlier count (th=1.96)</b>	14.3 %
<b>K means(k=3)</b>	13.1 %

As the results in Table 4.5 show, the average EER error rate in our experiment is much lower than all the EER results of the different anomaly detectors of Antal’s results, despite the fact that we used a much shorter password, the 4-digit PIN.

## **Chapter Five**

### **Conclusion and Future Work**

#### **5.1 Conclusion**

The work in this thesis presented a PIN authentication scheme based on the keystroke dynamics modality. The proposed scheme is comprised of an extended feature set of 23 primary features and 17 secondary features; we used the threshold 3.2 in the experiment we obtained compared to previous experiments, and six anomaly detectors; three single models and three ensemble models.

A data collection system is implemented on a Nexus-9 tablet under the Android operating system to be used for raw data features collection. In the experimental work, PIN typing data of 70 subjects were collected, where each subject typed the same PIN 51 times. The raw data vectors were converted into the authentication features vectors which were split into three subsets for each subject: training subset, genuine testing subset, and imposter testing subset. The investigation involved error analysis of the generated authentication data in Excel, using the EER metric and the proposed six anomaly detector models, to identify the anomaly detection model with the lowest EER value.

The results showed that the AAD Z-Score anomaly detector model achieved the lowest EER value among the single models, whereas the merged AAD and MAD ensemble model achieved the lowest overall EER value. Also, comparison with previous work that used similar primary features with a 12-character password showed that our results produced much lower EER value although we used a shorter passcode (4-digit PIN).

The analysis also investigated the effect of using a fixed Pass-Mark (threshold) for all subjects, to calculate the average Global EER, and a subject based Pass-Mark to produce the average subjects EER. The subjects EER was much lower than the Global EER as the Pass-Mark was tuned per subject, as in real-world authentication application it is expected that the Pass-Mark parameter will be initially based on global value, but can be tuned for each user to achieve optimum value for that user based on a trial period.

## **5.2 Suggestion for Future Work**

Some suggestions for future work can improve the research work in this field, based on the results of the current work. The following ideas are suggested for future research:

- Combine the proposed model with another modality such as the finger-drawn method.
- Improve the proposed models with additional features based on further experimentations.
- Investigate the inclusion of new sensors' data as they become available in new mobile phones.

## References

Al-Jarrah, M. (2013). Multi-factor authentication scheme using keystroke dynamics and two-part passwords. *International Journal of Academic Research*, Vol 5, No 3.

Alshanketi, F., Traore, I., & Awad, A. (2018). Multimodal mobile Keystroke dynamics biometrics combining fixed and variable passwords. *WILEY*.

Al-Khafaji, Sh. (2017). **An Anomaly Detection Model for Signature Authentication on Mobile Devices** (Unpublished Master thesis), Middle East University, Amman, Jordan.

Antal, M. (2016). The Mobikey Keystroke Dynamics Password Database: Benchmark Results. *Research Gate*, available:

<file:///C:/Users/ghofr/Desktop/Related%20work/Margit%20MOBIKEY%20keystroke%202016.pdf>

Al-Obaidi, N., (2016). **A New Statistical Anomaly Detector Model for Keystroke Dynamics on Touch Mobile Devices** (Unpublished Master thesis), Middle East University, Amman, Jordan.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Minkyu, C. (2009). Biometric Authentication: A Review, **International Journal of u- and e- Service, Science and Technology**, 2 (3).

Bours, P., & Mondal, S. (2015). Continuous Authentication with Keystroke Dynamics. Science Gate Publishing, *Recent Advances in User Authentication Using Keystroke Dynamics Biometrics*, pp. 41–58.

Bubeck, D. S. U., & Sanchez, D. (2003). **Biometric Authentication**. Universidade Estadual de San Diego.

Chandola, V., Banerjee, A., and Kumar, V. (2009). Anomaly detection: A survey. ACM Comput. 41(3), Article 15, P. 58, available: DOI = 10.1145/1541880.1541882 <http://doi.acm.org/10.1145/1541880.1541882>

Chang, T.Y., Tsai, C. J., & Lin, J. H. (2012). A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *Journal of Systems and Software*, 85(5), pp.1157-1165.

Gogoi, P., Borah, B., & Bhattacharyya, D.K. (2010). Anomaly Detection Analysis of Intrusion Data Using Supervised & Unsupervised Approach. *Journal of Convergence Information Technology*.

Harbach, M., Luca, A.D., & Egelman, S. (2016). The Anatomy of Smartphone Unlocking A Field Study of Android Lock Screens, *Privacy and Security Interfaces #chi4good*, CHI 2016, San Jose, CA, U SA.

Jayanthi, N.M., & Chandrasekar, C. (2016). Fusion based Multimodal Biometric Security for Social Networks Communication, *International Journal of Computer Applications* (0975 – 8887) 147(10).

Kalyani, CH. (2017). Various Biometric Authentication Techniques: A Review. *Journal of Biometrics & Biostatistics*.

Karnan, M., & Krishnaraj, N. (2012). A Model to Secure Mobile Devices Using Keystroke Dynamics through Soft Computing Techniques, *International Journal of Soft Computing and Engineering (IJSCE)*, ISSN, (2231-2307).

Killourhy K. S. (2012). **A scientific understanding of keystroke dynamics**, Ph.D. dissertation, Carnegie Mellon University, January 2012.

Kim, B., Khanna, R., and Koyejo, O. (2016). Examples are not Enough, Learn to Criticize! Criticism for Interpretability. *29<sup>th</sup> conference on Neural Information Processing System (NIPS)*. Barcelona, Spain.

Krislock, N., Wolkowicz, H., (2012). Euclidean Distance Matrices and Applications, *International series in operations research and management science*, 166.

Nguyen, T.V., Sae-Bae, N., & Memon, N. (2015). Finger-Drawn Pin Authentication On Touch Devices, *ACM*, (On-Line), available: [https://www.researchgate.net/publication/282926108\\_Finger-drawn\\_pin\\_authentication\\_on\\_touch\\_devices](https://www.researchgate.net/publication/282926108_Finger-drawn_pin_authentication_on_touch_devices)

Nguyen, T.V., Sae-Bae, N., & Memon, N. (2017). DRAW-A-PIN: Authentication using finger-drawn PIN on touch devices, *ScienceDirect*, (On-Line), available: [www.sciencedirect.com](http://www.sciencedirect.com)

Plateaux, A., Lacharme P., & Rosenberger, C. (2014). One-time biometrics for Online Banking and Electronic Payment Authentication, *HAL archives-ouvertes*, Caen, France.

Saifan, R., Salem, A., Zaidan, D., & Swidan, A. (2016). A Survey of behavioral authentication using keystroke dynamics Touch screens and mobile devices, *Journal of Social Sciences (COES&RJ-JSS)*, ISSN (E): 2305-9249 ISSN (P): 2305-9494, Publisher: Centre of Excellence for Scientific & Research Journalism, COES&RJ LLC, Online Issue:5 (1).

Shanmugavalli, V., Chandrasekar, V., & KrishnaSankar, P. (2013). Keystroke Dynamics for Authentication Based on Biometrics for Convincing User, *IJRIT International Journal of Research in Information Technology*, 1, Issue 12, 67-74.

Singh, Sh. (2018). A Comprehensive Guide to Ensemble Learning (with Python codes), *Analytics Vidhya*.

Young, J.R. (2018). **Keystroke Dynamics: Utilizing Key print Biometrics to Identify Users in Online Courses**, Department of Instructional Psychology and Technology, Brigham Young University.

## **Appendix A**

Samples of primary and secondary features vector, the generated templates and summary of the results of the (PIN-MOB) dataset

Table (A-1) sample of primary features vector from the (PIN-MOB) dataset

Hold 1	Hold 9	Hold 7	Hold 2	Hold Ent	UD 1.9	UD 9.7	UD 7.2	UD 2. Ent	DD 1.9	DD 9.7	DD 7.2	DD 2. Ent	Pressure	Pressure	Pressure	Pressure	Pressure	Area 1	Area 9	Area 7	Area 2	Area Ent
2.249944	4.499944	6.749831	2.999963	1.260859	0.647055	32.33322	0.749996	379.7068	1.85293	27.12299	1.853649	454.2477	0.635439	1.198083	10.6383	3.49534	4.448075	3.962751	10.79702	2.972063	2.318803	1.981374
5.749856	5.749928	0.999975	0.124998	0.999991	2.411751	3.385953	1.99999	19.12492	1.735284	4.507678	1.95121	22.69989	0.453885	1.198083	0.332446	0.499334	4.811183	3.962751	4.907736	2.972063	0.331257	0.990688
18.24954	5.62493	18.24954	0.374995	2.304328	1.529403	0.859646	1.499993	19.16659	5.147029	2.015378	4.829245	22.94989	2.814089	1.198083	2.659575	2.330227	5.718953	0.990688	2.944641	2.972063	1.656287	0
5.99985	3.874952	12.74968	2.999963	3.08693	6.294081	3.456128	1.899991	27.62488	7.02937	3.861527	4.146321	34.14983	0.453885	7.587859	5.651596	1.165113	1.180101	1.981375	0.981547	0.990688	2.318802	2.972061
7.249819	3.874952	5.249869	2.124973	3.434753	9.05877	3.315778	5.299974	176.4993	8.029365	2.076917	5.999971	212.4489	4.448076	7.388179	4.321808	2.163782	2.995642	2.972063	2.944641	1.981375	0.993772	1.981374
9.249769	1.124986	10.49974	4.874939	2.739107	8.235246	5.91226	5.699972	2.749989	6.735254	5.030754	7.414598	5.049975	0.453885	0.399361	6.981383	3.82823	0.272331	1.981375	2.944641	0	3.643832	1.981374
8.749781	3.874952	5.249869	2.124973	0.478257	7.588191	3.701741	14.89993	21.24991	8.970535	4.076911	15.36578	26.14987	4.811184	0.599041	1.662234	3.328895	2.995642	4.953438	2.944641	0.990688	0.993772	2.972061
4.499888	0.124998	8.749781	1.999975	0.391301	10.647	0.684208	7.94996	13.87494	11.02935	0.692306	9.268247	17.24991	0.998548	0	1.994681	0.832224	1.361655	3.962751	4.907736	0.990688	1.656288	0.990688
2.749931	3.124961	9.499763	3.99995	0.304345	22.23516	26.29815	19.8999	21.49991	20.91164	22.16916	17.36577	23.99988	0.998548	0.998403	0.332446	0.832224	4.448075	1.981375	8.833924	0.990688	0.331257	0
3.499913	5.124936	0.999975	0.124998	0.304345	13.17639	2.1228	5.249974	5.374978	11.6764	0.476922	4.731684	6.299969	0.090777	2.396166	12.96542	0.499334	2.087872	3.962751	2.944641	2.972063	1.656288	0.990688
1.499963	0.874989	0	1.874977	2.652151	24.82338	7.842078	15.74992	49.79146	24.49986	6.538441	15.17066	60.2997	1.906318	0.199681	6.981383	1.165113	3.903413	1.981375	2.944641	4.953438	1.656288	0.990688
0	0.124998	3.249919	0.999988	1.782593	12.35287	7.736815	19.8999	12.74995	11.6764	6.630749	19.85356	15.49992	1.906318	1.198083	5.651596	1.997337	0.998548	0.990688	2.944641	2.972063	0.993772	0.990688
5.249869	0	0.999975	0.999988	0.565212	20.17635	5.456121	4.799976	93.66628	20.73517	4.661524	4.292662	111.7994	1.180102	3.993611	2.659574	1.664448	2.087872	1.981375	0.981547	0	0.331257	0
0.249994	2.999963	4.749881	0	1.695637	18.23519	26.99991	3.99998	59.99975	17.4999	22.81331	4.634124	71.79964	3.358751	4.279333	6.981383	0.499334	0.090777	3.962751	0.981547	0	0.331257	1.981374
0.999975	4.999938	0.999975	2.999963	0.304345	16.05873	2.4035	3.149984	24.79156	15.14697	0.753844	2.682914	28.34986	7.716049	1.797125	0.99734	5.159788	1.906318	3.962751	2.944641	4.953438	0.993772	0
3.9999	4.124948	0.999975	3.874952	2.565195	8.588185	5.210508	1.199994	44.12482	6.970547	3.430759	0.780484	51.19974	3.177197	5.391374	1.329787	1.664448	1.724764	3.962751	2.944641	2.972063	1.656288	0.990688
0.249994	5.999925	3.249919	0.999988	0.043478	18.23519	4.333318	3.99998	97.24959	17.4999	2.199993	3.073156	116.0994	5.174292	0.798722	14.29521	1.498003	0.453885	2.972063	0.981547	0	1.656288	0.990687
0.749981	2.874964	2.999925	2.124973	0.304345	22.8234	4.052617	6.849966	8.416632	21.97046	2.723069	5.90241	9.049955	0.090777	3.194888	17.61968	0.832224	1.54321	0.990688	0.981547	2.972063	1.656288	0.990687
2.999925	4.374945	3.749906	1.999975	2.999974	57.52907	32.99988	2.799986	150.3744	56.14673	27.73838	1.804869	179.4491	5.718954	0.798722	5.984042	2.330227	3.177196	0.990688	2.944641	0.990688	0.993772	0.990687
2.499938	2.999963	2.999925	3.124961	3.260841	35.47038	3.491216	5.299974	56.87476	34.20568	2.199993	4.390222	66.79967	1.180102	2.595847	3.989362	9.320907	2.450981	3.962751	4.907735	2.972063	0.993772	0.990687
7.499813	0.249997	6.999825	1.62498	2.739107	6.294081	1.350872	5.299974	21.99991	7.38231	1.123073	6.341432	25.54987	2.995643	0.399361	3.324468	1.165113	0.635439	0	0.981547	0	0.331257	0.990687
7.9998	0.124998	10.74973	1.62498	1.43477	0.117646	0.087719	2.999985	16.0416	1.323522	0.015385	4.829245	18.39991	0.998548	0.599041	2.327128	0.166445	5.900507	3.962751	2.944641	1.981375	0.331257	0.990688

Table (A-2) sample of secondary feature set A extracted from the (PIN-MOB) dataset

	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO
69																	
70	DU 1.9	DU9.7	DU7.2	DU2.Ent	MedHold	MedPress	MedArea	TotHold	TotUD	UD/H	MedUD	MaxUD	MaxPress	MaxHold	MaxArea	Hold/Area	Hold/Pres
71	6.454506	3.291653	0.454543	15.58529	0.999988	0.99772	0	0.132075	4.937819	3.898958	10.01717	4.586196	0.499002	11.67151	319.149	0.732226	0.109343
72	3.181799	3.999983	1.969685	8.073131	0.874989	3.278221	0	1.603768	3.849737	4.341975	8.913732	2.195397	1.497005	11.65818	319.149	0.609857	2.357706
73	6.030266	7.999967	7.848437	12.80482	0.749991	0.712657	0	0.735846	5.953362	3.911454	11.1551	3.873554	0.249501	11.66984	0	0.980941	1.163841
74	2.090896	3.999983	32.93919	5.731679	0.124998	1.567845	0	1.339618	8.056986	7.155601	8.879249	9.482737	0.249501	11.66651	0	0.124358	1.473919
75	0.696965	3.333319	2.393925	1.341457	0	0.99772	0.990688	0.396225	0.875647	0.935564	1.155164	1.11494	0.748503	11.67318	0	0.646567	0.89714
76	1.242417	0.041666	0.515148	0.999995	0	1.567845	0	0.094339	0.647668	0.19807	0.224136	0.540229	0.998004	11.67484	106.383	0.246727	1.581772
77	2.272713	2.083325	0.999994	2.121941	0.999988	0.99772	0.990688	1.339618	1.497408	0.247328	1.672402	1.505744	3.992015	11.64151	106.383	1.527625	0.109343
78	0.757571	0.749997	0.454543	0.219511	0	0.427594	0	0.433961	1.217615	0.409334	0.810339	1.11494	1.247505	11.67651	0	0.246727	0.386547
79	0.272726	3.958317	0.454543	0.170731	0	0.427594	0	0.396225	0.357513	1.023412	0.568962	1.459767	1.497006	11.67818	319.149	0.246727	0.386547
80	1.303022	2.291657	1.909079	0.951215	0.874989	0.99772	2.972063	0.924525	0.160622	0.233147	0.982752	0.172413	0.748503	11.67318	0	1.344072	1.586462
81	0.818177	0.958329	0.030303	0.170731	0	1.282782	0	0.811318	0.544041	0.149766	0.499997	0.195402	0.998004	11.67484	319.149	0.246727	0.957995
82	1.787868	0.374998	0.999994	0.999995	0.999988	2.13797	2.972063	1.943389	1.797926	1.320475	1.948262	0.908044	1.247505	11.65984	0	1.252295	0.895678
83	1.727262	0.70833	1.424234	18.65845	0.999988	1.282782	0.990688	1.037732	3.031085	3.286117	1.396542	6.655157	3.243512	11.68984	0	1.527625	0.40029
84	0.757571	0.958329	0.999994	0.999995	0.999988	1.567845	0.990688	1.716975	0.637305	0.57145	0.017241	0.563217	2.495009	11.65151	319.149	2.464666	2.444597
85	1.181811	3.666651	0.515148	0.560973	0.999988	0.142531	0.990688	1.415089	0.005181	0.074265	0.017241	0.908044	2.495009	11.68484	0	0.23449	0.503241
86	0.757571	0.70833	0.999994	6.073141	0.999988	0.99772	0.990688	1.49056	0.005181	0.111824	0.120689	0.747125	0.499001	11.66484	0	2.464666	1.684937
87	0.21212	0.374998	0.454543	0.170731	0	0.427594	0	0.094339	0.699481	0.074265	0.051724	0.724136	0	11.66818	0	0.246727	0.386547
88	2.272713	1.041662	0.030303	0.999995	0	0.142531	0	0.396225	1.62176	0.649849	2.18964	1.091952	0.249501	11.66984	106.383	0.246727	0.06768
89	0.151514	2.624989	0.454543	0.560973	0.999988	0.997719	0.990688	0.735846	0.098445	1.038791	0.258619	0.724136	0.249501	11.66651	106.383	1.527625	1.384189
90	0.272726	0.333332	0.515148	0.560973	1.999975	2.423033	0	2.245275	0.367875	2.225695	1.155164	0.195402	0.748503	11.66318	0	1.711178	2.60293
91	0.151514	1.374994	0.939388	0.999995	0	0.997719	1.981375	0.094339	1.300517	0.231176	0.568962	1.091952	1.247505	11.65984	212.7659	1.377445	0.780211

## **Appendix B**

EER Analysis results of the (PIN-MOB) data using the AAD and  
MAD Ensemble model, and user pass-Mark.

User	User PM	FRR	FAR	EER
1	67	0.000	0.014	<b>0.72%</b>
2	61	0.050	0.043	<b>4.67%</b>
3	61	0.100	0.094	<b>9.71%</b>
4	66	0.000	0.000	<b>0.00%</b>
5	71	0.100	0.072	<b>8.62%</b>
6	68	0.200	0.152	<b>17.61%</b>
7	62	0.100	0.109	<b>10.43%</b>
8	70	0.000	0.072	<b>3.62%</b>
9	68	0.100	0.123	<b>11.16%</b>
10	65	0.050	0.094	<b>7.21%</b>
11	69	0.050	0.072	<b>6.12%</b>
12	62	0.050	0.080	<b>6.49%</b>
13	70	0.100	0.101	<b>10.07%</b>
14	65	0.100	0.080	<b>8.99%</b>
15	50	0.050	0.051	<b>5.04%</b>
16	61	0.100	0.109	<b>10.43%</b>
17	62	0.050	0.101	<b>7.57%</b>
18	61	0.050	0.058	<b>5.40%</b>
19	56	0.050	0.058	<b>5.40%</b>
20	62	0.100	0.094	<b>9.71%</b>
21	71	0.100	0.109	<b>10.43%</b>
22	68	0.100	0.094	<b>9.71%</b>
23	68	0.050	0.065	<b>5.76%</b>
24	67	0.100	0.094	<b>9.71%</b>
25	69	0.100	0.094	<b>9.71%</b>

26	67	0.100	0.123	<b>11.16%</b>
27	59	0.050	0.058	<b>5.40%</b>
28	69	0.100	0.072	<b>8.62%</b>
29	66	0.100	0.065	<b>8.26%</b>
30	68	0.050	0.138	<b>9.38%</b>
31	62	0.050	0.036	<b>4.31%</b>
32	53	0.000	0.000	<b>0.00%</b>
33	68	0.050	0.036	<b>4.31%</b>
34	64	0.100	0.072	<b>8.62%</b>
35	70	0.100	0.087	<b>9.35%</b>
36	60	0.050	0.065	<b>5.76%</b>
37	69	0.100	0.094	<b>9.71%</b>
38	65	0.050	0.051	<b>5.04%</b>
39	66	0.100	0.094	<b>9.71%</b>
40	64	0.050	0.051	<b>5.04%</b>
41	63	0.050	0.051	<b>5.04%</b>
42	58	0.050	0.065	<b>5.76%</b>
43	71	0.050	0.058	<b>5.40%</b>
44	65	0.050	0.051	<b>5.04%</b>
45	67	0.050	0.065	<b>5.76%</b>
46	67	0.050	0.029	<b>3.95%</b>
47	71	0.100	0.094	<b>9.71%</b>
48	65	0.050	0.043	<b>4.67%</b>
49	70	0.100	0.072	<b>8.62%</b>
50	66	0.050	0.043	<b>4.67%</b>
51	66	0.050	0.065	<b>5.76%</b>

52	65	0.100	0.123	<b>11.16%</b>
53	66	0.100	0.123	<b>11.16%</b>
54	56	0.050	0.036	<b>4.31%</b>
55	69	0.150	0.188	<b>16.92%</b>
56	69	0.050	0.051	<b>5.04%</b>
57	66	0.100	0.116	<b>10.80%</b>
58	60	0.150	0.159	<b>15.47%</b>
59	60	0.050	0.051	<b>5.04%</b>
60	67	0.100	0.094	<b>9.71%</b>
61	66	0.150	0.138	<b>14.38%</b>
62	70	0.100	0.101	<b>10.07%</b>
63	59	0.000	0.029	<b>1.45%</b>
64	64	0.050	0.043	<b>4.67%</b>
65	64	0.050	0.051	<b>5.04%</b>
66	61	0.100	0.094	<b>9.71%</b>
67	63	0.000	0.014	<b>0.72%</b>
68	69	0.050	0.036	<b>4.31%</b>
69	65	0.000	0.007	<b>0.36%</b>
70	64	0.100	0.094	<b>9.71%</b>
<b>Average</b>		7.14%	7.53%	<b>7.33%</b>