A New Statistical Anomaly Detector Model for Keystroke Dynamics on Touch Mobile Devices

نموذج جديد لكاشف تباين إحصائي لديناميكية الكتابة باللمس على الهواتف النقالة

Prepared by

Noor Mahmood Shakir Al-Obaidi

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

Amman, Jordan

May, 2016

II

AUTHORIZATION STATEMENT

I, Noor Mahmood Shakir Al-Obaidi, authorize the Middle East University to provide hard copies or soft copies of my thesis to libraries, institutions or individuals upon their request.

Name: **Noor Mahmood Shakir Al-Obaidi**

Data: 21/5/2016

Signature:

III

اقرار تفويض

أنا نور محمد شاكر العبيدي أفوض جامعة الشرق الأوسط بتزويد نسخ من رسالتي للمكتبات المعنية، المؤسسات، الهيئات عند طلبها.

الاسم: نور محمد شاكر العبيدي

التاريخ: 2016/5/21

التوقيع:

Examination Committee Decision

This is to certify that the thesis entitled **"A New Statistical Anomaly Detector Model for Keystroke Dynamics on Touch Mobile Devices"** was successfully defended and approved on 21/5/2016

Examination Committee Members	**Signature**
(Supervisor)	
Dr. Mudhafar Munir Al-Jarrah **Middle East University**	
(Head of the Committee and Internal Committee Members)	
Dr. Sadeq O. AlHamouz **Middle East University**	
(External Committee Members)	
Dr. Mohammad Shkoukani **Applied Science University**	

ACKNOWLEDGMENT

I want to thank ALLAH for his blessings that helped me achieve my dream.

I would like to thank my supervisor Dr. Mudhafar Al-Jarrah, who has been an inspiration to me during my master journey and gave me all the ideas, facilities and guidance to achieve this thesis, without him I would not have finished this thesis.

I am forever indebted to my father and my mother who supported me during this academic journey and throughout my whole life, they had more faith in me than I could ever imagined.

I must also acknowledge my sisters' encouragement which gave me the motivation to make this thesis realized.

I would also like to thank my friend Sajjad.A. Al-Robayei, who has helped me with his useful discussion and insight during the proposal phase of this thesis.

Dedication

This dissertation is lovingly dedicated to my father and my mother

TABLE OF CONTENTS

CHAPTER TWO

Background and Literature Review

CHAPTER THREE

The Proposed Keystroke Dynamics Model

CHAPTER FOUR

Experimental Results and Discussion

CHAPTER FIVE

Conclusion and Future work

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviations	Meaning
CER	Crossover Error Rate
CV	Coefficient of Variation
DD	Down-Down
DTM	Distance to Median
DU	Down-Up
EER	Equal Error Rate
FA	Finger Area
FAR	False Acceptance Rate
FRR	False Rejection Rate
FTAR	Failure To Acquire Rate
H	Hold
IPR	Impostor Pass Rate
KDA	Keystroke Dynamic-Based Authentication
KSD	Keystroke Dynamics
LMM	Linear Mixed-Effects Models
LT	Lower Threshold
P	Pressure
UD	Up-Down
UT	Upper Threshold
UU	Up-Up

A New Statistical Anomaly Detector Model for Keystroke Dynamics on Touch Mobile Devices

Prepared by
Noor Mahmood shakir Al-Obaidi
Supervisor
Dr. Mudhafar Al-Jarrah

Abstract

Keystroke Dynamics – the authentication technology that utilizes the typing rhythm to distinguish genuine users from impostors, has gone through continued developments to improve its detection capability. Recently, the keystroke dynamics model has been investigated as an authentication method on touch mobile devices, which resulted in shifting the attention from enhancing classifiers only, to adding new measurable features of mobile devices that can improve the classifiers' detection performance. The work in this thesis investigates keystroke dynamics, through empirical analysis of experimental datasets collected on mobile devices which included timing features as well as key-press pressure and finger area. A statistical median-based binary classifier (anomaly detector) is proposed, the Med-Min-Model, which utilizes the distance to the median in calculating the upper and lower thresholds of a feature. The two thresholds are determined in the training phase, and used later in the authentication (testing) phase to classify feature values that result from typing during the testing phase, as genuine or impostor.

An existing dataset is utilized in evaluating the Equal-Error-Rate (EER) of the proposed model in comparison with three verification models. The resulting EER value of the proposed model, using the existing dataset is 0.0679, which is much lower than EER value of the three verification models. The proposed model is implemented as a data collection and authentication system, for use on a touch tablet working under the Andriod operating system, which measured typing timing features, pressure, and finger area. The system is used in the collection of 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). Analysis of the new dataset shows a reduced EER value of 0.0494 compared to the EER value using the existing dataset.

The False-Acceptance-Rate (FAR) at 5% False-Rejection-Rate (FRR) was 5.79%, which points to the fact that further enhancement is needed to reduce the False-Acceptance-Rate. The proposed model used a pass-mark as a reference value for the resulting test-score of a typing attempt. Two methods were used in determining the pass-mark; a variable pass-mark for each subject which is tuned to get to the point of equal FAR and FRR, and a global (fixed) pass-mark for all subjects, that is derived from the average of pass-marks of all subjects.

An analysis using a global pass-mark showed a slightly higher EER (0.0548). The thesis ends with presenting conclusions and recommendations for future work based on results of the present research.

Keywords: keystroke dynamics, EER, FAR, FRR, anomaly detector, statistical classifier, mobile device.

نموذج جديد لكاشف تباين إحصائي لديناميكية الكتابة باللمس على الهواتف النقالة

إعداد

نور محمود شاكر العبيدي

إشراف

الدكتورمظفر الجراح

الملخص

ديناميكة الكتابة على لوح المفاتيح هي تقنية إثبات الاصالة التي تستخدم إيقاع الكتابة للتمييز بين المستفيد الاصيل والمحتال، وقد شهدت هذه التقنية تطور مستمر لتحسين إمكانية الكشف. إن تحسين قدرة إثبات الاصالة ارتكز بشكل رئيسي على اختيار مصنفات أفضل والتي أدت الى تخفيض معدلات الخطأ في التشخيص. شهد مجال ديناميكة الكتابة على لوح المفاتيح مؤخرا دراسة التحقق من هذه التقنية كطريقة لأثبات الاصالة على الاجهزة النقالة ذات خاصية اللمس، والذي نتج عنه توجيه اهتمام الابحاث من تحسين أداء المصنفات فقط الى إضافة خصائص قابلة للقياس للأجهزة النقالة والتي يمكن أن تؤدي الى تحسين أداء الكشف للمصنفات. العمل البحثي لهذه الاطروحة يهتم بدراسة ديناميكية الكتابة على الاجهزة النقالة من خلال تحليل لبيانات تجريبية تم جمعها باستخدام الاجهزة النقالة والتي اشتملت على الخصائص ذات القياس الزمني بالإضافة الى خاصيتي قيمة الضغط على المفتاح ومساحة لمس الاصبع لموقع المفتاح. تم في البحث عرض مصنف ثنائي (كاشف اختلاف) إحصائي يستند على المتوسط، والمسمى Med-Min-Diff، والذي يستخدم مقياس المسافة عن المتوسط لحساب العتبة العليا والدنيا لقيم الخصائص. تحتسب العتبتان خلال مرحلة التدريب للنظام وتستخدمان لاحقا خلال مرحلة الفحص لتصنيف قيمة خاصية مدخلة إن كانت لمستفيد أصيل أم لمحتال. المرحة الاولى للتحليل تمت باستخدام حزمة بيانات عامة لتجربة سابقة في تقييم مقياس "معدل الخطأ المتساوي" (EER) للنموذج المقترح وبالمقارنة مع نتائج ثلاثة نماذج تدقيق استخدمت في الدراسة السابقة، وكانت قيمة المقياس 0.0679 وهي أقل بكثير من القيم الناتجة عن نماذج التدقيق

الثلاثة. النموذج المقترح تم تنفيذه كنظام لجمع البيانات والتحقق من الاصالة، للعمل على لوح نقال له خاصية اللمس، تحت نظام التشغيل Andriod، ويقوم بقياس الخصائص الزمنية والضغط ومساحة الاصبع.

أستخدم النظام في تجربة لجمع حزمة بيانات جديدة (MEU–Mobile) من 56 شخص، حيث قام كل شخص بكتابة كلمة سر موحدة على اللوح النقال 51 مرة (تمثل 34 إدخال للتدريب و 17 إدخال للفحص). أظهر التحليل لحزمة البيانات الجديدة أن مقياس معدل الخطأ المتساوي باستخدام النموذج المقترح كان 0.0494 وهو أقل من قيمته لحزمة البيانات السابقة. تم حساب معدل القبول الخطأ (FAR) عندما يكون معدل الرفض الخطأ بحدود 5%، وكانت القيمة 5.79%. وذلك يؤشر الى الحاجة لخفض قيمة هذا المقياس المهم من خلال أبحاث تطويرية أخرى. اعتمد النموذج المقترح على مؤشر قبول (pass–mark) كقيمة مرجعية لتقييم نتيجة الفحص لعملية كتابة كلمة السر. استخدمت طريقتان لحساب مؤشر القبول: الطريقة الاولى اعتمدت مؤشر قبول متغير، يحسب لكل مشارك من خلال ضبط قيمته للوصول الى تساوي معدلي القبول الخطأ والرفض الخطأ، والطريقة الثانية اعتمدت حساب مؤشر قبول موحد لكل المشاركين والذي أحتسب من معدل مؤشر القبول المتغير لكل المشاركين. نتج عن التحليل باستخدام مؤشر القبول الموحد الى أن قيمة معدل الخطأ المتساوي كان.(5.48%) وهو أعلى بقليل من حالة استخدام مؤشر القبول المتغير. تتضمن الاطروحة استنتاجات وتوصيات لأعمال مستقبلية مستندة لنتائج البحث الحالي.

الكلمات المفتاحية: ديناميكة الكتابة على لوح المفاتيح، معدل الخطأ المتساوي، معدل الرفض الخطأ، معدل القبول الخطأ، كاشف اختلاف، مصنف إحصائي، جهاز نقال.

Chapter One

Introduction

1.1 Overview

The rapid increase in the use of information systems and information technology in every walk of life is making the users more dependent on computers and digital networks, all that have unveiled new risks to computer systems security. The traditional methods of providing security are failing to keep up with the risks. Thus, a lot of researchers attempt to look for new methods to provide better and more dependable security solutions.

Recently smart mobile phones, tablets and phablets, henceforth referred to as mobile devices, have become the main communication and computing tool for most people, which makes it necessary to protect the private and business data stored on these devices (Long, 2014). User authentication in access control has traditionally relied on passwords, which are vulnerable to be compromised by hackers or over the shoulder observers. Alternative authentication methods for mobile devices have been considered, using biometric features.

Biometrics is considered as a new method of research and development to achieve better security in access control. In general, the biometric systems offer several advantages over password-based authentication schemes, and can provide a much more accurate and reliable security protection, because it relies on unique features for identity verification.

Keystroke dynamics (KSD) is one of the biometrics-based authentication schemes which rely on the typing rhythm to verify users' identity. The keystroke dynamics technique has been the subject of research to improve the authentication accuracy through better anomaly detectors. In this thesis, the work is focused on improving keystroke dynamics based authentication on mobile devices, through an empirical study of user typing behavior (Kolakowska, 2013).

1.2 Problem Statement

The authentication of individuals who are attempting to access a computing resource is one of the most important topics in the field of security technology; hence, researchers and developers are attempting to find solutions for protecting these resources. Measurable features of the behavior of individuals, as well as classifier models, are the cornerstone in user authentication.

The problem addressed in this research is to study the use of keystroke dynamics on touch mobile devices, as an authentication approach, based on experimental data collection and analysis. Special features of the mobile devices are taken into consideration in the authentication process, using an enhanced anomaly detector that is formulated using the collected data.

1.3 Goal and Objectives

The major goal of this thesis is enhancing user authentication on touch mobile devices, using keystroke dynamics. To achieve this goal, the research work in this thesis has set the following objectives:

1. Analysis of an existing keystroke dynamics dataset of touch mobile devices.

2. Formulation of a new anomaly detector model.

3. Implementation of a data collection and authentication system.

4. Data collection and analysis.

1.4 Significance of Work

Research work on the development of new models and techniques for user authentication requires extensive experimental effort, to verify the effectiveness of the proposed models and techniques in verifying users' identity. The significance of the present work is in formulating and verifying a new authentication model that is based on empirical study of users' behavior on mobile devices, taking into account features of mobile devices. The results from such research are envisaged to improve the security of mobile devices, by providing a new anomaly detector model that can be part of an authentication tool, and at the same time provide a new dataset for further work by others in the field of biometrics-based research.

1.5 Methodology

The methodology of this research is founded on the experimental approach, through data collection and analysis, and the main steps of this methodology are as follows:

- Evaluate an existing public dataset using previous statistical models.
- Select and evaluate relevant features to be measured in the proposed model.
- Explore alternative anomaly detection models based on the statistical approach, with the median as the point of center for each feature.
- Implement the selected features and the anomaly detector model in a program for data collection on mobile devices.
- Collect experimental typing data from local subjects.
- Analyze the results, compare with other studies, and investigate additional features for enhancing anomaly detection efficacy and reducing error rates.

1.6 Thesis Outline

This thesis is divided into five chapters:

- Chapter one: contains general concepts of this thesis which include the overview, problem statement, goal and objective, significance of work, methodology and thesis outline.
- Chapter two: contains the literature review of the fields of biometrics and KSD, and the related work.
- Chapter three: contains the proposed KSD anomaly detection model, the feature set, error metrics, and the KSD software that implements the KSD model.
- Chapter four: presents the results and discussion of using the proposed model in analyzing a benchmark KSD, and the results of using the KSD system.
- Chapter five: contains conclusions and future work.

Chapter Two

Background and Literature Review

2.1 Background

The most frequently used form of authentication has been the password. Although it is simple, authentication using passwords is proving to be less effective due to many forms of attacks that can compromise the password, such as an infection with a key-logger worm.

In mobile devices, the risk is greater, as a mobile device is less protected compared to a PC, and is exposed to a wider range of threats due to the nature of the applications on such devices.

The rising trend in storing sensitive data on mobile devices, and the weaknesses of password authentication, has lead to new biometrics research to investigate alternative methods of authentication in which a user is identified by his behavioral or physiological traits. Keystroke dynamics has been investigated as an authentication method on desktop computers and more recently on mobile devices. Experimental work on using keystroke dynamics on mobile devices has shown promising results, and more research is being conducted at present to reduce error rates of authentication and to identify better authentication models and features that are related to mobile devices.

2.2 Biometric Technologies

Biometric technologies are described as the computerized methods of checking or authenticating the status of a person based on a physiological attribute or a behavioral style. Biometric technologies are getting popularity when applied together with common methods for authentication to produce an extra level of security. Mobile devices are being used in different application areas which require one form or another of authentication, in particular, biometrics-based authentication for mobile devices is becoming appropriate and considerably more accurate. Multi-biometric is becoming practically acceptable as it requires nothing to carry on remember, and it is providing more dependable authentication (Karnan, and Krishnaraj, 2012).

The physical characteristics and behavioral features of each user are considered as a natural choice for authentication. Biometrics techniques are more suitable for authentication and are considered as the secured way of determining someone's identity rather than secret keys or passwords, because it cannot be lost, stolen, or listened to, and it is not exposed to physical damage. Physiological features, such as fingerprints or iris, are good for verification because they provide unique authentication, and a lot of security systems are dependent on them (Monrose, and Rubin, 2000).

Available biometric measures that can be used in the authentication process are classified into three main groups:

- Something a person knows (e.g. a password).
- Something a person has (e.g. an ID card, credit card).
- Features of a person (physiological, behavioral).

Security measures which fall under sections (a) and (b) are less dependable as passwords can be stolen or guessed, and a physical artifact such as a credit card can be lost or copied illegally. Recently, attention is moving towards authentication by biometric techniques that include the third class of authentication (i.e., biometrics) as a solution for more secure methods of authentication. For the foreseeable future, these biometric solutions will not eliminate the need for ID cards, passwords, and PINs, but rather will provide a significantly higher level of authentication than passwords and cards alone, especially in situations where security requirements are high (Monrose, and Rubin, 2000).

2.2.1 Keystroke Dynamics

Keystroke dynamics is defined as a behavioral measurement method that recognizes users based on the individual's typing attributes such as a keystroke duration which is the time taken by a key hold, the time between keystrokes (inter-keystroke times), typing error, the force of keystrokes, etc. The analogy is made to the days of telegraphy when operators recognize each other by authenticating their pattern of typing dots and dashes, which was called "the Fist of the Sender" (Chang, et al., 2012).

The advantages of keystroke dynamics are noticeable in a computer environment as it presents a modest and simple method for enhanced access control. Static keystroke analysis is performed once during the login session, using a password text that has been used for training the authentication model. The dynamic analysis means a continuous or periodic monitoring of issued keystrokes, it is conducted during the login session and continues after the session. (Flior, & Kowalski, 2011).

There are some limitations of the keystroke dynamics scheme for authentication (Messerman, et al., 2011), as noted below:

Lower Accuracy: KSD biometrics are inferior regarding authentication accuracy because of the variations in typing rhythm that brought about by outer elements, for example, injury and fatigue. However, other biometric systems are not saved by such elements either.

Lower Permanence: It is necessary to update constantly the stored keystroke profile, which may resolve this issue. Writing pattern of a human may gradually change following the customization towards a password, maturing typing proficiency, adaptation to input devices, and other environmental factors. Therefore, most behavioral biometrics experience fewer permanence problems compared to physiological biometrics.

Over the years, researchers have identified various characteristics or attributes, feature extraction techniques, feature set selection, and classification methods to develop the authentication capabilities of keystroke biometrics (Karnan, et al., 2011).

Recently, touch screen mobile devices have become widely used as even the most basic equipment have touch features included. For implementing a KSD system with touch features for mobile devices, the KSD system is sometimes implemented on notebook touchpad or the mouse to simulate users' clicking on the touch panel, respectively. (Saevanee, and Bhatarakosol, 2008) proposed the pressure feature on the notebook touchpad and claim it can be utilized on the touch panel of mobile phones (Chang, et al., 2012).

The performances of the KSD systems are measured based on the authentication error rates (Teh, et al., 2012) which are described as follows:

1. False Rejection Rate (FRR): the system's rate of rejecting a legitimate user. FRR is also known as Type I error.
2. False Acceptance Rate (FAR): the system's rate of accepting an impostor. FAR is also known as Type II error.

3. Equal Error Rate (EER): the value at which FAR equals to FRR. It is considered as the most balanced authentication performance index. EER is also called the Crossover Error Rate (CER). The lower the ERR (or CER), the more reliable is the system (Karnan, & Krishnaraj, 2012).
4. Impostor Pass Rate (IPR): is the percentage of impostors wrongly matched to a genuine user's reference template, which is the same as the FAR metric.
5. The Failure to Acquire Rate (FTAR): in keystroke dynamics, an acquisition problem is defined as a typing mistake which forces the person to type the text again from scratch. This metric is important for the KSD biometric methodology, although it irritates a lot the user in keystroke dynamics (Giot, et al., 2012).

When these measures are closer to zero, it indicates that the system of authentication is better.

2.2.2 Feature Extraction in KSD

The features extraction from input data of any biometric system is an important procedure whose accuracy and thoroughness play an important role in the authentication results (Monrose, & Rubin, 2000).

In keystroke dynamics, various features can be extracted from the typing raw data Al-Jarrah, 2012), such as features below:

1. Hold (key-press duration).
2. Latency or Up-Down (UD): time difference between two key events.

3. Down-Down (DD) time between key-down of the first key and key-down of the second key.
4. Up-Up (UU) time between key-up of the first key and key-up of the second key.

All the above characteristics are used to generate a template for the particular user. In figure 2-1, the Hold is the time between key down and key up of a single key, latency is the time between key-up of first key and key down the second key.

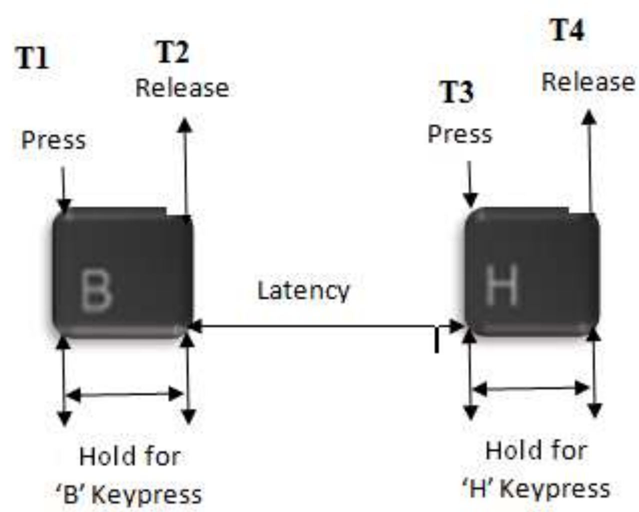

Figure (2-1): Hold, Latency for the Word —BH (Karnan & Krishnaraj, 2012).

While typographical input from computer keyboard has been the main focus of keystroke dynamics research, numerical base input from mobile devices has slowly earned attention since the widespread use of the cellular phone globally in the 20th century.

Early generation smartphones with touch sensitive screen, which could interact via finger or stylus, gained attention as a source of additional features for authentication. The direction of applying keystroke dynamics biometrics to the latest hardware technology and the availability of these devices open the door to new research dimension and possibility (Teh, et al., 2013).

2.3 Literature Review

The keystroke dynamics research area has evolved into several branches of specializations covering keystroke features, anomaly detection models and classifiers, physical desktop keyboard studies, touch mobile devices studies, dataset collection studies, and multi-model / multi-modality studies. In this section we will discuss selected research work that represents key areas of the keystroke dynamics area.

The Ph.D. thesis of Killourhy (2012) and the paper by Killourhy and Maxion (2009) represent 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.

The authors collected data from 51 subjects typing 400 passwords each, and implemented and evaluated 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"). In the process, 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.

The work of Antal, et al (2015) at Sunitia University (SU) 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 a 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.

The EER results for the three models showed lower (better) values than the CMU results on desktop keyboards, in spite of the much lower size of the dataset (2142 records for SU dataset vs. 20400 for the CMU dataset. It is shown experimentally that touchscreen-based features improve keystroke dynamics based identification and verification. Identification measurements were performed using several machine learning classification algorithms, of which the best performers were Random forests, Bayesian nets, and SVM, in a specific order.

In the case of identification measurements, the addition of touchscreen-based features to the default feature set induced an increase of over 10% in accuracy for each classifier. This improvement is harder to notice in the case of verification measurements where the equal error rate was reduced by 2.4% (Manhattan metric). In the data preprocessing stage, the author observed that several typing patterns contained deletions, and these were eliminated from the dataset.

The paper in (Kambourakis, et al., 2014) made an attempt to assess keystroke dynamics on smartphones equipped with a touchscreen. The implemented touch stroke system in the Android platform was executed using several scenarios and methodologies to estimate its efficacy in authenticating the end-user. This paper worked on selecting the most effective machine learning algorithm per methodology to be used as the classifier for the proposed system; which included Random Forest, KNN, and MLP. By the use of legacy scenarios used in keystroke analysis but also via the exploration of new biometric features and methodologies, the authors concluded that touch stroking has significant potential in designing enhanced authentication systems destined to future smartphones. Specifically, when considering the best results achieved during the experiments, one can argue that the FAR value of 3.5 is very promising. The same applies for the minimum EER value of 12.5.

Alariki and Manaf (2014) presented a comprehensive study of features employed in touch-based gesture. Several features were investigated like force, speed, pressure, and flexibility. This paper addressed the interesting topic of touch-based gesture authentication features, among the commonly available touch motion features supported platforms today. This paper presented three types of authentication and the comparison between them shows that choosing biometrics will lead to overcoming the difficulties of the password and token approaches. Touch-based gesture authentication system would make it more difficult for a shoulder surfer to replay the password, even if he observes the entire gesture.

A general framework for behavioral biometrics includes several components such as event acquisition, feature extraction, classifier, and database. This framework continues several phases: Enrollment phase consists of three parts; enter username, six times gesture and sample capture. Training phase consists of four parts: feature selection, extract the feature selected, classify and store in the database. Verification phase consists of five parts; feature selection, extract the feature selected, classify, comparison template and matching process. Three objectives of this research are feature extraction from the user; classify the features and overall performance of the scheme. The aim of this framework is to enhance biometrics authentication to maintain the security of the data on touch mobile phones. This framework will be significant in providing a biometric authentication system which in behavioral traits such as touch gesture-based. The paper made the important observation that negative samples are not available in the enrollment phase. Therefore, one-class classifiers are more suitable for use in real-world authentication systems.

The main limitation of the study is that the subjects of the experiment were mostly students with touchscreen experience ranging from moderate to advance. Another limitation of this study is the small sample size, which did not allow for testing of some of the methods.

The thesis by Al-Rahmani (2014), investigated the keystroke dynamics approach to enhance user authentication based on typing rhythm profile matching by using a statistical approach. An anomaly detector was presented which uses the median for each typing feature element of as the point of center to measure acceptance against, and a Distance-to-Median threshold values which gives the upper and lower limits for an acceptable feature element.

The proposed model was evaluated using the CMU public benchmark dataset of 20,400 records of password typing time measurement, collected by the Biometrics Laboratory of Carnegie Melon University, and this model contained two parts: training and the testing modules. The reported results have shown an improved performance in the anomaly detection of the proposed Med-Med model, compared to previous work using the same CMU dataset. The error rate (EER) is 0.070, a reduction of 27% compared to the top performing model in the CMU study, and a reduction of 12.5% compared to the Med-Std model (Al-Jarrah, 2012).

At the error rate of 0.07 (7%), the Hit Rate is 93%, which indicates that even though the proposed model has a higher anomaly detection performance, it does not deliver the required detection power expected in access control standards (CENELEC, European Standard, 2002).

The obtained results from the MEU experiment showed lower EER error rate and higher hit rate, compared to the results using the CMU dataset for the same Med-Med model, and the MEU experiment used 30 repetitions for training, compared to 200 in a case of CMU.

In the thesis by Ryan (2015), the feasibility of increasing mobile security through the application of keystroke dynamics was investigated. The author noted that classical keystroke dynamics algorithms for physical keyboards could be used on mobile devices with little to no modifications. The research observed that the nature of keystroke dynamics makes it an excellent solution for adding an extra layer of security to the mobile environment. The thesis explored the accuracy and application of several well-known keystroke dynamics algorithms in the mobile domain, and presented an implementation of a mobile application that provides improved security through mobile keystroke dynamics using the best of these, the Nearest Neighbor Mahalanobis Distance class.

The keystroke dynamics algorithms that were tested in a mobile environment performed relatively the same as they did in a traditional environment about best-to-worst ordering. The pure Euclidean distance was the least accurate, while Nearest Neighbor Mahalanobis distance was the most accurate. The Nearest Neighbor Mahalanobis and Nearest Neighbor Euclidean with Flight-Time weighting were both clearly superior to other methods, with the Nearest Neighbor Mahalanobis at an average EER of 22% and Nearest Neighbor Euclidean (Flight-Time weighted) at 32%, while other methods clustered around 50%.

In the thesis by Dedhia (2011), the author describes the using of Keystroke Dynamics for mobile devices running Android operating system, and the language used in the implementation is Java. The database system used in this work is SQLite.

The captured data are key down, key up times and the key ASCII codes. Four features, (key code, two keystroke latencies, and key duration) are analyzed while capturing samples from the user and stored in the database; the stored samples are then compared with previous samples to identify the user as authentic or the impostor.

The thesis shows that keystroke data collected from the user can be used for authentication, it enforces the usage of just a 10-digit phone number as a means of user authentication, rather than an alphanumeric username and a password, which has proven to be far more effective. The data is stored as samples, and the user can effectively be authenticated to match his typing rhythm using an algorithm. The keystroke data was collected from the user for each key pushed; processed to create factors such as dwell time, flight time, login time, and error rate which are stored in the database.

In the study by Ho (2014) at Stanford University, the author concentrated on desktop keyboards and measured three features: the duration of each key press, the latency between keystrokes, and the implicit measures of keystroke force through things like computer microphones. More up-to-date work has tested deploying keystroke dynamics on mobile devices; nevertheless, this project uses only keystroke timing features and often concentrates on passwords that are ten characters or longer. The author notes an observation made in a referenced paper which states that “an attacker can Figure most users' PIN codes after only eleven trials”. With the growth of smartphone theft, they see a fundamental need for stronger security mechanisms that shield a user's data on smartphones; therefore, this project aims to approach this problem by strengthening user authentication during a person unlocks/logs into a phone. Precisely, they construct and analyze four keystroke dynamic classifiers, which use a smartphone's sensors to learn the key tap behavior of the true owner.

This project makes a first trial at generating the accelerometer profile by calculating different statistics overall accelerometer readings in a login trial to create a total of twenty-one accelerometer features per training example; precisely, they calculate statistics like the mean, min, max, variance, first quartile, second quartile, and third quartile for the x, y, and z components of overall accelerometer readings in a training example. Therefore, each data sample consists of thirty-five features, which they extracted from the raw sensor data that the test phone collected.

The best obtained results, using the SVM model, demonstrates that keystroke dynamics can be an efficient means of enhancing the security of a user's data on smartphones; even on an extreme PIN of "1111", the SVM produces extraordinary results with a 5.6% FAR and a 7.6% FRR. With an overall false acceptance rate of 4.4%, password guessing becomes a difficult way for thieves to break into the user phone and access the user data; even if an attacker correctly guesses the user PIN, the author classifier will likely reject the attacker based on his anomalous tap dynamics. Moreover, the author false rejection rate of 5.3% seems to be low enough for this system to usable on real-world smartphones.

Shrivasatva (2011) discusses the importance of mobile security enhancement through keystroke dynamics. Implementation of keystroke dynamics on mobile phones is split into two primary phases. In the initial phase, data from the user's samples is collected and saved in the database. The next phase of the project is defined as an implementation of the algorithm and authentication of the users by data collected from the samples. This thesis will cover the second phase of the project. Smartphones used for the implementation of a project, are built on the Android operating system.

Based on the FRR and FAR values, ROC curve is plotted, and the crossing point of FRR and FAR curve is computed which gives the EER evaluation metric of security systems. In this project, it can be seen that FRR is crossing with FAR near to 0.38 on y-axis. This shows that the ERR of keystroke dynamics in this experiment is high. A biometric system is considered accurate if EER is very low. The above results showed the limitation of using only 10-digit numeric passwords. Alphanumeric passwords can provide higher accuracy results as the keypad for alphabets is larger than the numeric keypad and the number of keys used for typing passwords is larger too. The thesis emphasized the importance of keystroke dynamics for mobile devices. The implementation of keystroke dynamics on mobile devices is considered cost efficient and compatible, as the combination of external hardware is not needed. The conclusion of this thesis is based on examining the data stored by a user with the login input for authentication.

The thesis work of Al-Robayei (2016) aimed at enhancing the authentication power of the keystroke dynamics method through providing better anomaly detector models. The research adopts an empirical analysis approach in formulating anomaly detector models by examining a major keystroke dynamic benchmark dataset. The thesis presents a multi-model anomaly detector that comprises three statistical models that measure features of the typing rhythm to determine the authenticity of the typist based on a comparison with training templates of genuine users.

The three models use the distance to the median of a feature element to classify it as a genuine or impostor feature. The feature set consists of key-hold, the latency between two keys, and a composite feature of hold and latency. Two of the three models were formulated in this study; these are the Enhanced Med-Med model and the Absolute-Minimum model, and the third is an already published model that uses the standard deviation as a measure of distance to the median.

Also, the work involved the development of keystroke dynamics software for data collection during the training phase, and to be used as a dynamic authentication tool during the testing phase. The benchmark dataset was analyzed using the proposed models, and the results showed that the multi-model, the enhanced median-median model and the absolute-minimum models had equal error rates of 0.062, 0.063 and 0.069.

The author concludes that the power of anomaly detection can be enhanced through the combining of several good performing authentication models into a multi-model.

Sensor enhanced keystroke dynamics is presented by Giuffrida, et al., (2014), where a new biometric mechanism to authenticate users typing on mobile devices. The fundamental idea is to characterize the typing behavior of the user through unique sensor characteristics and rely on standard machine learning procedures to implement user authentication. To prove the effectiveness of the author's approach, they implemented an Android prototype system termed Unagi with two passwords, "internet" and "satellite". The author implementation supports many characteristic extraction and discovery algorithms for evaluation and identification objectives, this evaluation is implemented in three different configurations: keystroke timings only, sensor data only, and combination thereof.

Experimental results show that the accuracy yielded by sensor based features exceeds the accuracy of standard keystroke dynamics characteristics (i.e., keystroke timings) by up to two orders of magnitude, it is achieved 4.97% EER using only keystroke timings and 0.08% EER using only sensor data, and that their combination produces little accuracy benefits compared to a sensor-only configuration. With an EER of only 0.08% reported by the best detector/password in the author experiments, they believe theirs is the first encouraging trial to fill the hole between traditional keystroke dynamics methods and the accuracy required in real-world authentication systems. However, the reported low EER results are based on statistical (forged) attacks that are generated by considering the most frequent values of features in actual (human) attacks. Their results need to be verified by others to confirm the low EER values on sensor data.

2.4 Median-Based KSD Classifiers

2.4.1 Median-Median Model

The Med-Med model (Al-Rahmani, 2014) measures anomaly of a feature element based on its distance from the median of that feature element. A feature element value is considered genuine if it is within upper and lower thresholds; otherwise it is treated as an impostor value. The thresholds sets (upper and lower) are calculated during training, and used for classification (genuine or impostor) during testing. The lower threshold is taken to be the minimum value of a feature element set, while the upper threshold is calculated as the sum of the median and the distance to median (DTM). The DTM of a feature element is calculated as the product of the median of the feature element set and the constant fact of 0.7.

2.4.2 Median Vector Proximity Model

In (Al-Jarrah, 2012), an anomaly detector model was presented which was formulated on the assumption that the median metric should be the reference point of center of feature values rather than the mean, to eliminate the effect of outliers.

Distance to Median (DTM), or proximity, is the metric to classify a feature value as genuine or impostor. In this model, the DTM was selected to be the standard deviation of a feature set values, based on empirical analysis of the CMU dataset.

The lower and upper thresholds for a feature set element are calculated for each training data values of each element individually as follows:

Lower Threshold (LT) = Median – Standard Deviation

Upper Threshold (UT) = Median + Standard Deviation.

A testing phase feature value is accepted as genuine if it is within the upper and lower thresholds.

2.4.3 The Multi-Model KSD Model

In (Al-Robayei, 2016) a multi-model is presented, which is based on the concept of taking the vote of several classifiers to decide on the authentication outcome. Three models are included, which are based on the median approach. Two of the three models are formulated in this study; these are the Enhanced Med-Med model and the Absolute-Minimum model, while the third model is the standard deviation based model (Al-Jarrah, 2012). In addition, the work involved the development of a keystroke dynamics software tool for data collection during the training phase, and to be used as a dynamic authentication tool during the testing phase. The study presented results of the analysis of the CMU dataset (Killourhy, 2012), which gave an improved value of the EER metric using the multi-model, compared to previous studies.

Chapter Three

The Proposed Keystroke Dynamics Model for Mobile Devices

3.1 Introduction

User authentication on computers using behavioral biometrics is dependent on employing a classifier model (anomaly detector), and a set of features to be used during the classification phase. The classification phase of an authentication system relies on pre-stored training data on the selected feature set.

In this chapter, we are presenting an authentication model that aims to enhance the anomaly detection process in keystroke dynamics on mobile devices, and its implementation. The formulation of the new model is guided by two criteria:

a. Previous models that have shown good equal error rates (EER).

b. Public datasets of previous research in the same field.

The new model has been chosen to be based on measuring anomaly in reference to the distance to the median of a feature value, as reported in (Al-Rahmani, 2014), where using the median value reduces the effect of outlier values. Also, an empirical analysis of an existing public dataset is carried out, to help in getting an insight into possibilities of formulating a new enhanced model based on the notion of “learning from data”.

This chapter presents analysis of the public dataset, design of the new model, and description of the implemented mobile KSD system, which consists of data collection and user authentication modules.

3.2 Feature Set for Touch Mobile Devices

In previous research on keystroke dynamics that were based on the CMU comparative study, the measurable features where based on desktop keyboards, which included timing features only (Al-Rahmani, 2014) and (Al-Robayei, 2016).

Mobile devices have additional features that can be measured, including pressure, finger area and sensor readings. In this thesis we are adopting the same feature set of the SU work, with the addition of a 2-graph feature that covers the complete time of two successive keys. Details of the selected feature set are as follows:

- Hold (H): The elapsed time during key-press, which is the difference between key-down and key-up timestamps, also referred to as the dwell time.
- Up-Down (UD): The latency time between key-up of the first key in a typing sequence and key-down of the second key, also referred to as the flight time.
- 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 UD between the first and second keys.
- Down-Up (DU): 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 the first and second keys and Hold of the second key.
- Pressure (P): Maximum value of finger pressure on the screen during key-press.
- Finger Area (FA): Maximum value of finger area on the screen during key-press.

3.3 An Overview of Sapientia University Dataset

The selected public dataset for this research is the dataset collected at Sapientia University (Antal, et al., 2015), which has the following advantages:

1. It is available online at the university website.

2. The data is consistent and has been verified and used in several publications.

3. The password that has been used is the CMU password (".tie5Roanl"), which has become a standard password for comparison in the KSD research.

4. The data is collected on mobile devices.

The SU dataset contains timing features (Hold, UD, DD) and additional features of touch mobile devices that are the pressure and size of the finger area when a key is pressed. In the SU experiment the password consisted of 10 characters plus the enter key, which resulted in 41 features for timing data only, and 71 features for timing, pressure, and finger area, as explained in Tables (3-1) and (3-2). The dataset contains KSD records of 42 subjects, each subject has entered the same password 51 times (34 entries in training session and 17 in the testing session). The dataset is divided into two sub-datasets, timing only sub-dataset and timing with pressure and finger area sub-dataset. The SU dataset was collected on Android devices, tablet and a mobile phone.

Table (3-1): Timing Features

Feature name	Explanation	# of features
Key Hold time (H)	Time between key press and release	14
Down-Down time (DD)	Time between consecutive key presses	13
Up-Down tine (UD)	The time between key release and next key press	13
Average hold time (AH)	Average of key hold times	1
Total		**41**

Table (3-2): Timing Features + Touch Screen Features

Feature name	Explanation	# of features
Key Hold time (H)	Time between key press and release	14
Down-Down time (DD)	Time between consecutive key presses	13
Up-Down tine (UD)	The time between key release and next key press	13
Key hold Pressure (P)	Pressure at the moment of key press	14
Finger Area (FA)	Finger area at the moment of key press	14
Average hold time (AH)	Average of key hold times	1
Average Finger Area(AFA)	Average of key finger areas	1
Average Pressure (AP)	Average of key pressures	1
Total		**71**

3.4 Analysis of the SU dataset

Coefficient of Variation Analysis

The first analysis of the SU dataset is the coefficient of variation (CV), which is the ratio of standard deviation to average, of each feature element. Table (3-3) shows the average of the coefficient of variation of each of the feature categories (Hold, UD, DD, P, A). It can be seen that the latency features (UD and DD) have higher CV than Hold, therefore will have more distinguishing effect between different users. The pressure's CV is relatively high, which suggests that it is also sensitive to variations in typing pressure between different people.

The size of finger area has similar CV to the Hold feature, it is a weaker indicator of variation among people.

Table (3-3): Analysis of the Coefficient of Variation According to Features

Coefficient of Variation (CV)	Average
Hold	0.3200
DD	1.3316
UD	1.6424
Pressure	1.0102
Area	0.3698

EER Analysis Using the Med-Med model

The Med-Med model is used to calculate the EER metric's value for the SU dataset as shown in Tables (3-4) and Table (3-5), which presents EER results of the same dataset using three verification models, as reported in (Antal, et al., 2015).

As the models' comparison in Tables (3-4) and (3-5) show, the Med-Med model has out-performed the three verification models by having lower EER error rates, which is similar to the comparison outcome using the CMU desktop KSD dataset (Al-Rahmani, 2014), in spite of the large difference in dataset sizes (2142 in SU vs. 20,400 in CMU), and in hardware platforms. This supports our decision to use the median as the center point in the distanc e calculation of the proposed model.

Table (3-4): EER Analysis of the SU Dataset Using the Med-Med Model

Detector	H+DD+UD+AH (41features)	H+DD+UD+P+FA+AH+AP+AFA (71 features)
Med-Med model	9.38%	7.38%

Table (3-5): EER Analysis of the SU Dataset Using the Three Verification Models

Detector	H+DD+UD+AH(41 features)	H+DD+UD+P+FA+AH+AP+AFA(71 features)
Euclidean	17.5%	15.7%
Manhattan	15.3%	12.9%
Mahalanobis	23.3%	16.6%

3.5 Description of the Proposed Model

The proposed anomaly detector model is based on the following criteria:

- The point of center is the median for each feature element.
- Lower Threshold (LT) = Minimum of a feature element's values
- Distance to Median (DTM) = Median - Minimum
- Upper Threshold (UT) = Median + DTM x C, where C is a constant factor that allows the upper threshold to cover a wider area from the median than the lower threshold. The value of C is taken to be 1.1 (i.e. the upper threshold is 10% higher than the lower threshold). This value was obtained through experimental tuning to get the lowest EER.

- The Test-Score is the number of feature elements that are classified as genuine.
- The Pass-Mark (PMK) is the criterion that is used by the anomaly detector to compare the Test-Score with, to decide on the classification outcome (0 or 1).

3.6 Description of the Proposed System

The proposed mobile KSD data collection and authentication system uses the Med-Min-Diff model as a classifier. It provides two main functions:

- User registration, and data collection during the training phase.
- User authentication (testing phase).

The main user interface of the system provides the user with a list to select either to register a new user or to login as an existing user (authentication).

3.6.1 Training Algorithm

The training algorithm performs the tasks of registering a new user, collecting keystroke data and storing the resulting training template vectors in the database, as shown in Figure (3-1):

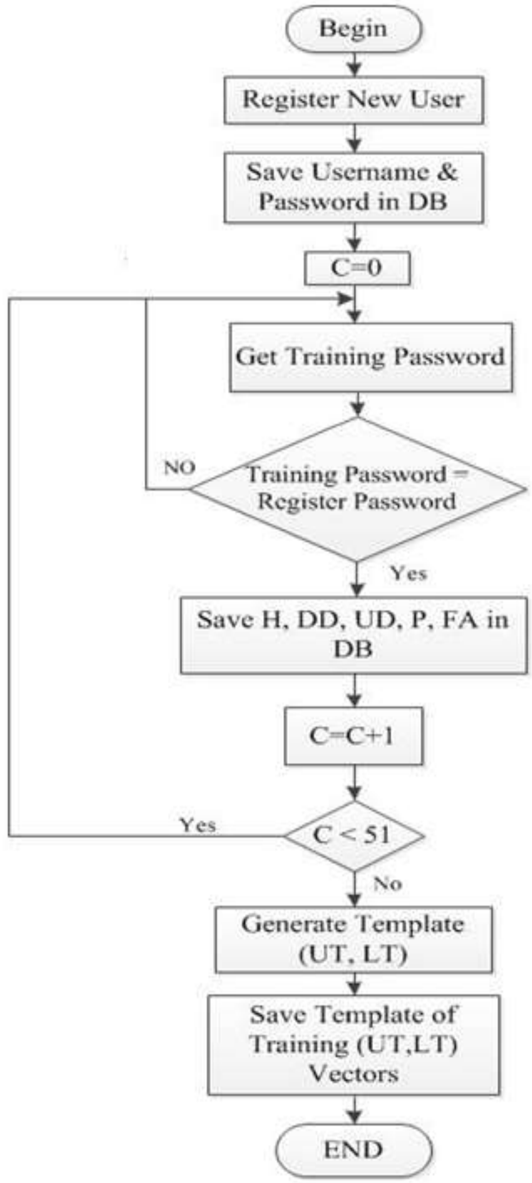

Figure (3-1): Training Algorithm

<u>Training Algorithm Steps</u>

Step1: Start algorithm.

Step2: The user enters the user-name and the registration password.

Step3: Initialize the data collection repetition counter to zero.

Step4: The user re-enters the password.

Step5: If the registered password matches the entered password then Go to Step 6

Else Go to step 4.

Step6: Features of the entered password (Hold, Down-Down, Up-Down, Pressure, Finger Area) are saved in the database.

Step7: Increase the repetition counter by one.

Step8: If the counter is less than the required number of training repetitions (51),

Then Go to Step (4)

Else Go to Step (9).

Step9: The system generates a template with two training vectors (Upper-Threshold and Lower-Threshold) for all feature elements, as follows:

Lower threshold = minimum value of the feature element

Distance to median = median - minimum

Upper threshold= median + DTM x C.

Step10: Save the template of the training vectors in the database.

Step11: Finish.

3.6.2 Authentication Algorithm

The authentication algorithm is used during the authentication (testing) phase, to check that the user is genuine or an impostor. The testing features vector (71 feature) is compared against the thresholds in the template, and the score is calculated.as shown in Figure (3-2):

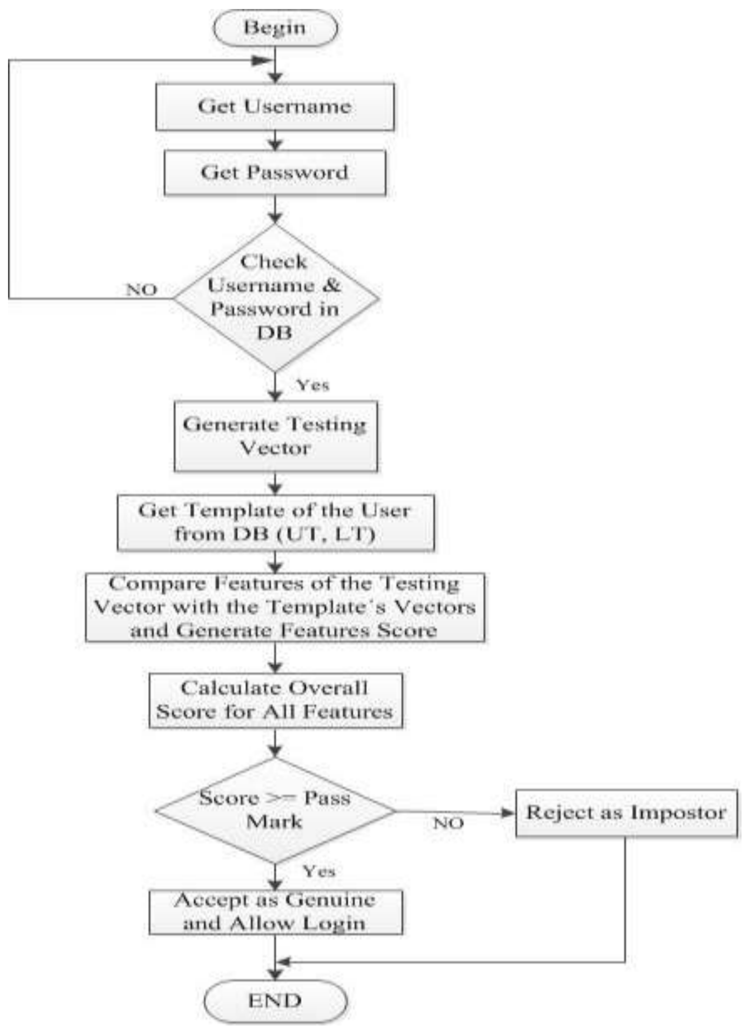

Figure (3-2): Authentication Algorithm

Authentication Algorithm Steps

Step1: Start algorithm.

Step2: The user enters the user-name and the password used in training.

Step3: Check if the user-name exists in the database and the password matches the password in database then Go to step4 if the match is successful

Else Go to step2.

Step4: Generate the testing vector which contains 71 features (Hold, Down-Down, Up-Down, Pressure, Finger Area, Average Hold, Average Pressure, Average Finger Area).

Step5: Get the template vectors from the database that contains upper and lower thresholds.

Step6: Compare the testing vector with the template´s vectors and generate a score for each feature in the testing vector.

Step7: Calculate the overall test-score for all features.

Step8: Check if the test-score is more than or equal to the pass-mark (which was set by the admin) Then Go to step9.

Else Go to step10.

Step9: Accept the user as genuine and allow the login

Step10: Reject the user as an impostor.

Step11: Finish.

3.7 Interfaces of the Mobile KSD System

The proposed mobile KSD system is designed to determine whether a user who is attempting to login to the system is authorized or not. The system provides three interfaces for the training and testing phases, as below:

1- The mobile KSD's main application interface, which provides entry to the system.

2- Training screen which represents the training phase, including registering a new user.

3- Authentication screen which represents the authentication (testing) phase, to verify that the user is genuine or an impostor.

3.7.1 The KSD Main Application Interface

The KSD application is implemented on a touch tablet or smartphone running the Android operating system, as shown in Figure (3-3):-

Figure (3-3): KSD Application Icon

The main interface provides the user with two options, to register a new user or to login as an existing user, as shown Figure (3-4):

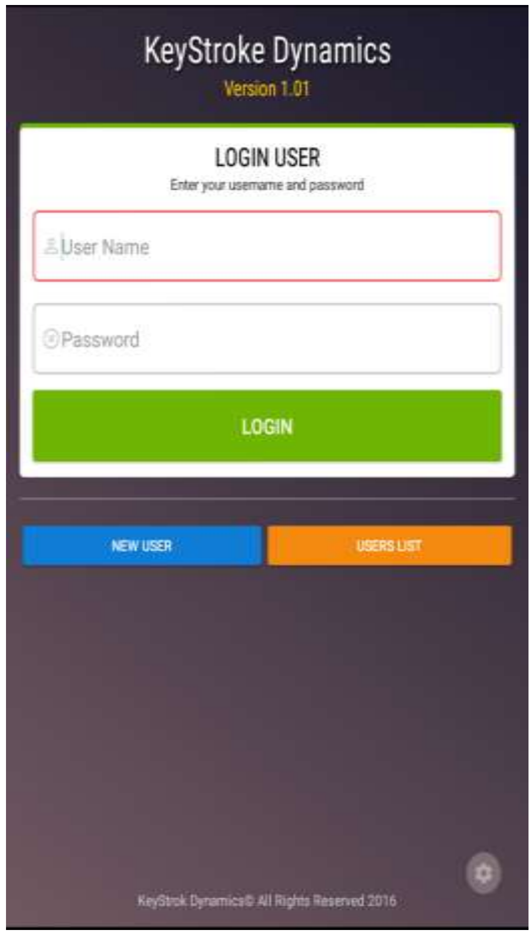

Figure (3-4): The KSD Application's Main Interface

3.7.2 Training Screen

When the user clicks on new user button, the application will display an interface to enter name and password, as shown in Figure (3-5):

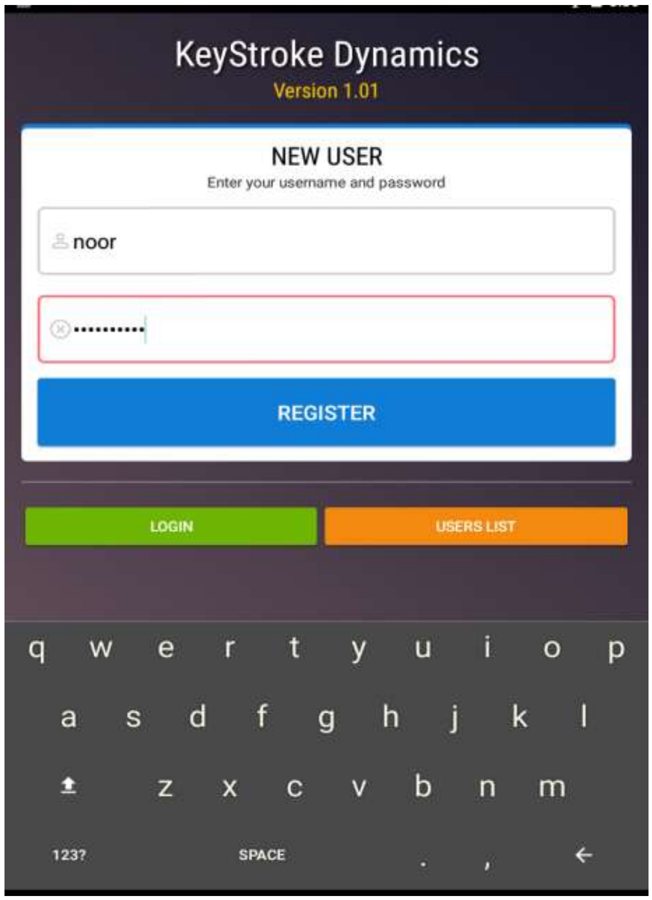

Figure (3-5): New User Interface

The user is required to enter the password a pre-configured number of repetitions, using the training data collection interface, as shown in the two Figures (3-6, 3-7):

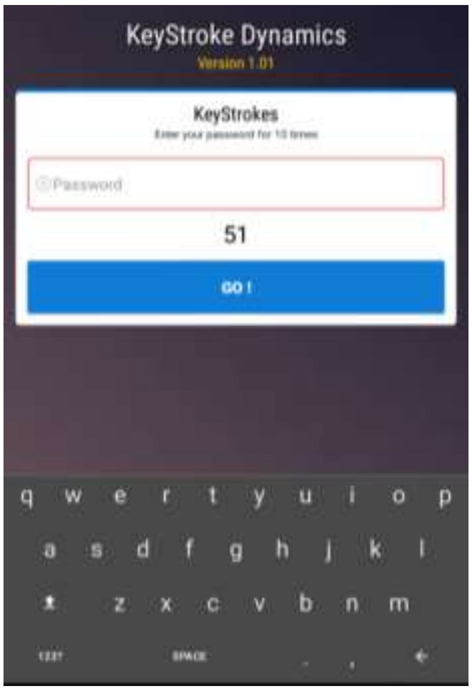

Figure (3-6): Password Entry No. 51

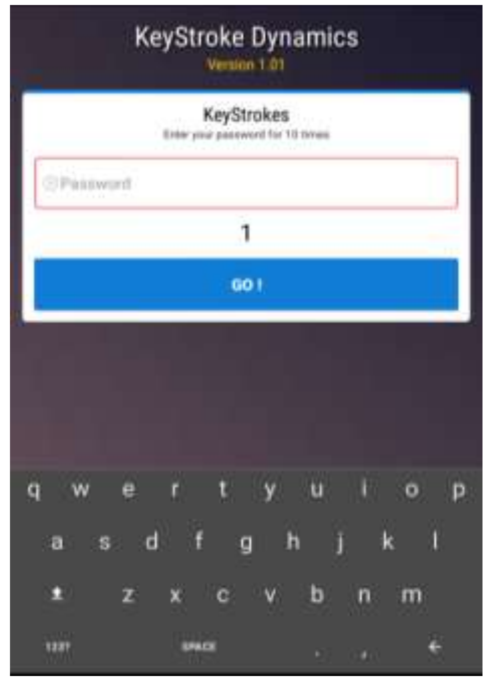

Figure (3-7): Password Entry No. 1

After completion of data entry of the password the required number of repetitions, the user clicks the register button, as shown in Figure (3-8):

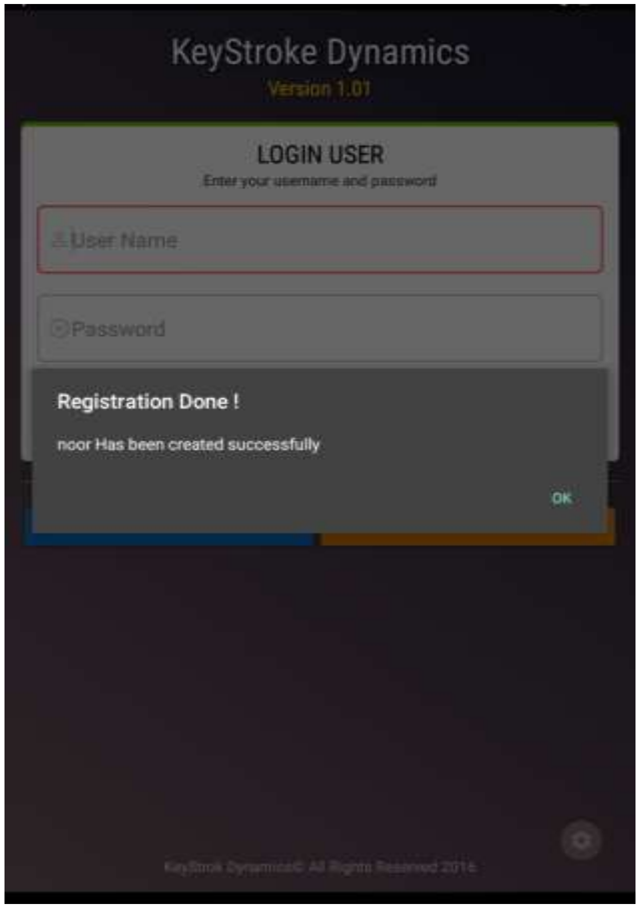

Figure (3-8): Data Collection Completion Screen

If the entered user name exists in the database, it will be rejected as a duplicate entry, as shown in Figure (3-9):

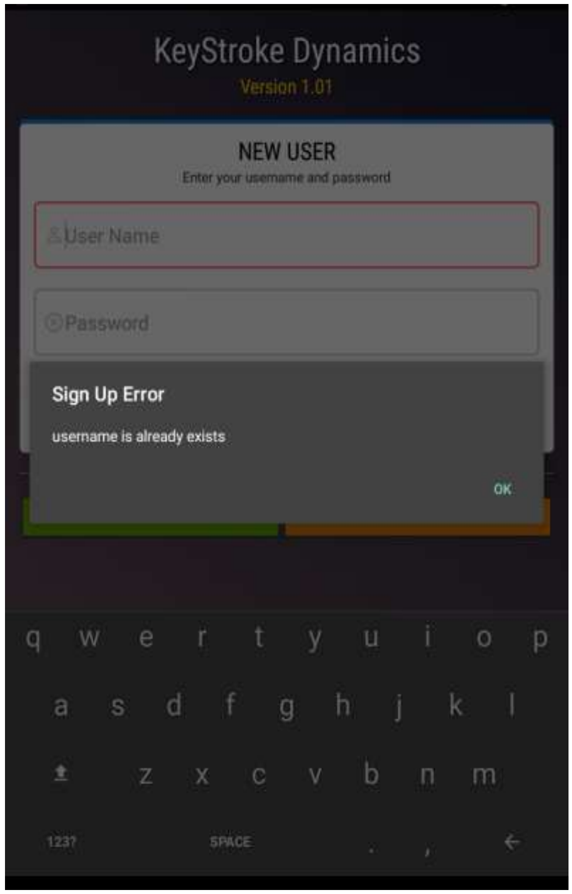

Figure (3-9): New User Duplicate Rejection Screen

3.7.3 Authentication Screen

The authentication process starts when the user enters user name and password, as shown in Figure (3-10):

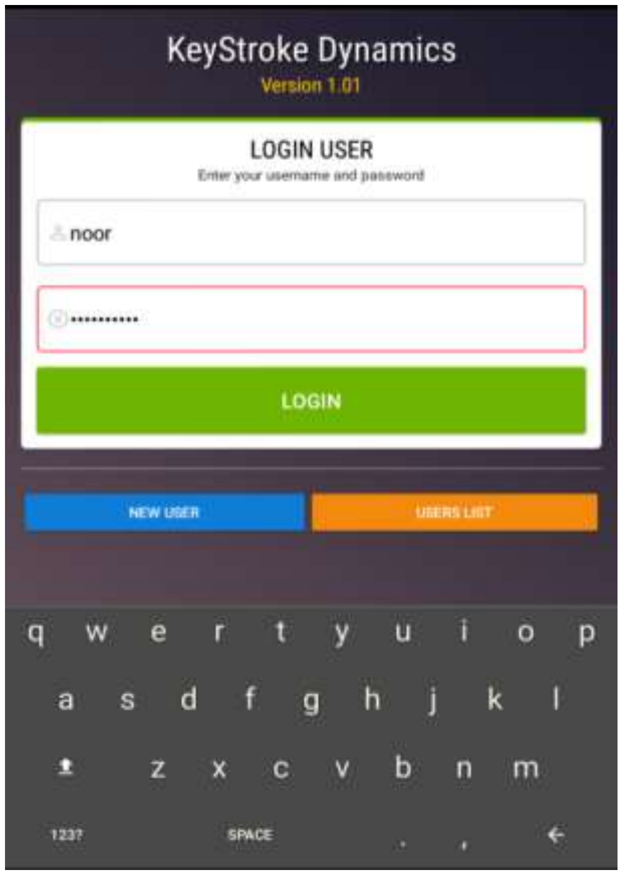

Figure (3-10): Login (Authentication) Screen

If the entered user name doesn't exist or the user has entered a password that doesn't match the training password, the login process will be rejected due to error, as shown in Figure (3-11).

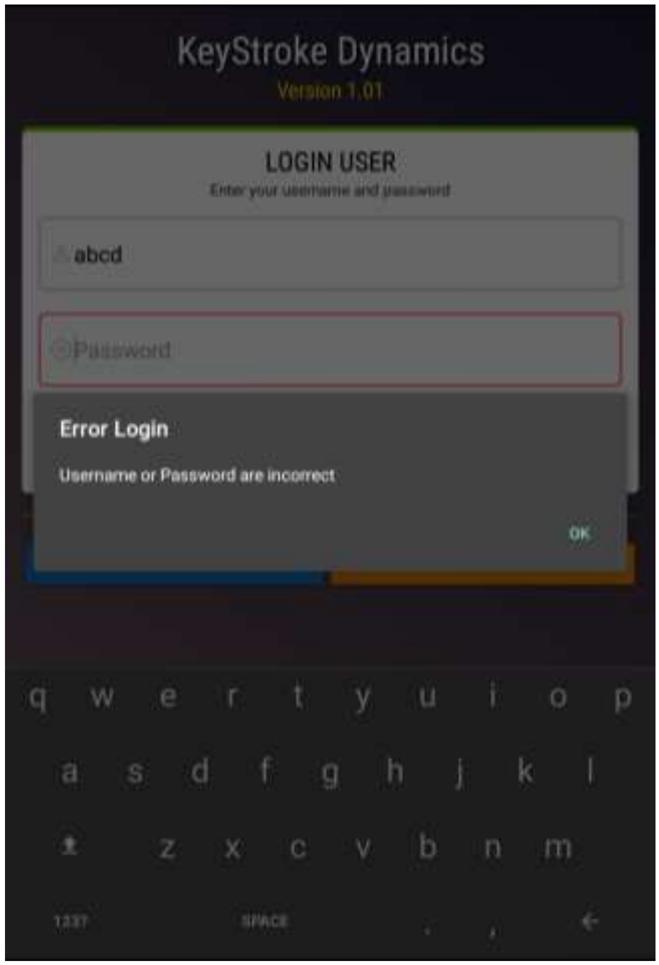

Figure (3-11): Error Login

If the user name and password entry are successful, the authentication process takes place and the login attempt is either accepted as genuine, as in Figure (3-12), or rejected as impostor, as in Figure (3-13).

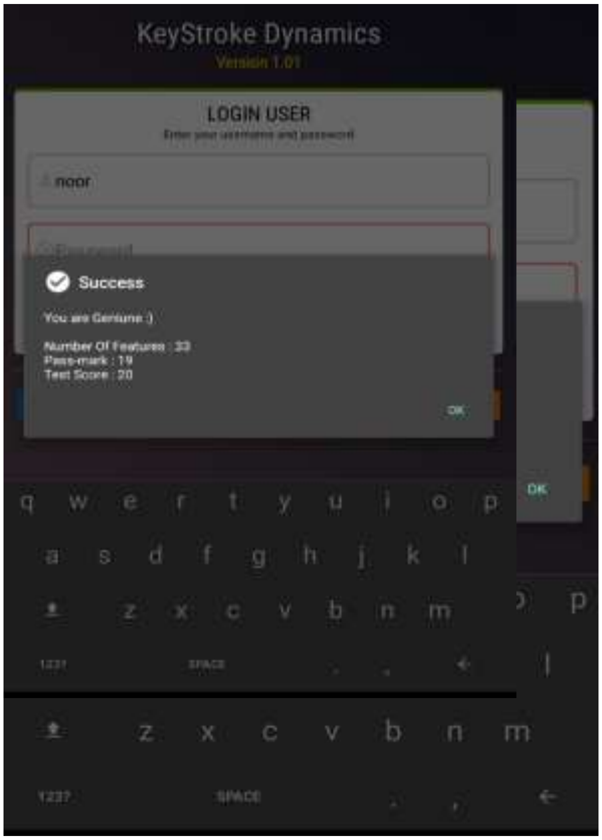

Figure (3-12): Login Success as Genuine User

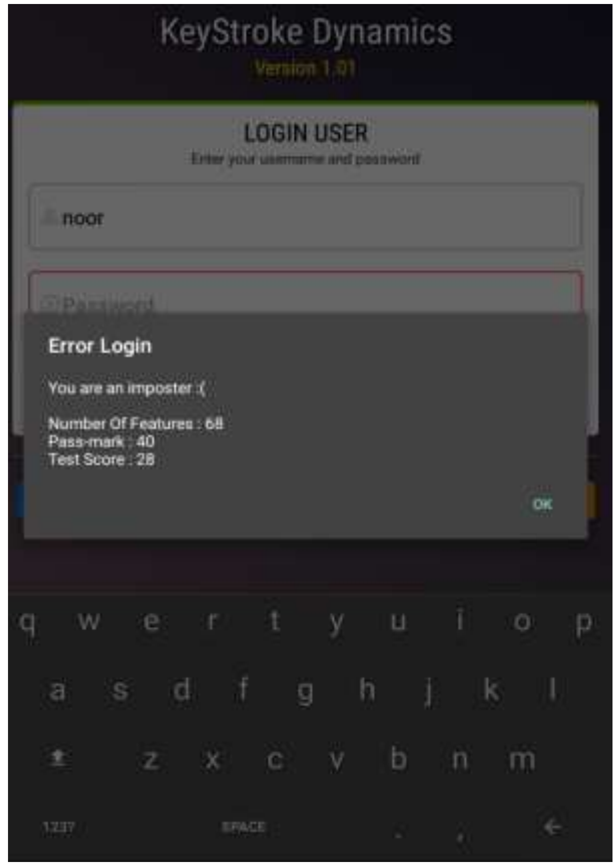

Figure (3-13): Login Rejection as Impostor

Chapter Four

Experimental Results and Discussion

4.1 Overview

This chapter presents the experimental results obtained by using the proposed Med-Min-Diff keystroke dynamics authentication model, and its implementation on an Android platform. The proposed system was used in collecting data from a group of subjects, and analyses of this data are presented in the following sections. For comparison purposes we apply the proposed model in the analysis of the SU dataset.

4.2 Evaluation Methods and Metrics

The results will be evaluated using the three standard error metrics (EER, FAR, FRR), which are used by KSD researchers to evaluate and compare the performance of anomaly detector models. In this thesis we will carry out three types of evaluation using the three metrics, as follows:

1. EER analysis using a different pass-mark per subject, in which the pass-mark is tuned for each subject individually.

2. EER analysis using a global pass-mark for all subjects, which is based on the average pass-mark obtained for all subjects.

3. FAR at 5% FRR analysis. In this analysis, the pass-mark for each user is tuned to achieve 5% FRR, and the corresponding FAR is measured at that point. The purpose of this test is to calculate the rate of acceptance of impostors as genuine users, at an acceptable level of rejection rate of genuine users. The idea behind it is that 5% rejection of genuine users is acceptable, which represents a normal rejection rate due to mistyping in general login attempts (Killourhy, 2012).

4.3 Data Collection

The experimental data collection task is performed along the lines of the work that generated the SU dataset (Antal, et al., 2015), using the same hardware (Nexus 7 tablet), and the same CMU password (".tie5Roanl"). The first subset of the collected data represents 41 feature elements of timing only (14 Hold, 13 DD, 13 UD, Avg. of Hold), which have resulted from typing the 10-chacter password, noting that the extra four feature elements per feature category are due to three shift keys and one enter key. The second subset of the collected data represents 71 feature elements of timing and touch screen (14 Hold, 13 DD, 13 UD, 14 Pressure, 14 Finger Area, Avg. of Hold, Avg. of Pressure, Avg. of Finger Area).

The keystroke data are collected in two sessions for each subject, the first session is the training session which consists of 34 typing attempts, and the second session is the testing session which consists of 17 typing attempts.

There are 56 subjects that we collected data from, from the University (staff and students) and from outside.

4.4 Coefficient of Variation Analysis

The collected data are analyzed using the coefficient of variation of the selected features (H, UD, DD, P, A). The coefficient of variation is the ratio of the standard deviation to the average of a set of values. It is an indicator of the spread or dispersion of data. The CV analysis results for the features in this work are shown in Table 4.1. The results present the average of the coefficient of variation for each feature element. It can be seen that the latency features (UD and DD) have higher CV values than Hold, similar to the

CV results on the CMU dataset (Al-Robayei, 2016). This suggests that the latency features will have more distinguishing effect between different users. The pressure's CV is relatively high compared to other features. Therefore, this indicates that it is sensitive to variations in the typing pressure among different subjects. The size of finger area has similar CV to hold, so it is a weaker indicator of variation among subjects.

Table (4-1): Coefficient of Variation Analysis

Feature	Average of the Coefficient of Variation
Hold	0.2468
DD	1.2315
UD	1.4482
Pressure	1.1187
Finger Area	0.2975

4.5 EER Analysis of the SU Dataset Using the Proposed Model

In this section we present three analyses of the SU dataset using the proposed Med-Min-Diff model. The results have been published in (Al-Obaidi & Al-Jarrah, 2016).

4.5.1 EER Analysis Using Variable Pass-Mark

The SU dataset is analyzed using the proposed model which calculates the EER value, where the pass-mark is determined separately for each subject. The analysis is done on both the 41 features timing data only, and the 71 features of timing and touch screen data as shown in Table 4.2, which combines the previous results of the three verification models and the new results using the proposed model. It can be seen that the new model has resulted in much lower EER in both cases of 41 and 71 features.

Table (4-2): EER Comparison Between the Three Verification Models and the Proposed Model Using the SU Dataset (Antal, M., & et al., 2015)

Detector	H+DD+UD+AH (41features)	H+DD+UD+P+FA+AH+AP+AFA (71 features)
Euclidean	17.5%	15.7%
Manhattan	15.3%	12.9%
Mahalanobis	23.3%	16.6%
Med-Min-Diff	8.53%	6.79%

Detailed analysis of all subjects data in the SU dataset, using the proposed model, are shown in Table 4.3 for the 41 features subset and Table 4.4 for the 71 features subset.

Table (4-3): EER Analysis of the SU Dataset 41 Features (Hold, DD, UD, 1 Avg) Using the Med-Min-Diff Model

		Genuine Test		**Impostor Test**				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	30	16	1	193	12	0.059	0.059	**0.0587**
2	33	16	1	196	9	0.044	0.059	**0.0514**
3	30	16	1	193	12	0.059	0.059	**0.0587**
4	33	15	2	172	33	0.161	0.118	**0.1393**
5	34	17	0	195	10	0.049	0.000	**0.0244**
6	29	17	0	204	1	0.005	0.000	**0.0024**
7	29	17	0	202	3	0.015	0.000	**0.0073**

8	31	14	3	180	25	0.122	0.176	**0.1492**
9	34	16	1	194	11	0.054	0.059	**0.0562**
10	30	12	5	151	54	0.263	0.294	**0.2788**
20	29	16	1	192	13	0.063	0.059	**0.0611**
21	32	16	1	194	11	0.054	0.059	**0.0562**
24	31	17	0	197	8	0.039	0.000	**0.0195**
25	30	14	3	179	26	0.127	0.176	**0.1516**
26	31	16	1	193	12	0.059	0.059	**0.0587**
27	31	16	1	199	6	0.029	0.059	**0.0440**
28	29	14	3	165	40	0.195	0.176	**0.1858**
29	29	17	0	205	0	0.015	0.029	**0.0146**
35	31	16	1	196	9	0.044	0.059	**0.0514**
36	32	14	3	167	38	0.185	0.176	**0.1809**
37	32	14	3	169	36	0.176	0.176	**0.1760**
38	31	15	2	190	15	0.073	0.118	**0.0954**
40	29	16	1	189	16	0.078	0.059	**0.0684**
41	25	15	2	189	16	0.078	0.118	**0.0978**
50	29	15	2	180	25	0.122	0.118	**0.1198**
51	28	15	2	183	22	0.107	0.118	**0.1125**
53	35	17	0	202	3	0.015	0.000	**0.0073**
54	30	15	2	193	12	0.059	0.118	**0.0881**
55	29	17	0	204	1	0.005	0.000	**0.0024**
65	33	17	0	203	2	0.010	0.000	**0.0049**
66	30	16	1	190	15	0.073	0.059	**0.0660**
68	29	13	4	152	53	0.259	0.235	**0.2469**
69	34	16	1	194	11	0.054	0.059	**0.0562**

70	29	11	6	153	52	0.254	0.353	**0.3033**
71	30	16	1	194	11	0.054	0.059	**0.0562**
73	30	16	1	192	13	0.063	0.059	**0.0611**
80	30	16	1	198	7	0.034	0.059	**0.0465**
81	32	16	1	193	12	0.059	0.059	**0.0587**
82	28	17	0	205	0	0.000	0.000	**0.0000**
83	32	16	1	190	15	0.073	0.059	**0.0660**
84	29	16	1	198	7	0.034	0.059	**0.0465**
85	31	15	2	166	39	0.190	0.118	**0.1539**
Average	**30.55**	**15.52**	**1.48**	**187.95**	**17.05**	**0.08**	**0.09**	**0.0853**

Table (4-4): EER Analysis of the SU Dataset 71 Features (Hold, DD, UD, Pressure, Area, 3 Avgs)

Using the Med-Min-Diff Model

		Genuine-Test		**Impostor-Test**				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	**54**	**17**	**0**	**198**	**7**	**0.034**	**0.000**	**0.0171**
2	**61**	**17**	**0**	**202**	**3**	**0.015**	**0.000**	**0.0073**
3	**56**	**17**	**0**	**200**	**5**	**0.024**	**0.000**	**0.0122**
4	**61**	**16**	**1**	**198**	**7**	**0.034**	**0.059**	**0.0465**
5	**60**	**17**	**0**	**200**	**5**	**0.024**	**0.000**	**0.0122**
6	**41**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
7	**55**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
8	**57**	**17**	**0**	**200**	**5**	**0.024**	**0.000**	**0.0122**
9	**50**	**16**	**1**	**194**	**11**	**0.054**	**0.059**	**0.0562**

10	**51**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
20	**47**	**17**	**0**	**192**	**13**	**0.063**	**0.000**	**0.0317**
21	**56**	**16**	**1**	**196**	**9**	**0.044**	**0.059**	**0.0514**
24	**58**	**17**	**0**	**202**	**3**	**0.015**	**0.000**	**0.0073**
25	**56**	**16**	**1**	**189**	**16**	**0.078**	**0.059**	**0.0684**
26	**58**	**16**	**1**	**195**	**10**	**0.049**	**0.059**	**0.0538**
27	**56**	**17**	**0**	**202**	**3**	**0.015**	**0.000**	**0.0073**
28	**54**	**14**	**3**	**177**	**28**	**0.137**	**0.176**	**0.1565**
29	**56**	**17**	**0**	**204**	**1**	**0.005**	**0.000**	**0.0024**
35	**53**	**14**	**3**	**159**	**46**	**0.224**	**0.176**	**0.2004**
36	**54**	**12**	**5**	**152**	**53**	**0.259**	**0.294**	**0.2763**
37	**51**	**13**	**4**	**150**	**55**	**0.268**	**0.235**	**0.2518**
38	**55**	**13**	**4**	**166**	**39**	**0.190**	**0.235**	**0.2128**
40	**54**	**15**	**2**	**181**	**24**	**0.117**	**0.118**	**0.1174**
41	**52**	**16**	**1**	**194**	**11**	**0.054**	**0.059**	**0.0562**
50	**53**	**17**	**0**	**199**	**6**	**0.029**	**0.000**	**0.0146**
51	**55**	**16**	**1**	**196**	**9**	**0.044**	**0.059**	**0.0514**
53	**63**	**17**	**0**	**203**	**2**	**0.010**	**0.000**	**0.0049**
54	**51**	**16**	**1**	**188**	**17**	**0.083**	**0.059**	**0.0709**
55	**52**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
65	**56**	**17**	**0**	**195**	**10**	**0.049**	**0.000**	**0.0244**
66	**55**	**16**	**1**	**197**	**8**	**0.039**	**0.059**	**0.0489**
68	**53**	**15**	**2**	**183**	**22**	**0.107**	**0.118**	**0.1125**
69	**59**	**16**	**1**	**194**	**11**	**0.054**	**0.059**	**0.0562**

70	**51**	**11**	**6**	**138**	**67**	**0.327**	**0.353**	**0.3399**
71	**49**	**15**	**2**	**171**	**34**	**0.166**	**0.118**	**0.1418**
73	**55**	**17**	**0**	**201**	**4**	**0.020**	**0.000**	**0.0098**
80	**49**	**15**	**2**	**188**	**17**	**0.083**	**0.118**	**0.1003**
81	**50**	**16**	**1**	**182**	**23**	**0.112**	**0.059**	**0.0855**
82	**47**	**17**	**0**	**198**	**7**	**0.034**	**0.000**	**0.0171**
83	**57**	**16**	**1**	**197**	**8**	**0.039**	**0.059**	**0.0489**
84	**56**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
85	**57**	**16**	**1**	**190**	**15**	**0.073**	**0.059**	**0.0660**
Average	**54.14**	**15.90**	**1.10**	**190.38**	**14.62**	**0.07**	**0.06**	**0.0679**

4.5.2 EER Analysis of the SU Dataset Using a Global Pass-Mark

A global (fixed) pass-mark is determined for the entire population, based on the average of pass-mark values obtained in the variable pass-mark analysis. An EER analysis using the global pass-mark is performed for the 41 and 71 features data, as shown in Table 4.5 and Table 4.6. The average EER for both 41 and 71 features are slightly higher than the local pass-mark results, but they are still much lower than the verification models.

Table (4-5): EER Analysis of the SU Dataset 41 Features (Hold, DD, UD, 1 Avg)

Using Med-Min-Diff Model with a Global Pass-Mark

		Genuine Test		Impostor Test				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	29	17	0	183	22	0.107	0.000	0.0537
2	29	17	0	169	36	0.176	0.000	0.0878
3	29	16	1	187	18	0.088	0.059	0.0733
4	29	17	0	116	89	0.434	0.000	0.2171
5	29	17	0	161	44	0.215	0.000	0.1073
6	29	17	0	204	1	0.005	0.000	0.0024
7	29	17	0	202	3	0.015	0.000	0.0073
8	29	17	0	166	39	0.190	0.000	0.0951
9	29	17	0	142	63	0.307	0.000	0.1537
10	29	14	3	139	66	0.322	0.176	0.2492
20	29	16	1	192	13	0.063	0.059	0.0611
21	29	17	0	177	28	0.137	0.000	0.0683
24	29	17	0	188	17	0.083	0.000	0.0415
25	29	17	0	173	32	0.156	0.000	0.0780
26	29	17	0	174	31	0.151	0.000	0.0756
27	29	17	0	192	13	0.063	0.000	0.0317
28	29	14	3	165	40	0.195	0.176	0.1858
29	29	17	0	205	0	0.015	0.029	0.0146
35	29	16	1	180	25	0.122	0.059	0.0904
36	29	17	0	126	79	0.385	0.000	0.1927

37	**29**	**16**	**1**	**144**	**61**	**0.298**	**0.059**	**0.1782**
38	**29**	**16**	**1**	**173**	**32**	**0.156**	**0.059**	**0.1075**
40	**29**	**16**	**1**	**189**	**16**	**0.078**	**0.059**	**0.0684**
41	**29**	**12**	**5**	**201**	**4**	**0.020**	**0.294**	**0.1568**
50	**29**	**15**	**2**	**180**	**25**	**0.122**	**0.118**	**0.1198**
51	**29**	**14**	**3**	**185**	**20**	**0.098**	**0.176**	**0.1370**
53	**29**	**17**	**0**	**142**	**63**	**0.307**	**0.000**	**0.1537**
54	**29**	**17**	**0**	**184**	**21**	**0.102**	**0.000**	**0.0512**
55	**29**	**17**	**0**	**204**	**1**	**0.005**	**0.000**	**0.0024**
65	**29**	**17**	**0**	**189**	**16**	**0.078**	**0.000**	**0.0390**
66	**29**	**17**	**0**	**182**	**23**	**0.112**	**0.000**	**0.0561**
68	**29**	**13**	**4**	**152**	**53**	**0.259**	**0.235**	**0.2469**
69	**29**	**17**	**0**	**140**	**65**	**0.317**	**0.000**	**0.1585**
70	**29**	**11**	**6**	**153**	**52**	**0.254**	**0.353**	**0.3033**
71	**29**	**16**	**1**	**191**	**14**	**0.068**	**0.059**	**0.0636**
73	**29**	**17**	**0**	**186**	**19**	**0.093**	**0.000**	**0.0463**
80	**29**	**17**	**0**	**197**	**8**	**0.039**	**0.000**	**0.0195**
81	**29**	**17**	**0**	**172**	**33**	**0.161**	**0.000**	**0.0805**
82	**29**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
83	**29**	**17**	**0**	**164**	**41**	**0.200**	**0.000**	**0.1000**
84	**29**	**16**	**1**	**198**	**7**	**0.034**	**0.059**	**0.0465**
85	**29**	**16**	**1**	**142**	**63**	**0.307**	**0.059**	**0.1831**
Average	**29.00**	**16.17**	**0.83**	**174.14**	**30.86**	**0.15**	**0.05**	**0.1001**

Table (4-6): EER Analysis of the SU Dataset 71 Features (Hold, DD, UD, Pressure, Area, 3 Avgs)

Using Med-Min-Diff Model with a Global Pass-Mark

		Genuine-Test		Impostor-Test				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	52	17	0	195	10	0.049	0.000	0.0244
2	52	17	0	174	31	0.151	0.000	0.0756
3	52	17	0	191	14	0.068	0.000	0.0341
4	52	17	0	125	80	0.390	0.000	0.1951
5	52	17	0	186	19	0.093	0.000	0.0463
6	52	17	0	205	0	0.000	0.000	0.0000
7	52	17	0	203	2	0.010	0.000	0.0049
8	52	17	0	196	9	0.044	0.000	0.0220
9	52	16	1	196	9	0.044	0.059	0.0514
10	52	17	0	205	0	0.000	0.000	0.0000
20	52	15	2	203	2	0.010	0.118	0.0637
21	52	17	0	191	14	0.068	0.000	0.0341
24	52	17	0	188	17	0.083	0.000	0.0415
25	52	17	0	158	47	0.229	0.000	0.1146
26	52	17	0	168	37	0.180	0.000	0.0902
27	52	17	0	199	6	0.029	0.000	0.0146
28	52	17	0	159	46	0.224	0.000	0.1122
29	52	17	0	202	3	0.015	0.000	0.0073
35	52	15	2	148	57	0.278	0.118	0.1978

36	**52**	**16**	**1**	**131**	**74**	**0.361**	**0.059**	**0.2099**
37	**52**	**11**	**6**	**156**	**49**	**0.239**	**0.353**	**0.2960**
38	**52**	**16**	**1**	**136**	**69**	**0.337**	**0.059**	**0.1977**
40	**52**	**17**	**0**	**172**	**33**	**0.161**	**0.000**	**0.0805**
41	**52**	**16**	**1**	**194**	**11**	**0.054**	**0.059**	**0.0562**
50	**52**	**17**	**0**	**198**	**7**	**0.034**	**0.000**	**0.0171**
51	**52**	**17**	**0**	**187**	**18**	**0.088**	**0.000**	**0.0439**
53	**52**	**17**	**0**	**174**	**31**	**0.151**	**0.000**	**0.0756**
54	**52**	**15**	**2**	**190**	**15**	**0.073**	**0.118**	**0.0954**
55	**52**	**17**	**0**	**205**	**0**	**0.000**	**0.000**	**0.0000**
65	**52**	**17**	**0**	**185**	**20**	**0.098**	**0.000**	**0.0488**
66	**52**	**16**	**1**	**180**	**25**	**0.122**	**0.059**	**0.0904**
68	**52**	**16**	**1**	**180**	**25**	**0.122**	**0.059**	**0.0904**
69	**52**	**17**	**0**	**138**	**67**	**0.327**	**0.000**	**0.1634**
70	**52**	**11**	**6**	**153**	**52**	**0.254**	**0.353**	**0.3033**
71	**52**	**11**	**6**	**187**	**18**	**0.088**	**0.353**	**0.2204**
73	**52**	**17**	**0**	**189**	**16**	**0.078**	**0.000**	**0.0390**
80	**52**	**13**	**4**	**195**	**10**	**0.049**	**0.235**	**0.1420**
81	**52**	**11**	**6**	**192**	**13**	**0.063**	**0.353**	**0.2082**
82	**52**	**12**	**5**	**203**	**2**	**0.010**	**0.294**	**0.1519**
83	**52**	**17**	**0**	**154**	**51**	**0.249**	**0.000**	**0.1244**
84	**52**	**17**	**0**	**202**	**3**	**0.015**	**0.000**	**0.0073**
85	**52**	**17**	**0**	**174**	**31**	**0.151**	**0.000**	**0.0756**
Average	**52.00**	**15.93**	**1.07**	**180.17**	**24.83**	**0.12**	**0.06**	**0.0921**

4.5.3 FAR Analysis at 5% FRR

The SU dataset 71 features subset are analyzed to obtain the average FAR at the 5% FRR rate, as shown in Table 4.7. This analysis was not performed in the SU study, and it is included here as it was presented in the CMU work (Killourhy, 2012).The results indicate that the false acceptance rate of impostors should be reduced with further refinement of the keystroke dynamics model, with the aim of reaching an acceptable level of FAR.

Table (4-7): FAR Analysis of the SU Dataset at 5% FRR for the 71 Features (Hold, DD, UD, Pressure, Area,3 Avgs) Using the Med-Min-Diff model

		Genuine-Test		Impostor-Test			
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**
1	55	16	1	200	5	2.44%	5.88%
2	62	16	1	203	2	0.98%	5.88%
3	57	16	1	203	2	0.98%	5.88%
4	61	16	1	198	7	3.41%	5.88%
5	61	16	1	200	5	2.44%	5.88%
6	58	16	1	205	0	0.00%	5.88%
7	59	16	1	205	0	0.00%	5.88%
8	57	17	0	200	5	2.44%	0.00%
9	50	16	1	194	11	5.37%	5.88%
10	56	16	1	205	0	0.00%	5.88%
20	47	17	0	192	13	6.34%	0.00%
21	56	16	1	196	9	4.39%	5.88%
24	59	16	1	203	2	0.98%	5.88%

25	56	16	1	189	16	7.80%	5.88%
26	58	16	1	195	10	4.88%	5.88%
27	57	16	1	203	2	0.98%	5.88%
28	53	16	1	168	37	18.05%	5.88%
29	56	17	0	204	1	0.49%	0.00%
35	51	16	1	138	67	32.68%	5.88%
36	52	16	1	131	74	36.10%	5.88%
37	43	16	1	107	98	47.80%	5.88%
38	53	16	1	145	60	29.27%	5.88%
40	53	17	0	177	28	13.66%	0.00%
41	52	16	1	194	11	5.37%	5.88%
50	54	16	1	202	3	1.46%	5.88%
51	55	16	1	196	9	4.39%	5.88%
53	64	16	1	204	1	0.49%	5.88%
54	51	16	1	188	17	8.29%	5.88%
55	59	16	1	205	0	0.00%	5.88%
65	56	17	0	195	10	4.88%	0.00%
66	55	16	1	197	8	3.90%	5.88%
68	52	16	1	180	25	12.20%	5.88%
69	59	16	1	194	11	5.37%	5.88%
70	46	17	0	79	126	61.46%	0.00%
71	48	16	1	169	36	17.56%	5.88%
73	56	16	1	201	4	1.95%	5.88%
80	48	17	0	186	19	9.27%	0.00%

81	50	16	1	182	23	11.22%	5.88%
82	48	16	1	200	5	2.44%	5.88%
83	57	16	1	197	8	3.90%	5.88%
84	59	16	1	205	0	0.00%	5.88%
85	57	16	1	190	15	7.32%	5.88%
Average	**54.67**	**16.17**	**0.83**	**186.31**	**18.69**	**9.12%**	**4.90%**

4.6 Analysis Results of the MEU-Mobile Dataset Using the Proposed Model

The MEU-Mobile dataset has been analyzed using the proposed model (Med-Min-Diff), and the results are discussed in the following sub-sections.

4.6.1 EER Analysis Using Variable Pass-Marks

The MEU-Mobile dataset is analyzed using the proposed model which calculates the EER value, where the pass-mark is determined separately for each subject. The analysis is done on both the 41 features timing data only, and 71 features which included timing and touch screen features. Table 4.8 presents the 41 features results while Table 4.9 presents the 71 features results and the following observations are noted about the results:

- The EER results for the 71 features are lower than the 41 features.
- The EER results for the 71 features and 41 features are slightly lower than the results of the SU dataset using the same model. The difference can be attributed to difference in number of subjects (42 vs. 56), or implementation differences as each experiment used its own software.

Table (4-8): EER Analysis of the MEU-Mobile Dataset 41 Features (Hold, DD, UD, 1 Avg) Using the Med-Min-Diff Model

		Genuine-Test		Impostor-Test				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	30	15	2	255	20	0.073	0.118	0.0952
2	31	17	0	264	11	0.040	0.000	0.0200
3	32	14	3	222	53	0.193	0.176	0.1846
4	29	15	2	245	30	0.109	0.118	0.1134
5	27	17	0	260	15	0.055	0.000	0.0273
6	30	15	2	233	42	0.153	0.118	0.1352
7	29	15	2	244	31	0.113	0.118	0.1152
8	29	14	3	238	37	0.135	0.176	0.1555
9	31	14	3	234	41	0.149	0.176	0.1628
10	29	15	2	246	29	0.105	0.118	0.1116
11	29	16	1	261	14	0.051	0.059	0.0549
12	32	15	2	233	42	0.153	0.118	0.1352
13	29	16	1	254	21	0.076	0.059	0.0676
14	30	16	1	246	29	0.105	0.059	0.0821
15	31	17	0	268	7	0.025	0.000	0.0127
16	29	16	1	261	14	0.051	0.059	0.0549
17	30	16	1	248	27	0.098	0.059	0.0785
18	30	15	2	253	22	0.080	0.118	0.0988
19	30	17	0	266	9	0.033	0.000	0.0164
20	27	13	4	229	46	0.167	0.235	0.2013

21	**32**	**17**	**0**	**271**	**4**	**0.015**	**0.000**	**0.0073**
22	**31**	**15**	**2**	**236**	**39**	**0.142**	**0.118**	**0.1297**
23	**31**	**13**	**4**	**217**	**58**	**0.211**	**0.235**	**0.2231**
24	**30**	**16**	**1**	**264**	**11**	**0.040**	**0.059**	**0.0494**
25	**26**	**17**	**0**	**270**	**5**	**0.018**	**0.000**	**0.0091**
26	**33**	**14**	**3**	**229**	**46**	**0.167**	**0.176**	**0.1719**
27	**31**	**17**	**0**	**268**	**7**	**0.025**	**0.000**	**0.0127**
28	**33**	**15**	**2**	**259**	**16**	**0.058**	**0.118**	**0.0879**
29	**29**	**16**	**1**	**258**	**17**	**0.062**	**0.059**	**0.0603**
30	**27**	**16**	**1**	**252**	**23**	**0.084**	**0.059**	**0.0712**
31	**25**	**14**	**3**	**229**	**46**	**0.167**	**0.176**	**0.1719**
32	**30**	**16**	**1**	**253**	**22**	**0.080**	**0.059**	**0.0694**
33	**31**	**14**	**3**	**224**	**51**	**0.185**	**0.176**	**0.1810**
34	**31**	**17**	**0**	**267**	**8**	**0.029**	**0.000**	**0.0145**
35	**32**	**17**	**0**	**275**	**0**	**0.000**	**0.000**	**0.0000**
36	**31**	**15**	**2**	**244**	**31**	**0.113**	**0.118**	**0.1152**
37	**33**	**16**	**1**	**241**	**34**	**0.124**	**0.059**	**0.0912**
38	**30**	**17**	**0**	**267**	**8**	**0.029**	**0.000**	**0.0145**
39	**30**	**17**	**0**	**270**	**5**	**0.018**	**0.000**	**0.0091**
40	**31**	**16**	**1**	**262**	**13**	**0.047**	**0.059**	**0.0530**
41	**28**	**16**	**1**	**260**	**15**	**0.055**	**0.059**	**0.0567**
42	**30**	**16**	**1**	**265**	**10**	**0.036**	**0.059**	**0.0476**
43	**31**	**17**	**0**	**273**	**2**	**0.007**	**0.000**	**0.0036**
44	**29**	**16**	**1**	**243**	**32**	**0.116**	**0.059**	**0.0876**

45	**33**	**17**	**0**	**264**	**11**	**0.040**	**0.000**	**0.0200**
46	**32**	**13**	**4**	**210**	**65**	**0.236**	**0.235**	**0.2358**
47	**32**	**16**	**1**	**261**	**14**	**0.051**	**0.059**	**0.0549**
48	**32**	**17**	**0**	**267**	**8**	**0.029**	**0.000**	**0.0145**
49	**32**	**13**	**4**	**238**	**37**	**0.135**	**0.235**	**0.1849**
50	**33**	**15**	**2**	**272**	**3**	**0.011**	**0.118**	**0.0643**
51	**33**	**16**	**1**	**252**	**23**	**0.084**	**0.059**	**0.0712**
52	**30**	**15**	**2**	**217**	**58**	**0.211**	**0.118**	**0.1643**
53	**29**	**16**	**1**	**258**	**17**	**0.062**	**0.059**	**0.0603**
54	**32**	**17**	**0**	**267**	**8**	**0.029**	**0.000**	**0.0145**
55	**30**	**16**	**1**	**250**	**25**	**0.091**	**0.059**	**0.0749**
56	**31**	**15**	**2**	**246**	**29**	**0.105**	**0.118**	**0.1116**
Average	**30.32**	**15.61**	**1.39**	**251.05**	**23.95**	**0.09**	**0.08**	**0.0845**

Table (4-9): EER Analysis of the MEU-Mobile Dataset 71 Features (Hold, DD, UD, Pressure, Area, 3 Avgs) Using the Med-Min-Diff Model

		Genuine-Test		Impostor-Test				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	55	17	0	268	7	0.025	0.000	0.0127
2	55	16	1	259	16	0.058	0.059	0.0585
3	55	16	1	254	21	0.076	0.059	0.0676
4	53	16	1	258	17	0.062	0.059	0.0603
5	51	16	1	262	13	0.047	0.059	0.0530
6	54	16	1	253	22	0.080	0.059	0.0694
7	52	15	2	261	14	0.051	0.118	0.0843
8	51	16	1	261	14	0.051	0.059	0.0549
9	53	15	2	248	27	0.098	0.118	0.1079
10	51	16	1	253	22	0.080	0.059	0.0694
11	52	15	2	257	18	0.065	0.118	0.0916
12	56	16	1	266	9	0.033	0.059	0.0458
13	51	16	1	256	19	0.069	0.059	0.0640
14	56	16	1	252	23	0.084	0.059	0.0712
15	53	15	2	263	12	0.044	0.118	0.0806
16	53	16	1	259	16	0.058	0.059	0.0585
17	54	16	1	267	8	0.029	0.059	0.0440
18	55	17	0	271	4	0.015	0.000	0.0073
19	55	17	0	274	1	0.004	0.000	0.0018
20	48	15	2	243	32	0.116	0.118	0.1170
21	53	17	0	267	8	0.029	0.000	0.0145

22	**54**	**16**	**1**	**251**	**24**	**0.087**	**0.059**	**0.0730**
23	**56**	**15**	**2**	**235**	**40**	**0.145**	**0.118**	**0.1316**
24	**52**	**16**	**1**	**267**	**8**	**0.029**	**0.059**	**0.0440**
25	**53**	**17**	**0**	**275**	**0**	**0.000**	**0.000**	**0.0000**
26	**56**	**15**	**2**	**251**	**24**	**0.087**	**0.118**	**0.1025**
27	**52**	**17**	**0**	**269**	**6**	**0.022**	**0.000**	**0.0109**
28	**58**	**16**	**1**	**262**	**13**	**0.047**	**0.059**	**0.0530**
29	**52**	**17**	**0**	**273**	**2**	**0.007**	**0.000**	**0.0036**
30	**47**	**17**	**0**	**271**	**4**	**0.015**	**0.000**	**0.0073**
31	**51**	**16**	**1**	**269**	**6**	**0.022**	**0.059**	**0.0403**
32	**53**	**16**	**1**	**258**	**17**	**0.062**	**0.059**	**0.0603**
33	**52**	**16**	**1**	**251**	**24**	**0.087**	**0.059**	**0.0730**
34	**54**	**17**	**0**	**269**	**6**	**0.022**	**0.000**	**0.0109**
35	**54**	**17**	**0**	**275**	**0**	**0.000**	**0.000**	**0.0000**
36	**56**	**16**	**1**	**260**	**15**	**0.055**	**0.059**	**0.0567**
37	**61**	**16**	**1**	**265**	**10**	**0.036**	**0.059**	**0.0476**
38	**53**	**17**	**0**	**268**	**7**	**0.025**	**0.000**	**0.0127**
39	**52**	**17**	**0**	**267**	**8**	**0.029**	**0.000**	**0.0145**
40	**55**	**17**	**0**	**272**	**3**	**0.011**	**0.000**	**0.0055**
41	**53**	**17**	**0**	**271**	**4**	**0.015**	**0.000**	**0.0073**
42	**53**	**16**	**1**	**264**	**11**	**0.040**	**0.059**	**0.0494**
43	**53**	**17**	**0**	**275**	**0**	**0.000**	**0.000**	**0.0000**
44	**52**	**16**	**1**	**254**	**21**	**0.076**	**0.059**	**0.0676**
45	**59**	**17**	**0**	**270**	**5**	**0.018**	**0.000**	**0.0091**

46	**53**	**16**	**1**	**254**	**21**	**0.076**	**0.059**	**0.0676**
47	**56**	**17**	**0**	**272**	**3**	**0.011**	**0.000**	**0.0055**
48	**57**	**17**	**0**	**273**	**2**	**0.007**	**0.000**	**0.0036**
49	**55**	**14**	**3**	**244**	**31**	**0.113**	**0.176**	**0.1446**
50	**56**	**17**	**0**	**272**	**3**	**0.011**	**0.000**	**0.0055**
51	**55**	**16**	**1**	**260**	**15**	**0.055**	**0.059**	**0.0567**
52	**54**	**15**	**2**	**246**	**29**	**0.105**	**0.118**	**0.1116**
53	**56**	**16**	**1**	**262**	**13**	**0.047**	**0.059**	**0.0530**
54	**53**	**16**	**1**	**256**	**19**	**0.069**	**0.059**	**0.0640**
55	**53**	**16**	**1**	**255**	**20**	**0.073**	**0.059**	**0.0658**
56	**55**	**16**	**1**	**250**	**25**	**0.091**	**0.059**	**0.0749**
Average	**53.75**	**16.16**	**0.84**	**261.39**	**13.61**	**0.05**	**0.05**	**0.0494**

4.6.2 EER Analysis Using a Global Pass-Mark

A global (fixed) pass-mark is determined for the entire population, based on the average of pass-marks obtained in the variable pass-mark analysis in Table 4.8 and table 4.9. An EER analysis using the global pass-mark is performed for the 41 and 71 features data, as shown in Tables 4.10 and 4.11. The following observations are made on the results:

- The average EER for the 71 features is lower than the 41 features, which indicates that adding more features improves the authentication outcome.
- The average EER for the 71 and 41 features are slightly higher than the variable pass-mark EER, because tuning the pass-mark for each subject produces better results.

Table (4-10): EER Analysis of the MEU-Mobile Dataset 41 Features (Hold, DD, UD, 1 Avg) Using the Med-Min-Diff Model with a Global Pass-Mark

		Genuine-Test		Impostor-Test				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	29	17	0	245	30	0.109	0.000	0.0545
2	29	17	0	252	23	0.084	0.000	0.0418
3	29	17	0	174	101	0.367	0.000	0.1836
4	29	15	2	245	30	0.109	0.118	0.1134
5	29	14	3	265	10	0.036	0.176	0.1064
6	29	15	2	223	52	0.189	0.118	0.1534
7	29	15	2	244	31	0.113	0.118	0.1152
8	29	14	3	238	37	0.135	0.176	0.1555
9	29	17	0	217	58	0.211	0.000	0.1055
10	29	15	2	246	29	0.105	0.118	0.1116
11	29	16	1	261	14	0.051	0.059	0.0549
12	29	17	0	176	99	0.360	0.000	0.1800
13	29	16	1	254	21	0.076	0.059	0.0676
14	29	17	0	242	33	0.120	0.000	0.0600
15	29	17	0	251	24	0.087	0.000	0.0436
16	29	16	1	261	14	0.051	0.059	0.0549
17	29	16	1	239	36	0.131	0.059	0.0949
18	29	16	1	247	28	0.102	0.059	0.0803
19	29	17	0	264	11	0.040	0.000	0.0200

20	**29**	**10**	**7**	**248**	**27**	**0.098**	**0.412**	**0.2550**
21	**29**	**17**	**0**	**268**	**7**	**0.025**	**0.000**	**0.0127**
22	**29**	**17**	**0**	**213**	**62**	**0.225**	**0.000**	**0.1127**
23	**29**	**16**	**1**	**202**	**73**	**0.265**	**0.059**	**0.1621**
24	**29**	**17**	**0**	**263**	**12**	**0.044**	**0.000**	**0.0218**
25	**29**	**14**	**3**	**275**	**0**	**0.000**	**0.176**	**0.0882**
26	**29**	**17**	**0**	**169**	**106**	**0.385**	**0.000**	**0.1927**
27	**29**	**17**	**0**	**265**	**10**	**0.036**	**0.000**	**0.0182**
28	**29**	**17**	**0**	**227**	**48**	**0.175**	**0.000**	**0.0873**
29	**29**	**16**	**1**	**258**	**17**	**0.062**	**0.059**	**0.0603**
30	**29**	**15**	**2**	**267**	**8**	**0.029**	**0.118**	**0.0734**
31	**29**	**11**	**6**	**263**	**12**	**0.044**	**0.353**	**0.1983**
32	**29**	**16**	**1**	**248**	**27**	**0.098**	**0.059**	**0.0785**
33	**29**	**16**	**1**	**180**	**95**	**0.345**	**0.059**	**0.2021**
34	**29**	**17**	**0**	**258**	**17**	**0.062**	**0.000**	**0.0309**
35	**29**	**17**	**0**	**275**	**0**	**0.000**	**0.000**	**0.0000**
36	**29**	**17**	**0**	**214**	**61**	**0.222**	**0.000**	**0.1109**
37	**29**	**17**	**0**	**196**	**79**	**0.287**	**0.000**	**0.1436**
38	**29**	**17**	**0**	**261**	**14**	**0.051**	**0.000**	**0.0255**
39	**29**	**17**	**0**	**269**	**6**	**0.022**	**0.000**	**0.0109**
40	**29**	**17**	**0**	**257**	**18**	**0.065**	**0.000**	**0.0327**
41	**29**	**16**	**1**	**265**	**10**	**0.036**	**0.059**	**0.0476**
42	**29**	**17**	**0**	**259**	**16**	**0.058**	**0.000**	**0.0291**
43	**29**	**17**	**0**	**270**	**5**	**0.018**	**0.000**	**0.0091**

44	**29**	**16**	**1**	**243**	**32**	**0.116**	**0.059**	**0.0876**
45	**29**	**17**	**0**	**236**	**39**	**0.142**	**0.000**	**0.0709**
46	**29**	**17**	**0**	**173**	**102**	**0.371**	**0.000**	**0.1855**
47	**29**	**17**	**0**	**222**	**53**	**0.193**	**0.000**	**0.0964**
48	**29**	**17**	**0**	**247**	**28**	**0.102**	**0.000**	**0.0509**
49	**29**	**16**	**1**	**198**	**77**	**0.280**	**0.059**	**0.1694**
50	**29**	**17**	**0**	**222**	**53**	**0.193**	**0.000**	**0.0964**
51	**29**	**16**	**1**	**202**	**73**	**0.265**	**0.059**	**0.1621**
52	**29**	**16**	**1**	**208**	**67**	**0.244**	**0.059**	**0.1512**
53	**29**	**16**	**1**	**258**	**17**	**0.062**	**0.059**	**0.0603**
54	**29**	**17**	**0**	**248**	**27**	**0.098**	**0.000**	**0.0491**
55	**29**	**17**	**0**	**240**	**35**	**0.127**	**0.000**	**0.0636**
56	**29**	**17**	**0**	**225**	**50**	**0.182**	**0.000**	**0.0909**
Average	**29.00**	**16.16**	**0.84**	**238.14**	**36.86**	**0.13**	**0.05**	**0.0917**

Table (4-11): Global EER Analysis of the MEU-Mobile Dataset 71 Features (Hold, DD, UD, Pressure, Area, 3 Avgs) Using the Med-Min-Diff Model with a Global Pass-Mark

		Genuine-Test		Impostor-Test				
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**	**EER**
1	52	17	0	246	29	0.105	0.000	0.0527
2	52	17	0	242	33	0.120	0.000	0.0600
3	52	17	0	240	35	0.127	0.000	0.0636
4	52	17	0	255	20	0.073	0.000	0.0364
5	52	14	3	265	10	0.036	0.176	0.1064
6	52	17	0	247	28	0.102	0.000	0.0509
7	52	15	2	261	14	0.051	0.118	0.0843
8	52	16	1	266	9	0.033	0.059	0.0458
9	52	17	0	245	30	0.109	0.000	0.0545
10	52	15	2	256	19	0.069	0.118	0.0934
11	52	15	2	257	18	0.065	0.118	0.0916
12	52	17	0	244	31	0.113	0.000	0.0564
13	52	16	1	262	13	0.047	0.059	0.0530
14	52	17	0	221	54	0.196	0.000	0.0982
15	52	17	0	251	24	0.087	0.000	0.0436
16	52	16	1	252	23	0.084	0.059	0.0712
17	52	17	0	262	13	0.047	0.000	0.0236
18	52	17	0	260	15	0.055	0.000	0.0273
19	52	17	0	267	8	0.029	0.000	0.0145
20	52	13	4	270	5	0.018	0.235	0.1267
21	52	17	0	262	13	0.047	0.000	0.0236

22	**52**	**16**	**1**	**235**	**40**	**0.145**	**0.059**	**0.1021**
23	**52**	**16**	**1**	**216**	**59**	**0.215**	**0.059**	**0.1367**
24	**52**	**16**	**1**	**267**	**8**	**0.029**	**0.059**	**0.0440**
25	**52**	**17**	**0**	**274**	**1**	**0.004**	**0.000**	**0.0018**
26	**52**	**17**	**0**	**208**	**67**	**0.244**	**0.000**	**0.1218**
27	**52**	**17**	**0**	**269**	**6**	**0.022**	**0.000**	**0.0109**
28	**52**	**17**	**0**	**218**	**57**	**0.207**	**0.000**	**0.1036**
29	**52**	**17**	**0**	**273**	**2**	**0.007**	**0.000**	**0.0036**
30	**52**	**16**	**1**	**275**	**0**	**0.000**	**0.059**	**0.0294**
31	**52**	**15**	**2**	**270**	**5**	**0.018**	**0.118**	**0.0679**
32	**52**	**17**	**0**	**254**	**21**	**0.076**	**0.000**	**0.0382**
33	**52**	**16**	**1**	**251**	**24**	**0.087**	**0.059**	**0.0730**
34	**52**	**17**	**0**	**266**	**9**	**0.033**	**0.000**	**0.0164**
35	**52**	**17**	**0**	**274**	**1**	**0.004**	**0.000**	**0.0018**
36	**52**	**17**	**0**	**224**	**51**	**0.185**	**0.000**	**0.0927**
37	**52**	**17**	**0**	**230**	**45**	**0.164**	**0.000**	**0.0818**
38	**52**	**17**	**0**	**266**	**9**	**0.033**	**0.000**	**0.0164**
39	**52**	**17**	**0**	**267**	**8**	**0.029**	**0.000**	**0.0145**
40	**52**	**17**	**0**	**268**	**7**	**0.025**	**0.000**	**0.0127**
41	**52**	**17**	**0**	**270**	**5**	**0.018**	**0.000**	**0.0091**
42	**52**	**17**	**0**	**256**	**19**	**0.069**	**0.000**	**0.0345**
43	**52**	**17**	**0**	**273**	**2**	**0.007**	**0.000**	**0.0036**
44	**52**	**16**	**1**	**254**	**21**	**0.076**	**0.059**	**0.0676**
45	**52**	**17**	**0**	**251**	**24**	**0.087**	**0.000**	**0.0436**

46	**52**	**17**	**0**	**249**	**26**	**0.095**	**0.000**	**0.0473**
47	**52**	**17**	**0**	**261**	**14**	**0.051**	**0.000**	**0.0255**
48	**52**	**17**	**0**	**264**	**11**	**0.040**	**0.000**	**0.0200**
49	**52**	**17**	**0**	**212**	**63**	**0.229**	**0.000**	**0.1145**
50	**52**	**17**	**0**	**263**	**12**	**0.044**	**0.000**	**0.0218**
51	**52**	**16**	**1**	**242**	**33**	**0.120**	**0.059**	**0.0894**
52	**52**	**16**	**1**	**232**	**43**	**0.156**	**0.059**	**0.1076**
53	**52**	**17**	**0**	**239**	**36**	**0.131**	**0.000**	**0.0655**
54	**52**	**17**	**0**	**250**	**25**	**0.091**	**0.000**	**0.0455**
55	**52**	**17**	**0**	**249**	**26**	**0.095**	**0.000**	**0.0473**
56	**52**	**17**	**0**	**232**	**43**	**0.156**	**0.000**	**0.0782**
Average	**52.00**	**16.54**	**0.46**	**252.38**	**22.63**	**0.08**	**0.03**	**0.0548**

4.6.3 FAR Analysis at 5% FRR

The MEU-Mobile dataset, 71 features, is analyzed to obtain the average FAR at the 5% FRR rate, as shown in Table 4.12. This analysis is done through tuning the variable pass-mark to obtain an FAR value at FRR of around 5%. The results indicate that the false acceptance rate of impostors is close to the false rejection of genuine users at 5%. However, false acceptance of impostors is more serious than false rejection of genuine users; therefore further refinement of the keystroke dynamics model is needed to reach lowers level of FAR.

Table (4-12): 5% FRR Analysis of the MEU-Mobile Dataset 71 Features (Hold, DD, UD, Pressure, Area, 3 Avgs) Using the Med-Min-Diff Model

		Genuine-Test		Impostor-Test			
Subject	**PMK**	**TA**	**FR**	**TR**	**FA**	**FAR**	**FRR**
1	55	17	0	268	7	2.55%	0.00%
2	55	16	1	259	16	5.82%	5.88%
3	55	16	1	254	21	7.64%	5.88%
4	53	16	1	258	17	6.18%	5.88%
5	51	16	1	262	13	4.73%	5.88%
6	54	16	1	253	22	8.00%	5.88%
7	50	16	1	249	26	9.45%	5.88%
8	53	16	1	267	8	2.91%	5.88%
9	52	17	0	245	30	10.91%	0.00%
10	50	16	1	245	30	10.91%	5.88%
11	49	16	1	224	51	18.55%	5.88%
12	56	16	1	266	9	3.27%	5.88%
13	51	16	1	256	19	6.91%	5.88%
14	56	16	1	252	23	8.36%	5.88%
15	52	17	0	251	24	8.73%	0.00%
16	54	16	1	265	10	3.64%	5.88%
17	54	16	1	267	8	2.91%	5.88%
18	55	17	0	271	4	1.45%	0.00%
19	56	16	1	275	0	0.00%	5.88%
20	46	16	1	216	59	21.45%	5.88%
21	55	16	1	268	7	2.55%	5.88%

22	**54**	**16**	**1**	**251**	**24**	**8.73%**	**5.88%**
23	**52**	**16**	**1**	**216**	**59**	**21.45%**	**5.88%**
24	**52**	**16**	**1**	**267**	**8**	**2.91%**	**5.88%**
25	**55**	**17**	**0**	**275**	**0**	**0.00%**	**0.00%**
26	**54**	**16**	**1**	**232**	**43**	**15.64%**	**5.88%**
27	**55**	**16**	**1**	**271**	**4**	**1.45%**	**5.88%**
28	**58**	**16**	**1**	**262**	**13**	**4.73%**	**5.88%**
29	**53**	**16**	**1**	**275**	**0**	**0.00%**	**5.88%**
30	**48**	**16**	**1**	**271**	**4**	**1.45%**	**5.88%**
31	**51**	**16**	**1**	**269**	**6**	**2.18%**	**5.88%**
32	**54**	**16**	**1**	**262**	**13**	**4.73%**	**5.88%**
33	**52**	**16**	**1**	**251**	**24**	**8.73%**	**5.88%**
34	**55**	**16**	**1**	**271**	**4**	**1.45%**	**5.88%**
35	**57**	**16**	**1**	**275**	**0**	**0.00%**	**5.88%**
36	**56**	**16**	**1**	**260**	**15**	**5.45%**	**5.88%**
37	**61**	**16**	**1**	**265**	**10**	**3.64%**	**5.88%**
38	**55**	**16**	**1**	**270**	**5**	**1.82%**	**5.88%**
39	**53**	**16**	**1**	**271**	**4**	**1.45%**	**5.88%**
40	**57**	**16**	**1**	**272**	**3**	**1.09%**	**5.88%**
41	**54**	**16**	**1**	**273**	**2**	**0.73%**	**5.88%**
42	**53**	**16**	**1**	**264**	**11**	**4.00%**	**5.88%**
43	**50**	**17**	**0**	**266**	**9**	**3.27%**	**0.00%**
44	**52**	**16**	**1**	**254**	**21**	**7.64%**	**5.88%**
45	**60**	**16**	**1**	**272**	**3**	**1.09%**	**5.88%**

46	**53**	**16**	**1**	**254**	**21**	**7.64%**	**5.88%**
47	**56**	**17**	**0**	**272**	**3**	**1.09%**	**0.00%**
48	**58**	**16**	**1**	**274**	**1**	**0.36%**	**5.88%**
49	**54**	**16**	**1**	**236**	**39**	**14.18%**	**5.88%**
50	**56**	**17**	**0**	**272**	**3**	**1.09%**	**0.00%**
51	**55**	**16**	**1**	**260**	**15**	**5.45%**	**5.88%**
52	**52**	**16**	**1**	**232**	**43**	**15.64%**	**5.88%**
53	**56**	**16**	**1**	**262**	**13**	**4.73%**	**5.88%**
54	**53**	**16**	**1**	**256**	**19**	**6.91%**	**5.88%**
55	**53**	**16**	**1**	**255**	**20**	**7.27%**	**5.88%**
56	**55**	**16**	**1**	**250**	**25**	**9.09%**	**5.88%**
Average	**53.82**	**16.14**	**0.86**	**259.09**	**15.91**	**5.79%**	**5.04%**

4.7 EER Analysis of the MEU-Mobile Dataset Using the Proposed Model with an Extra Feature

We have considered adding an extra feature to the proposed model, to investigate enhancing the authentication. The extra feature is a 2-graph feature which represents the total time of two consecutive keys, which we call Down-Up (DU), the elapsed time between key-down of the first key and key-up of the second key. Table 4.13 shows the EER analysis of the MEU-Mobile dataset using the extra feature. The EER in this case is slightly higher than the result without it (5.13 with the extra feature vs. 4.94 without). The extra feature did not reduce the EER value, which suggests that just adding features might not improve detection, unless the features have a unique property to measure, as in the case of area and pressure which resulted in lower EER.

Table (4-13): EER Analysis of the MEU-Mobile Dataset 84 Features (Hold, DD, UD, Pressure, Area, DU, 3 Avgs) Using the Med-Min-Diff Model

Subject	PMK	Genuine-Test		Impostor-Test		FAR	FRR	EER
		TA	FR	TR	FA			
1	64	17	0	271	4	0.015	0.000	**0.73%**
2	64	16	1	263	12	0.044	0.059	**5.12%**
3	65	16	1	255	20	0.073	0.059	**6.58%**
4	62	16	1	262	13	0.047	0.059	**5.30%**
5	58	16	1	258	17	0.062	0.059	**6.03%**
6	62	16	1	254	21	0.076	0.059	**6.76%**
7	58	16	1	256	19	0.069	0.059	**6.40%**
8	59	16	1	258	17	0.062	0.059	**6.03%**
9	61	15	2	249	26	0.095	0.118	**10.61%**
10	60	16	1	259	16	0.058	0.059	**5.85%**
11	58	15	2	247	28	0.102	0.118	**10.97%**
12	56	17	0	205	70	0.255	0.000	**12.73%**
13	58	16	1	258	17	0.062	0.059	**6.03%**
14	65	16	1	259	16	0.058	0.059	**5.85%**
15	62	17	0	266	9	0.033	0.000	**1.64%**
16	62	16	1	257	18	0.065	0.059	**6.21%**
17	60	16	1	260	15	0.055	0.059	**5.67%**
18	65	17	0	272	3	0.011	0.000	**0.55%**
19	61	17	0	269	6	0.022	0.000	**1.09%**
20	55	15	2	241	34	0.124	0.118	**12.06%**
21	63	17	0	269	6	0.022	0.000	**1.09%**
22	64	16	1	259	16	0.058	0.059	**5.85%**

23	64	14	3	226	49	0.178	0.176	**17.73%**
24	58	16	1	264	11	0.040	0.059	**4.94%**
25	60	17	0	275	0	0.000	0.000	**0.00%**
26	66	15	2	249	26	0.095	0.118	**10.61%**
27	61	17	0	269	6	0.022	0.000	**1.09%**
28	67	16	1	261	14	0.051	0.059	**5.49%**
29	60	17	0	275	0	0.000	0.000	**0.00%**
30	50	16	1	262	13	0.047	0.059	**5.30%**
31	55	16	1	259	16	0.058	0.059	**5.85%**
32	62	16	1	263	12	0.044	0.059	**5.12%**
33	61	15	2	251	24	0.087	0.118	**10.25%**
34	65	17	0	272	3	0.011	0.000	**0.55%**
35	59	17	0	275	0	0.000	0.000	**0.00%**
36	64	16	1	256	19	0.069	0.059	**6.40%**
37	71	16	1	264	11	0.040	0.059	**4.94%**
38	62	17	0	268	7	0.025	0.000	**1.27%**
39	61	17	0	270	5	0.018	0.000	**0.91%**
40	64	17	0	271	4	0.015	0.000	**0.73%**
41	59	17	0	268	7	0.025	0.000	**1.27%**
42	61	16	1	261	14	0.051	0.059	**5.49%**
43	61	17	0	275	0	0.000	0.000	**0.00%**
44	60	16	1	256	19	0.069	0.059	**6.40%**
45	70	17	0	272	3	0.011	0.000	**0.55%**
46	62	16	1	249	26	0.095	0.059	**7.67%**
47	65	17	0	269	6	0.022	0.000	**1.09%**
48	69	17	0	273	2	0.007	0.000	**0.36%**

49	63	15	2	237	38	0.138	0.118	**12.79%**
50	65	17	0	270	5	0.018	0.000	**0.91%**
51	63	16	1	259	16	0.058	0.059	**5.85%**
52	63	15	2	245	30	0.109	0.118	**11.34%**
53	64	16	1	260	15	0.055	0.059	**5.67%**
54	63	17	0	265	10	0.036	0.000	**1.82%**
55	63	16	1	260	15	0.055	0.059	**5.67%**
56	64	15	2	251	24	0.087	0.118	**10.25%**
Average	**61.91**	**16.20**	**0.80**	**259.77**	**15.23**	**0.06**	**0.05**	**5.13%**

Chapter Five

Conclusion and Future Work

5.1Conclusion

This thesis has investigated user authentication on mobile devices using the Keystroke Dynamics approach. An anomaly detector (Med-Min-Diff) is developed to classify user typing behavior as either genuine or impostor, based on pre-collected training data. The model was implemented on an Android mobile device, and it was used in the collection of a dataset of the typing rhythm data of 56 subjects (MEU-Mobile dataset). Features of the dataset included pressure and finger area as well as the timing features. An empirical analysis was conducted to evaluate the error-metrics (EER, FRR, FAR).

Conclusions of this work are summarized as follows:

1. The proposed model has resulted in lower EER value (0.0679 for the 71 features data), using the SU dataset, compared with results of the three verification models.

2. The proposed model has resulted in lower EER value (0.0494 for the 71 features data), using the MEU-Mobile dataset, compared with results of the three verification models. The difference between results of using the same model on the two datasets can be attributed to the effect of doing a rehearsal, in the MEU experiment, of 10 typing attempts before the actual training.

3. Error metrics evaluation of the MEU-Mobile dataset using the proposed model, with a global (fixed) pass-mark has resulted in a value that is very close to the variable pass-mark case (5.48 vs. 4.94), using the 71 features data. This suggests that the proposed model can be used with a pre-determined pass-mark for all subjects.

4. The False Acceptance Rate (FAR) at 5% False Rejection Rate (FRR) is 5.79%, which is very close to the FRR result. The 5% FRR can be accepted as a rejection rate of genuine users, but the FAR value needs to be further reduced.

5.2Future Work

Based on the results of this research and the knowledge and experience gained during the research process, the following suggestions for future work are presented:

1. Investigating the inclusion of additional features from sensors of recent mobile devices, to enhance authentication using the proposed model.

2. Investigating the reduction of the number of repetitions during the training phase, to avoid user boredom, by adding features that could compensate the reduced number of repetitions.

3. Extending the proposed model to continuous authentication on mobile devices.

4. Collecting a larger dataset, from subjects of various backgrounds, and investigating the effect of subjects' groups on the authentication results.

5. Collecting an alternative dataset with simpler passwords and analyzing the effect on error metrics.

6. Experimenting with the implemented system to measure authentication outcome where each subject has his own password.

References

References

Alariki, A. A., & Manaf, A. A. (2014). Biometrics Authentication Using Touch-Based Gesture Features for Intelligent Mobile Devices. International Conference of Recent Trends in Information and Communication Technologies. IRICT. (pp. 528-538).

Al-Jarrah, M. M. (2012). Anomaly detector for keystroke dynamics based on medians vector proximity. Journal of Emerging Trends in Computing and Information Sciences, Vol. (3), No.(6), (pp.988-993).

Al-Obaidi, N. M. & Al-Jarrah, M. (2016). Statistical Median-Based Classifier Model for Keystroke Dynamics on Mobile Devices, Sixth International Conference on Digital Information Processing and Communications, Lebanese University, ISBN: 978-1-4673-7504-7, IEEE.

AL-Rahmani, A. O. (2014). An Enhanced Classifier for Authentication in Keystroke Dynamics Using Experimental Data. Master dissertation, Middle East University.

Al-Robayei, A.A. (2016). A Multi Model Keystroke Dynamics Anomaly Detector For User Authentication. Amman-Jordan: MEU (master thesis).

Antal, M., & Szabó, L. Z. (2015). An evaluation of one-class and two-class classification algorithms for keystroke dynamics authentication on mobile devices.

Antal, M., Szabó, L. Z., & László, I. (2015). Keystroke dynamics on android platform. Procedia Technology, Vol.(19), (pp.820-826).

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, Vol.(85), No.(5), (pp.1157-1165).

Dedhia, R. K. (2011). Keystroke Dynamics For Mobile Devices–Data Collection (Doctoral dissertation, San Diego State University).

Flior, E., & Kowalski, K. (2011). Continuous biometric user authentication in online examinations. In *2010 Seventh International Conference on Information Technology* (pp. 488-492). IEEE.

Giot, R., Ninassi, A., El-Abed, M., & Rosenberger, C. (2012). Analysis of the acquisition process for keystroke dynamics. In Biometrics Special Interest Group (BIOSIG), IEEE, BIOSIG-Proceedings of the International Conference of the (pp.1-6).

Giuffrida, C., Majdanik, K., Conti, M., &Bos, H. (2014). I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 92-111). Springer International Publishing.

Ho, G. (2014). Tapdynamics: strengthening user authentication on mobile phones with keystroke dynamics. Technical report, Stanford University.

Kambourakis, G., Damopoulos, D., Papamartzivanos, D., &Pavlidakis, E. (2014). Introducing touchstroke: keystroke-based authentication system for smartphones. Security and Communication Networks.

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, (pp.2231-2307).

Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. Applied Soft Computing, Vol.(11), No.(2), (pp.1565-1573).

Killourhy, K. S. (2012). A scientific understanding of keystroke dynamics (No.CMU-CS-12-100).Carnegie Mellon University, Department of Computer Science.

Killourhy, K. S., Maxion, R. A. (2009). Comparing anomaly-detection algorithms for keystroke dynamics. In Dependable Systems and Networks. IEEE/IFIP International Conference. pp. 125-134.

Kolakowska, A. (2013). A review of emotion recognition methods based on keystroke dynamics and mouse movements. In Human System Interaction (HSI), the 6th International Conference on (pp. 548-555). IEEE.

Long, L. (2014). Biometrics: The Future of Mobile Phones.University of Southampton.

Messerman, A., Mustafic, T., Camtepe, S. A., &Albayrak, S. (2011). Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In Biometrics (IJCB), 2011 International Joint Conference on (pp. 1-8). IEEE.

Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. Future Generation computer systems, Vol.(16), No.(4), (pp. 351-359).

Ryan, S. (2015). Mobile keystroke dynamics: assessment and implementation (Doctoral dissertation, California State University, Northridge).

Shrivasatva, M. (2011). Keystroke Dynamics for Mobile Devices–Algorithm and Authentication (Doctoral dissertation, San Diego State University).

Teh, P. S., Teoh, A. B. J., &Yue, S. (2013). A survey of keystroke dynamics biometrics. The Scientific World Journal.

Teh, P. S., Yue, S., & Teoh, A. B. (2012). Feature fusion approach on keystroke dynamics efficiency enhancement. International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol.(1), No.(1), (pp. 20-31).