User Authentication Based on Statistical Mouse Dynamics Biometrics

التحقق من هوية المستفيد على أساس القياسات الحيوية الاحصائية لفأرة الحاسوب

Prepared By

Yousef Abdelrahman Abdelaziz Abudayeh

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

January-2020

Authorization

I, Yousef Abudayeh, authorize Middle East University to provide Libraries, Organizations, and Individuals with copies of my thesis on Request.

Name: Yousef Abudayeh

Signature: 

Date: 25/1/2020

Thesis Committee Decision

This Thesis "**User Authentication Based On Statistical Mouse Dynamics Biometrics**", was discussed and certified on 25/1/2020.

Thesis Committee Decision signature:

Dr.Mudhafar Al-Jarrah (Supervisor / Chairman) .....

Dr.Bassam Al-Shargabi Internal Examiner .....

Prof. Mokhled Al-Tarawneh External Examiner .....

User Authentication Based on Statistical Mouse Dynamics Biometrics

Prepared By: Yousef Abdelrahman abdelaziz Abudayeh

Supervisor: Dr. Mudhafar Al-Jarrah

Abstract

With the development of Information and Communication Technologies (ICT), our reliance on these technologies is increasing dramatically. Huge amount of users' data is generated, processed, and stored. This massive data needs to be protected and kept secured from unauthorized. In order to secure the data to sustain the system reliability, a system should meet three main security service: Confidentiality, Integrity, and Availability (CIA). To achieve confidentiality, authentication is used as the first security layer before accessing information systems.

Authentication is the study of how to recognize the genuine user from others to protect the data from any unauthorized access. Mainly, there are two types of authentication, the first one is traditional authentication which is divided into two types, knowledge-based authentication and object-based authentication (Further information will be explained later). The second type is biometric authentication which is the process in which a user is recognized automatically based on a feature vector extracted from either his physiological or behavioral characteristics.

In this thesis the research will be done on Mouse Dynamics Biometric (MDB) which is one of the methods from the behavioral biometric authentication that studies the behaviors of a person when interacting with a Graphical User Interface (GUI) interface using a mouse as an input device. The approach is evaluated on a dataset from

30 users. Extensive experimental results are included to demonstrate the efficacy of the proposed model, which achieves a false-acceptance rate of 3.4%, and a false-rejection rate of 3% and Equal Error Rate (EER) of 3.22% which the average of the False Acceptance Rate and the False Rejection Rate. Experiments are provided to compare the current approach with other approaches in the literature.

Keywords: Mouse Dynamics, Behavioral Biometrics, User Authentication, Anomaly Detection, Equal Error Rate (EER), Calculated Features, Measured Features.

التحقق من هوية المستفيد على أساس القياسات الحيوية الاحصائية لفأرة الحاسوب

إعداد: يوسف عبد الرحمن عبد العزيز أبودية

المشرف: الدكتور مظفر الجراح

الملخص

مع تطور تكنولوجيا المعلومات والاتصالات (ICT) ، يزداد اعتمادنا على هذه التقنيات بشكل كبير. يتم إنشاء كمية هائلة من بيانات المستخدمين ومعالجتها وتخزينها. يجب حماية هذه البيانات الضخمة والحفاظ عليها آمنة من الأشخاص الغير مخولين. للحفاظ على موثوقية بيانات النظام ، يجب أن يوفر النظام ثلاثة خدمات أمنية رئيسية: السرية والنزاهة والتوافر(CIA) . لتحقيق السرية ; يتم استخدام المصادقة كطبقة الأمان الأولى قبل الوصول إلى أنظمة المعلومات.

المصادقة هي دراسة كيفية التعرف على المستخدم الحقيقي من غيره لحماية البيانات من أي وصول غير مخول به. بشكل رئيسي ، هناك نوعان من المصادقة ، الأول هو المصادقة التقليدية التي تنقسم إلى نوعين ، المصادقة المستندة إلى المعرفة والتوثيق القائم على الكائن (سيتم شرح مزيد من المعلومات لاحقًا). النوع الثاني هو المصادقة البيومترية وهي العملية التي يتم فيها التعرف على المستخدم تلقائيًا استنادًا إلى خصائصه الفسيولوجية أو السلوكية.

في هذه الأطروحة ، سيتم إجراء البحث على Mouse Dynamics Biometric (MDB) والتي تعد واحدة من طرق المصادقة البيومترية السلوكية التي تدرس سلوكيات الشخص عند التفاعل مع واجهة المستخدم الرسومية (GUI) باستخدام الماوس كمدخل للجهاز. يتم تقييم النهج على مجموعة بيانات من 30 مستخدمًا. يتم تضمين نتائج تجريبية شاملة لإثبات فعالية النموذج المقترح ، والذي يحقق معدل قبول خاطئ قدره 3.4 ٪ ، ومعدل رفض كاذب قدره 3 ٪ ومعدل الخطأ المتساوي (EER) بنسبة 3.22 ٪ وهو متوسط القبول الخاطئ و الرفض الكاذب. يتم توفير التجارب لمقارنة النهج الحالي مع مناهج أخرى.

الكلمات المفتاحية: ديناميكيات الفأرة ، القياسات الحيوية السلوكية ، مصادقة المستخدم ، كشف الشذوذ ، معدل الخطأ المتساوي (EER) ، الخصائص المحسوبة ، الخصائص المقاسة.

Acknowledgment

All praises are attributed to Almighty Allah whose blessings enabled me to complete this thesis successfully. I would like to express my sincere gratitude to my family and my wonderful mother for her unlimited love and support, she taught me the value of knowledge and have stood beside me at all times, providing endless support, encouragement and love. It is my pleasure to acknowledge the guidance and support to my supervisor Dr. Mudhafar Al-Jarrah.

Dedication

This thesis is dedicated to my family who has always been a constant source of support, encouragement during the challenges of our whole college life, and have been taught us to work hard for the things that we aspire to achieve.

Table of Contents

List of Figures

List of Tables

List of Equations

List of Abbreviations

MDB	Mouse Dynamics Biometric
GUI	Graphical User Interface
MM	Mouse Moving
DD	Drag and Drop
PC	Point and Click
FAR	False Acceptance Rate
FRR	False Rejection Rate
EER	Equal Error Rate
OS	Operating System
PCA	Principle Component Analysis
SVM	Support Vector Machine
CNN	Convolutional Neural Network
AUC	Area Under the Curve
WLSR	Weighted Least Square Regression
LVQ	Learning Vector Quantization
ADAM	Average Deviation Authentication Model
AM	Arithmetic Mean
TEP	Trial and Error Process
SDAM	Standard Deviation Authentication Model
STD	Standard Deviation
AAD	Absolut Average Deviation
UI	User Interface

UM	User Mode
GM	Global Mode
PM	Pass Mark
TA	True Acceptance
FR	False Rejection
TR	True Rejection
FA	False Acceptance
DF	Distance Factor
TE	Trial and Error Process
CSV	Comma Separated Values

Chapter One

Introduction

1.1 Overview Mouse Dynamics Biometric

In the last decades, a wide technological expansion has lead us to covert our transactions and our personal data to be done in a technological way by using computers, laptops, or even with smartphones. This type of conversion endangers the data from being stolen, as a result research effort has focused on ways to protect the data from unauthorized access.

Authentication is a method that is used to determine whether a user is genuine ("allowed to access the system") or an impostor ("prohibited from access to the system") (Almalki et al., 2019). This Thesis will tackle the data protection issue using the Mouse Dynamics Biometric (MDB) which is one of the behavioral authentication methods that deals with the identity signature of a user by using a computer's mouse or a laptop's touchpad.

Biometrics are automated methods of authentication based on measurable human physiological or behavioral characteristics (Matyas & Riha 2003). Biometrics based on the physiological characteristics take the measurements from the human body such as hand scanning, iris scanning, fingerprint scanning. Where the biometrics that based on the behavioral characteristics take the measurements from the human actions such as the typing patterns of a human, speaking, handwriting (Trewin et al., 2012) and the mouse movements of a human (Awad & Traore 2007).

Mouse dynamics can be described as the behavioral characteristics of the actions received from the mouse input device for a specific user while interacting with a specific Graphical User Interface (GUI). The first step in understanding the actions received from the input device is to identify the categories where those actions fall. (Awad & Traore 2007)

A mouse action can be classified into one of the following categories: (Awad & Traore 2007)

1. Mouse Moving (MM) action: general mouse movement.
2. Drag and Drop (DD) mouse action: the action starts with the mouse button down, movement, and then mouse button up.
3. Point and Click (PC) mouse action: mouse movement followed by a click or a double click.
4. Silence: there are no actions that come from the mouse input device.

1.2 Mouse Dynamics Biometric Analysis

The usage of mouse dynamics has several benefits over any other traditional authentication methods. Firstly, biometrics cannot be forgotten, or stolen (Gamboa & Fred 2003). Secondly, mouse dynamics biometric uses not only the static authentication (which is an authentication process that can be performed during the login phase), more over it uses the continuous authentication as well (which is an authentication process that detects the changes of the user during the established session) (Hinbarji, et al., 2015). Although mouse dynamics authentication has several advantages, it has several challenges too, such as reaching high authentication accuracy, reducing the

authentication delay (Feher et al., 2012), and controlling confounding effects while using different kinds of mouse types.

Finally, with regarding the challenges that will appear in this work MDB technique will still be very useful and comfortable technique than the others to get a relatively high accuracy.

1.3 Problem Statement

People dependence on laptop and computer devices has significantly increased, these devices store sensitive and personal information that needs to be secure. User authentication is one of the main processes to protect such data. Many users use passwords, but a password can be stolen, so another verification step is needed that involves authentication data that cannot be replicated. The problem addressed in this work is enhancing user authentication through behavioral biometrics such as mouse dynamics.

1.4 Scope of Work

In this research work, we study signature authentication that is based on mouse movements. This will be achieved through identifying measured features of mouse movement, building a data collection system and collecting a dataset of mouse movements from a group of users, formulating authentication features and anomaly detectors and analyzing the collected data to identify the features and anomaly detectors that lead to lower authentication errors.

1.5 Goal and Objectives

The goal of this work is to investigate and develop a user authentication model based on mouse dynamics.

The following objectives will be taken into consideration:

1- Identify mouse dynamics measured features
2- Generate mouse dynamics dataset for a group of users
3- Select and formulate calculated authentication features that are extracted from the measured features
4- Select the most suitable anomaly detection models
5- Tune the authentication feature set to obtain the lowest EER
6- Evaluate the detection performance of the selected anomaly detectors based on the EER metric which is the average of the False Acceptance Rate along with the False Rejection Rate.

1.6 Motivation

The large amount of data and the availability of cloud computing need to provide highly secure and sensitive authentication methods which for instance based on this work.

1.7 Significance of Work

This work will provide user authentication models based on mouse dynamics biometrics to achieve high accuracy by reducing EER.

1.8 Questions to be answered

This thesis aims to provide a clear answer for the below questions:

1. How to generate the dataset for a user's signature?
2. What are the calculated authentication features?
3. How to extract the calculated authentication features from the generated dataset?
4. What is the most suitable model will be used to provide a highly accurate system?
5. How to evaluate the False Acceptance Rate (FAR), the False Rejection Rate (FRR), as well as the Equal Error Rate (EER) based on the evaluated results?

1.9 Thesis Organization

This thesis will discuss the MDB authentication subject as below:

1. Chapter one will give a general discussion about MDB authentication and the steps needed to get applied regarding the challenges for each step.
2. Chapter two will explain the authentication definition along with its types and will give a full definition of MDB authentication as well and review some of related work.
3. In chapter three the discussion will be made on describing each step mentioned in chapter one to implement the system and it will describe some of models that can be applied along with the adopted system.
4. While in chapter four the real implementation of the system will be shown and the generated results from each adopted model will be summarized to choose the

optimal one between them. After that, a comparison will be made between the chosen model from this work and other related works to prove that this work is more reliable to get applied than the others.

5. Finally, chapter five will summarize all chapters within the documentation with mentioning the future work we aspire to achieve.

Chapter Two

Background and Theoretical Review

2.1 Background

The quest for a reliable and convenient security mechanism to authenticate a computer user has existed since the inadequacy of conventional password mechanism was realized, first by the security community, and then gradually by the public. As data are moved from traditional localized computing environments to the new Cloud Computing environments, the need for better authentication has become more pressing. Recently, several large scale password leakages exposed users to an unprecedented risk of disclosure and abuse of their information. These incidents seriously shook public confidence in the security of the current information infrastructure; the inadequacy of password-based authentication mechanisms is becoming a major concern for the entire information society.

One of various potential solutions to this problem, a particularly promising technique is mouse dynamics. Mouse dynamics measures and assesses a user's mouse behavior characteristics for use as a biometric. Compared with other biometrics such as face scanning biometric, fingerprint scanning biometric, iris scanning biometric, and voice recognition (Jain et al., 2006), mouse dynamics biometric is less intrusive and requires no specialized hardware to capture biometric information. Hence it is suitable for the current Internet environment. When a user tries to log into a computer system, mouse dynamics only requires them to provide the login name and to perform a certain sequence of mouse operations. Extracted behavioral features, based on mouse movements, clicks, and even the silence of the mouse (when the mouse does not move

in any direction), are compared to a legitimate user's profile. A match authenticates the user; otherwise her access is denied.

Furthermore, a user's mouse behavior characteristics can be continually analyzed during her subsequent usage of a computer system for identity monitoring or intrusion detection (Continuous authentication).

Mouse dynamics has attracted more and more research interest over the last decade. Although previous research has shown promising results, mouse dynamics is still a newly emerging technique, and has not reached an acceptable level of performance, as an example the European standard for commercial biometric technology requires 0.001% of False Acceptance Rate (FAR) and 1% of False Rejection Rate (FRR) and as an overall result it requires 0.5005% of Equal Error Rate (EER) (Nakkabi et al., 2010). Most existing approaches for mouse dynamics based user authentication result in a low authentication accuracy or an unreasonably long authentication time. Either of these may limit applicability in real world systems, because few users are willing to use an unreliable authentication mechanism, or to wait for several minutes to log into a system. Moreover, previous studies have favored using data from real world environments over experimentally controlled environments, but this realism may cause unintended side effects by introducing confounding factors such as effects due to different mouse devices, that may affect experimental results. Such confounds can make it difficult to attribute experimental outcomes solely to user behavior, from hand to computing environment. (Jorgensen & Yu 2011) (Shen et al., 2009).

It should be also noted that most mouse dynamics research used data from both the impostors and the legitimate user to train the classification or detection model. However, in the scenario of mouse dynamics based user authentication, usually only the data from the legitimate user are readily available, since the user would choose her specific sequence of mouse operations and would not share it with others. In addition, no datasets are published in previous research, which makes it difficult for third party verification of previous work and precludes objective comparisons between different approaches.

Finally, it good to be mentioned that this thesis will adopt the approach of finding the user's generated pattern and distinguish it from any other pattern which came from any other user by considering mouse movements only, and as a future work this approach will be extended to include the user's clicks, the user's drag and drop operations, and even the mouse silence will be taken into consideration too.

2.2 Authentication Definition

Authentication is the process of positively verifying a user’s identity, device or other entity in a computer system, often as a prerequisite to allowing access to resources in the system (Velásquez et.al 2018). The credentials provided are compared to those on a file in a database of the authorized user's information on a local Operating System (OS) or within an authentication server.

The authentication process always runs at the start of the application before the permission checks occur, and before any other code is allowed to proceed. Different systems may require different types of credentials to ascertain a user's identity.

Authentication can be divided into two main types as follow:

- Traditional Authentication
- Biometric Authentication

The figure below introduces the authentication methods with an example of each method. (Amin, et al., 2014).

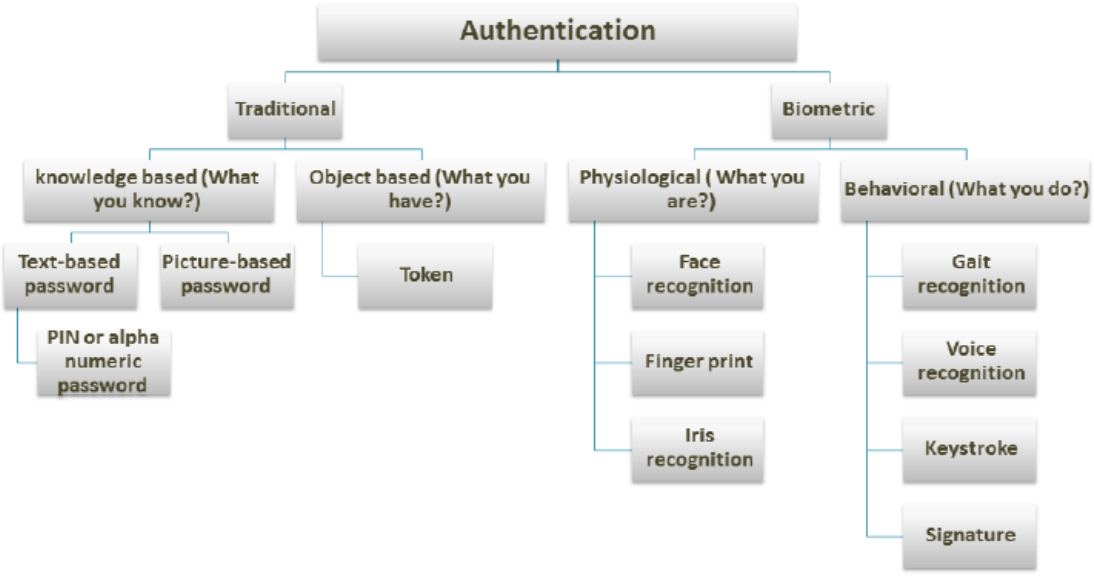

Figure (2-1): Authentication methods

The following subsections will give a brief explanation of each method along with its own techniques too.

2.2.1 Traditional Authentication

Basically, Traditional authentication methods can be divided to either knowledge based or object based authentication.

Knowledge based authentication techniques are the most common used authentication techniques. They are based on "What users know?" to identify him. They include two classes: text-based and picture-based passwords. For further information, review. (Amin, et.al 2014).

Object based authentication techniques were developed as a second factor for authentication besides password. These techniques include token-based authentication. The token are physical devices storing passwords (i.e. Remote garage door opener.). For further information, review. (Amin, et.al 2014).

2.2.2 Biometric Authentication

The traditional techniques do not actually represent users and have so many flaws within it while on the other hand, biometric authentication techniques depend on the users' unique features to identify the users.

The biometric authentication is the process in a which a user is recognized automatically based on a feature vector extracted from either his physiological or behavioral characteristics. Based on this, biometric approaches are typically divided into two categories: physiological and behavioral biometrics. (Koong et al., 2014)

Physiological biometrics depend on physical attributes of a person such as face, eye, fingerprint, or even the whole hand. Generally, it is based on the fact that these person's attributes do not change over time (Koong et al., 2014). Conversely, behavioral characteristics depend on an associated behavior of a person such that what user does

such as handwriting, speaking, and typing (Hoang et al., 2013) (Koong et al., 2014). This behavior is recorded of a period of time while the person doing his job from his temporal trait.

The main difference between the physiological and behavioral biometrics is that behavioral is more difficult to detect and emulate because it depends on an interaction of users with their own devices to extract specific and accurate habits (Amin et al., 2014). As mentioned before this work will adopt the research and development cycle of the MDB technique which belong to the behavioral biometric class. The following section will spot the light on the behavioral biometric class, then the section that comes after it will give a full explanation about the MDB technique.

2.3 Behavioral Biometrics

Behavioral biometrics authentication is the method that studies the user's behavior on a certain amount of time to extract a useful feature that can be used to distinguish the target user from other any user. A lot of studies were made to develop and improve this type of authentication that enforce our security systems and immune it from any unauthorized access (i.e. studies such as voice recognition, keystrokes discrimination, MDB).

The thesis will work on identifying the user from the generated pattern that comes from his mouse movements (signature biometrics). The figure below will show the steps that will be worked on. (Amin, et.al 2014)

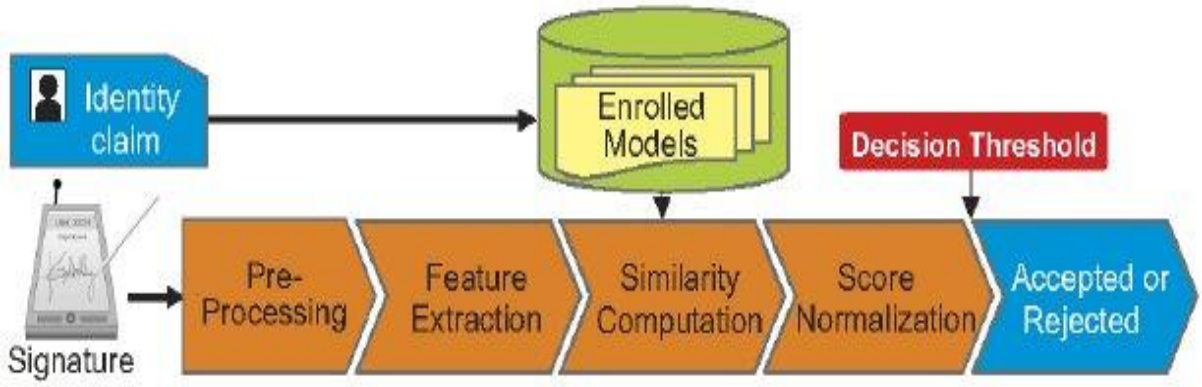

Figure (2-2): Signature biometrics steps

2.4 Mouse Dynamics Biometric Definition and Related Works

The Mouse Dynamics Biometric (MDB) is a behavioral biometric technology that extracts and analyzes the movement characteristics of the mouse input device when a computer user interacts with a Graphical User Interface (GUI) for identification purposes.

The MDB technique can be used during the login phase (Static authentication), or even while user is working during the established session (Continuous authentication). This variety of usages gave MDB technique the attention to study among other behavioral biometric techniques. The works mentioned below are related ones to our study:

M.Antal, E.Zsigmond (2019) have tackled the problem of the dataset challenges due to short test periods. They have proposed an approach to detect the dataset impostors based on performance analyses. In order to achieve that, they have classified the mouse sessions into three types, based on Ahmed and Traore (Awad & Traore 2007) method, which contain: General mouse movement, point click, and drag-and-drop actions. This data then was divided into two steps: segmentation and threshold. After that, they used Random Forest Algorithm to extract the features. In their experiment, they used Balabit dataset, which contains 65 sessions, each of which with 60905 actions, copied into 10 folds.

C.Shen et al. (2013) addressed the data security issues resulted from the transformation of the data from the local environment to the cloud based environment, degraded the security of character-based authentication techniques. They have suggested an authentication technique according to a fixed mouse operation function. In order to fulfill that, they used Holistic features and Procedural features for feature extraction. While for training and projection they used Eigensapce computation, with Kernel Principal Component Analysis (KPCA) training, and projection. For classification they used Support Vector Machine (SVM). The dataset that they have used contains several moue behavior samples collected from 37 users following strict mouse operation tasks to result in 5550 samples, to be used feature extraction. In their experiment they used an HP computer with a Core 2 Duo 3.0 GHz processor, 2 GB of RAM and 1280 1024 resolution and LCD monitor. To validate their approach, the experimental results were as follows: false-acceptance rate of 8.74%, and a false-rejection rate of 7.69% with a corresponding authentication time of 11.8 seconds.

A.Ahmed and I.Traore (2007) focused on the problem of high cost for hardware components that the current biometric based on. They have developed a technique used to model the behavioral characteristics from the captured data using artificial neural networks and they show an architecture and implementation for the detector, which cover all the phases of the biometric data flow including the detection process. The dataset was collected over a total of 998 sessions with an average of 45 sessions per user. The entire experiment lasted nine weeks. Overall, 284 hours of raw mouse data was collected, with an average input of 12 hours and 55 minutes per user.

After that, they used feed-forward multilayer perceptron network algorithm. In their experiment they used 49 collected session (3 to 10 sessions per user). The screen resolution used for this session was 1,024 768. The traveled distances are less than or equal to 1,200 pixels, and actions with smaller distances occur more often than those with longer distances. To prove their contribution, the experimental results were as follows: achieving a FAR of 2.4649 percent and a FRR of 2.4614 percent.

In T. Hu et al. (2019) studied the use of the intranet by meddlesome that doesn't have permission to access. They have suggested a method that depends on mouse bio behavioral characteristics and deep learning that discover the authorized and reduce an attack. In order to reach that, the dataset collected by record timestamp, button, state, x and y. After that they used Data Preprocessing and Overall Architecture of Convolutional Neural Network (CNN) algorithm. In their experiment they have implemented the model in its training and testing phases, in both security and communication networks, where it was based on Python3.5.2, Tensorfow r1.4, CUDA Version 8.0.61, cudnn-8.0-windows10- x64-v6.0, windows10, and NVIDIA GTX 1060 6GB GPU. To prove their contribution, the experimental results were as follows: The average of FAR :2.94% and the average of FRR: 2.28%.

In S. Hu et al. (2017) investigated the problem of biometric security as a fundamental problem in user authentication. They proposed a simulation method to detect weaknesses in this authentication technique. To achieve that, Mouse movement data of 24 users were used. For each user, the 5000 positive sample are separated to 3500 for training and 1500 for testing. They extracted 232 features for each move-to

and left-click sample. After that, they compared between different classification algorithms, such as CNN, Random forest, gradient boosting decision tree, multiplayer perception, support vector machine, and concluded that CNN provides the more enhanced results. In their experiment, the 5000 positive samples are separate to 3500 for training and 1500 for testing, to show the efficiency of their solution. The average recall was bigger than 50% models with an average success rate up to 78.3%.

In P.Chong et al.(2018) used a deep learning approach, exceptionally a two-dimensional convolutional neural network (2D-CNN). They learned the characteristics of users' mouse movements for authentication. They collected mouse dynamics movements and converted them to images of the mouse trajectories. In their experiment, they used Balabit and TWOS datasets that compared against 1D-CNN. The authors showed that even by removing the temporal aspect of mouse movements, they still could achieve state-of-the-art authentication results on different mouse datasets. The results were as follows: Balabit proposed 2D-CNN the average of Area under the Curve (AUC) was 0.96 and the average of Equal Error Rate (EER) was 0.10. TWOS proposed 2D-CNN the average of AUC was 0.93 and the average of EER was 0.13.

C. Anupashree, S.Kulkarni and P.Baraki (2016) the authors studied the problem of the slowness for static authentication compared with other systems that are developed rapidly. They proposed a new model where user draws a gesture using a mouse. In order to fulfill that, they used gesture creation module, data acquisition and preparation module, feature extraction module and classification module. These gestures are collected and evaluation through a cover Markov model classifier. They considered 17

different gestures drawn by users using a mouse. Mouse gesture was drawn by considering data points with coordinate values. During the registration phase, the user recorded mouse gestures over the computer screen multiple times. The movement is registered and evaluated through other systems which related with it. Finally, this collected data were performed in the registration phase. To show the efficiency of their solution, experimental tests were conducted, achieving an efficiency of 78%.

Hema. D and Bhanumathi. S (2016) focused on the problem of increasing the weaknesses for password based on authentication. They described user behavior-based security. In order to get that, they transformed the recorded behavior as inputs that systems can understand. These recordings were executed in a training system. During the training phase, every movement of mouse was recorded. This data was processed to calculate the features based on the distances between the points to build a user profile. After that, they used feature learning algorithm, optical character recognition and time-based one-time password algorithm. Their experiments considered feature representations with 100, 200, 400, 800, 1200, and 1600 learned features.

P.Pilankar & P.Padiya (2016) targeted the problem of password-based system because it is not secure and it has many disadvantages that are too hard to remember or too easy to guess. They have proposed an approach to provide additional mouse dynamics to the existing work, by doing two levels of classification, initially, the collected data, which was outlier removal, using Peirce's criterion and data smoothing Weighted Least Square Regression (WLSR). After that they used Learning Vector

Quantization (LVQ), which is used to correctly classify the genuine user from the impostor.

S.Almalki et al. (2019) performed an evaluation of different classification techniques on a mouse dynamics dataset, the Balabit Mouse Challenge dataset. They used three mouse actions to identify the user; mouse move, point and click, and drag and drop. They used three machine-learning classifiers in Verification and authentication methods; the Decision Tree classifier, the K-Nearest Neighbors classifier, and the Random Forest classifier. The results showed a perfect accuracy in authentication and verification mode. All the classifiers achieve a perfect accuracy of 100% in the verification mode. In authentication mode, all the classifiers achieved the highest accuracy (ACC) and Area Under Curve (AUC) from scenario B using the point and click action data: (Decision Tree - ACC: 87.6%, AUC: 90.3%), (K-Nearest Neighbors - ACC: 99.3%, AUC: 99.9%), and (Random Forest - ACC: 89.9%, AUC: 92.5%).

Zhang (2015) addressed the problem of the weakness of the traditional authentication method that it is easy for hackers to break and reach to the personal data. Passwords are one of this methods which are stolen and forgotten. He proposed to use mouse action from an authenticated user that only do the right action. If the user doesn’t do the right movement the system will reject him.

Hinbarji et al. (2015) proposed a user authentication method based on mouse movements alone. They used a back propagation neural network as the classifier with the curvature features. They have presented the accuracy of the system in terms of 3 different values of session length: 100 curve with EER 9.8%, 200 curve with ERR 7.2% and 300 curve with EER 5.3%. They used ten participants to test and validate their model.

Sayed et al. (2013) have proposed biometric authentication using mouse gesture for static authentication to create pattern by moving the mouse around. The method which attempts to find the time differences between two similar patterns is learning vector quantization (LVQ) neural network. They used an experimental evaluation with 39 users, in which they achieved a false acceptance ratio of 5.26% and a false rejection ratio of 4.59%.

Shen et al. (2014) presented a study of anomaly-detection algorithms in mouse dynamics. The evaluation was performed on a dataset containing 17,400 samples from 58 users and 17 detectors were applied. The equal-error rates for the six top-performing detectors were between 8.81% and 11.63% with detection time of 6.1 seconds. The results showed that Nearest Neighbor (Manhattan) detector has the lowest error rates on the data which was 8.81%.

Feher et al. (2012) introduced a method for continuously verifying users based on individual mouse action. They extracted new features form a hierarchy of mouse actions. These new features are inserted with previous work's features. Moreover, a multi-class classifier was utilized to verify user identity. The evaluation was performed using a dataset collected from different users. Results showed a significant enhancement in the accuracy when applying the newly inserted features. EER was 8.53%.

Table (2-1): Summary of the Review of Related Work

Writer	Idea	Technique	feature	No. of user	FRR	FAR
Margit Antal, El″od Egyed-Zsigmond	A new data splitting technique for better feature extraction	Statistical analysis and spectral curve	mouse movement action, Point Click action, Drag and Drop action, mouse released events, the threshold for the time field	65 users	-	-
Shen et al	fixed mouse-operation task.	One classifier statistical testing method	Single click statistics Double click statistics Movement offset Movement elapsed time Speed curve against time Acceleration curve against time	37 users	7.69%	8.74%
Ahmed Awad and Issa Traore	behavioral biometrics based on mouse dynamics	artificial neural networks (feed-forward algorithm)	mouse coordinates and computes several features such as speeds, accelerations, angular velocities, curvature, and the derivative of the curvature curve	22 user	2.4614 %	2.4649 %

Teng Hu et al.	authentication method based on mouse biobehavioral characteristics and deep learning	Data Preprocessing and Overall Architecture of CNN	moving coordinates, moving distance, angle, and moving time were constructed	35 users	2.28%	2.94%
Shujie Hu et al.	a mouse movement simulation method	Convolutional Neural Network (CNN)	speed, acceleration, and curvature	24 users	-	-
Penny Chong et al.	They have addressed this problem by learning the features with a CNN, without a need to manual feature design with a CNN, without a need to manual feature design	Convolutional neural network (CNN)	angle, curvature, and velocity in a heuristic manner	24 users	-	-
C.A. Anupashree, Spoorthi S. Kulkarni and Parashuram Baraki	a new model where the user draws a gesture using a mouse	Gesture creation module. Data acquisition and preparation module. Feature extraction module. Classification module.	Horizontal coordinate, Vertical coordinate, Absolute time, Horizontal velocity, Tangential velocity, Tangential acceleration, Tangential jerk, The path from the origin in pixel, Stop angle of the tangent, Curvature, Curvature rate of change.	17 users	-	-

Hema. D, Bhanumathi. S	described user behavior-based security	the feature learning algorithm, optical character recognition, and time-based one-time password algorithm	holistic and procedural features	-	-	-
Ms.Pooja S Pilankar, Mrs.Puja Padiya	provide additional mouse dynamics to the existing work dynamics to the existing work	Peirce's criterion and Weighted Least Square Regression (WLSR) and for classification, Learning Vector Quantization (LVQ).	Horizontal coordinate, Vertical coordinate, Instantaneous time, Horizontal velocity, Vertical velocity, Tangential velocity, Tangential acceleration, The path from the origin in pixels, The slope angle of the tangent, Curvature	-	-	-
S.Almalki et al.	evaluation of different classification techniques on a mouse dynamics dataset, the Balabit Mouse Challenge dataset	the Decision Tree classifier, the K-Nearest Neighbors classifier, and the Random Forest classifier	mouse move, point and click, and drag and drop	-	-	-

Zhang	use mouse action from an authenticated user that only do the right action. If the user doesn't do the right movement the system will reject him	Linux Kernal Design	Mouse movements	-	-	-
Hinbarji et al.	user authentication method based on mouse movements alone	back propagation neural network	Mouse movements	10 users	-	-

Sayed et al.	biometric authentication using mouse gesture for static authentication to create pattern by moving the mouse around	learning vector quantization (LVQ) neural network	Mouse gesture	39 users	4.59%	5.26%
Shen et al.	a study of anomaly-detection algorithms in mouse dynamics	17 different detectors	Movement direction Movement distance Click type	58 users	-	-

Feher et al.	a method for continuously verifying users based on individual mouse action	multi-class classifier	individual mouse action	25	-	-

Chapter Three

Methodology and Proposal Modeling

3.1 Methodology Approach

Mouse Dynamics Biometric (MDB) authentication can be done with several approaches each one of them has its own pros and cons. This thesis will follow the steps below:

1- Measured features Identification: Identify mouse dynamics measured features.

2- Authentication features identification: Select and formulate calculated authentication features that are extracted from measured features.

3- Data collection system: Generate mouse dynamics dataset for a group of users.

4- Anomaly detector model selection: Select the most suitable anomaly detection models.

5- Authentication process: In the authentication process the user must have an enrollment data within the system to apply the process. All the user's files will be imported to extract the calculated authentication feature from them. After that, a model will be applied to both the extracted authentication feature from the signed signature that needs authentication and the imported authentication features from each imported comma separated values (CSV) file. Finally, the signature will be counted either as a genuine signature or a forgery signature.

6- Evaluation result: Evaluate the detection performance of the selected anomaly detectors based on the EER metric which is the average of the False Acceptance Rate along with the False Rejection Rate.

The flowchart below will summarize the methodology steps.

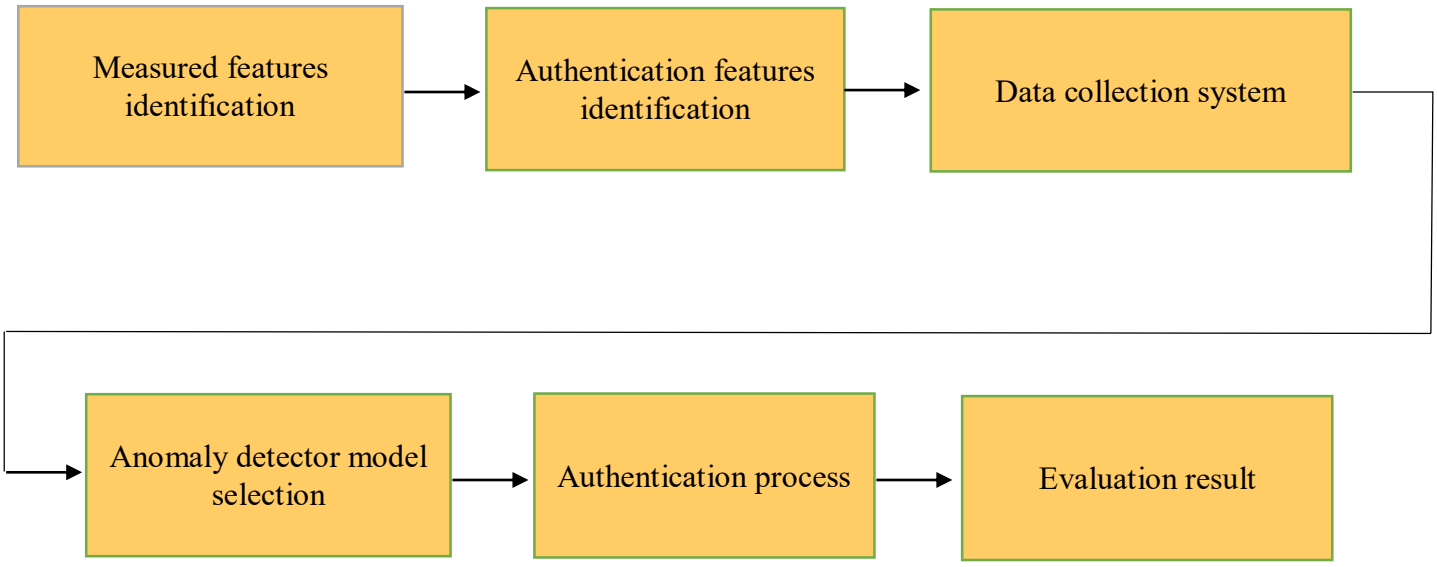

Figure (3-1): Methodology Steps

The incoming sections will show the real implementation for the adopted methodology.

3.2 Enrolment phase

While the user signing a set of features will be calculated simultaneously, the below table 3-1 will show the features with a brief information about each one.

Table (3-1): Measured Features Description

Feature	Description
X Coordinate	X Coordinate in pixel location
Y Coordinate	Y Coordinate in pixel location
Timestamp	Timestamp for the current position
Velocity X	Velocity of movements along the X-axis
Velocity Y	Velocity of movements along the Y-axis

After the sign has been signed, several features will be calculated depending on the generated features. The below table 3-2 will show the features with a brief description about each one:

Table (3-2): Extended Measured Features Description

Feature	Description
Time Difference	The difference time between two coordinates
X-Coordinates Difference	The horizontal distance between two coordinates
Y-Coordinates Difference	The vertical distance between two coordinates
R	The arc length between the coordinates (The square root of X-Coordinates difference squared plus Y-Coordinates difference squared)

The generated signature's dataset will have all of these features calculated as a measured feature for each reading (Dataset will contain several measured features within it). Finally, by having the dataset the calculated authentication feature can be extracted through data analysis based on training the authentication features to be obtain the lowest EER values for the selected anomaly detectors.

The extracted calculated authentication feature will contain a number of features too, each of these will be summarized in table 3-3:

Table (3-3): Calculated Authentication Features Description

Feature	Description
Number of Points	Number of row features within the dataset
Total Time Differences	The total of the time differences
Median of Time Differences	The median of the time differences
Max of Time Differences	The maximum Time Difference among the other row features
Total X-Coordinates Differences	The total of the X-Coordinate differences
Median of X-Coordinates Differences	The median of the X-Coordinate differences
Total Y-Coordinates Differences	The total of the Y-Coordinate differences
Median of Y-Coordinates Differences	The median of the Y-Coordinate differences
TY/TX	The total of the Y-Coordinate differences over the total of the X-Coordinate differences
Median of X Velocities	The median of the X velocities

Max of X Velocities	The maximum X Velocity among the other row features
Median of Y Velocities	The median of the Y velocities
Max of Y Velocities	The maximum Y Velocity among the other row features
Median of R	The median of the arc lengths
Max of R	The maximum arc length among the other row features

All of extracted measured features along with their own authentication feature will be exported to CSV file.

3.3 Signature Authentication

This section explains how the authentication works as well as mentioning different models that can be used along with it but in the end this work will use the most suitable model that gives a high degree of accuracy.

Signature authentication process will be done by taking all of the calculated authentication features from each imported signature files along with the extracted authentication feature from the signed signature. After that, a model (Anomaly detector) will be applied to authenticate whether the signature is it genuine or is it forgery.

Equal error rate (EER) is a biometric security system algorithm used to evaluate the systems' performance. The EER can be measured, firstly by repeating the signature authentication process several times with considering the existence of the forgery signatures among all ones. Secondly, calculating the False Acceptance Rate (FAR) and the False Rejection Rate (FRR). Hereafter is a full definition for the EER, FAR, and FRR.

False Acceptance Rate is the ratio of the accepted forgery signatures over all the entered signatures.

$$FAR = \frac{Number\ of\ accepted\ forgery\ signatures}{Number\ of\ all\ entered\ signatures} \quad (1)$$

False Rejection Rate is the ratio of the rejected genuine signatures over all the entered signatures.

$$FRR = \frac{Number\ of\ rejected\ genuine\ signatures}{Number\ of\ all\ entered\ signatures} \quad (2)$$

Equal Error Rate is the average of the False Acceptance Rate along with the False Rejection Rate.

$$EER = \frac{FAR+FRR}{2} \quad (3)$$

The subsections below will mention the classification methods with explaining which one the thesis will adopt, then will explain a set of algorithms that belongs to the selected classification method.

3.3.1 Classification Methods

There are variety of techniques for machine learning but classification is most widely used technique (Singh et.al., 2013). Authentication that based on features is a classic application of machine learning using the classification methods. There is a lot of classification applications such as speech recognition, handwriting recognition, biometric identification, document classification.

For our work, the anomaly detection method is used, because for an authentication process that is based on a user's behavior, the behavioral data of the user is available for enrollment in order to determine the user's profile. However, it is not possible to predict the profile of all others, so there are no negative training values.

Anomaly detection (one-class classification) it is a way of authenticating a person based on his correct biometric features, without having access to negative data samples. This is the case where a security system is trained for user authentication of the individual's profile of input, without knowledge of how impostors would input their data. Each person has his own signature profile and his way of signing, which an authentication attempts to capture. The extracted training data is the only data available to the anomaly detector, the one-class classifier. Any input that does not suite the profile of the genuine user will be imposter, so the one-class classifier knows the features of the genuine users, and any user who doesn't resemble the genuine user will be rejected. To evaluate the detection performance of a one-class classifier, we need the positive and negative data to evaluate the classifier's capability in distinguishing between genuine and impostor users. The

anomaly detector can make mistakes, by false rejecting a genuine person or false accepting an impostor. A template of the user's profile needs to be designed and tuned to avoid two error cases of detection of false acceptance and false rejection (Chandola, et. al, 2009). The performance evaluation of an anomaly detector will measure the Equal-Error-Rate (EER), the point at which the false reject rate (FRR) equals the false acceptance rate (FAR), for a set input from a group of users.

The proposed anomaly detector is based on the outlier concept (Xu, et.al, 2019), Where thresholds of acceptable features value are determined through enrolled, hence any feature value outside the thresholds are treated as imposter values. To determine the thresholds (upper limit and lower limit) for each authentication feature, we measure the distance from the mean of each features. Two distance metrics are used, based on two statistical functions, the Standard Deviation (STD), and the Absolut Average of Deviation (AAD). The statistical functions are multiplied by an empirically calculated constant, to calculated the maximum allowable distance from the mean.

3.3.2 Average Deviation Authentication Model (ADAM)

This model measures the maximum and minimum distance from the mean of a feature, using the Absolute Average of Deviation (AAD), multiplied by an empirically calculated distance factor.

Where:

- AAD is the Absolute Average of Deviation and it has the equation as below:

  $$AAD = \frac{\sum_{i=1}^{N} \|x_i - \overline{X}\|}{N} \quad (4)$$

  Where:

  - The numerator is the summation of the absolute deviation which is the absolute difference between each value of the statistical variable set (Any property set from the useful features properties) and the arithmetic mean of that set.
  - The Arithmetic Mean (AM) is the average of a statistical variable set and it has the formula as below:

$$\overline{X} = \frac{\sum_{i=1}^{N} X_i}{N} \quad (5)$$

- N is the number of elements within the given set.

- The distance factor is calculated experimentally by tuning its value to reach the lowest EER value, and it is the same value for all features.

3.3.3 Standard Deviation Authentication Model (SDAM)

In this model, the anomaly detection model is based measuring the distance from the mean of a set of training features values, using the standard deviation of the feature values as the basic distance metric. The purpose is to determine whether a testing feature value is an outlier value or a genuine value by comparing the features value with upper and lower thresholds. The thresholds are calculated using the standard deviation (STD) of a set of training features value, multiplied by a distance factor which is calculated experimentally to give the lowest EER value.

Where:

- STD is the Standard Deviation which can be described as the value that expressed how much the elements of a set differ from the Arithmetic Mean (AM) value of the set itself. The formula of the STD is as below:

  $$STD = \sqrt{\frac{\sum_{i=1}^{N}(X_i - \overline{X})^2}{N-1}} \quad (6)$$

  Where:

  - $\overline{X}$ is the Arithmetic Mean (AM) as explained in section 3.3.2.

- N is the number of elements within the given set.

- The distance factor is calculated experimentally by tuning its value to reach the lowest EER value, and it is the same value for all feature

Chapter Four

Implementation and Experimental Results

4.1 Methodology Implementation

In order to identify the user's signature from others it is a must to the system to have the accurate and sufficient data that related the signed user. When the system's user opens the executable file, a Form will launch with a User Interface (UI) design as in figure 4-1.

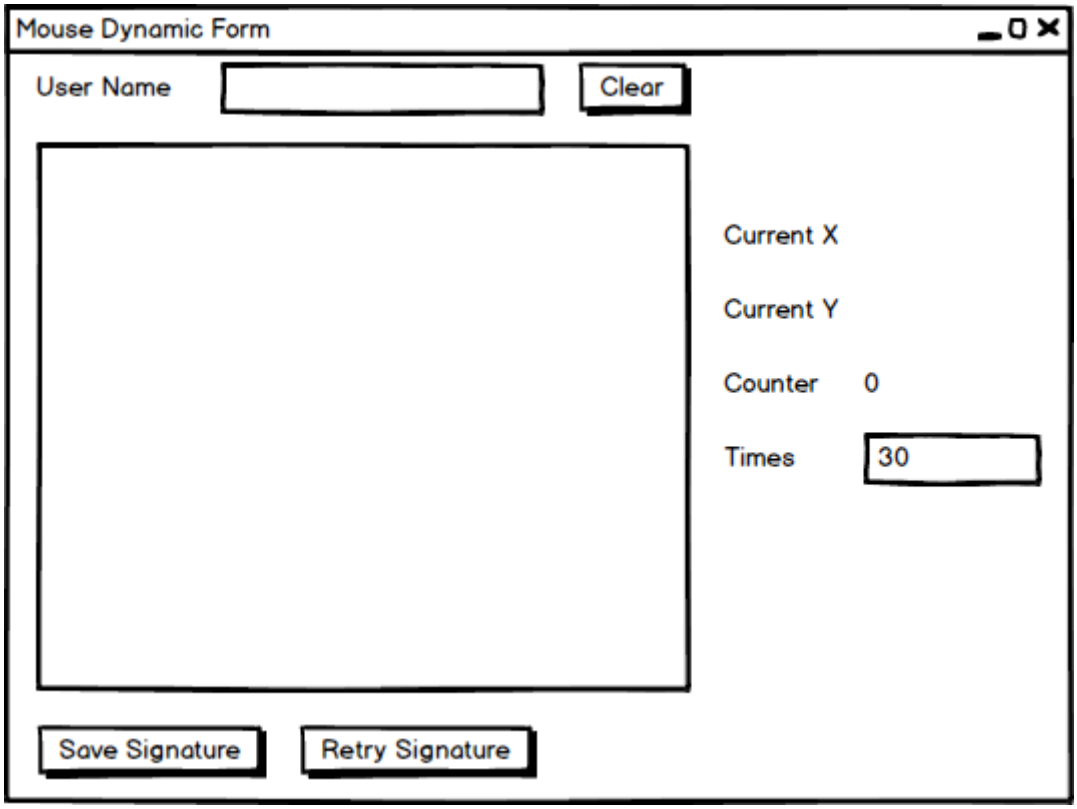

Figure (4-1): Mouse Dynamics Form UI Design

As a first step to enter the user's signature, the user must insert his name in the text box otherwise the process will not proceed. After the name has been inserted, the signature has to be signed in the proper place (signing area) to it.

In the first signing process and while the user is signing a set of features will be evaluated simultaneously as described in Chapter 3, Section 3.2, then after clicking the Save Signature button a set of other features will be calculated depending on the calculated features. Finally, depending on the generated dataset the user's authentication feature can be extracted from it and both of them will be exported in a CSV file to a selected path depending on the user's selection. The properties explanation of the measured features and the authentication features can be found in Chapter 3.

The process above will be repeated 30 times in order to have the sufficient data about the user's signature and to test our applied model too, then all of these data will be exported automatically to the same path of the first exported file. The flow chart 4-2 below shows the methodology implementation.

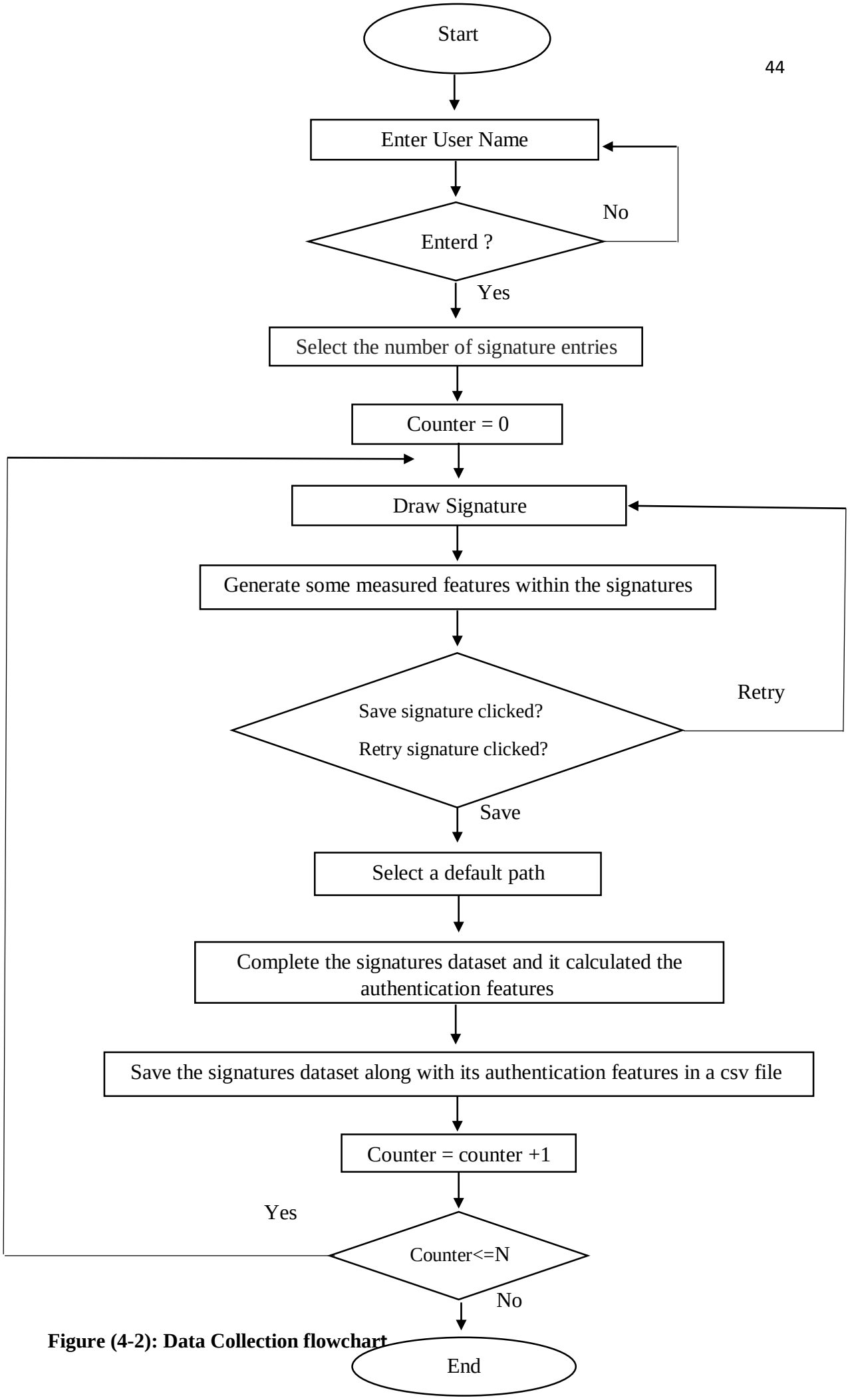

Figure (4-2): Data Collection flowchart

4.2 Average Deviation Authentication Model (ADAM) Analysis

As mentioned in the chapter three, the ADAM model is an enhancement of the Absolut Average Deviation (AAD) statistical metric multiplied by a distance factor as in equation 4 of chapter three.

There are several factors that used to optimize the result of the EER, one of these factors was the Distance factor that was measured by Trial and Error (TE) process and after applying the process several times the optimal distance factor was 3.3.

Another factor was the mode selection of the model whether it is a User Mode (UM) or a Global Mode (GM). When GM mode is selected it makes the Pass Mark (PM) (Al-jarrah,2012) equals for all target users, while on the other hand when the UM mode is selected the PM will vary for each user depending on the generated datasets along with its authentication features to give the optimal EER results. Table 4-1 and Table 4-2 will summarize the analysis of the experimental results that came from applying each GM mode and UM mode respectively.

Table (4-1): ADAM Result Analysis in GM Mode

		Genuine-Test		Imposter-Test				
User	**User PM**	**TA**	**FR**	**TR**	**FA**	**FRR**	**FAR**	***EER***
1	**11**	**9**	**1**	**57**	**1**	**0.100**	**0.017**	***5.86%***
2	**11**	**10**	**0**	**56**	**2**	**0.000**	**0.034**	***1.72%***
3	**11**	**9**	**1**	**58**	**0**	**0.100**	**0.000**	***5.00%***
4	**11**	**9**	**1**	**58**	**0**	**0.100**	**0.000**	***5.00%***
5	**11**	**10**	**0**	**52**	**6**	**0.000**	**0.103**	***5.17%***
6	**11**	**9**	**1**	**52**	**6**	**0.100**	**0.103**	***10.17%***
7	**11**	**9**	**1**	**55**	**3**	**0.100**	**0.052**	***7.59%***
8	**11**	**10**	**0**	**56**	**2**	**0.000**	**0.034**	***1.72%***
9	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***

10	**11**	**10**	**0**	**51**	**7**	**0.000**	**0.121**	***6.03%***
11	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
12	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
13	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
14	11	10	0	56	2	0.000	0.034	*1.72%*
15	**11**	**9**	**1**	**57**	**1**	**0.100**	**0.017**	***5.86%***
16	**11**	**9**	**1**	**57**	**1**	**0.100**	**0.017**	***5.86%***
17	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
18	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
19	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
20	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
21	**11**	**10**	**0**	**55**	**3**	**0.000**	**0.052**	***2.59%***
22	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
23	**11**	**8**	**2**	**58**	**0**	**0.200**	**0.000**	***10.00%***
24	**11**	**9**	**1**	**56**	**2**	**0.100**	**0.034**	***6.72%***
25	**11**	**10**	**0**	**55**	**3**	**0.000**	**0.052**	***2.59%***
26	**11**	**9**	**1**	**55**	**3**	**0.100**	**0.052**	***7.59%***
27	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
28	**11**	**8**	**2**	**58**	**0**	**0.200**	**0.000**	***10.00%***
29	**11**	**10**	**0**	**56**	**2**	**0.000**	**0.034**	***1.72%***
30	**11**	**9**	**1**	**53**	**5**	**0.100**	**0.086**	***9.31%***

Table (4-2): ADAM Results Analysis in UM Mode

		Genuine-Test		**Imposter-Test**				
User	**User PM**	**TA**	**FR**	**TR**	**FA**	**FRR**	**FAR**	***EER***
1	**10**	**9**	**1**	**56**	**2**	**0.100**	**0.034**	***6.72%***
2	**13**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
3	**9**	**9**	**1**	**56**	**2**	**0.100**	**0.034**	***6.72%***
4	**10**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
5	**12**	**10**	**0**	**54**	**4**	**0.000**	**0.069**	***3.45%***
6	**11**	**9**	**1**	**52**	**6**	**0.100**	**0.103**	***10.17%***
7	**11**	**9**	**1**	**55**	**3**	**0.100**	**0.052**	***7.59%***
8	**11**	**10**	**0**	**56**	**2**	**0.000**	**0.034**	***1.72%***
9	**10**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
10	**11**	**10**	**0**	**51**	**7**	**0.000**	**0.121**	***6.03%***
11	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
12	**12**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
13	**11**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
14	**12**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
15	**9**	**9**	**1**	**51**	**7**	**0.100**	**0.121**	***11.03%***
16	**10**	**9**	**1**	**55**	**3**	**0.100**	**0.052**	***7.59%***
17	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
18	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***

19	**11**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
20	**12**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
21	**11**	**10**	**0**	**55**	**3**	**0.000**	**0.052**	***2.59%***
22	**8**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
23	**8**	**9**	**1**	**56**	**2**	**0.100**	**0.034**	***6.72%***
24	**9**	**10**	**0**	**56**	**2**	**0.000**	**0.034**	***1.72%***
25	**12**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
26	**11**	**9**	**1**	**55**	**3**	**0.100**	**0.052**	***7.59%***
27	**8**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
28	**9**	**9**	**1**	**55**	**3**	**0.100**	**0.052**	***7.59%***
29	**12**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
30	**11**	**9**	**1**	**53**	**5**	**0.100**	**0.086**	***9.31%***

When applying the GM mode on the ADAM model it gives an average EER of 3.89%, while applying the UM mode on the ADAM model it gives an average EER of 3.33%.

With having a plenty of signature data for 30 target users and each one of them is calculated through applying the GM mode and UM mode, the evaluating of the EER with more accuracy has been applicable. But as we can see from the above readings, it seems to us that applying UM mode gives lesser EER than applying the GM mode and that leads to the reliable system we aspire to achieve.

4.3 Standard Deviation Authentication Model (SDAM) Analysis

Referring to section 3.3.3, the SDAM model can be explained as the product of the Standard Deviation (STD) with the Distance Factor which can be measured by applying TE process to give the most efficient system performance that has the lowest EER and that value was 2.9.

As ADAM model the SDAM model has two selection modes that can be applied on the target data, just to solidify these values were GM and UM modes. Tables 4-3 and 4-4 will show the measured readings for GM and UM modes respectively

Table (4-3): SDAM Results Analysis in GM Mode

		Genuine-Test		Imposter-Test				
User	User PM	TA	FR	TR	FA	FRR	FAR	*EER*
1	11	9	1	57	1	0.100	0.017	*5.86%*
2	11	10	0	53	5	0.000	0.086	*4.31%*
3	11	9	1	58	0	0.100	0.000	*5.00%*
4	11	9	1	58	0	0.100	0.000	*5.00%*
5	11	10	0	52	6	0.000	0.103	*5.17%*
6	11	9	1	52	6	0.100	0.103	*10.17%*
7	11	9	1	55	3	0.100	0.052	*7.59%*
8	11	10	0	56	2	0.000	0.034	*1.72%*
9	11	10	0	57	1	0.000	0.017	*0.86%*
10	11	10	0	50	8	0.000	0.138	*6.90%*
11	11	10	0	57	1	0.000	0.017	*0.86%*
12	11	10	0	57	1	0.000	0.017	*0.86%*
13	11	10	0	57	1	0.000	0.017	*0.86%*
14	11	10	0	56	2	0.000	0.034	*1.72%*
15	11	9	1	57	1	0.100	0.017	*5.86%*
16	11	9	1	57	1	0.100	0.017	*5.86%*
17	11	10	0	58	0	0.000	0.000	*0.00%*
18	11	10	0	57	1	0.000	0.017	*0.86%*
19	11	10	0	58	0	0.000	0.000	*0.00%*
20	11	10	0	57	1	0.000	0.017	*0.86%*
21	11	10	0	54	4	0.000	0.069	*3.45%*
22	11	10	0	58	0	0.000	0.000	*0.00%*
23	11	8	2	58	0	0.200	0.000	*10.00%*
24	11	9	1	56	2	0.100	0.034	*6.72%*
25	11	10	0	55	3	0.000	0.052	*2.59%*
26	11	10	0	55	3	0.000	0.052	*2.59%*
27	11	10	0	58	0	0.000	0.000	*0.00%*
28	11	8	2	58	0	0.200	0.000	*10.00%*
29	11	10	0	56	2	0.000	0.034	*1.72%*
30	11	10	0	53	5	0.000	0.086	*4.31%*

Table (4-4): SDAM Results Analysis in UM Mode

		Genuine-Test		Imposter-Test				
User	User PM	TA	FR	TR	FA	FRR	FAR	*EER*
1	10	9	1	55	3	0.100	0.052	*7.59%*
2	12	10	0	56	2	0.000	0.034	*1.72%*
3	9	9	1	56	2	0.100	0.034	*6.72%*
4	10	10	0	58	0	0.000	0.000	*0.00%*
5	12	10	0	54	4	0.000	0.069	*3.45%*
6	11	9	1	52	6	0.100	0.103	*10.17%*
7	11	9	1	55	3	0.100	0.052	*7.95%*
8	11	10	0	56	2	0.000	0.034	*1.72%*
9	10	10	0	57	1	0.000	0.017	*0.86%*
10	11	10	0	50	8	0.000	0.138	*6.90%*
11	11	10	0	57	1	0.000	0.017	*0.86%*
12	12	10	0	58	0	0.000	0.000	*0.00%*
13	11	10	0	57	1	0.000	0.017	*0.86%*
14	12	10	0	58	0	0.000	0.000	*0.00%*
15	9	9	1	51	7	0.100	0.121	*11.03%*
16	10	9	1	55	3	0.100	0.052	*7.59%*
17	11	10	0	58	0	0.000	0.000	*0.00%*
18	11	10	0	57	1	0.000	0.017	*0.86%*
19	11	10	0	58	0	0.000	0.000	*0.00%*
20	12	10	0	58	0	0.000	0.000	*0.00%*
21	13	10	0	58	0	0.000	0.000	*0.00%*
22	8	10	0	58	0	0.000	0.000	*0.00%*
23	8	9	1	55	3	0.100	0.052	*759%*
24	9	10	0	55	3	0.000	0.052	*2.59%*
25	12	10	0	57	1	0.000	0.017	*0.86%*
26	11	10	0	55	3	0.000	0.052	*2.59%*
27	8	10	0	58	0	0.000	0.000	*0.00%*
28	9	9	1	55	3	0.100	0.052	*7.59%*
29	12	10	0	57	1	0.000	0.017	*0.86%*
30	12	9	1	56	2	0.100	0.034	*6.72%*

More readings, means more accurate results for measuring system performance and in our case with having 30 readings it now easy to apply the mean of the EER for each mode as in the previous section. After calculating the mean of the EER for the GM mode it gives 3.72%, while in the case of UM it gives 3.22%. It is obvious now to decide that using the UM mode gives lesser average of EER which leads to more accurate detection to gain the reliability of the system we built.

4.4 Average Deviation Authentication Model and Standard Deviation Authentication Model Comparison

In terms of similarity between the ADAM model and the SDAM model they both have the value that makes the improvement to the common statistical rules we know and it measured experimentally (by applying the TE process) which is the Distance factor (DF) , also they both have the values that separate between the genuine and the forgery regions named as the Upper-Limit and the Lower-Limit (Any value fall between these limits is considered as a genuine value, otherwise is considered as forgery), also these limits calculated experimentally.

Applying these models to the adopted system give different EER result that can be considered as the major factor to select which model can be used along with our system, Table 4-5 will summarize the calculated values for every model along with its different modes.

Table (4-5): Models Comparison

Factors	ADAM Model in GM Mode	ADAM Model in UM Mode	SDAM Model in GM Mode	SDAM Model in UM Mode
Distance Factor	3.3	3.3	2.9	2.9
Average FRR	4.7%	3.3%	4%	3%
Average FAR	3.1%	3.3%	3.4%	3.4%
Average EER	3.89%	3.33%	3.72%	3.22%

Finally, the above results show that regardless of the similarity between the two models, the SDAM model gives lesser average of EER than ADAM model which means that applying SDAM will lead to the accuracy we aspire to achieve, so for that reason SDAM model was chosen above the other model in the thesis adopted system. In the incoming section, a comparison will be made between the chosen model from this work and different models from other thesis.

4.5 Analysis Result Without Distance Factor

To investigate the effect of the distance factor, which is obtained empirically, further analyses were performed on the collected experimental results, using the two models but with a distance factor of one, i.e. without using a distance factor. Tables 4-6, 4-7, 4-8, 4-9 shows the detailed analyses using the two models in global and user modes and with distance factor of one.

4.5.1 Average Deviation Authentication Model (ADAM) Analysis (without distance factor)

Table (4-6): ADAM Result Analysis in GM Mode (without distance factor)

		Genuine-Test		Imposter-Test				
User	User PM	TA	FR	TR	FA	FRR	FAR	*EER*
1	11	1	9	58	0	0.900	0.000	*45.00%*
2	11	3	7	58	0	0.700	0.000	*35.00%*
3	11	1	9	58	0	0.900	0.000	*45.00%*
4	11	5	5	58	0	0.500	0.000	*25.00%*

5	11	4	6	58	0	0.600	0.000	*30.00%*
6	11	0	10	58	0	1.000	0.000	*50.00%*
7	11	5	5	58	0	0.500	0.000	*25.00%*
8	11	1	9	58	0	0.900	0.000	*45.00%*
9	11	0	10	58	0	1.000	0.000	*50.00%*
10	11	0	10	58	0	1.000	0.000	*50.00%*
11	11	3	7	58	0	0.700	0.000	*35.00%*
12	11	5	5	58	0	0.500	0.000	*25.00%*
13	11	1	9	58	0	0.900	0.000	*45.00%*
14	11	5	5	58	0	0.500	0.000	*25.00%*
15	11	0	10	58	0	1.000	0.000	*50.00%*
16	11	2	8	58	0	0.800	0.000	*40.00%*
17	11	4	6	58	0	0.600	0.000	*30.00%*
18	11	2	8	58	0	0.800	0.000	*40.00%*
19	11	0	10	58	0	1.000	0.000	*50.00%*
20	11	1	9	58	0	0.900	0.000	*45.00%*
21	11	5	5	58	0	0.500	0.000	*25.00%*
22	11	7	3	58	0	0.300	0.000	*15.00%*
23	11	2	8	58	0	0.800	0.000	*40.00%*
24	11	0	10	58	0	1.000	0.000	*50.00%*
25	11	3	7	58	0	0.700	0.000	*35.00%*
26	11	6	4	58	0	0.400	0.000	*20.00%*
27	11	7	3	58	0	0.300	0.000	*15.00%*
28	11	1	9	58	0	0.900	0.000	*45.00%*
29	11	3	7	58	0	0.700	0.000	*35.00%*
30	11	5	5	58	0	0.500	0.000	*25.00%*

Table (4-7): ADAM Results Analysis in UM Mode (without distance factor)

		Genuine-Test		Imposter-Test				
User	User PM	TA	FR	TR	FA	FRR	FAR	*EER*
1	4	9	1	51	7	0.100	0.121	*11.03%*
2	7	10	0	56	2	0.000	0.034	*1.72%*
3	5	8	2	50	8	0.200	0.138	*16.90%*
4	6	10	0	58	0	0.000	0.000	*0.00%*
5	7	10	0	54	4	0.000	0.069	*3.45%*
6	5	7	3	46	12	0.300	0.207	*25.34%*
7	7	10	0	57	1	0.000	0.017	*0.86%*
8	6	8	2	48	10	0.200	0.172	*18.62%*
9	5	9	1	51	7	0.100	0.121	*11.03%*

10	7	9	1	51	7	0.100	0.121	*11.03%*
11	6	9	1	56	2	0.100	0.034	*6.72%*
12	6	10	0	56	2	0.000	0.034	*1.72%*
13	6	7	3	49	9	0.300	0.155	*22.76%*
14	6	9	1	55	3	0.100	0.052	*7.59%*
15	5	6	4	50	8	0.400	0.138	*26.90%*
16	6	7	3	51	7	0.300	0.121	*21.03%*
17	4	10	0	55	3	0.000	0.052	*2.59%*
18	6	10	0	56	2	0.000	0.034	*1.72%*
19	5	10	0	51	7	0.000	0.121	*6.03%*
20	7	10	0	58	0	0.000	0.000	*0.00%*
21	6	9	1	55	3	0.100	0.052	*7.59%*
22	7	10	0	58	0	0.000	0.000	*0.00%*
23	5	9	1	56	2	0.100	0.034	*6.72%*
24	5	8	2	51	7	0.200	0.121	*16.03%*
25	6	10	0	52	6	0.000	0.103	*5.17%*
26	6	7	3	46	12	0.300	0.207	*25.34%*
27	8	10	0	58	0	0.000	0.000	*0.00%*
28	5	8	2	54	4	0.200	0.069	*13.45%*
29	6	9	1	52	6	0.100	0.103	*10.17%*
30	6	8	2	49	9	0.200	0.155	*17.76%*

4.5.2 Standard Deviation Authentication Model (SDAM) Analysis (without distance factor)

Table (4-8): SDAM Results Analysis in GM Mode (without distance factor)

		Genuine-Test		Imposter-Test				
User	User PM	TA	FR	TR	FA	FRR	FAR	*EER*
1	11	2	8	58	0	0.800	0.000	*40.00%*
2	11	5	5	58	0	0.500	0.000	*25.00%*
3	11	2	8	58	0	0.800	0.000	*40.00%*
4	11	6	4	58	0	0.400	0.000	*20.00%*
5	11	5	5	58	0	0.500	0.000	*25.00%*
6	11	1	9	57	1	0.900	0.017	*45.86%*
7	11	7	3	58	0	0.300	0.000	*15.00%*
8	11	2	8	58	0	0.800	0.000	*40.00%*
9	11	6	4	58	0	0.400	0.000	*20.00%*
10	11	6	4	58	0	0.400	0.000	*20.00%*

11	11	5	5	58	0	0.500	0.000	*25.00%*
12	11	5	5	58	0	0.500	0.000	*25.00%*
13	11	2	8	57	1	0.800	0.017	*40.86%*
14	11	6	4	58	0	0.400	0.000	*20.00%*
15	11	0	10	58	0	1.000	0.000	*50.00%*
16	11	5	5	58	0	0.500	0.000	*25.00%*
17	11	7	3	58	0	0.300	0.000	*15.00%*
18	11	6	4	58	0	0.400	0.000	*20.00%*
19	11	2	8	58	0	0.800	0.000	*40.00%*
20	11	7	3	58	0	0.300	0.000	*15.00%*
21	11	7	3	58	0	0.300	0.000	*15.00%*
22	11	9	1	58	0	0.100	0.000	*5.00%*
23	11	3	7	58	0	0.700	0.000	*35.00%*
24	11	1	9	58	0	0.900	0.000	*45.00%*
25	11	8	2	58	0	0.200	0.000	*10.00%*
26	11	7	3	58	0	0.300	0.000	*15.00%*
27	11	9	1	58	0	0.100	0.000	*5.00%*
28	11	2	8	58	0	0.800	0.000	*40.00%*
29	11	6	4	58	0	0.400	0.000	*20.00%*
30	11	8	2	57	1	0.200	0.017	*10.86%*

Table (4-9): SDAM Results Analysis in UM Mode (without distance factor)

		Genuine-Test		Imposter-Test				
User	**User PM**	**TA**	**FR**	**TR**	**FA**	**FRR**	**FAR**	***EER***
1	5	9	1	53	5	0.100	0.086	*9.31%*
2	9	10	0	56	2	0.000	0.034	*1.72%*
3	6	9	1	52	6	0.100	0.103	*10.17%*
4	6	10	0	58	0	0.000	0.000	*0.00%*
5	9	9	1	53	5	0.100	0.086	*9.31%*
6	7	9	1	50	8	0.100	0.138	*11.90%*
7	9	10	0	57	1	0.000	0.017	*0.86%*
8	8	9	1	55	3	0.100	0.052	*7.59%*
9	6	9	1	54	4	0.100	0.069	*8.45%*
10	8	7	3	52	6	0.300	0.103	*20.17%*
11	8	10	0	58	0	0.000	0.000	*0.00%*
12	6	10	0	56	2	0.000	0.034	*1.72%*
13	8	9	1	56	2	0.100	0.034	*6.72%*
14	7	9	1	51	7	0.100	0.121	*11.03%*

15	**6**	**8**	**2**	**49**	**9**	**0.200**	**0.155**	***17.76%***
16	**7**	**8**	**2**	**47**	**11**	**0.200**	**0.190**	***19.48%***
17	**6**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
18	**7**	**10**	**0**	**57**	**1**	**0.000**	**0.017**	***0.86%***
19	**7**	**9**	**1**	**56**	**2**	**0.100**	**0.034**	***6.72%***
20	**8**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
21	**6**	**9**	**1**	**54**	**4**	**0.100**	**0.069**	***8.45%***
22	**7**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
23	**6**	**10**	**0**	**56**	**2**	**0.000**	**0.034**	***1.72%***
24	**5**	**9**	**1**	**49**	**9**	**0.100**	**0.155**	***12.76%***
25	**8**	**9**	**1**	**52**	**6**	**0.100**	**0.103**	***10.17%***
26	**7**	**9**	**1**	**46**	**12**	**0.100**	**0.207**	***15.34%***
27	**8**	**10**	**0**	**58**	**0**	**0.000**	**0.000**	***0.00%***
28	**6**	**9**	**1**	**54**	**4**	**0.100**	**0.069**	***8.45%***
29	**8**	**9**	**1**	**56**	**2**	**0.100**	**0.034**	***6.72%***
30	**8**	**9**	**1**	**50**	**8**	**0.100**	**0.138**	***11.90%***

Table 4-10 shows comparison between the two approaches of using an empirically calculated distance factor and a distance factor of one, for the two models and in global and user modes. It is evident from the results that using the empirically calculated distance factor has produced lower EER results for all cases of models and modes.

Table (4-10): Comparison of Authentication Models with and Without Distance Factor

The proposed model	ADAM		SDAM	
With distance factor	ADAM With distance factor= 3.3		SDAM With distance factor= 2.9	
	EER GM	EER UM	EER GM	EER UM
	3.89%	3.33%	3.72%	3.22%
Without distance factor	ADAM Without distance factor		SDAM Without distance factor	
	EER GM	EER UM	EER GM	EER UM
	36.33%	9.98%	25.59%	7.31%

4.6 Previous Study Comparison

This section will discuss the comparison between calculated results from the adopted SDAM model and other existing works results, Table 4-11 will summarize some of the existing works results.

Table (4-11): Some Existing Works Results

Paper	Target Users	Average FRR	Average FAR	Average EER
Shen et al.	37	7.69%	8.74%	8.215%
Shen et al.	58	11.63%	8.81%	10.22%
Feher et al.	25	-	-	8.53%
Hinbarji et al.	10	-	-	9.8%
SDAM in UM (the proposed model)	30	3%	3.4%	3.22%
SDAM in GM (the proposed model)	30	4%	3.4%	3.72%

After showing the readings gained from other works, the comparison become easier than before. All of the above works show more average of EER than the selected model from this work which gives 3.72% by applying the GM mode and 3.22% by applying the UM mode and that means the adopted model will give more accurate results than some of the existing works in this field.

Chapter Five

Conclusion and Future Work

5.1 Conclusion

This thesis presents the implementation of the Mouse Dynamics Biometric (MDB) authentication models which can be described as a behavioural biometric technology that extracts and analyses the movement characteristics of the mouse input device when a computer user interacts with a Graphical User Interface (GUI) for identification purposes. Performance evaluation results show that Standard Deviation Authentication Model (SDAM) model outperforms Average Deviation Authentication Model (ADAM) model in EER where it is in (SDAM) model 3.22% and in (ADAM) model 3.33%. The results also show that both proposed models outperformed their rivals in the literature in terms of the EER metric. A critical analysis of the proposed work revealed that the average EER when using different pass-mark per user is less than that when using same pass-mark in global. Also using a distance factor will achieve a lower EER than not using it.

5.2 Future Work

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

- Improve the proposed models with additional features based on further experimentations and then reduce the equal error rate.

- Implement a dynamic authentication tool based on two-step verification that combines password verification and signature verification based on mouse dynamics using the proposed MDB model.
- Combining the MDB model with another behavioral biometric model such as keystroke dynamics to enhance the detection accuracy through multi-modal authentication.

References

Ahmed, A. A., & Traore, I. (2007). A New Biometric Technology Based on Mouse Dynamics. ***IEEE Transactions on Dependable and Secure Computing***, 4(3), 165-179. doi:10.1109/tdsc.2007.70207

Al-jarrah, M. M.,(2012), An Anomaly Detector for Keystroke Dynamics Based on Medians Vector Proximity.

Almalki, S., Chatterjee, P., & Roy, K. (2019). Continuous Authentication Using Mouse Clickstream Data Analysis. ***Security, Privacy, and Anonymity in Computation, Communication, and Storage***, 76-85. doi:10.1007/978-3-030-24900-7_6

Amin, R., Gaber, T., ElTaweel, G., & Hassanien, A. E. (2014). Biometric and Traditional Mobile Authentication Techniques: Overviews and Open Issues. ***Bio-inspiring Cyber Security and Cloud Services: Trends and Innovations***, 423-446. doi:10.1007/978-3-662-43616-5_16

Antal, M., & Egyed-Zsigmond, E. (2019). Intrusion detection using mouse dynamics. ***IET Biometrics***, 8(5), 285-294. doi:10.1049/iet-bmt.2018.5126

Anupashree, C., Kulkarni, S. S., & Baraki, P. (2016). An Innovative Approach to Authenticate a Person using Mouse Gesture Dynamics. ***Bonfring International Journal of Software Engineering and Soft Computing***, 6(Special Issue), 180-182. doi:10.9756/bijsesc.8271

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection. ***ACM Computing Surveys***, 41(3), 1-58. doi:10.1145/1541880.1541882

Chao Shen, Zhongmin Cai, Xiaohong Guan, Youtian Du, & Maxion, R. A. (2013). User Authentication Through Mouse Dynamics. ***IEEE Transactions on Information Forensics and Security***, 8(1), 16-30. https://doi.org/10.1109/tifs.2012.2223677

Chong, P., Tan, Y. X., Guarnizo, J., Elovici, Y., & Binder, A. (2018). Mouse Authentication Without the Temporal Aspect – What Does a 2D-CNN Learn? 2018 ***IEEE Security and Privacy Workshops (SPW)***. doi:10.1109/spw.2018.00011

Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., & Schclar, A. (2012). User identity verification via mouse dynamics. ***Information Sciences***, 201, 19-36. doi:10.1016/j.ins.2012.02.066

Gamboa, H., Fred, A.,L.N., An Identity Authentication System Based On Human Computer Interaction Behaviour (2003).

Hema, D., & Bhanumathi, S. (2016). Mouse behaviour based multi-factor authentication using neural networks. 2016 ***International Conference on Circuit, Power and Computing Technologies (ICCPCT)***. doi:10.1109/iccpct.2016.7530312

Hinbarji, Z., Albatal, R., & Gurrin, C. (2015). Dynamic User Authentication Based on Mouse Movements Curves. ***MultiMedia Modeling***, 111-122. doi:10.1007/978-3-319-14442-9_10

Hoang, T., Nguyen, T., Luong, C., Do, S., & Choi, D. (2013). Adaptive Cross-Device Gait Recognition Using a Mobile Accelerometer. ***Journal of Information Processing Systems***, 9(2), 333-348. doi:10.3745/jips.2013.9.2.333

Hu, S., Bai, J., Liu, H., Wang, C., & Wang, B. (2017). Deceive Mouse-Dynamics-Based Authentication Model via Movement Simulation. 2017 ***10th International Symposium on Computational Intelligence and Design (ISCID)***. doi:10.1109/iscid.2017.134

Hu, T., Niu, W., Zhang, X., Liu, X., Lu, J., & Liu, Y. (2019). An Insider Threat Detection Approach Based on Mouse Dynamics and Deep Learning. ***Security and Communication Networks***, 2019, 1-12. doi:10.1155/2019/3898951

Jain, A., Ross, A., & Pankanti, S. (2006). Biometrics: A Tool for Information Security. ***IEEE Transactions on Information Forensics and Security***, 1(2), 125-143. doi:10.1109/tifs.2006.873653

Jorgensen, Z., & Yu, T. (2011). On mouse dynamics as a behavioral biometric for authentication. ***Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security - ASIACCS '11***. doi:10.1145/1966913.1966983

Koong, C., Yang, T., & Tseng, C. (2014). A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices. ***The Scientific World Journal***, 2014, 1-12. doi:10.1155/2014/781234

Matyas, V., & Riha, Z. (2003). Toward reliable user authentication through biometrics. ***IEEE Security & Privacy***, 1(3), 45-49. doi:10.1109/msecp.2003.1203221

Nakkabi, Y., Traore, I., & Ahmed, A. A. (2010). Improving Mouse Dynamics Biometric Performance Using Variance Reduction via Extractors with Separate

Features. ***IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans***, 40(6), 1345-1353. doi:10.1109/tsmca.2010.2052602

Pilankar, P. S., & Padiya, P. (2016). Multi-phase mouse dynamics authentication system using behavioural biometrics. 2016 ***International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)***. doi:10.1109/scopes.2016.7955786

Sayed, B., Traore, I., Woungang, I., & Obaidat, M. S. (2013). Biometric Authentication Using Mouse Gesture Dynamics. ***IEEE Systems Journal***, 7(2), 262-274. doi:10.1109/jsyst.2012.2221932

Shen, C., Cai, Z., Guan, X., & Maxion, R. (2014). Performance evaluation of anomaly-detection algorithms for mouse dynamics. ***Computers & Security***, 45, 156-171. https://doi.org/10.1016/j.cose.2014.05.002

Shen, C., Cai, Z., Guan, X., Sha, H., & Du, J. (2009). Feature Analysis of Mouse Dynamics in Identity Authentication and Monitoring. 2009 ***IEEE International Conference on Communications***. https://doi.org/10.1109/icc.2009.5199032

Singh, M., Sharma, S., Kaur, A., Performance Analysis of Decision Trees. ***International Journal of Computer Applications*** 2013; 71.

Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K., & Ben-David, S. (2012). Biometric authentication on a mobile device. ***Proceedings of the 28th Annual Computer Security Applications Conference on - ACSAC '12***. doi:10.1145/2420950.2420976

Velásquez, I., Caro, A., & Rodríguez, A. (2018). Authentication schemes and methods: A systematic literature review. ***Information and Software Technology***, 94, 30-37***. https://doi.org/10.1016/j.infsof.2017.09.012***

Xu, X., Liu, H., & Yao, M. (2019). Recent Progress of Anomaly Detection. Complexity, 2019, 1-11. ***https://doi.org/10.1155/2019/2686378***

Zhang, X. (2015). Human user authentication based on mouse dynamics: a feasibility study. ***https://doi.org/10.31274/etd-180810-4479***

Appendix A: Sample of The Proposed Measured Features and Extended Measured Features

Table (A.1): Sample of the proposed measured features and extended measured features

Index	X	Y	TimeStamp	VelocityX	VelocityY	Dt	dX	Dy	R
1	84	305	637098674760070000	0	0				
1	85	303	637098674760694000	0.021277	-0.04255319	624768	1	2	2.236068
1	88	301	637098674761940000	0.043011	-0.04301075	1246080	3	2	3.605551
1	93	295	637098674762413000	0.06383	-0.07092199	472192	5	6	7.81025
1	99	285	637098674762878000	0.080214	-0.10695187	465920	6	10	11.6619
1	104	275	637098674763350000	0.08547	-0.12820513	471424	5	10	11.18034
1	108	265	637098674763819000	0.085409	-0.14234875	468736	4	10	10.77033
1	113	255	637098674764285000	0.088415	-0.15243902	466816	5	10	11.18034
1	122	239	637098674764752000	0.101333	-0.176	466176	9	16	18.35756
1	127	229	637098674765224000	0.101896	-0.18009479	472832	5	10	11.18034
1	136	215	637098674765693000	0.110874	-0.19189765	468608	9	14	16.64332
1	146	191	637098674766162000	0.120155	-0.22093023	468608	10	24	26
1	152	163	637098674766630000	0.120782	-0.25222025	467840	6	28	28.63564
1	160	142	637098674767099000	0.124795	-0.26765189	469632	8	21	22.47221
1	169	125	637098674767567000	0.129573	-0.27439024	468352	9	17	19.23538
1	174	116	637098674768032000	0.128023	-0.2688478	464640	5	9	10.29563
1	177	109	637098674768505000	0.124	-0.26133333	472832	3	7	7.615773

Appendix B: The Calculated Authentication Features for Thirty Users

Table (B.1): The calculated authentication features for user one

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
1	51	18731264	349312	583552	285	5	149	2	0.523	-0.04	-0.009	0.0643	0.1012	6.325	34.13
1	49	17611008	345856	855168	292	5	172	3	0.589	-0.007	0.0287	0.082	0.1167	7.211	20.62
1	52	19166720	343872	1160448	233	4	121	2	0.519	-0.025	0.0291	0.0534	0.0882	4.357	20.25
1	50	17856256	342848	1016960	292	6	177	3	0.606	-0.029	0.0291	0.0763	0.104	6.994	16.16
1	47	17804032	345600	1074304	227	5	142	3	0.626	-0.023	0.0104	0.0724	0.1351	6.325	13.93
1	47	18207616	343680	1380992	328	7	177	3	0.54	-0.043	-0.005	0.1131	0.1801	8.544	22.02
1	53	20052864	343296	2233344	252	4	157	3	0.623	-0.033	0.0213	0.0676	0.1479	5	16.4
1	49	17488512	337024	1310336	268	5	147	2	0.549	-0.028	0.0196	0.0582	0.0858	6.325	26
1	53	21343744	349184	1422080	227	3	114	2	0.502	-0.031	0.0175	0.0433	0.0571	4.472	15.52
1	47	16807808	342016	1056896	303	5	149	3	0.492	-0.075	-0.01	0.0836	0.1129	6.403	19.92
1	57	21053696	346496	1106816	222	4	143	2	0.644	-0.022	0.0314	0.0729	0.1265	5.385	12.37
1	67	24301184	341760	1405312	208	2	149	2	0.716	-0.034	0.0237	0.0321	0.069	4.472	14.56
1	59	20766720	341760	889600	241	3	172	2	0.714	-0.02	0.0441	0.0611	0.1002	5.385	15.26
1	47	17436672	348160	724736	223	4	130	2	0.583	-0.033	0.0007	0.071	0.1111	6.083	13
1	56	19703552	342464	538368	244	4	106	1	0.434	-0.042	0.0222	0.0432	0.0665	4.736	14
1	65	24009344	344704	1049984	185	3	140	2	0.757	-0.022	0.0183	0.0523	0.0854	4.123	10
1	53	18661248	344192	596480	214	4	140	2	0.654	-0.023	0.0188	0.0742	0.1086	5.657	12.04
1	59	21123328	339968	1014912	213	4	137	2	0.643	-0.036	0.0209	0.0506	0.0713	5.099	10
1	52	18577792	345408	732800	240	3	140	2.5	0.583	-0.032	0.0252	0.0643	0.1005	5	16.12
1	45	16290304	338304	1007360	280	6	143	3	0.511	-0.049	-0.002	0.083	0.1269	7.211	19.24
1	44	16643072	341440	1726336	214	4	128	3	0.598	-0.021	0.0182	0.0718	0.1137	6	15.3
1	51	18256000	342016	989312	202	4	134	2	0.663	-0.028	0.0196	0.0451	0.0749	5	17.8
1	63	24037760	348416	734720	195	3	137	2	0.703	-0.021	0.0215	0.0482	0.0771	4.123	14.21

1	56	21295744	344896	1477376	190	3	137	2	0.721	-0.027	0.0214	0.041	0.0578	4	12.53
1	70	26448000	343040	1267584	239	2.5	138	1	0.577	-0.028	0.0267	0.0525	0.0835	4.123	13.89
1	61	23966848	346880	1972608	219	3	137	2	0.626	-0.032	0.013	0.0528	0.1018	4.472	16.28
1	68	65428224	344000	4E+07	208	3	132	2	0.635	-0.029	0.0252	0.04	0.0645	4	11.7
1	60	22281472	337920	1329920	229	3	142	2	0.62	-0.031	0.0315	0.0638	0.0981	5	10
1	71	25415168	340096	1250688	250	3	121	1	0.484	-0.029	0.0348	0.0482	0.0751	4	18.38
1	69	57817984	346496	3.3E+07	281	3	273	1	0.972	-0.03	0.0288	0.0393	0.0694	4.123	63.95

Table (B.2): The calculated authentication features for user two

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
2	39	217410816	468736	1.6E+08	228	5	134	2	0.5877	0.0124	0.245	0.0522	0.0761	7	22.1
2	30	15777536	468672	2030720	196	5.5	134	4	0.6837	0.0383	0.348	0.0643	0.0909	8.274	25.1
2	24	13746560	468608	1871616	245	8	150	5	0.6122	0.0825	0.426	0.11	0.157	10.85	31.1
2	25	34951296	468608	2.3E+07	282	6	170	4	0.6028	0.0453	0.471	0.1119	0.1728	12.65	49.5
2	26	30683648	468736	1.6E+07	298	8	153	3	0.5134	0.0622	0.383	0.0903	0.1342	11.08	47
2	22	32541184	468672	1.9E+07	297	6.5	159	4	0.5354	0.0319	0.309	0.11	0.1899	14.96	48.1
2	19	9842560	468736	1092480	261	13	192	7	0.7356	0.0676	0.66	0.1503	0.2727	19.85	51
2	19	9682816	468608	1095680	255	9	175	6	0.6863	0.0388	0.591	0.1434	0.1983	14.21	55.9
2	20	49894784	468736	4E+07	311	12.5	168	5	0.5402	0.0806	0.731	0.163	0.2132	15.45	49.5
2	22	10778752	468672	937216	264	6	193	6	0.7311	0.0584	0.539	0.119	0.1449	11.91	55.2
2	22	10656128	468672	781184	291	12	180	5.5	0.6186	0.0453	0.645	0.1062	0.1433	17.56	44.6
2	19	10867840	468736	2255744	315	12	154	5	0.4889	0.0854	0.915	0.1437	0.224	22.56	54.1
2	22	10493184	468608	624512	291	8.5	177	6	0.6082	0.1061	0.702	0.1177	0.1564	13.16	51.2
2	19	9372800	468608	933248	268	14	197	10	0.7351	0.022	0.696	0.0784	0.1059	18.44	57.4
2	22	9264768	465792	941312	306	10	205	7	0.6699	0.0428	0.567	0.1207	0.1593	12.95	50.6
2	19	9248640	468736	777088	302	12	202	8	0.6689	0.0427	0.638	0.1327	0.1922	14.76	72.8
2	20	23953280	468928	1.5E+07	299	10	208	6.5	0.6957	0.0842	0.84	0.1534	0.2167	19.26	59.7
2	21	10775552	468736	1094784	262	10	191	7	0.729	0.0706	0.369	0.0983	0.1418	16.64	35.8
2	18	10158848	468672	1722496	288	14	154	5	0.5347	0.1045	0.691	0.1346	0.184	16.76	54.1
2	19	8909952	468608	472832	254	12	183	7	0.7205	0.0821	0.567	0.1398	0.1776	15.62	42.3
2	23	29773568	468736	1.9E+07	251	7	172	5	0.6853	0.0446	0.44	0.0913	0.1133	12	38.8
2	19	9372928	468608	932992	261	10	149	7	0.5709	0.0262	0.596	0.128	0.1808	16	56.6
2	18	9214592	468608	936576	272	14.5	163	7.5	0.5993	0.1008	1.043	0.1519	0.1902	19.12	49.4
2	21	76872448	468736	6.8E+07	229	8	191	6	0.8341	0.1	0.591	0.1261	0.1601	12.53	44.4
2	20	38597504	468672	2.9E+07	274	9.5	165	5.5	0.6022	0.0885	0.734	0.1129	0.1323	16.07	46.4

2	19	9683584	468736	937344	250	9	139	5	0.556	0.0572	0.819	0.1456	0.2252	12.21	41.2
2	22	42592768	468608	3.3E+07	217	7.5	162	4	0.7465	0.0899	0.4	0.0784	0.1406	9.497	44.7
2	19	9563392	468736	933248	328	12	175	3	0.5335	0.0701	0.586	0.125	0.1673	17.89	66.1
2	20	53050624	468608	4.3E+07	241	8.5	143	7	0.5934	0.0917	0.471	0.078	0.1117	14.22	35
2	19	8908928	468736	475520	215	6	131	4	0.6093	0.0972	0.539	0.1238	0.157	13.6	43.3

Table (B.3): The calculated authentication features for user three

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
3	27	12808576	468736	622720	250	6	255	5	1.02	-0.067	0.153	-0.024	0.0038	11.66	39.6
3	28	13902720	468608	937216	237	4.5	198	5.5	0.8354	-0.048	0.134	-0.043	-0.006	12.6	33.1
3	28	34136448	468736	2.1E+07	256	5.5	260	8	1.0156	-0.085	0.199	-0.045	-0.007	15.06	35
3	29	14217856	468736	778624	246	7	266	5	1.0813	-0.036	0.189	-0.058	-0.003	15	36
3	29	14211200	468608	1093504	266	8	242	5	0.9098	-0.046	0.221	-0.043	-0.004	12	36
3	28	28018944	468544	1.6E+07	264	4.5	249	7	0.9432	-0.098	0.149	-0.058	-0.019	14.87	42
3	26	29323648	468608	1.8E+07	262	5.5	203	4	0.7748	-0.069	0.14	-0.054	-0.01	15.12	41.2
3	32	36773632	468608	2.1E+07	273	4	216	5.5	0.7912	-0.092	0.203	-0.027	-0.005	10.33	35.5
3	23	40625408	468736	2.9E+07	237	3	156	5	0.6582	-0.094	0.154	-0.03	-0.009	11.66	48
3	28	13282304	468672	625024	261	7	187	5.5	0.7165	-0.064	0.142	-0.029	-0.003	13.52	31.8
3	28	14684032	468608	1093376	270	5.5	215	5	0.7963	-0.12	0.17	-0.007	0.0107	12.09	51.1
3	28	13743616	468672	933120	311	7.5	225	5	0.7235	-0.07	0.274	0.0001	0.0156	12.42	48.5
3	28	13743616	468672	933120	311	7.5	225	5	0.7235	-0.07	0.274	0.0001	0.0156	12.42	48.5
3	28	13614208	468608	1116800	276	7.5	197	4.5	0.7138	-0.099	0.193	-0.026	-0.005	14.49	31.3
3	30	32783872	468928	1.9E+07	308	4.5	199	5	0.6461	-0.125	0.162	-0.03	0.0064	11	84.1
3	30	15158400	469184	937728	259	4.5	242	6	0.9344	-0.059	0.137	-0.041	-0.013	12.73	39.1
3	29	13749376	468608	623232	296	10	182	5	0.6149	-0.072	0.162	-0.031	-0.004	12.21	30
3	29	13904896	468608	780928	243	5	212	4	0.8724	-0.105	0.103	-0.036	-0.013	10	50.1
3	29	35733376	468608	2.2E+07	284	7	217	4	0.7641	-0.049	0.216	-0.032	-0.007	15.3	35
3	29	14530688	468608	937472	331	7	179	5	0.5408	-0.082	0.269	-0.024	-9E04	12.04	41
3	28	26621952	468672	1.3E+07	254	6	228	6	0.8976	-0.083	0.135	-0.028	-0.005	14.4	31.8

3	29	35983360	468736	2.2E+07	258	4	196	5	0.7597	-0.103	0.129	-0.029	-0.014	11.4	44
3	33	33901952	468736	1.7E+07	314	8	152	3	0.4841	-0.051	0.207	-0.013	-0.001	11.18	31.1
3	32	15463424	468608	1093504	284	8	159	3.5	0.5599	-0.076	0.189	-0.007	0.006	10.1	34.5
3	29	14244096	468608	1249792	314	9	175	3	0.5573	-0.064	0.299	-0.017	-8E04	14	33.1
3	30	40558336	468736	2.6E+07	317	7.5	162	4	0.511	-0.069	0.199	-0.011	0.0058	11.2	44.3
3	27	13124864	468608	939008	282	8	153	4	0.5426	-0.064	0.209	-0.003	0.0145	13.45	33
3	30	29638784	468608	1.5E+07	275	9.5	155	3	0.5636	-0.063	0.196	-0.019	-0.003	13.76	32.1
3	29	31795200	468736	1.8E+07	291	6	165	4	0.567	-0.068	0.222	-0.014	0.004	10.82	37
3	37	50060800	468608	3.3E+07	301	5	153	3	0.5083	-0.084	0.149	-0.003	0.0062	8.944	41

Table (B.4): The calculated authentication features for user four

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
4	8	3688192	461184	461312	106	13	125	14.5	1.1792	-0.22	-0.088	0.3765	0.76	20.94	45.22
4	8	3168256	399168	464896	110	15	119	14.5	1.0818	-0.19	-0.081	0.3204	0.7368	18.44	40.72
4	8	17748480	461312	1E+07	146	18	128	17	0.8767	-0.16	0.0313	0.4126	0.7179	26.13	43.6
4	6	2526592	459648	475776	239	17	102	16.5	0.4268	-0.19	0.2802	0.3969	0.6222	32.99	105.5
4	8	3420672	461120	463488	123	12.5	106	12	0.8618	-0.1	0.0642	0.3487	0.5652	20.59	35.47
4	8	3054976	348800	464512	105	11	112	5	1.0667	-0.27	-0.134	0.4875	1.2537	14.1	52.43
4	8	3580672	461248	477696	77	8.5	131	9	1.7013	-0.04	0.0366	0.3399	1.1765	20.12	41.76
4	9	3620864	414080	462208	108	10	142	16	1.3148	-0.13	0.0233	0.3674	0.7143	21.38	44.01
4	8	3280640	443840	461824	88	9	134	16.5	1.5227	-0.11	0.0099	0.3876	0.6374	23.53	38.28
4	8	3269376	460544	463360	158	24.5	150	18.5	0.9494	-0.13	0.069	0.3554	0.6126	32.26	41.4
4	8	3185792	386112	504960	165	18.5	109	9	0.6606	-0.29	-0.087	0.33	0.913	22.61	61.55
4	8	3375616	459392	480768	87	10	115	15.5	1.3218	-0.07	0.0144	0.3518	0.6087	22.21	30.46
4	7	2685440	340608	462592	111	17	128	7	1.1532	-0.12	0.0175	0.5088	0.9022	27.66	57.14
4	7	2962304	459776	461696	62	9	121	11	1.9516	-0.11	-0.03	0.3568	0.663	21.1	33.96
4	10	3629696	344576	459520	159	9.5	121	13	0.761	-0.1	0.1498	0.3725	0.6625	23.56	46.01
4	8	3090688	349824	468352	87	11	136	11	1.5632	-0.1	0.0086	0.2709	0.8085	21.21	57.07
4	7	2597376	350464	467328	132	18	128	13	0.9697	-0.09	0.0974	0.3333	0.6531	29.07	40.16
4	8	3101952	345792	479872	133	17	130	12.5	0.9774	-0.18	-0.069	0.4028	0.72	20.45	39.56
4	9	3462912	342912	463744	106	5	152	10	1.434	-0.21	-0.151	0.3252	1.0732	14.14	57.7
4	7	2828928	407040	508544	128	15	157	26	1.2266	-0.19	-0.099	0.4011	1.1304	28.07	71.45
4	9	3501696	350336	483200	131	13	137	17	1.0458	-0.18	-0.085	0.3871	0.6525	25.5	44.6
4	8	3351168	441536	478976	91	7	152	18	1.6703	-0.22	-0.126	0.3838	0.9487	19.53	66.89
4	9	3730816	445952	461824	83	6	91	10	1.0964	-0.12	0	0.2778	0.5797	11.66	33.11
4	8	3400576	458816	463744	80	11	98	11.5	1.225	-0.08	0.0161	0.3041	0.5875	15.5	33.84

4	8	3290496	424192	476288	102	10.5	100	9.5	0.9804	-0.08	0.069	0.3345	0.6413	19.94	39.12
4	8	3556352	461568	464384	76	7.5	95	9	1.25	-0.08	0.0087	0.2594	0.5543	19.5	27.31
4	8	3381504	460480	461696	118	12	110	9.5	0.9322	-0.15	-0.02	0.2702	0.7391	19.91	43.42
4	8	3224064	419392	464768	153	20	119	15.5	0.7778	-0.2	0.0051	0.3711	0.7671	21.98	45.54
4	9	3233152	329088	461184	87	13	116	10	1.3333	-0.12	-0.041	0.2582	0.7975	13.89	40.85
4	8	3552000	461312	466688	116	17	142	17	1.2241	-0.14	-0.025	0.3666	0.7935	26.72	55.54

Table (B.5): The calculated authentication features for user five

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
5	42	188107264	468608	2E+08	193	3	227	3.5	1.176	-0.057	0.0283	0.0746	0.5122	6.202	28.16
5	34	16246528	472704	534016	204	5	234	4.5	1.147	-0.074	-0.015	0.0962	0.4581	9	40.02
5	35	83735424	472960	5E+07	197	4	228	6	1.157	-0.054	0.038	0.0729	0.2225	9.055	24.35
5	35	71393024	474368	5E+07	213	5	214	5	1.005	-0.062	0.0321	0.0939	0.4405	9	27.73
5	34	33755264	470784	2E+07	247	7	229	4	0.927	-0.089	-0.006	0.0711	0.4224	9.327	36.4
5	38	18872064	468736	1E+06	186	4	230	4	1.237	-0.045	0.033	0.071	0.229	7.536	25.63
5	26	12389760	468608	543360	277	10	241	5	0.87	-0.145	-0.06	0.1181	0.6531	14.88	55.23
5	39	76422016	471680	6E+07	194	4	260	4	1.34	-0.071	-0.02	0.0931	0.4013	7.81	30.02
5	34	35968128	501056	2E+07	216	6	209	4	0.968	-0.079	0.01	0.0848	0.449	7.936	33.62
5	30	14495616	469824	551296	200	7	258	6.5	1.29	-0.05	0.0477	0.127	0.4679	10.6	31.78
5	30	14276352	470272	540928	198	5.5	254	6.5	1.283	-0.068	0.0162	0.1056	0.4486	11.05	27.29
5	29	31124736	472960	2E+07	215	6	221	6	1.028	-0.061	0.064	0.1217	0.422	12	22.2
5	27	31053952	472704	2E+07	201	8	205	5	1.02	-0.091	-0.012	0.0981	0.2727	13.45	23.02
5	32	38927488	468672	2E+07	270	6	286	5	1.059	-0.069	0.1174	0.1467	0.7429	11	47.38
5	31	29425792	468608	1E+07	235	7	230	6	0.979	-0.087	0.0309	0.0992	0.4545	11.66	29.73
5	35	31591296	468608	2E+07	278	6	274	6	0.986	-0.105	-0.026	0.1266	0.5455	9.22	39.41
5	34	16094336	468608	624896	242	6	264	5	1.091	-0.088	0	0.1001	0.4255	9.768	34.01
5	32	14996480	468608	472832	176	5	224	4.5	1.273	-0.061	0.0379	0.1214	0.5085	8.303	33.53
5	32	14838656	468736	624512	222	7	215	3	0.968	-0.08	0.0306	0.0976	0.5134	9.68	26.93
5	33	15346560	468608	472832	203	5	265	6	1.305	-0.083	-0.008	0.0976	0.4829	11.05	35.51
5	27	12575616	468736	473088	188	5	195	4	1.037	-0.031	0.1754	0.0981	0.4479	10.77	34.41
5	32	31727104	468672	2E+07	278	7	256	6.5	0.921	-0.09	0.0347	0.1019	0.5561	11.52	44.38

5	34	33068800	468672	1E+07	199	5	195	3.5	0.98	-0.056	0.0598	0.0761	0.2949	9.055	23.19
5	33	15773696	468608	781824	291	8	286	9	0.983	-0.081	0.0821	0.1215	0.4626	12.81	40
5	33	33610624	468736	2E+07	230	6	246	5	1.07	-0.085	0.0043	0.1096	0.3883	10.77	26.42
5	33	15465088	468736	473600	185	5	214	5	1.157	-0.072	-0.008	0.1008	0.4096	8.602	29.73
5	32	14842112	468608	472704	225	6	220	4.5	0.978	-0.091	0.0149	0.101	0.4539	10.65	25.06
5	37	33602816	468608	2E+07	216	5	241	5	1.116	-0.083	-0.043	0.096	0.3262	8.062	27.02
5	34	32946560	468608	2E+07	215	4.5	205	5	0.953	-0.085	-0.021	0.0635	0.2851	9.528	26.08
5	33	15655040	468736	781056	178	4	174	3	0.978	-0.073	0.032	0.0735	0.3936	7.071	24.17

Table (B.6): The calculated authentication features for user six

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
6	33	55907840	468608	3.7E+07	300	5	254	3	0.8467	0.0819	0.245	0.0182	0.3617	12.17	53
6	41	43121920	468736	2E+07	406	4	264	4	0.6502	0.0787	0.16	0.0307	0.3404	7.211	94
6	46	26886144	468736	2807552	358	2.5	240	4	0.6704	0.0555	0.094	0.0177	0.2344	5.465	68.3
6	46	83270784	468736	3.2E+07	246	2	209	2	0.8496	0.0561	0.106	0.0147	0.2394	5.398	36
6	41	45561856	468736	2.4E+07	199	3	271	5	1.3618	0.0378	0.086	0.0142	0.2051	7.616	29.4
6	39	62254848	468736	4.2E+07	259	3	189	4	0.7297	0.0425	0.068	0.0224	0.1673	7.211	36.3
6	48	48126720	468736	2.3E+07	269	2	243	4	0.9033	0.0448	0.122	0.0225	0.1915	5.55	36.3
6	41	21751040	468608	1592320	273	2	277	4	1.0147	0.0491	0.167	0.0128	0.2394	7.071	52.4
6	35	18905856	468608	1250176	303	4	283	8	0.934	0.0926	0.269	0.0223	0.3333	12.04	43.4
6	31	43075200	468736	2.3E+07	424	3	274	9	0.6462	0.0701	0.139	0.0233	0.3	14.42	128
6	36	51372288	468736	2.9E+07	277	3	263	7	0.9495	0.0602	0.099	0.032	0.1755	8.911	43.7
6	34	19526784	468736	1562112	331	4	288	9	0.8701	0.0658	0.139	0.0281	0.2567	10.91	60
6	45	78423168	468736	5.3E+07	321	3	264	4	0.8224	0.0524	0.081	0.0339	0.2181	8.544	61
6	46	56658432	468672	3E+07	283	3	348	6	1.2297	0.0579	0.191	0.0357	0.5957	9.216	64
6	39	19555840	468736	1245440	281	4	270	6	0.9609	0.0547	0.117	0.0326	0.3913	9.849	52
6	43	23921792	468864	2099072	292	4	303	5	1.0377	0.0552	0.108	0.0282	0.3085	11	36
6	43	23492736	468736	1562112	303	4	312	6	1.0297	0.0555	0.1	0.0413	0.2567	9.487	38.2
6	39	19689856	468736	1254784	406	3	303	7	0.7463	0.0546	0.106	0.0411	0.2766	10.2	116
6	41	22406528	468736	1563904	336	3	365	9	1.0863	0.0631	0.115	0.03	0.2553	11.4	65.9

6	37	19899136	468736	1405824	296	3	257	5	0.8682	0.0562	0.101	0.0377	0.2926	9.487	72
6	47	22816640	468736	937344	244	2	348	7	1.4262	0.0416	0.117	0.0314	0.2234	7.28	42
6	44	21535360	468608	1090688	292	2	395	9	1.3527	0.0549	0.21	0.0352	0.3966	12.32	63.1
6	48	24598144	468608	1247616	302	2	398	7	1.3179	0.0543	0.191	0.0438	0.4332	10.22	71.4
6	41	20619776	468608	1248384	362	2	361	10	0.9972	0.075	0.194	0.0232	0.3529	12.21	58
6	46	48896128	468736	2.4E+07	313	2	386	6	1.2332	0.048	0.077	0.0117	0.1269	6.854	76.3
6	42	54801408	468608	3.2E+07	271	3	454	10	1.6753	0.0594	0.117	0.031	0.2109	12.54	43.1
6	39	21207296	468736	1252096	445	4	332	8	0.7461	0.0702	0.129	0.0315	0.2313	11.31	97
6	54	37257728	468736	4292480	281	1	313	4.5	1.1139	0.0241	0.048	0.0122	0.0528	6.708	59.7
6	48	44829440	468608	2.1E+07	269	2.5	469	8	1.7435	0.0585	0.133	0.0299	0.3096	10	35.1
6	50	60384000	468672	3.5E+07	263	1.5	463	8.5	1.7605	0.0509	0.175	0.035	0.3632	10.02	41.8

Table (B.7): The calculated authentication features for user seven

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
7	19	8908544	468736	473088	169	7	262	11	1.5503	0.087	0.184	-0.076	0.234	15.26	44
7	16	7498240	468608	472832	168	9	275	12.5	1.6369	0.1169	0.229	-0.098	0.3696	18.16	55.6
7	16	7185920	468032	471552	217	10.5	279	11	1.2857	0.1493	0.326	-0.123	0.0851	18.1	60.4
7	17	17977856	468608	1.1E+07	195	8	288	17	1.4769	0.125	0.193	-0.114	0.4348	20.88	47.9
7	20	9375872	468608	472704	170	6	237	9.5	1.3941	0.0779	0.155	-0.059	0.1702	10.92	49.6
7	21	82661504	468736	7.3E+07	174	6	265	7	1.523	0.1087	0.262	-0.11	0.1489	12.37	43.5
7	20	27598848	468544	1.9E+07	186	5.5	234	7.5	1.2581	0.0809	0.175	-0.082	0.1522	14.52	47.8
7	20	35597056	468672	2.1E+07	195	5	202	6	1.0359	0.1117	0.234	-0.083	0.0426	14.19	57.9
7	24	11561856	468608	939392	192	4.5	258	9	1.3438	0.0718	0.14	-0.071	0.1183	9.528	55.1
7	19	8930560	468608	625152	143	5	224	5	1.5664	0.0982	0.2	-0.08	0.0851	13	39.4
7	24	54713216	468672	4.4E+07	227	6.5	189	7.5	0.8326	0.1073	0.168	-0.055	0.0745	12.5	37.9
7	16	7498240	468672	472832	198	10	302	10	1.5253	0.1006	0.197	-0.104	0.1489	21.7	57
7	18	8909952	468672	1091712	281	7	266	11	0.9466	0.0933	0.183	-0.125	0.2553	20.25	81
7	17	30157056	468608	2.3E+07	249	11	295	17	1.1847	0.1258	0.298	-0.099	0.4565	20.62	68.3
7	16	7498240	468608	472832	232	9	325	15.5	1.4009	0.1314	0.197	-0.083	0.4468	21.18	66.9
7	20	25782144	468544	1.7E+07	204	5	232	9	1.1373	0.1248	0.261	-0.122	0.1489	13.01	45.9
7	20	9216640	468608	471424	227	6	255	12.5	1.1233	0.1263	0.277	-0.082	0.234	13.83	41.4
7	17	7973888	468736	474240	220	7	317	15	1.4409	0.1098	0.184	-0.16	0.1489	23.71	55.6
7	17	24657920	468736	1.6E+07	216	7	292	16	1.3519	0.1277	0.286	-0.159	0.1277	21.84	52.8
7	17	7848320	468608	473472	210	7	281	12	1.3381	0.0851	0.128	-0.135	0.0638	22.02	61.1
7	18	8149888	468608	472960	223	9	243	11.5	1.0897	0.1336	0.273	-0.089	0.2826	17.42	51.2
7	18	8283520	468608	472704	100	3.5	233	10.5	2.33	0.052	0.109	-0.091	0.1522	13.97	41

7	19	24733312	468736	1.6E+07	158	6	245	8	1.5506	0.0691	0.144	-0.114	0.1064	14.42	49.9
7	18	8478848	468672	508800	197	6.5	237	10.5	1.203	0.0675	0.151	-0.092	0.0851	14.97	61.1
7	18	22331392	468672	1.4E+07	210	6.5	357	15.5	1.7	0.1036	0.181	-0.154	0.1505	19.93	69.4
7	16	7665792	469504	680960	213	8.5	291	13.5	1.3662	0.0957	0.17	-0.107	0.234	19.85	53.7
7	18	21764224	468608	1.4E+07	186	4.5	236	12.5	1.2688	0.0557	0.12	-0.094	0.1702	16.56	47.4
7	19	9062144	468608	624896	182	7	247	10	1.3571	0.0888	0.191	-0.09	0.2128	13.34	58.6
7	19	20690176	468608	1.2E+07	144	4	217	10	1.5069	0.0518	0.112	-0.103	0.1064	13.04	42.4
7	19	85044224	468608	7.7E+07	171	6	235	10	1.3743	0.1053	0.209	-0.064	0.2609	14.42	55.7

Table (B.8): The calculated authentication features for user eight

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
8	25	11715968	468736	5E+05	155	3	62	2	0.4	-0.023	0.0032	-0.005	0.0638	3.606	24.19
8	28	18885376	468608	3E+06	190	2	101	3	0.532	-0.022	0.008	-0.017	0.0904	5.05	31.78
8	26	13748736	468608	1E+06	178	4	54	1	0.303	-0.029	0.0202	-0.013	0.0745	5.957	22.56
8	31	17353984	468736	2E+06	157	2	56	1	0.357	-0.016	0.0151	-0.011	0.032	2	23.09
8	32	18347776	468608	2E+06	121	1.5	80	2	0.661	-0.02	0	0.0165	0.116	3.581	21
8	35	49245824	468736	2E+07	168	2	67	2	0.399	-0.02	0	0	0.0638	3.162	27.66
8	24	50847616	468736	3E+07	149	2	52	1	0.349	-0.032	-0.016	0.0056	0.1348	4.062	37
8	26	15461120	468672	2E+06	173	2	89	3	0.514	-0.028	0.0216	-0.012	0.1071	5.465	28.44
8	23	68114048	469888	5E+07	188	2	51	1	0.271	-0.021	0.0081	-0.002	0.1075	4.472	37.48
8	28	14840320	468736	1E+06	302	2.5	97	2.5	0.321	-0.023	0	0.0167	0.078	5	67
8	31	18433280	469120	1E+06	133	2	55	1	0.414	-0.014	0	0.0124	0.0857	2.828	23.35
8	26	14083584	468736	2E+06	182	1.5	58	1	0.319	-0.01	0.0071	-0.004	0.0988	3	45
8	22	11723776	468736	2E+06	273	3.5	91	2.5	0.333	-0.014	0.0401	0.003	0.1149	7.64	51
8	26	14375680	468736	2E+06	196	3	87	2	0.444	-0.032	0.0208	0.0079	0.088	5.521	47
8	22	49925632	468928	4E+07	201	3	86	2	0.428	-0.024	0.0099	0.0175	0.1782	6.723	35
8	23	13279232	468608	2E+06	168	4	74	2	0.44	-0.048	0	-0.006	0.189	5.657	31.06
8	22	11095296	469248	9E+05	178	3.5	66	1	0.371	-0.056	0	-0.011	0.1505	7.14	31
8	23	42167040	468736	3E+07	201	3	67	2	0.333	-0.047	0.0179	0.0016	0.123	6.083	36
8	22	11036416	468736	1E+06	228	2	66	2.5	0.289	-0.035	0.0344	-0.016	0.0766	3.864	65
8	20	47960320	468672	4E+07	159	1.5	58	2	0.365	-0.023	0.0263	0.0137	0.129	4.062	46.39
8	22	44644224	468672	3E+07	164	1.5	62	3	0.378	-0.022	0	0.0121	0.1346	4.236	43.29
8	26	12423680	468608	8E+05	260	4	95	1.5	0.365	-0.05	0	0.0055	0.1246	9.048	48
8	25	50799232	468736	4E+07	259	3	120	3	0.463	-0.042	0.0217	0.0204	0.2571	8.602	55

8	24	41147264	468800	3E+07	236	3.5	106	3	0.449	-0.069	0.0162	0.0018	0.1844	6.724	47.8
8	24	11881088	468672	9E+05	209	2.5	60	2	0.287	-0.027	0	0.0063	0.1064	5.465	44.28
8	23	69604096	468608	6E+07	204	3	73	2	0.358	-0.032	0.0017	0.0102	0.1225	4	54.33
8	22	38525952	468672	2E+07	211	2	63	1	0.299	-0.023	0.0424	-0.005	0.1522	6.541	53.6
8	20	10343168	468608	1E+06	185	2.5	80	3	0.432	-0.037	0.005	0.0145	0.2258	5.744	55.73
8	23	54279936	468864	4E+07	204	3	93	2	0.456	-0.051	-0.007	0.0032	0.2086	7.28	36.67
8	19	38142336	468736	3E+07	236	2	59	3	0.25	-0.034	0.0555	-0.009	0.1809	4.243	56

Table (B.9): The calculated authentication features for user nine

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
9	61	44072704	468608	1.4E+07	443	6	419	6	0.9458	0.0638	0.153	-0.082	0.1151	10.77	28.6
9	82	42062080	468608	2380544	477	6	381	3.5	0.7987	0.0808	0.155	-0.049	0.0895	8.515	29.4
9	70	38106496	468736	2958336	390	4	442	4	1.1333	0.0722	0.135	-0.074	0.0996	7.64	38.9
9	71	84790656	468608	5E+07	460	5	374	5	0.813	0.0814	0.145	-0.069	0.0826	8.246	21
9	87	73302784	468736	3E+07	358	3	386	4	1.0782	0.0426	0.109	-0.046	0.0859	6.403	18
9	85	74635008	468608	3.3E+07	399	4	468	5	1.1729	0.0606	0.118	-0.046	0.1197	7.81	27.8
9	95	66016512	468608	1.9E+07	432	4	525	5	1.2153	0.0663	0.13	-0.053	0.1006	7.071	21.2
9	73	34842368	468608	937216	347	4	429	6	1.2363	0.0639	0.123	-0.062	0.1079	7.81	22.8
9	84	40908928	468608	1855616	395	4	487	5	1.2329	0.0524	0.135	-0.05	0.1343	7.211	28.4
9	70	34117248	468608	1874560	366	4	470	7	1.2842	0.0628	0.128	-0.075	0.1327	9.22	24.7
9	86	58324224	468608	1.7E+07	387	4	474	5	1.2248	0.0681	0.156	-0.088	0.1229	7.246	23
9	63	29528448	468608	472960	441	5	506	6	1.1474	0.0896	0.146	-0.077	0.1415	12	31.3
9	71	57998976	468608	1.8E+07	404	4	461	6	1.1411	0.0639	0.111	-0.085	0.1286	9.22	24.2
9	66	31867520	468672	1247872	386	5	497	6.5	1.2876	0.0689	0.113	-0.083	0.1345	10.37	25.7
9	70	51325184	468672	1.8E+07	430	4.5	492	7	1.1442	0.0883	0.149	-0.091	0.1363	10.1	23.3
9	64	30774016	468608	937344	425	6	463	5.5	1.0894	0.0851	0.129	-0.087	0.1275	10.17	24
9	60	28118272	468608	472832	325	3	405	6	1.2462	0.0516	0.086	-0.078	0.1075	10.02	24.5
9	63	29839104	468608	624896	374	5	461	7	1.2326	0.0691	0.164	-0.073	0.1297	9.22	35.4
9	65	50990080	468736	1.8E+07	351	4	489	7	1.3932	0.064	0.114	-0.072	0.1399	10.44	22.8
9	52	24555008	468608	778496	398	6	452	8	1.1357	0.1156	0.223	-0.144	0.0944	11.85	28.7
9	68	58313600	468608	2.7E+07	367	4	483	6	1.3161	0.057	0.123	-0.072	0.1364	9.61	25.7
9	62	72996864	468608	4.4E+07	319	5	460	6	1.442	0.0838	0.128	-0.093	0.1247	9.22	28.8
9	63	31088512	468608	1873408	390	5	459	8	1.1769	0.0899	0.132	-0.082	0.1278	11.18	23.7

9	68	56587008	468608	2.5E+07	329	4	444	6	1.3495	0.0814	0.107	-0.068	0.125	8.366	18.4
9	62	29079552	468608	622720	354	5	452	7	1.2768	0.0692	0.156	-0.078	0.1296	10.05	26.8
9	64	73096064	468608	4.2E+07	343	4	454	7.5	1.3236	0.0844	0.14	-0.101	0.1189	9	23.9
9	57	26583936	468736	472960	363	4	448	8	1.2342	0.0688	0.097	-0.101	0.1118	11	23.3
9	62	29430144	468608	629120	341	4	409	6	1.1994	0.0775	0.15	-0.079	0.1193	10.1	21.4
9	58	27371648	468672	624256	337	5	424	7	1.2582	0.0807	0.182	-0.114	0.1026	9.924	27
9	52	145838592	468736	1E+08	348	6	428	8	1.2299	0.0976	0.145	-0.104	0.1098	10.82	32.9

Table (B.10): The calculated authentication features for user ten

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
10	30	77053696	355456	6.7E+07	142	2.5	156	4.5	1.0986	-0.006	0.099	-0.038	0.0135	7.141	19
10	42	15501696	355968	1008256	124	2	123	3	0.9919	0.0076	0.106	-0.015	0.0334	5.05	9.43
10	29	10206208	353664	373504	205	5	283	9	1.3805	0.0018	0.081	-0.028	0.0356	14.32	31.4
10	27	9516032	351616	391552	218	6	216	7	0.9908	0.0233	0.155	-0.043	0.0267	10.05	39.1
10	34	12416256	345792	903296	204	4.5	206	5	1.0098	0.008	0.086	-0.036	0.0339	8.062	34
10	43	15350400	352384	418560	199	3	191	4	0.9598	0.0183	0.144	-0.012	0.0488	7	21.1
10	34	12051200	354816	397056	177	3.5	187	4.5	1.0565	0.0168	0.105	-0.023	0.0338	7.616	29.5
10	38	14392576	358336	503168	150	3	118	3	0.7867	0.0161	0.077	-0.009	0.0102	4.562	20.6
10	31	11001344	351744	395904	197	5	156	4	0.7919	-0.008	0.051	-0.023	0.0262	7.071	29.2
10	41	14631680	358016	417664	193	3	116	3	0.601	0.0062	0.064	-0.007	0.031	5	29.4
10	35	13154688	349312	793600	167	3	124	3	0.7425	0.0147	0.096	-0.013	0.0212	4.243	33.1
10	44	16288000	350720	697344	154	2	129	2	0.8377	0.0093	0.042	-0.01	0.0353	3.606	38.5
10	40	13934464	347904	377728	163	2.5	136	3	0.8344	0.0135	0.078	-0.013	0.0265	5.242	18.2
10	31	11005696	352640	387968	298	4	153	4	0.5134	0.0043	0.252	-0.031	0.0141	10	36.1
10	28	9887616	355776	396800	135	3	198	5	1.4667	0.0059	0.062	-0.045	0.0205	7.14	24.1
10	29	10162048	347648	385408	187	5	242	7	1.2941	0.0095	0.128	-0.062	0.0236	13	26.2
10	28	9737856	347392	369664	233	5	226	6	0.97	0.0348	0.26	-0.071	0.0061	12.22	34
10	34	12776576	354176	500864	198	3	233	6	1.1768	0.0118	0.108	-0.035	0.0216	10.41	30.1
10	44	15977600	356096	726912	159	2	163	3	1.0252	0.0064	0.079	-0.005	0.0556	5	22.1
10	30	10464000	348224	390912	236	5	225	7	0.9534	0.0183	0.212	-0.039	0.0214	11.89	29.5
10	33	11987200	323456	481280	282	6	209	4	0.7411	0.0171	0.153	-0.026	0.0371	9.22	34.8
10	31	11481728	352768	470400	252	4	203	4	0.8056	0.0411	0.196	-0.03	0.0152	8.944	44.7
10	38	13775616	352832	634112	257	4	151	3	0.5875	0.0257	0.258	-0.018	0.0097	9.22	30.1

10	36	12733056	353856	422016	233	3.5	224	4	0.9614	0.0203	0.249	-0.039	0.0158	8.145	31.1
10	25	10092672	355200	1414144	284	7	256	7	0.9014	0.014	0.152	-0.054	0.0244	15.65	62.8
10	37	26383104	355712	1.3E+07	229	4	163	4	0.7118	0.0098	0.096	-0.018	0.009	7.211	25
10	35	13642752	348544	1766016	319	5	177	5	0.5549	0.0225	0.189	-0.022	0.0121	8.944	44.9
10	53	19620608	351744	873344	173	2	104	1	0.6012	0.0147	0.068	-0.007	0.0322	3.162	16.5
10	37	14247168	354176	856320	225	4	146	3	0.6489	0.0304	0.127	-0.004	0.0357	7.071	38.3
10	37	13676672	354432	803328	269	6	139	3	0.5167	0.019	0.149	-0.002	0.032	7.211	33.1

Table (B.11): The calculated authentication features for user eleven

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
11	35	16583424	468608	625024	168	2	302	8	1.7976	0.073	0.237	0.0274	0.3656	9.487	37
11	33	30885888	468736	1.4E+07	191	4	315	7	1.6492	0.0831	0.301	0.0388	0.5914	8.602	40.2
11	32	32919424	468608	1.8E+07	151	2	339	8	2.245	0.0736	0.28	0.0497	0.6129	10.15	43.8
11	31	14528896	468736	473216	132	1	287	8	2.1742	0.0766	0.277	0.0391	0.5319	10	31.8
11	32	26406144	468672	1.2E+07	158	2	311	7.5	1.9684	0.0722	0.269	0.0322	0.3333	9.709	33.1
11	29	13590400	468608	472832	168	3	251	9	1.494	0.0939	0.362	0.0469	0.4787	10.05	28.8
11	31	39068672	468608	2.5E+07	128	2	208	3	1.625	0.0831	0.287	0.039	0.3936	6	26.9
11	28	13907456	468672	781952	128	2	181	4	1.4141	0.0734	0.438	0.0188	0.5417	7.729	33.4
11	30	24709376	468608	1.1E+07	157	1.5	279	7.5	1.7771	0.0804	0.255	0.0383	0.4894	12	45
11	30	29551104	468736	1.5E+07	136	2.5	232	5.5	1.7059	0.069	0.161	0.0295	0.3441	9.015	32.8
11	27	12500736	468608	622592	152	3	188	3	1.2368	0.0762	0.213	0.0231	0.5319	9.055	42
11	29	26944384	468608	1.4E+07	118	1	170	4	1.4407	0.0766	0.304	0.016	0.4783	7.071	26.1
11	31	28584320	468608	1.4E+07	165	1	200	3	1.2121	0.0904	0.287	0.0246	0.4043	5.657	30.4
11	27	12499712	468608	472832	159	3	235	6	1.478	0.0992	0.383	0.0293	0.4468	9.434	37.2
11	27	13119744	468608	781056	140	2	222	5	1.5857	0.0772	0.34	0.0194	0.5106	8.944	37.8
11	28	13743872	468608	785280	146	2	263	6	1.8014	0.0896	0.255	0.0586	0.6064	8.109	39.2
11	29	36571392	468736	2.3E+07	116	1	199	4	1.7155	0.0669	0.255	0.0305	0.4362	5	31.3
11	27	29309056	468608	1.7E+07	145	2	217	6	1.4966	0.0741	0.239	0.025	0.5	8.246	37
11	28	37645696	468736	1.4E+07	153	2	208	6	1.3595	0.1024	0.362	0.0323	0.4255	8.559	25.6
11	28	24677504	468672	1.2E+07	136	0.5	207	4.5	1.5221	0.0827	0.25	0.0322	0.4375	7.972	32.8
11	29	40515200	468608	1.4E+07	157	1	245	4	1.5605	0.0777	0.277	0.0422	0.5532	10.05	37.1
11	29	23727872	468608	1.1E+07	142	1	223	7	1.5704	0.0894	0.277	0.0256	0.5	9	36.4
11	28	26581248	468608	1.4E+07	146	3	242	6	1.6575	0.0963	0.309	0.0305	0.4681	9.056	40.5

11	28	12965504	468608	472704	138	2	169	4.5	1.2246	0.0814	0.183	0.0342	0.3043	8.366	26.9
11	27	12499968	468608	472832	132	2	216	7	1.6364	0.0804	0.117	0.029	0.3511	10	28.3
11	27	46572800	468608	2.1E+07	130	4	196	5	1.5077	0.0725	0.191	0.029	0.3617	8.602	25.2
11	28	23639808	468608	1.1E+07	157	3	235	6.5	1.4968	0.0896	0.255	0.0403	0.4681	11.1	31.1
11	26	12201472	468672	626176	157	2	176	5	1.121	0.0881	0.234	0.0118	0.3978	7.434	29.1
11	24	28676096	468608	1.8E+07	121	2.5	215	5.5	1.7769	0.0868	0.234	0.0407	0.5319	11.09	31.1
11	25	49921792	468864	1.7E+07	121	1	209	7	1.7273	0.0926	0.34	0.0342	0.5106	10	28.8

Table (B.12): The calculated authentication features for user twelve

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
12	83	38763904	468608	472960	207	2	319	4	1.5411	0	0.018	-0.019	0.0442	5	14.9
12	80	37197568	468608	624896	193	2	251	3	1.3005	0	0.021	-0.021	0.0433	4.472	13
12	89	41839360	468608	784256	225	2	305	3	1.3556	0	0.03	-0.016	0.05	5	14.2
12	86	40660736	468608	1137280	211	2	314	4	1.4882	0	0.024	-0.021	0.0488	5	10.3
12	77	37412992	468608	1426944	229	2	356	5	1.5546	-0.001	0.02	-0.034	0.043	6	11
12	72	48131328	468608	1.5E+07	303	4	358	5	1.1815	0.0035	0.026	-0.029	0.0432	7	17.8
12	72	49877760	468672	1.7E+07	239	3	321	5	1.3431	0	0.02	-0.028	0.0333	6	19
12	87	61360384	468736	2.1E+07	254	3	344	4	1.3543	0	0.027	-0.017	0.0573	5	15.8
12	75	65373440	468608	1.3E+07	238	3	357	5	1.5	-0.001	0.012	-0.029	0.0249	6	15.6
12	87	56235264	468608	1.6E+07	232	2	324	3	1.3966	-0.002	0.021	-0.019	0.05	5	13.9
12	79	36935296	468608	622208	234	2	311	4	1.3291	0	0.024	-0.024	0.0472	5.385	12.1
12	71	33278464	468608	475520	246	3	381	6	1.5488	0.0006	0.021	-0.043	0.0382	7.071	14.2
12	86	39759104	468608	472960	273	3	365	4	1.337	0	0.025	-0.018	0.046	6	15.3
12	75	59169024	468608	1.3E+07	233	2	348	5	1.4936	0.0017	0.018	-0.024	0.0196	6.083	14.9
12	76	35962112	468672	937344	230	2	353	4	1.5348	0.0055	0.019	-0.02	0.0574	5.242	18.4
12	71	32777728	468608	472960	256	3	330	5	1.2891	0	0.022	-0.032	0.0268	6.708	23.3
12	78	66104192	468608	1.7E+07	307	3	351	5	1.1433	0.0011	0.024	-0.025	0.0366	6.364	16.5
12	79	53576192	468608	1.7E+07	276	3	370	5	1.3406	0.0017	0.023	-0.019	0.0578	6.403	17.1
12	75	58806784	468608	1.3E+07	250	3	335	4	1.34	0.0045	0.029	-0.028	0.0529	6.083	13.4
12	73	34422784	468608	1405696	310	4	335	5	1.0806	0.0027	0.033	-0.032	0.0304	7.28	16.3
12	87	80330112	468608	3.8E+07	230	2	340	4	1.4783	0	0.029	-0.031	0.05	5	10.3
12	81	37833216	468608	475008	287	2	371	5	1.2927	0	0.02	-0.024	0.036	6.325	26.3
12	79	53843456	468608	1.7E+07	272	3	365	4	1.3419	0.0011	0.024	-0.022	0.0368	6	20.1

12	78	52859008	468608	1.6E+07	305	3	328	3.5	1.0754	0.0008	0.021	-0.022	0.045	6.202	17.3
12	81	37841792	468608	480512	328	4	336	5	1.0244	0	0.03	-0.028	0.0472	6.403	19.1
12	88	53599872	468608	1.3E+07	295	3	301	3	1.0203	-0.002	0.034	-0.016	0.0432	5.521	12.1
12	76	48446464	468608	1.4E+07	318	3.5	357	5	1.1226	0	0.024	-0.03	0.0344	6.403	22.1
12	79	37808384	468608	1251456	316	3	340	4	1.0759	0	0.028	-0.024	0.0495	6	20
12	74	54078336	468608	2E+07	224	2	299	3	1.3348	0	0.016	-0.021	0.0322	5.099	22.8
12	71	47587456	468608	1.5E+07	295	4	285	4	0.9661	-8E-04	0.018	-0.022	0.0359	6.083	15.6

Table (B.13): The calculated authentication features for user thirteen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
13	17	6434304	365056	535296	247	3	77	4	0.3117	0	0.274	0.0218	0.1782	6.083	68.2
13	18	6490368	351552	549632	253	5	94	3	0.3715	-0.059	0.189	0.0511	0.4118	14.23	54.9
13	19	7202048	356608	657664	297	6	106	3	0.3569	0.0144	0.346	0.0599	0.3364	11.4	79.6
13	18	6485248	360768	397696	261	3	142	4	0.5441	0.0035	0.342	0.09	0.4286	10.89	126
13	21	10296576	368640	1391488	171	2	68	1	0.3977	0	0.168	0.0157	0.3824	3.162	68.1
13	17	7234816	361472	1088000	186	3	65	2	0.3495	0.0094	0.209	0.0372	0.2029	4.472	58.1
13	18	25866624	345664	2E+07	333	4	107	3.5	0.3213	0.0559	0.383	0.0419	0.1695	7.906	118
13	16	6193152	359872	681600	224	5.5	103	4.5	0.4598	0.0281	0.288	0.0414	0.3026	11.61	61
13	14	5381504	365440	629504	243	4.5	120	8	0.4938	-0.028	0.338	0.0155	0.2778	10.09	110
13	19	25231616	367488	1.7E+07	237	2	97	3	0.4093	0.0284	0.277	0.0328	0.2476	6.083	76
13	16	5853824	348416	630528	250	5	71	3.5	0.284	0.0058	0.317	0.0639	0.3143	9.816	70.5
13	17	6238336	356224	553472	157	3	81	3	0.5159	0	0.179	0.0599	0.4857	5.385	46.5
13	18	7377536	344512	1097600	204	1	80	2.5	0.3922	-0.034	0.223	0.0395	0.3824	3.864	57.7
13	19	8186752	356736	1245056	195	1	71	3	0.3641	-0.008	0.18	0.0297	0.1884	5.099	49.5
13	28	12823936	342144	1575424	249	1	71	1.5	0.2851	-0.004	0.171	0.0365	0.1547	2.236	109
13	18	23436160	343680	1.7E+07	208	3	81	3.5	0.3894	0.0291	0.267	0.0362	0.2453	7.536	91.1
13	19	7646464	372736	508288	208	5	64	2	0.3077	-0.007	0.198	0.0482	0.2621	9.434	44
13	19	7711104	334464	961536	176	2	52	1	0.2955	-0.015	0.176	0.0387	0.2985	7.211	52
13	20	27721856	346432	1.9E+07	189	3	59	1	0.3122	-0.048	0.182	0.0191	0.2388	6.041	66.2
13	15	6196224	349184	882304	242	3	53	2	0.219	-0.039	0.337	0.0444	0.3623	7.28	97
13	15	25091456	385792	1.6E+07	201	3	61	2	0.3035	-0.056	0.233	0	0.1829	6.403	85
13	16	5749248	350400	498304	287	6	87	3.5	0.3031	-0.051	0.33	0.0133	0.3824	10.85	86.4
13	15	6062464	359040	987136	175	4	50	3	0.2857	0.0097	0.196	0.0292	0.2941	8.062	51.1

13	15	6792704	351872	958080	199	4	56	2	0.2814	0	0.239	0.0117	0.1611	7.071	89
13	14	7694464	366464	1518336	257	2	39	2	0.1518	-0.013	0.295	0.0126	0.169	3.924	99
13	15	28399360	372736	2.1E+07	186	2	60	2	0.3226	-0.065	0.206	0.0279	0.1835	7.28	79
13	14	28128768	365504	2.1E+07	183	4	62	3	0.3388	-0.077	0.21	0.0281	0.338	12.06	61
13	13	34757888	367872	2.4E+07	267	2	80	3	0.2996	-0.034	0.378	0.0314	0.2535	8.062	143
13	17	6931072	359680	921216	158	1	39	0	0.2468	-0.028	0.179	0.0154	0.25	2.828	51
13	17	7545600	349440	1411712	223	3	56	2	0.2511	-0.045	0.246	0.0123	0.2778	6.403	83

Table (B.14): The calculated authentication features for user fourteen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
14	25	193389440	470400	1E+08	168	6	200	6	1.1905	-0.001	0.0284	0.0879	0.224	10.82	25
14	33	35182976	468736	2E+07	191	5	205	5	1.0733	-0.002	0.0293	0.07	0.1534	9.055	22.8
14	29	33369216	468608	2E+07	158	4	157	5	0.9937	-0.005	0.0274	0.054	0.1228	8	24.41
14	33	34090880	468608	2E+07	197	5	167	4	0.8477	-0.014	0.0189	0.0469	0.0916	9.055	19.92
14	24	28717696	468608	2E+07	182	7.5	153	4.5	0.8407	-0.007	0.0364	0.0832	0.1663	10.45	25.55
14	26	11932288	468608	472960	182	7	160	4	0.8791	-0.004	0.0356	0.0787	0.1734	10.02	24.84
14	28	13126912	468608	475008	192	5	151	5	0.7865	-0.02	0.0091	0.0564	0.1085	9.61	25
14	27	29530752	468608	2E+07	191	6	172	5	0.9005	-0.009	0.0301	0.0703	0.1502	9.22	30.23
14	23	10782080	468608	472704	182	6	165	8	0.9066	-0.014	0.0241	0.0844	0.1947	11.18	31.38
14	23	28656128	468608	2E+07	190	7	180	6	0.9474	-0.019	0.0223	0.0875	0.2104	12.53	26.93
14	26	26524160	468736	1E+07	208	6.5	209	7	1.0048	-0.028	0.0016	0.0882	0.2226	13.04	25.5
14	27	25777280	468736	1E+07	180	5	164	5	0.9111	0.0023	0.0411	0.0669	0.156	9	30.87
14	32	28258432	468736	1E+07	194	5	198	6	1.0206	0.0015	0.0398	0.0735	0.1566	8.801	32.7
14	28	26571008	468608	1E+07	134	4	172	5.5	1.2836	-0.017	0.0031	0.0695	0.1601	8.031	18.03
14	26	39071744	468736	3E+07	186	5	185	7	0.9946	-0.027	0.003	0.0648	0.1581	10.72	29.55
14	38	32611200	468672	2E+07	150	3.5	167	4	1.1133	-0.004	0.0158	0.0393	0.0884	6.325	16.64
14	29	35935872	468608	2E+07	170	5	184	6	1.0824	-0.032	-0.006	0.0723	0.1635	8.602	22.56
14	34	15933696	468608	472704	133	3.5	142	3	1.0677	-0.01	0.0094	0.0424	0.0985	6.556	13.6
14	36	48261888	468736	2E+07	180	4	176	5	0.9778	-0.008	0.0179	0.0409	0.0966	7.905	18.97
14	36	32726400	468736	2E+07	190	4	184	4	0.9684	-0.008	0.0213	0.0581	0.1115	7.246	19.24
14	30	14058240	468608	472832	170	5.5	163	4	0.9588	-0.029	-0.001	0.0328	0.1096	8.154	17.89
14	28	12995712	468608	473088	171	4.5	157	5	0.9181	-0.013	0.012	0.057	0.1208	8.154	22.47
14	28	38730112	468608	3E+07	183	5	171	6	0.9344	-0.008	0.0285	0.0609	0.1453	8.531	25

14	28	28593024	468608	2E+07	161	4.5	138	5	0.8571	-0.005	0.0296	0.06	0.1165	8.303	25.3
14	31	26689024	468608	1E+07	166	4	150	4	0.9036	-0.011	0.0188	0.0616	0.1359	7.28	20.22
14	25	11721600	468736	475392	166	6	165	7	0.994	-0.015	0.0125	0.0828	0.1818	10	24.84
14	23	24642432	468736	1E+07	139	5	174	8	1.2518	-0.017	0.016	0.0769	0.1787	11.4	19.24
14	32	29281920	468672	2E+07	127	3	155	4	1.2205	0.0056	0.0229	0.0555	0.1267	7.616	14.56
14	25	23222784	468608	1E+07	158	6	167	5	1.057	-0.011	0.0197	0.0808	0.1947	9.434	21.93
14	39	56341376	468736	2E+07	164	4	155	4	0.9451	-0.013	0.0059	0.0409	0.0825	6	15.62

Table (B.15): The calculated authentication features for user fifteen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
15	51	41124736	335104	2E+07	177	2	307	4	1.7345	0.0609	0.212	-0.006	0.2879	6	35.5
15	54	48574336	347584	2.8E+07	188	2.5	314	5	1.6702	0.0681	0.196	-0.015	0.1915	7.071	25.7
15	50	35682816	351744	1.7E+07	176	2	372	5	2.1136	0.0529	0.136	-0.02	0.1143	7.343	25
15	59	23644288	333056	1003520	161	2	287	3	1.7826	0.0442	0.087	-0.019	0.0744	4.472	19.6
15	48	20147456	341952	965504	162	3	315	5.5	1.9444	0.0566	0.117	0.0007	0.2469	7.343	29.8
15	54	12264524	345088	7.9E+07	216	3	315	4	1.4583	0.0371	0.112	-0.012	0.1429	6.662	28.3
15	53	38133504	337024	1.8E+07	188	2	286	3	1.5213	0.0386	0.103	-0.022	0.1818	5.831	24
15	46	47125888	349888	1.3E+07	189	2	315	4	1.6667	0.0748	0.185	-0.006	0.1733	7.246	32.2
15	48	37701120	335104	2E+07	161	3	231	3	1.4348	0.0543	0.132	-0.018	0.1212	5.828	28.4
15	41	16315648	335616	830336	175	3	244	4	1.3943	0.0815	0.228	-0.023	0.24	7.071	23.4
15	53	21055360	345984	622336	169	2	239	3	1.4142	0.0345	0.107	-0.026	0.065	6.325	15.1
15	46	19468288	364800	771968	187	2.5	262	3	1.4011	0.0595	0.132	-0.03	0.0816	6.541	30.4
15	46	18441984	339392	1026688	174	2	250	3.5	1.4368	0.0614	0.199	-0.037	0.0577	6.516	20.2
15	49	33446912	340480	1.3E+07	182	2	250	4	1.3736	0.0556	0.186	-0.016	0.102	6	21.1
15	45	17325952	344832	910464	165	3	250	4	1.5152	0.0509	0.148	-0.005	0.12	6.708	22
15	37	30643712	337536	1.7E+07	221	3	282	5	1.276	0.0729	0.204	0.0102	0.2234	9.055	38.9
15	41	41989760	358016	2.4E+07	185	4	245	5	1.3243	0.0476	0.102	-0.008	0.1136	8.062	22.6
15	52	54730880	335488	2E+07	213	3	316	4	1.4836	0.0695	0.191	0.0019	0.2647	7.106	30.3
15	46	19644032	337536	1571456	163	2	273	4	1.6748	0.0591	0.173	0.0004	0.1928	7.211	22
15	48	39024768	337600	2.1E+07	175	3	240	4	1.3714	0.0459	0.126	0.0061	0.2353	6.083	21.6
15	43	29987072	344320	1.5E+07	204	3	258	4	1.2647	0.0731	0.193	-0.016	0.0909	8.246	22.8
15	41	16021504	341376	827648	164	2	200	3	1.2195	0.0441	0.139	-0.011	0.0882	6.083	21.6

15	38	16986496	340288	1164032	204	4.5	246	3	1.2059	0.0683	0.141	-0.008	0.0489	8.395	26.9
15	55	78782336	356736	2.6E+07	228	2	213	3	0.9342	0.0582	0.305	-0.014	0.0789	6	26.2
15	40	16726400	340096	1003520	213	3	238	5	1.1174	0.054	0.164	-0.033	0.0909	10	23.3
15	43	32348928	355456	1.2E+07	184	2	269	4	1.462	0.0716	0.213	-0.028	0.0833	8.544	22.5
15	42	37540352	424000	1.9E+07	228	5	258	3.5	1.1316	0.0512	0.167	-0.021	0.0857	8.154	30
15	36	15198592	352448	1012608	233	4	207	3	0.8884	0.0836	0.3	-0.039	0.0857	8.272	30
15	39	15838336	338176	854656	222	4	271	4	1.2207	0.075	0.211	-0.011	0.0714	9.487	34.9
15	50	40500224	360256	1.8E+07	194	2	240	3	1.2371	0.0599	0.197	-0.01	0.0857	5.915	26.9

Table (B.16): The calculated authentication features for user sixteen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
16	26	158581504	468736	1E+08	367	5	110	2.5	0.2997	0.0533	0.447	0.0585	0.0957	5.465	64.8
16	28	14840320	468736	1250688	381	6.5	93	2.5	0.2441	0.0619	0.496	0.0577	0.112	7.659	71.3
16	27	13141376	468608	938496	431	10	98	3	0.2274	0.0745	0.532	0.0818	0.1489	10.44	60
16	32	34218880	468608	1.8E+07	292	5.5	108	3	0.3699	0.0463	0.447	0.0584	0.0697	7.107	49.3
16	23	11182592	468608	1091968	313	8	104	3	0.3323	0.0627	0.43	0.0942	0.1505	8.544	62.5
16	24	11407744	468736	1090048	294	8.5	83	3.5	0.2823	0.0461	0.277	0.064	0.0851	9.082	67.7
16	31	39860480	468608	2.3E+07	329	6	103	3	0.3131	0.0273	0.305	0.0564	0.1206	6.708	80.9
16	28	14840320	468608	2338944	224	4	88	2.5	0.3929	0.0231	0.245	0.0508	0.1064	4.472	69.9
16	42	41479808	468736	2E+07	266	2	101	1	0.3797	0.033	0.234	0.035	0.0566	3.476	63.6
16	23	11091200	468608	779392	280	10	121	5	0.4321	0.0552	0.593	0.1134	0.2593	11.18	64.8
16	27	12968320	468608	777856	317	2	118	2	0.3722	0.0469	0.4	0.0904	0.15	4.123	60.3
16	27	13914880	468608	1249152	243	4	90	2	0.3704	0.0426	0.404	0.0623	0.1489	5	53.9
16	24	12340864	468608	1405824	213	4	79	2	0.3709	0.0274	0.33	0.0652	0.1277	5.608	40.2
16	23	11770240	468608	1249280	309	5	99	2	0.3204	0.0522	0.553	0.0998	0.1915	5.099	49.1
16	23	26297216	468736	1.6E+07	275	3	106	3	0.3855	0.0141	0.426	0.0956	0.2553	4.243	58.4
16	23	27984384	468608	1.7E+07	252	5	91	4	0.3611	0.0354	0.323	0.0798	0.129	6.403	57.1
16	26	34600832	468608	2.3E+07	278	5	80	2	0.2878	0.0404	0.383	0.0448	0.0638	6.075	65.1
16	28	35607040	468608	2.3E+07	299	2	101	2	0.3378	0.0444	0.564	0.0585	0.076	3.476	69.6
16	25	26891136	468608	1.5E+07	313	3	114	5	0.3642	0.0586	0.565	0.098	0.2391	5.099	70.2
16	22	10969344	468608	1090560	338	6	99	4	0.2929	0.0755	0.54	0.0887	0.16	7.503	108
16	21	10306560	468608	777088	309	6	94	4	0.3042	0.034	0.511	0.0638	0.1064	6.708	75.7
16	22	34197504	468608	2.4E+07	262	5.5	102	3.5	0.3893	0.0414	0.362	0.0736	0.0997	7.211	61.8

16	34	45629440	468608	3.1E+07	329	4	103	2	0.3131	0.0523	0.383	0.049	0.1489	5.099	48.7
16	30	14059136	468736	472832	309	6	122	3	0.3948	0.0561	0.266	0.0774	0.117	6.89	56.1
16	23	10939136	468608	628096	287	6	93	3	0.324	0.0515	0.394	0.082	0.1489	6.708	69.1
16	22	10642432	468736	781056	383	10.5	104	2.5	0.2715	0.0563	0.688	0.1065	0.2391	11.21	67
16	23	43967232	468736	3.3E+07	260	3	88	2	0.3385	0.0502	0.409	0.0882	0.1398	8.544	66
16	21	9840768	468608	472320	259	6	73	3	0.2819	0.0256	0.312	0.0576	0.086	6.325	74.5
16	19	9841408	469632	781184	292	8	85	3	0.2911	0.0741	0.766	0.0823	0.1489	10.2	62
16	19	9220992	468608	624896	296	11	66	2	0.223	0.0825	0.766	0.0638	0.1064	11	64.4

Table (B.17): The calculated authentication features for user seventeen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
17	66	33146752	468608	2499072	212	2	196	2	0.9245	-0.015	0.048	0.0025	0.0373	3.606	30.5
17	72	45778048	468736	9145472	242	2	197	1	0.814	-0.017	0.045	0.0026	0.0313	4.123	33.9
17	71	41412480	468736	2564992	250	1	163	1	0.652	-0.011	0.016	0.0045	0.0278	3	29.7
17	74	86597504	468736	4.1E+07	314	2	196	1	0.6242	-0.013	0.02	0.0042	0.0318	2.828	34
17	81	163655808	468736	4.4E+07	252	2	179	1	0.7103	-0.016	0.018	0.0025	0.0206	3	22.6
17	59	36413696	468736	3322368	272	3	170	2	0.625	-0.019	0.024	0.0018	0.0345	4	49.2
17	71	81651072	468608	2.8E+07	280	3	130	1	0.4643	-0.018	0.041	0.0022	0.0179	4.123	16.6
17	75	38188032	468608	2073856	283	3	177	2	0.6254	-0.02	0.032	-8E-04	0.0294	4.123	19.4
17	86	100554880	468608	3.2E+07	302	2.5	181	1.5	0.5993	-0.026	0.024	0.002	0.0269	4	17
17	86	128537856	468608	3.5E+07	285	2	224	1	0.786	-0.022	0.021	0.0039	0.0354	3.384	24.2
17	77	81285632	468608	4.1E+07	235	2	155	1	0.6596	-0.022	0.003	0.0027	0.0208	3	25.6
17	71	39236736	468736	3238784	309	3	181	2	0.5858	-0.039	0.021	0.001	0.0224	4.123	44.8
17	82	122655872	468736	3E+07	307	2	225	1.5	0.7329	-0.015	0.014	0.0008	0.04	3.162	41.7
17	77	106384000	468736	6.5E+07	270	2	176	1	0.6519	-0.018	0.017	0	0.0241	3.606	35.8
17	62	87112320	468736	2.9E+07	234	2	190	1	0.812	-0.041	0	0	0.0296	4.062	26.4
17	71	67497856	468608	3E+07	307	2	210	1	0.684	-0.021	0.013	0.0033	0.0307	4.123	32.2
17	85	105760512	468736	3.4E+07	273	1	163	1	0.5971	-0.021	0.008	0.0021	0.0113	3	45.7
17	82	131274240	468608	5.1E+07	282	2	152	1	0.539	-0.009	0.014	0.0039	0.0226	2.532	40.2
17	73	91272320	468736	2.9E+07	326	2	190	2	0.5828	-0.029	0.008	0.0044	0.0345	4	57.2
17	91	76765696	468736	2.7E+07	265	2	168	1	0.634	-0.021	0.011	0.0015	0.0248	2.236	31.4
17	79	87776512	468608	2.8E+07	334	2	229	1	0.6856	-0.025	0.015	0.0015	0.0379	4	41.9
17	74	37704960	468608	1598976	299	3.5	183	2	0.612	-0.026	0.011	0.0045	0.0239	4.472	23.6

17	86	69083520	468608	2.3E+07	295	2	181	1	0.6136	-0.01	0.017	0.0041	0.0333	3	32
17	84	96018560	468608	2.7E+07	295	2	181	1	0.6136	-0.022	0.005	0.0021	0.0263	3	28
17	68	62554368	468608	2.7E+07	324	2	208	2	0.642	-0.019	0.009	0.0009	0.0284	3.606	38.9
17	82	87814912	468736	2.8E+07	258	2	160	1	0.6202	-0.013	0.023	0.0005	0.0217	3	25.1
17	66	86619776	468608	2.7E+07	334	4	195	2	0.5838	-0.042	0.007	0.004	0.0338	5	40.5
17	71	127692288	468736	4E+07	233	2	161	1	0.691	-0.015	0.019	0.0015	0.0285	3	28.3
17	72	66153088	468608	2.6E+07	236	1.5	163	2	0.6907	-0.011	0.012	0.0012	0.0279	3	35
17	67	100329088	468736	4.1E+07	276	2	183	1	0.663	-0.023	0.015	-0.001	0.0369	3.162	45.5

Table (B.18): The calculated authentication features for user eighteen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
18	65	236253184	468608	2E+08	149	2	68	1	0.4564	0.0305	0.05	0.0213	0.0276	2.236	11.2
18	64	38330496	468736	4263808	143	2	79	1	0.5524	0.0226	0.045	0.0224	0.0249	2.236	7.62
18	55	30084992	468608	2122624	148	3	69	1	0.4662	0.0282	0.052	0.0256	0.0309	3	6.71
18	41	23458816	468608	3137792	139	3	73	2	0.5252	0.0368	0.061	0.033	0.0362	3.606	8.54
18	60	80354304	468608	4.8E+07	160	2.5	90	1	0.5625	0.0255	0.065	0.0322	0.0365	2.995	7.21
18	55	62646144	468608	2.8E+07	148	2	82	1	0.5541	0.0426	0.091	0.0332	0.0427	2.828	10.4
18	41	24792448	468608	3290240	133	3	71	2	0.5338	0.0493	0.074	0.0381	0.0429	3.162	9.85
18	43	51674752	468736	2.2E+07	143	3	72	1	0.5035	0.0446	0.063	0.0302	0.0363	3.162	8.94
18	36	19316224	468608	2287616	141	4	85	2	0.6028	0.0688	0.088	0.0484	0.0571	4.472	10.3
18	39	19715712	468736	1715584	130	3	80	2	0.6154	0.0426	0.073	0.0418	0.0851	3.606	11.7
18	36	20093312	468736	2409088	159	4	75	2	0.4717	0.0743	0.128	0.0395	0.0431	4.472	13.4
18	45	22496512	468736	1562112	157	3	90	2	0.5732	0.0515	0.07	0.0398	0.0429	4.123	9.43
18	51	27725312	468608	2727552	153	3	88	1	0.5752	0.0415	0.091	0.0387	0.0638	3.162	8.06
18	43	21124096	468608	1405952	170	4	87	2	0.5118	0.0526	0.082	0.0429	0.0488	4.472	8.94
18	44	51903488	468672	2.9E+07	167	4	86	2	0.515	0.0542	0.088	0.037	0.0483	4.298	9.22
18	60	64742656	468736	3.6E+07	199	3	100	2	0.5025	0.0511	0.062	0.0344	0.0463	3.606	8.25
18	47	24910976	468608	1739392	153	3	90	2	0.5882	0.0419	0.072	0.0424	0.0634	3.606	7.62
18	38	46332928	468608	2.7E+07	167	5	78	2	0.4671	0.0522	0.092	0.042	0.0512	5.242	10.3
18	40	62099968	468608	2.1E+07	165	4	80	2	0.4848	0.0413	0.101	0.0406	0.0499	4.472	10.3
18	37	20335744	468736	2486656	158	4	77	2	0.4873	0.064	0.085	0.0446	0.0534	4.472	9.85

18	45	22042496	468608	1405952	168	4	92	2	0.5476	0.043	0.091	0.0462	0.0613	4.123	12.5
18	46	46204672	468672	1.9E+07	189	4	77	1	0.4074	0.0432	0.101	0.0408	0.0591	4.298	10
18	50	26903040	468608	2221440	157	3	75	1	0.4777	0.0417	0.073	0.034	0.0638	3.606	8.94
18	42	45493504	468672	2.5E+07	161	4	104	2	0.646	0.0712	0.093	0.0513	0.0645	5.193	10
18	40	20542080	468672	2260864	199	4.5	87	2	0.4372	0.0633	0.128	0.0451	0.0596	5.05	16.2
18	41	22881536	468608	2511744	164	4	85	2	0.5183	0.0582	0.08	0.0428	0.05	4.123	13.4
18	47	24082560	468608	2137088	158	3	61	1	0.3861	0.0381	0.055	0.0291	0.0361	3.606	11.2
18	36	18504448	468672	2226688	163	4	79	2	0.4847	0.0481	0.074	0.043	0.0493	4.357	13
18	51	58473472	468608	2.6E+07	147	3	77	1	0.5238	0.032	0.052	0.0278	0.033	3.162	7.62
18	42	22763648	468608	2852480	172	4	93	2	0.5407	0.0464	0.1	0.0488	0.0564	4.472	9.43

Table (B.19): The calculated authentication features for user nineteen

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
19	25	11716096	468736	472832	266	12	379	13	1.4248	0.1269	0.404	-0.084	-0.006	17.72	40.2
19	36	29692288	468608	1.3E+07	243	6	333	11	1.3704	0.0791	0.268	-0.06	-0.011	12.78	33.3
19	40	50069504	468736	1.4E+07	289	7	390	11	1.3495	0.0967	0.293	-0.064	0	14.12	32.8
19	34	15933824	468608	472832	268	7	362	9	1.3507	0.1101	0.247	-0.073	-0.021	13.73	31.1
19	41	33145984	468608	1.5E+07	241	6	362	6	1.5021	0.0754	0.278	-0.063	-0.013	10.82	26.1
19	35	29635968	468608	1.4E+07	270	8	407	10	1.5074	0.1029	0.344	-0.078	-0.028	13.45	40.5
19	40	68832384	468736	5.1E+07	301	7	499	11.5	1.6578	0.1057	0.335	-0.085	-0.031	14.59	34.5
19	39	18281088	468736	472832	313	8	503	12	1.607	0.1104	0.436	-0.065	-0.01	14.04	34.1
19	41	37196160	468608	1.9E+07	242	6	420	10	1.7355	0.0713	0.286	-0.053	0.0101	11.66	32.4
19	35	28183552	468736	1.2E+07	245	6	429	14	1.751	0.1005	0.336	-0.092	-0.021	15.62	30
19	40	18745600	468736	472576	243	5.5	449	9.5	1.8477	0.0877	0.26	-0.071	-0.028	14.28	29
19	38	31051648	468608	1.4E+07	249	5	382	9.5	1.5341	0.1022	0.378	-0.062	-0.025	10.72	39.9
19	44	20620160	468608	472704	244	5	408	8	1.6721	0.0732	0.269	-0.075	0.0153	9.924	37.1
19	52	34864000	468608	1.1E+07	256	4	421	8	1.6445	0.064	0.267	-0.058	0.0601	9.635	23.7
19	40	18745600	468608	472832	289	6	451	10.5	1.5606	0.0971	0.321	-0.064	0	15.07	28.3
19	43	19838976	468608	472832	288	6	529	12	1.8368	0.0904	0.383	-0.085	0.0101	13.04	30.2
19	40	18610944	468608	472704	265	6	461	10.5	1.7396	0.1009	0.273	-0.108	-0.029	12.76	30.5
19	52	37785216	468608	1.4E+07	256	5	408	8	1.5938	0.0541	0.291	-0.043	0.0639	9.434	30
19	54	26100992	468608	1405952	260	4	413	8	1.5885	0.0608	0.241	-0.047	0.057	9.668	20
19	51	24213120	468736	785280	245	4	410	8	1.6735	0.0652	0.224	-0.058	0.0585	9.899	23.6

19	40	18542848	468608	483328	246	5	404	10	1.6423	0.0852	0.363	-0.063	-0.012	10.91	38.9
19	50	45721472	468736	1.6E+07	281	5	482	11	1.7153	0.0704	0.261	-0.072	0.0595	12.18	25.5
19	52	24526208	468608	785408	248	4	452	8	1.8226	0.0601	0.269	-0.066	0.0624	9.217	31.1
19	47	50785280	468736	2.9E+07	262	5	441	9	1.6832	0.078	0.277	-0.06	0.0556	10.82	31.4
19	56	37323776	468736	1.1E+07	279	5	472	8	1.6918	0.0476	0.19	-0.048	0.0768	9.667	25.5
19	48	67324672	468608	4.5E+07	306	6	493	9.5	1.6111	0.0778	0.397	-0.058	0.0673	11.42	39.1
19	51	37179392	468736	1.4E+07	303	5	451	9	1.4884	0.0747	0.291	-0.051	0.0747	10.3	32.4
19	52	24369280	468736	472832	301	5	450	8.5	1.495	0.0676	0.285	-0.05	0.0736	10.3	35.8
19	57	26748672	468608	629120	270	4	408	6	1.5111	0.0593	0.263	-0.043	0.0601	8.944	25.1
19	53	24715520	468608	472832	295	5	400	7	1.3559	0.0689	0.27	-0.04	0.0707	9.899	26

Table (B.20): The calculated authentication features for user twenty

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
20	58	59861632	468608	3.3E+07	210	3	203	2	0.9667	0.0181	0.145	0.011	0.0608	5.099	16.6
20	65	32697088	468608	2704128	195	3	188	2	0.9641	0.0188	0.075	-0.007	0.0569	4	13.4
20	61	48490240	468608	1.8E+07	195	3	222	2	1.1385	0.0165	0.1	0.0238	0.0671	5	15.2
20	48	34979968	468608	1.3E+07	182	3.5	212	4	1.1648	0.0228	0.149	-0.009	0.0534	6.364	15.2
20	45	21681408	468608	1406080	200	4	253	4	1.265	0.021	0.091	-0.018	0.0519	7.28	19.3
20	51	40425600	468736	1.5E+07	279	5	294	6	1.0538	0.026	0.213	-0.019	0.0803	9.487	20
20	51	26048768	468736	2259456	249	4	306	5	1.2289	0.0247	0.144	0.0016	0.0914	9.22	28.6
20	45	23431936	468608	1405952	222	3	281	6	1.2658	0.0273	0.121	-0.028	0.0467	9.22	20
20	47	35136384	468608	1.3E+07	253	5	356	7	1.4071	0.0177	0.133	-0.026	0.0603	11	21.1
20	47	23607680	468352	1721088	278	4	331	8	1.1906	0.0255	0.181	-0.043	0.0781	11.05	25
20	52	25150976	468608	1406080	197	3	292	5.5	1.4822	0.017	0.097	-4E-04	0.0823	7.545	22.2
20	41	21092480	468608	1716736	247	5	298	7	1.2065	0.041	0.164	-0.038	0.0231	11.7	22.1
20	42	36912896	468608	1.6E+07	247	4	304	6	1.2308	0.0411	0.157	-0.048	0.0173	11.72	22.8
20	47	24017024	468608	1986944	268	5	358	8	1.3358	0.041	0.298	-0.014	0.0672	12.04	23.7
20	43	21263360	468608	1506816	229	4	366	7	1.5983	0.0366	0.186	-0.02	0.0502	13.04	22.2
20	45	38169472	468608	1.6E+07	253	4	331	5	1.3083	0.0342	0.183	-0.066	0.0601	11	25.2
20	51	25158272	468736	1246720	239	3	345	6	1.4435	0.0269	0.142	-0.048	0.0965	10	20.1
20	51	24462592	468608	1902464	290	4	333	6	1.1483	0.0243	0.139	-0.038	0.0818	9.22	22.5
20	39	18590976	468608	933120	241	5	279	7	1.1577	0.0452	0.191	-0.044	0.0338	9.487	26.2
20	48	37456640	468608	1.5E+07	240	4	268	4	1.1167	0.0283	0.179	-0.027	0.064	7.64	20.2
20	50	39018240	468608	1.6E+07	242	3.5	232	4.5	0.9587	0.0427	0.164	-0.029	0.0629	7.071	18
20	45	21488512	468608	1095040	231	4	231	4	1	0.0359	0.156	-0.049	0.0436	8.246	30

20	44	37951488	468736	1.8E+07	203	3	258	5	1.2709	0.0162	0.118	-0.034	0.0446	9	23
20	41	19537024	468608	1093504	227	4	272	5	1.1982	0.0372	0.169	-0.029	0.032	11.4	21.3
20	44	20932608	468608	776832	223	3.5	264	4.5	1.1839	0.0266	0.139	-0.052	0.0524	9.61	18.4
20	43	20348288	468608	937216	221	5	266	4	1.2036	0.0294	0.152	-0.043	0.0372	7.28	29
20	45	21592960	468608	936320	207	2	239	5	1.1546	0.036	0.182	-0.059	0.0461	7	21.4
20	39	32520448	468608	1.5E+07	233	5	236	6	1.0129	0.0304	0.146	-0.032	0.0264	10	19.8
20	40	29514112	468608	1.2E+07	205	3.5	249	5	1.2146	0.0348	0.294	-0.043	0.0363	9	25
20	37	31771264	468736	1.5E+07	192	3	245	6	1.276	0.0227	0.128	-0.038	0.0304	10.05	26

Table (B.21): The calculated authentication features for user twenty-one

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
21	20	7564288	356032	731776	193	8	69	4	0.3575	-0.026	0.078	0.0563	0.1002	8.279	30.1
21	28	11401216	344960	1757952	147	3.5	62	2	0.4218	0.0108	0.09	0.052	0.0864	5.193	32.6
21	36	44418560	328640	3.1E+07	130	2.5	65	2	0.5	-0.006	0.034	0.0388	0.0642	4	17
21	31	10909312	350976	375808	135	2	74	2	0.5481	-0.039	0.016	0.0457	0.0765	4.472	16.1
21	32	11240960	351744	382208	191	5	75	2	0.3927	-0.007	0.066	0.07	0.1036	5.5	30.6
21	42	14899072	351488	406784	150	3	60	1	0.4	-0.017	0.033	0.035	0.0485	3.803	11
21	38	16574336	353408	1720960	136	3	61	1	0.4485	-0.006	0.019	0.0299	0.0506	4.123	11.7
21	35	12406272	348288	494080	137	3	50	1	0.365	0.0029	0.048	0.0419	0.0608	3.606	19.6
21	35	12376192	355456	397824	149	4	61	1	0.4094	-0.018	0.022	0.0397	0.0666	5	19.4
21	39	14252928	345984	988800	148	3	73	2	0.4932	-0.031	0.014	0.0347	0.0598	3.606	13.4
21	31	10961280	355840	380416	161	4	68	2	0.4224	-0.028	0.023	0.0524	0.082	5.385	15.5
21	32	11385856	353408	425856	143	3.5	70	2	0.4895	-0.019	0.027	0.0333	0.0684	4.123	15
21	35	12112256	342272	381056	100	3	63	1	0.63	-0.01	0.015	0.0297	0.0589	3.606	9.22
21	36	12541696	349568	395008	165	4	73	2	0.4424	-0.036	0.014	0.0493	0.0724	4.357	12.4
21	35	32903680	345088	2.1E+07	167	3	62	1	0.3713	0.0081	0.049	0.0379	0.0656	4.123	18.2
21	33	11544960	352512	389248	155	3	67	2	0.4323	-0.011	0.03	0.0583	0.0807	5.385	13
21	32	11299328	347712	422400	164	3.5	72	2	0.439	-0.037	0.023	0.0626	0.0787	4.298	17.5
21	50	17763072	338368	642560	119	2	69	1	0.5798	-0.018	0.026	0.0304	0.0469	2.236	11.2
21	37	13255680	344832	889600	181	4	67	2	0.3702	-0.037	0.007	0.045	0.0584	5	16.3
21	31	11643648	340608	1018240	166	4	81	2	0.488	-0.025	0.018	0.0694	0.0987	5.831	17
21	38	12952960	333312	472064	146	2	66	1.5	0.4521	-0.011	0.022	0.0461	0.062	3.081	17

21	32	10924544	337344	384000	125	4	56	1.5	0.448	-0.025	0.012	0.047	0.061	4.062	12.1
21	36	12719232	343936	627584	146	2.5	73	2	0.5	-0.02	0.025	0.0555	0.0754	4.123	14.9
21	34	11625984	341696	381440	181	4	64	2	0.3536	-0.021	0.038	0.0422	0.0619	4.472	15.1
21	35	11868288	336256	369024	185	3	73	2	0.3946	-0.011	0.049	0.0583	0.0938	4.243	25.3
21	35	12412544	339712	887808	167	2	74	2	0.4431	-0.011	0.039	0.0654	0.0812	4.123	17
21	36	12585856	344576	382848	157	3	77	2	0.4904	-8E-04	0.038	0.0648	0.0817	4.736	14.3
21	38	13247616	347456	383872	142	2.5	82	2	0.5775	-0.019	0.022	0.0585	0.0775	3.606	14
21	25	8754688	350080	389632	181	6	72	3	0.3978	-0.018	0.054	0.0767	0.0913	7.81	19.4
21	27	31547392	363136	2.2E+07	190	7	63	2	0.3316	-0.019	0.048	0.0683	0.0934	7.071	22

Table (B.22): The calculated authentication features for user twenty-two

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
22	210	861284864	355520	4E+08	170	1	191	1	1.1235	0.002	0.029	0.0054	0.0373	1	7.07
22	204	87627136	347264	2835712	160	1	169	1	1.0563	0.0032	0.031	0.0044	0.0363	1	6.32
22	202	90441216	357312	2445440	134	0	163	1	1.2164	0.002	0.027	0.0028	0.0308	1	5.83
22	192	79892736	351168	3716608	176	1	190	1	1.0795	0.0025	0.035	0.0021	0.0407	1.414	8.94
22	195	162913536	357888	4.6E+07	177	1	178	1	1.0056	0.0014	0.029	0.0012	0.0316	1	12.2
22	130	119228032	359040	3.6E+07	144	1	143	1	0.9931	-0.002	0.027	0.0035	0.0293	2	6
22	154	102525440	355648	3.9E+07	136	1	153	1	1.125	-0.004	0.027	0.0042	0.0344	1.414	5
22	141	304753920	354560	1.9E+08	115	1	164	1	1.4261	-0.003	0.018	0.0028	0.0336	1	11
22	143	57748864	351872	2579328	110	1	139	1	1.2636	-0.004	0.019	0.0033	0.0298	1	7.28
22	151	71139328	353408	3321728	115	1	130	1	1.1304	-0.003	0.022	0.0054	0.0281	1	8.06
22	171	212727296	338688	9.3E+07	168	1	186	1	1.1071	0.0013	0.025	0.0018	0.0359	1.414	14.9
22	165	128083456	355456	5.5E+07	149	1	149	1	1	-0.001	0.031	0.0021	0.0287	1	11.2
22	131	59975424	358656	1811072	110	1	95	0	0.8636	-0.003	0.022	0.0019	0.0213	1	9.22
22	161	69178240	358656	2428160	111	1	127	1	1.1441	-0.001	0.019	0.0021	0.02	1	5.66
22	186	79700864	349760	2399360	131	1	159	1	1.2137	-6E-04	0.024	0.0008	0.0327	1	7.28
22	157	61605376	356096	1280384	103	1	160	1	1.5534	0	0.023	0.0024	0.0315	1	4.12
22	158	69095552	352064	2797312	125	1	141	1	1.128	-0.002	0.026	0.0047	0.0299	1	7.28
22	148	59718784	346112	2351616	114	1	146	1	1.2807	-0.004	0.019	0.0035	0.0296	1	9.06
22	175	192679552	354688	1.2E+08	146	1	165	1	1.1301	-0.002	0.032	0.0022	0.037	1.414	5.1

22	139	55125120	349952	4010880	150	1	169	1	1.1267	-0.008	0.027	0.0033	0.0391	1.414	5.83
22	133	58071552	351616	2786304	127	1	126	1	0.9921	-0.003	0.027	0.0024	0.0289	1.414	7.81
22	181	79818368	353920	3337472	140	1	150	1	1.0714	-0.002	0.024	0.0025	0.0232	1	13
22	163	130193792	353152	4.4E+07	115	1	143	1	1.2435	0	0.023	0.0021	0.0316	1	4.47
22	187	156992896	343680	7.6E+07	159	1	199	1	1.2516	-0.002	0.032	0.001	0.0416	1.414	8.54
22	196	79887616	355712	3520256	136	1	178	1	1.3088	-0.002	0.025	0.0015	0.032	1	6
22	147	65453824	362112	2281344	135	1	159	1	1.1778	-0.004	0.02	0.0006	0.0288	1	6.08
22	165	66277120	353536	1399936	114	1	158	1	1.386	-7E-04	0.019	0.0019	0.0277	1	5.83
22	144	58366464	348928	2895744	109	1	152	1	1.3945	-0.002	0.023	0.0043	0.0338	1.414	5
22	174	73616000	353664	3482496	143	1	163	1	1.1399	-0.002	0.029	0.0017	0.0344	1.414	7.21
22	150	91207552	353536	3.2E+07	132	1	161	1	1.2197	0	0.026	0.0028	0.0321	1.414	5.83

Table (B.23): The calculated authentication features for user twenty-three

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
23	54	83905664	468672	5.9E+07	547	8.5	224	3	0.4095	-0.015	0.067	0.0299	0.1393	9.842	32
23	45	21088768	468608	473088	448	8	252	5	0.5625	-0.004	0.054	0.048	0.2051	11.66	36.9
23	39	18031488	468736	473216	531	11	299	7	0.5631	-0.016	0.102	0.0615	0.237	15.3	40.6
23	36	29015552	468608	1.3E+07	656	17	250	5	0.3811	-0.047	0.04	0.0683	0.2853	23.6	59.3
23	37	45395840	468608	1.6E+07	548	14	247	5	0.4507	-0.021	0.079	0.0513	0.2162	17	43.2
23	35	16024064	468608	472960	550	15	215	5	0.3909	-0.034	0.069	0.0513	0.2432	17.03	43
23	34	15806976	468608	472832	443	12	257	7	0.5801	-0.022	0.052	0.0617	0.2991	14.5	43.5
23	39	37710720	468608	2E+07	508	10	242	4	0.4764	-0.021	0.058	0.0631	0.2375	14.87	42.1
23	42	36736512	468608	1.8E+07	518	11	246	4	0.4749	-0.025	0.047	0.041	0.2187	13.73	33.1
23	36	16621696	468608	472960	538	10.5	266	6	0.4944	-0.042	0.025	0.0502	0.2381	15	51
23	38	17808256	468608	472832	503	11.5	237	5.5	0.4712	-0.025	0.057	0.0426	0.1944	14.57	41.4
23	37	17213312	468608	473088	507	12	217	5	0.428	-0.018	0.102	0.0427	0.1919	15.81	46
23	43	36087296	468608	1.6E+07	516	10	255	5	0.4942	-0.039	0.031	0.0439	0.2004	11.4	38.1
23	40	18591104	468736	472832	639	10	245	4	0.3834	-0.037	0.048	0.0439	0.2062	13.95	60.7
23	33	30720896	468736	1.6E+07	558	14	219	6	0.3925	-0.018	0.126	0.0613	0.232	16.03	55.2
23	38	36387200	468608	1.7E+07	594	12.5	246	5	0.4141	-0.039	0.052	0.0475	0.2062	14.8	48.1
23	38	17808384	468736	472448	563	13.5	244	6	0.4334	-0.036	0.059	0.0534	0.2347	14.44	40.4
23	36	16874112	468608	472960	599	15	213	4	0.3556	-0.037	0.059	0.043	0.2249	16.28	53
23	35	16257536	468608	475136	518	10	222	6	0.4286	-0.028	0.072	0.0581	0.2628	16.28	51
23	38	48809344	468672	1.4E+07	598	12	255	4	0.4264	-0.031	0.056	0.0495	0.2866	16.57	52

23	38	31577984	468608	1.4E+07	530	11	225	5	0.4245	-0.036	0.052	0.0457	0.2187	14.58	38.1
23	40	31095296	468736	1.3E+07	481	10	199	4	0.4137	-0.028	0.052	0.0365	0.1873	12.04	49
23	32	15963776	468544	1719168	414	7.5	255	8	0.6159	-0.06	0.02	0.0539	0.2409	16.34	49
23	35	31735552	468608	1.6E+07	437	10	226	5	0.5172	-0.017	0.082	0.0598	0.315	11.18	35.8
23	32	28790144	468672	1.5E+07	372	9	183	3	0.4919	-0.028	0.038	0.0539	0.2705	11.61	36.7
23	33	32807808	468736	1.8E+07	397	11	192	5	0.4836	-0.002	0.107	0.0555	0.2436	12.17	38
23	35	16402432	468608	472960	475	12	222	5	0.4674	-0.025	0.046	0.0465	0.2187	15.13	51
23	31	14378880	468608	475904	568	15	186	4	0.3275	-0.059	0.044	0.0556	0.2234	17.03	55
23	35	16248064	468608	472832	492	12	220	6	0.4472	-0.05	0.018	0.0426	0.2317	15	43
23	28	12651776	468608	472832	469	15	189	5	0.403	-0.035	0.102	0.0482	0.2249	18.52	52.2

Table (B.24): The calculated authentication features for user twenty-four

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
24	19	33338240	468736	2.5E+07	77	4	220	9	2.8571	0.0825	0.16	0.0695	0.1915	11	35.8
24	17	7968128	468608	472832	82	4	254	11	3.0976	0.0823	0.191	0.1064	0.3085	13.04	37.9
24	19	8460160	468608	624896	82	3	183	7	2.2317	0.0833	0.129	0.1123	0.2043	10.2	31.4
24	18	8435456	468608	937344	134	5	245	12	1.8284	0.0958	0.229	0.1124	0.3298	15.65	34.5
24	18	7831808	468032	472704	125	6.5	201	11	1.608	0.1137	0.172	0.0984	0.3191	13.52	34.2
24	19	8773248	468608	624512	133	6	198	8	1.4887	0.1209	0.28	0.0576	0.2128	12.65	31.6
24	16	8290048	468736	1249664	133	8.5	218	10	1.6391	0.1324	0.218	0.0714	0.3125	14.98	57.2
24	15	6581760	468224	472832	108	5	161	8	1.4907	0.126	0.201	0.0764	0.2424	13.93	37.7
24	14	6561024	468672	471680	122	6	220	13.5	1.8033	0.0912	0.154	0.1163	0.5319	19.34	38.6
24	14	6126848	468608	492160	116	8.5	231	14.5	1.9914	0.1071	0.176	0.1204	0.5532	18.99	44
24	13	6120320	468736	496640	99	6	232	16	2.3434	0.1064	0.156	0.1639	0.7872	22.2	45.4
24	14	6284032	468608	472832	107	6	197	14	1.8411	0.1234	0.177	0.1018	0.5319	18.01	49.1
24	14	24413312	469248	1.8E+07	106	6	186	10	1.7547	0.1148	0.202	0.1123	0.4894	15.58	41.7
24	15	6717184	466944	473728	110	6	215	15	1.9545	0.1068	0.15	0.113	0.3871	18.03	40.6
24	14	5785984	467712	471936	104	4.5	228	18	2.1923	0.1198	0.235	0.1288	0.5532	21.92	55.6
24	15	6895360	468608	470784	156	10	247	19	1.5833	0.184	0.273	0.1321	0.5319	22.63	48.3
24	13	6093696	468608	472704	131	12	239	21	1.8244	0.1495	0.241	0.1453	0.587	25.24	41.6
24	14	5986304	468672	472704	124	7.5	218	12	1.7581	0.1363	0.182	0.0931	0.4468	20.62	42
24	15	23520512	468736	1.7E+07	98	6	239	15	2.4388	0.122	0.15	0.1014	0.3617	17.12	46.3
24	13	6591488	468992	963200	82	5	218	18	2.6585	0.0925	0.124	0.1197	0.4301	18.44	35.4
24	13	6104576	468608	627840	128	8	225	17	1.7578	0.1738	0.261	0.1149	0.5208	25.08	40.7
24	13	5973888	468864	474752	113	8	240	17	2.1239	0.1565	0.246	0.1579	0.617	17	48.8

24	12	5017088	465600	471424	114	9	269	20	2.3596	0.153	0.221	0.2027	0.9783	23.18	52.6
24	13	17601024	468736	1.2E+07	98	5	221	10	2.2551	0.1459	0.218	0.1433	0.6596	16.12	65.3
24	12	5469568	468608	472320	88	8.5	239	15	2.7159	0.1456	0.312	0.1967	0.6809	18.75	49
24	12	5313408	468608	470784	108	8	190	10.5	1.7593	0.1557	0.262	0.0903	0.4894	17.76	58.5
24	13	5958528	468608	471680	115	7	206	17	1.7913	0.1049	0.255	0.1577	0.4894	21.63	53.3
24	12	5775872	468608	937344	70	5	230	18.5	3.2857	0.1374	0.19	0.1136	0.5625	21.86	47.1
24	13	5623552	465792	473088	79	5	242	17	3.0633	0.1186	0.184	0.2299	0.8043	17.72	51.9
24	12	5621376	468608	471808	100	9	229	12	2.29	0.168	0.234	0.2206	0.6383	16.09	68.4

Table (B.25): The calculated authentication features for user twenty-five

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
25	52	49319296	468672	2.2E+07	257	4	232	4	0.9027	-0.072	0.085	0.025	0.2766	7.671	23
25	39	39246848	468608	1.7E+07	330	6	251	6	0.7606	-0.124	0	0.0282	0.2234	11.18	28.5
25	57	58612096	468608	1.7E+07	185	3	200	3	1.0811	-0.041	0.057	0.0138	0.1214	5	16.1
25	54	29191296	468736	2964096	166	2	157	3	0.9458	-0.038	0.014	0.0173	0.0693	5	17
25	51	40529920	468608	1.6E+07	214	2	188	3	0.8785	-0.068	0.042	0.0249	0.1631	6.083	14.8
25	63	101016576	468736	5.6E+07	172	3	190	3	1.1047	-0.042	0.021	0.0135	0.2	5	12.2
25	58	63760512	468608	1.9E+07	177	2.5	166	3	0.9379	-0.044	0.021	0.0137	0.0904	4.736	16.8
25	53	57211136	468608	1.6E+07	229	4	216	4	0.9432	-0.05	0.085	0.0252	0.1223	7	14.9
25	54	25972096	468608	1598720	166	3	193	3	1.1627	-0.039	0.064	0.0247	0.1596	5	12.7
25	59	127790976	468736	9.9E+07	213	3	208	3	0.9765	-0.043	0.043	0.0169	0.1064	5	16.3
25	54	42467968	468672	1.5E+07	203	3	204	3	1.0049	-0.053	0.128	0.0266	0.1604	5.608	16
25	50	43233280	468608	1.7E+07	221	4	221	5	1	-0.069	0.043	0.0266	0.1631	7.106	17
25	54	62052608	468608	1.8E+07	190	3	201	3	1.0579	-0.05	0.074	0.0264	0.133	5.828	20.6
25	47	44520832	468608	1.7E+07	185	3	189	3	1.0216	-0.059	0.043	0.0238	0.2473	6	27.9
25	50	27775104	468608	3322112	185	3	151	3	0.8162	-0.043	0.029	0.0184	0.0857	4.736	14.3
25	51	27360640	468736	2341632	184	3	181	4	0.9837	-0.045	0.021	0.0195	0.117	5.385	13.9
25	46	39155712	468608	1.3E+07	210	3	200	4	0.9524	-0.063	0.065	0.0425	0.1357	7.071	16.3
25	52	49490560	468736	2.2E+07	218	3	226	4	1.0367	-0.071	0	0.0176	0.1489	6	19
25	52	50329088	468672	1.7E+07	214	3	182	3	0.8505	-0.067	0.022	0.0182	0.1357	6	16.4
25	53	27951616	468736	2414720	222	3	194	4	0.8739	-0.06	0.064	0.0236	0.1282	6.083	17
25	42	36921856	468608	1.3E+07	238	5	174	4	0.7311	-0.08	0.043	0.032	0.1383	7.071	21
25	54	67382400	468608	2.2E+07	156	2	191	3	1.2244	-0.042	0.064	0.0187	0.1197	5.099	12.8

25	53	45162880	468608	1.8E+07	204	3	183	3	0.8971	-0.049	0.106	0.0204	0.1489	6	17
25	46	24919424	468608	2417664	234	3	197	4	0.8419	-0.062	0.064	0.0275	0.1915	7.545	23.3
25	40	49629312	468608	1.7E+07	247	5.5	190	4.5	0.7692	-0.082	0.043	0.0269	0.1915	9.082	26.1
25	41	48340480	468736	1.3E+07	182	3	187	4	1.0275	-0.061	0.064	0.0213	0.1571	6.403	15.3
25	46	56617216	468608	3.2E+07	195	2	207	4	1.0615	-0.055	0.021	0.0248	0.1702	6.403	20.2
25	40	51273472	468608	3E+07	159	2.5	152	3.5	0.956	-0.05	0.053	0.0283	0.1206	6.162	18.2
25	41	55069952	468608	1.8E+07	160	3	168	3	1.05	-0.052	0.064	0.0355	0.1773	5.657	15.3
25	58	43273344	468736	1.2E+07	171	3	209	3	1.2222	-0.04	0.054	0.0203	0.1143	5.521	14.4

Table (B.26): The calculated authentication features for user twenty-six

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
26	28	997979136	358656	9.9E+08	129	2.5	222	4	1.7209	0.0621	0.298	-0.079	-0.034	6.041	40.5
26	23	9318016	359680	821888	160	5	262	4	1.6375	0.1238	0.381	-0.156	-0.101	10.3	50.3
26	22	9739136	342976	1269504	129	4	230	8	1.7829	0.0914	0.294	-0.1	-0.035	10.53	34
26	23	10483584	329088	1571072	138	4	194	4	1.4058	0.0796	0.284	-0.099	-0.065	11.18	35.5
26	32	11825152	325952	790400	192	2	268	3	1.3958	0.0722	0.295	-0.074	-0.017	9.272	40.8
26	22	9181824	360128	1188992	107	2.5	237	6.5	2.215	0.0694	0.202	-0.144	-0.085	12.11	30.1
26	33	16321536	362496	2163072	179	2	252	6	1.4078	0.0498	0.243	-0.066	-0.023	8.062	41
26	23	11431168	352000	1780352	136	3	199	6	1.4632	0.0672	0.317	-0.081	-0.035	11.05	42
26	28	11458432	352256	1267712	154	1.5	267	6.5	1.7338	0.0753	0.264	-0.083	-0.022	9.11	41
26	24	10272896	365120	1005568	114	2	195	3	1.7105	0.0734	0.294	-0.07	-0.033	9.492	32.3
26	25	11952128	359424	2085760	144	3	232	5	1.6111	0.0631	0.245	-0.087	-0.042	7.616	41
26	50	22886400	349568	2598912	115	1	202	2	1.7565	0.031	0.098	-0.048	0.0021	3.162	19.1
26	36	25270656	364480	3270528	118	2	181	3.5	1.5339	0.0343	0.127	-0.043	-0.024	7.259	17.1
26	26	31526400	348544	2.2E+07	124	2	200	2.5	1.6129	0.0573	0.186	-0.056	0	6.078	36.7
26	29	15247232	362624	1729920	157	4	241	4	1.535	0.0568	0.296	-0.056	-0.024	8.544	37.2
26	31	15115392	350208	1850752	132	2	250	5	1.8939	0.0615	0.178	-0.077	-0.024	8.944	26
26	29	48614144	355456	3.6E+07	106	1	212	3	2	0.0588	0.292	-0.067	-0.029	6	35.7
26	36	19359104	355136	3181440	122	1.5	216	1.5	1.7705	0.0372	0.179	-0.052	0	2.699	34.9
26	31	16729600	359936	2020352	125	1	192	2	1.536	0.0418	0.22	-0.047	-0.02	5.099	40.1
26	22	11314688	359040	1577216	149	4.5	212	4	1.4228	0.0678	0.314	-0.069	-0.025	9.015	34
26	29	13693184	351104	1693056	137	3	213	3	1.5547	0.0468	0.204	-0.053	-0.016	9.434	24.4
26	33	13582080	342016	1051904	143	1	226	4	1.5804	0.0704	0.333	-0.058	-0.017	6	32.8

26	37	18160256	350976	2555904	164	3	225	3	1.372	0.0562	0.218	-0.097	-0.016	6.403	29
26	52	23271168	351040	1873408	157	1.5	204	2	1.2994	0.0431	0.202	-0.032	0.0065	3.606	21
26	34	35183872	348800	2.2E+07	187	3	221	6	1.1818	0.0724	0.234	-0.064	-0.019	8.366	39.8
26	37	23918592	358272	3963648	169	4	187	3	1.1065	0.0464	0.114	-0.038	0	6.083	20
26	46	71214080	360000	4.5E+07	143	1	212	2	1.4825	0.0245	0.13	-0.043	0.0043	2.532	28.3
26	34	39209600	350592	2.4E+07	159	2	253	3	1.5912	0.0598	0.294	-0.056	-0.006	4.915	38.5
26	28	12774784	352896	1740672	151	2.5	208	4.5	1.3775	0.0678	0.255	-0.053	-0.018	9	32
26	30	34365440	357696	2.1E+07	182	2	212	5.5	1.1648	0.0846	0.255	-0.072	-0.036	8.031	33

Table (B.27): The calculated authentication features for user twenty-seven

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
27	83	39084032	468608	779776	384	4	407	5	1.0599	0.0453	0.072	0.0242	0.1336	7.071	22.8
27	88	42201472	468608	1564928	307	3	369	4	1.202	0.034	0.058	0.0196	0.234	6.364	14
27	101	48806912	468736	1911552	222	2	357	4	1.6081	0.0208	0.048	0.0136	0.1064	5	9.43
27	93	44097408	468608	937216	329	3	408	5	1.2401	0.028	0.065	0.0199	0.2234	6.083	23.4
27	101	48766976	468608	1559424	262	2	409	4	1.5611	0.0279	0.08	0.0164	0.2151	5.831	12.7
27	121	57225984	468608	1246464	330	2	385	3	1.1667	0.0281	0.049	0.0079	0.234	5	14
27	130	166238976	468608	1E+08	291	2	382	3	1.3127	0.0213	0.048	0.0059	0.089	4.243	10
27	126	60111872	468608	1659776	330	2	403	3	1.2212	0.0251	0.055	0.0136	0.1064	4.472	12.2
27	119	56760320	468608	1414016	333	2	413	3	1.2402	0.0271	0.05	0.0111	0.1149	5.099	11.4
27	116	73794560	468608	1.9E+07	308	2	438	4	1.4221	0.0237	0.05	0.0154	0.1352	5.05	13.4
27	105	65780224	468608	1.5E+07	315	3	377	4	1.1968	0.0266	0.066	0.0164	0.1081	5.657	12
27	101	64500224	468608	1.5E+07	321	3	383	4	1.1931	0.0309	0.076	0.0105	0.1571	5.385	14.3
27	109	51577600	468608	1093504	310	2	348	3	1.1226	0.0242	0.071	0.0118	0.1034	5.099	12.2
27	115	82531968	468608	1.7E+07	303	2	425	4	1.4026	0.0288	0.062	0.0082	0.1714	5	13
27	91	58256896	468608	1.4E+07	303	3	355	3	1.1716	0.033	0.064	0.0169	0.0905	5.831	14.1
27	108	51108480	468608	1253376	412	3	418	4	1.0146	0.0374	0.08	0.0134	0.0925	6.083	17.5
27	95	82829696	468608	1.9E+07	315	2	414	4	1.3143	0.0273	0.068	0.0195	0.1915	7	13.4
27	108	76643840	468608	2.6E+07	298	2	379	4	1.2718	0.0284	0.065	0.0112	0.0963	5.385	11
27	105	49836288	468608	1249792	308	3	388	4	1.2597	0.0269	0.067	0.0101	0.2179	5.099	12.1
27	86	40771712	468608	933632	327	3	386	4	1.1804	0.0352	0.065	0.0232	0.1915	7.071	14.6
27	104	50316160	468608	3049728	287	2	415	4	1.446	0.0249	0.059	0.0127	0.139	5.521	12.8
27	99	46698880	468608	1406080	297	2	429	4	1.4444	0.0346	0.071	0.0146	0.1571	6.325	13.4

27	108	50136832	468608	623232	307	2	390	4	1.2704	0.0321	0.061	0.0102	0.1171	5.099	12
27	101	47726336	468608	781056	317	3	457	4	1.4416	0.035	0.065	0.0101	0.152	6	16.5
27	129	74996224	468608	1.4E+07	309	2	370	3	1.1974	0.0244	0.04	0.0101	0.129	4.123	11.7
27	105	66226560	468608	1.7E+07	263	2	314	3	1.1939	0.0266	0.064	0.013	0.1728	4.472	9.9
27	110	52178176	468608	1090432	309	3	370	3	1.1974	0.0312	0.056	0.0161	0.0961	5	12.1
27	103	49005568	468608	785408	275	2	403	4	1.4655	0.0292	0.059	0.0143	0.1497	5.099	12.5
27	109	50802304	468608	474624	337	3	435	4	1.2908	0.0311	0.056	0.0131	0.2188	5.657	13.6
27	104	48265728	468608	623104	331	3	390	4	1.1782	0.0337	0.095	0.0109	0.1658	5.831	13

Table (B.28): The calculated authentication features for user twenty-eight

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
28	74	30529280	335552	1986688	447	6	259	3	0.5794	0.0304	0.324	0.0361	0.0593	7.246	26
28	78	53136768	336640	21520384	418	4	266	3	0.6364	0.0484	0.189	0.0405	0.0747	6.162	20.9
28	65	48132608	364288	21643648	367	5	237	3	0.6458	0.0077	0.139	0.0238	0.0471	7.211	22
28	78	47966976	340416	15413888	458	5	273	2.5	0.5961	0.0482	0.198	0.0275	0.0608	7	24
28	69	29232000	355328	1007360	448	5	300	4	0.6696	0.0294	0.403	0.0381	0.0689	8.544	22
28	78	29066112	346176	842752	433	5.5	312	4	0.7206	0.0282	0.146	0.0272	0.0569	7.936	20.6
28	65	48382592	337280	24313856	494	7	262	3	0.5304	0.0425	0.364	0.0304	0.0678	8.544	34.4
28	75	48136064	337152	17436928	458	5	245	3	0.5349	0.0369	0.191	0.0328	0.0608	6.708	18.4
28	70	27705344	347008	845056	482	5.5	299	4	0.6203	0.0277	0.282	0.0301	0.0504	7.81	26.2
28	68	27132800	333952	1594496	441	5	243	3	0.551	0.0226	0.22	0.0283	0.0469	7.28	21.8
28	65	45895808	342272	19447424	385	5	321	4	0.8338	0.0247	0.141	0.0325	0.067	8.062	24.2
28	71	29241984	335744	1253376	439	6	270	3	0.615	0.0178	0.314	0.0371	0.0683	7.616	21.1
28	65	50845696	336640	24135040	382	5	270	4	0.7068	0.028	0.22	0.0409	0.0716	7.211	23.3
28	68	30172160	348736	1374336	436	6	275	3	0.6307	0.0205	0.147	0.0334	0.0579	8.366	22.2
28	67	69351040	463744	21217536	456	6	283	3	0.6206	0.0202	0.176	0.0466	0.0798	8.485	23.8
28	77	50454144	336640	19984512	419	4	301	3	0.7184	0.035	0.134	0.0232	0.0511	7.211	26
28	68	26850944	348352	1168640	424	6.5	228	3	0.5377	0.0271	0.257	0.0326	0.0577	7.808	15.8
28	68	29141504	339008	1664384	426	5	254	3	0.5962	0.0261	0.173	0.0269	0.0486	7.071	24.6
28	68	47131136	347392	19989888	464	6	262	3	0.5647	0.0309	0.163	0.037	0.0623	8.031	34.9
28	67	27155200	338816	1500928	409	5	268	4	0.6553	0.0346	0.168	0.0303	0.0469	7.211	19.9

28	65	51670400	340352	26570240	400	5	228	3	0.57	0.0183	0.162	0.0314	0.0472	7.211	29.7
28	65	71107712	350208	27195904	414	5	267	3	0.6449	0.0229	0.206	0.0458	0.0861	7.616	24.4
28	59	42785408	342656	15489408	533	7	270	4	0.5066	0.0488	0.424	0.0335	0.0733	10.44	25.5
28	64	25669760	337408	1644928	462	7	257	3	0.5563	0.0478	0.353	0.0368	0.0678	8.744	21.2
28	65	153375232	333952	1.29E+08	485	7	211	3	0.4351	0.0182	0.241	0.0377	0.0691	8.062	26.4
28	55	48276224	363392	25482112	522	8	282	5	0.5402	0.0346	0.169	0.042	0.0798	10.2	41
28	67	74707200	339712	47471360	386	5	268	3	0.6943	0.0203	0.217	0.0302	0.0578	7.211	19.2
28	66	48659840	338816	23149696	399	5	230	3	0.5764	0.0313	0.229	0.0401	0.0731	7.839	23.2
28	68	27180160	338304	836096	411	5	272	3	0.6618	0.0282	0.231	0.0296	0.0632	7.448	22.6
28	65	26316288	334592	1347328	386	6	220	3	0.5699	0.0175	0.192	0.0314	0.053	7.071	19.2

Table (B.29): The calculated authentication features for user twenty-nine

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
29	38	35886592	468608	18550016	166	3	184	3	1.1084	-0.049	-0.012	0.0192	0.3226	5.465	31.78
29	33	26684800	468608	11529216	188	2	167	4	0.8883	-0.064	-0.007	0.0173	0.3333	5.3852	36.401
29	36	37929216	468608	21216128	155	2	153	3	0.9871	-0.05	-0.017	0.0251	0.3723	5	25.08
29	29	13745152	468608	780800	217	2	220	5	1.0138	-0.08	-0.005	0.0425	0.3262	7.2801	63.953
29	31	26386560	468736	11669504	259	4	270	6	1.0425	-0.102	-0.032	0.0511	0.5231	10.817	38.21
29	32	42866816	468928	14535680	268	4	197	5	0.7351	-0.089	-0.01	0.0421	0.3298	8.8401	55.973
29	26	30760064	468736	16855680	229	5	247	7.5	1.0786	-0.079	-0.006	0.0402	0.5106	9.3268	48.826
29	27	12984960	468608	937344	179	4	201	7	1.1229	-0.072	-0.002	0.0423	0.4894	11	41.4
29	27	46978944	468864	34633856	158	2	200	5	1.2658	-0.068	-0.016	0.0413	0.4706	8.544	38.288
29	29	14219648	468608	1093504	165	2	217	6	1.3152	-0.054	-0.012	0.0509	0.5474	7.2111	47.011
29	28	29453056	468608	16717312	183	2.5	218	6	1.1913	-0.049	0.0039	0.0453	0.4409	8.3012	42.72
29	28	12848512	468608	624896	246	4	173	6.5	0.7033	-0.095	0.0048	0.0327	0.2979	9.3966	52.469
29	32	15781248	468608	937344	180	2.5	197	4.5	1.0944	-0.071	-0.019	0.0379	0.6087	7.3079	31.305
29	29	13464960	468480	629120	233	3	210	5	0.9013	-0.096	-0.014	0.045	0.4894	9.434	56.939
29	27	12502016	468736	472576	243	4	213	6	0.8765	-0.102	-0.017	0.0447	0.4787	10.198	68.949
29	29	27230720	468736	14091648	211	2	192	5	0.91	-0.066	-0.007	0.0328	0.4894	10.198	51.546
29	28	13120384	468736	472704	155	3	202	4	1.3032	-0.068	-0.021	0.0415	0.4731	7.8262	40.361
29	31	14258816	468608	480896	152	2	190	4	1.25	-0.075	-0.02	0.0346	0.4468	6.0828	39.962
29	27	27034240	468608	15011968	203	4	225	7	1.1084	-0.086	-0.015	0.0365	0.4149	8.9443	46.098
29	29	41373824	468608	14111744	203	5	208	7	1.0246	-0.071	0.0053	0.0474	0.4255	9.8995	46.872
29	28	23913472	468608	11399808	158	3	195	5	1.2342	-0.062	0	0.0463	0.4894	8.0311	26.173
29	28	33065344	468608	19785088	162	4.5	147	3	0.9074	-0.073	-0.029	0.0275	0.3478	6.5	35.228
29	27	26465536	468608	13630080	179	3	216	6	1.2067	-0.073	-0.015	0.0479	0.4842	10	42.638
29	27	12653312	468608	622976	186	4	201	6	1.0806	-0.078	-0.016	0.0298	0.5652	10.05	32.558
29	25	27455616	468736	16048256	158	5	177	6	1.1203	-0.076	-0.029	0.0373	0.5532	7.6158	38.328

29	28	22960128	468672	10547840	184	3	145	4	0.788	-0.055	0	0.0345	0.3617	7.6586	37.121
29	26	27059328	468608	14857472	152	4	176	3.5	1.1579	-0.063	-0.01	0.0333	0.3763	8.772	37.59
29	26	24026496	468608	12439296	156	4	194	6	1.2436	-0.086	-0.028	0.0409	0.4149	8.9721	33.302
29	25	26803456	468608	15712896	195	5	178	5	0.9128	-0.094	-0.015	0.0637	0.6471	11	31.064
29	25	25830272	468736	14577664	186	5	176	5	0.9462	-0.078	-0.009	0.0428	0.6957	8.6023	43.463

Table (B.30): The calculated authentication features for user thirty

User	#Points	TotTime	MedT	Max T	TotX	MedX	TotY	MedY	TY/TX	MedVx	Max vx	MedVy	Max vy	MedR	MaxR
30	34	13558400	342784	2196864	209	6	121	3	0.5789	0.0595	0.219	0.049	0.0767	7.448	18.4
30	34	13273984	343808	1312768	208	4.5	143	3	0.6875	0.0485	0.459	0.097	0.1474	7.808	26.9
30	32	11886080	343872	1189632	183	6	122	3	0.6667	0.0646	0.304	0.0914	0.1356	8.559	15.7
30	34	12154112	334016	1026816	242	8	100	2	0.4132	0.0633	0.298	0.0839	0.1176	8.303	18.1
30	40	17488640	340608	1635328	176	4	134	1.5	0.7614	0.0344	0.284	0.053	0.112	6.041	18.6
30	42	79361664	353600	4.4E+07	209	4	143	3	0.6842	0.0453	0.313	0.082	0.1148	6.364	17.5
30	38	13720064	338944	906752	219	5.5	118	3	0.5388	0.04	0.287	0.0707	0.125	6.854	15.8
30	44	48721920	349760	3E+07	196	3.5	106	1.5	0.5408	0.0248	0.361	0.0541	0.1053	5	13.3
30	31	11532544	347008	1137024	283	9	136	3	0.4806	0.0685	0.529	0.1092	0.19	10.77	20.2
30	36	13644032	340800	993280	219	5.5	114	2	0.5205	0.045	0.231	0.0624	0.0938	6.662	24.5
30	31	12662144	355968	1920384	227	7	123	4	0.5419	0.0574	0.486	0.0762	0.1151	9	20.2
30	45	16570240	324864	1384832	208	4	118	2	0.5673	0.0367	0.294	0.0693	0.1218	5.385	15.3
30	31	11794432	343296	1056896	225	7	109	3	0.4844	0.0548	0.383	0.0806	0.1305	9.055	21.5
30	27	10607488	333440	1801344	246	9	163	4	0.6626	0.0723	0.429	0.1329	0.2029	11.66	22.5
30	37	16543872	353408	2170752	256	6	133	2	0.5195	0.0487	0.6	0.0562	0.118	7.211	25.8
30	29	10556928	343936	861952	318	11	183	4	0.5755	0.0782	0.722	0.1592	0.2607	15.23	32.6
30	51	79877632	347904	6.2E+07	207	3	95	1	0.4589	0.0279	0.294	0.0444	0.0604	4	15
30	48	18383360	343040	1574016	242	4	100	2	0.4132	0.0399	0.326	0.0468	0.0649	5.099	17
30	28	11448960	350848	1004800	264	8.5	165	6	0.625	0.082	0.656	0.1057	0.1507	11.89	25.2
30	32	14393728	336000	3179008	189	6.5	117	3	0.619	0.0444	0.313	0.0779	0.1302	8	14
30	42	14958592	326656	1270016	204	4	100	2	0.4902	0.0467	0.304	0.0675	0.0944	5.744	13.9
30	33	12021632	352896	751744	236	7	136	4	0.5763	0.0532	0.306	0.0915	0.1323	8.544	19.4