USER AUTHENTICATION IN PUBLIC CLOUD COMPUTING THROUGH ADOPTION OF ELECTRONIC PERSONAL SYNTHESIS BEHAVIOR

MOHANAAD TALAL SHAKIR

COLLEGE OF GRADUATE STUDIES
UNIVERSITI TENAGA NASIONAL

2020

USER AUTHENTICATION IN PUBLIC CLOUD COMPUTING THROUGH ADOPTION OF ELECTRONIC PERSONAL SYNTHESIS BEHAVIOR

MOHANAAD TALAL SHAKIR

A Thesis Submitted to the College of Graduate Studies, Universiti Tenaga Nasional in Fulfilment of the Requirements for the Degree of

Doctor of Philosophy in Information and Communication Technology

April 2020

DECLARATION

I hereby declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently submitted for any other degree at Universiti Tenaga Nasional or at any other institutions. This thesis may be made available within the university library and may be photocopies and loaned to other libraries for the purpose of consultation.

MOHANAAD TALAL SHAKIR

Date : 22-4-2020

ABSTRACT

Public cloud computing is one of the deployment services that can be accessed by all potential users through a website or program interface, at any time, from anywhere, and by using any device. Authentication layer works to allow the legitimate user only to access into the public cloud. It allows one single instance of software to serve various clients. Password-based authentication is considered the cheapest and most popular and commonly used methods of computer authentication. However, illegitimate access is considered one of the most significant challenges in public cloud computing. In the same context, Many researchers have reported password leaks as a major issue. Multi-factors authentication (MFA) model, such as a password with a Smart card, SMS, and Biometric, is suggested by many researchers to avoid this problem. It is considered hard to break as compared to the use of password-based authentication alone. One of the most critical issues in MFA in public cloud computing is related to the accuracy of authenticating legitimate user access when facing stolen password attacks. In this thesis, the research gap related to the accuracy of authenticating a legitimate user is brought to light. The problem is in multi-factor authentication with public cloud computing, the performance of user authentication in password-based authentication needs to move from traditional security processes to intelligent security processes. This thesis proposes electronic personal synthesis behavior (EPSB) for improving the accuracy of user authentication in a public cloud. It aims to improve the accuracy of authentication in public cloud computing by dealing directly with behavior recognition, confidence range, and finally generated the electronic personal synthesis behavior (EPSB). Moreover, the learning process of the proposed algorithm for behavior recognition designed as a matching factor with a password during the authentication process. The evaluation criteria conducted according to the accuracy, acceptance and use. Firstly, an experiment by simulation on the stolen password conducted to examine the accuracy of authenticating a legitimate user according to the EPSB approach. Secondly, a questionnaire prepared to examine the acceptance and use of EPSB. Finally, the implemented algorithm tested by comparing the accuracy of the current authentication framework with and without an EPSB algorithm. The results of adopting $\text{EPSB}_{\text{algorithm}}$ in authentication process lead to the mitigation of stolen password attacks' effects and the shift from traditional authentication strategies to intelligent authentication operations.

ACKNOWLEDGMENT

First of all, praises be to Allah (S.W.T) for giving me strength, ability, confidence and patience to complete my PhD thesis. Indeed, without his help and will, nothing is accomplished. I also must thank our prophet Mouhammed (P.B.U.H) for encouraging us to seek for knowledge, as he said "There is no one who goes out of his house in order to seek knowledge, but the angels lower their wings in approval of his action".(Sunan Ibn Majah);

I would like to express my most sincere gratitude to my supervisor Dr. Asmidar Abu Bakar, and co-supervisor Asoc. Prof. Dr. Yunus Yusoff for their guidance and support throughout this work. They have been a great source of inspiration for me. No words can express how grateful I am to them;

I would like to thank Universiti Tenaga National for providing me with the facility for completing this thesis;

For my father, mother, brothers and sisters, who support me during all study time;

To my wife, for their unwavering patience to help me, and for the sacrifices they made so that I could make my dream come true;

To my children Bareq, Qhasag, Banan, Khalid, Arqam and Ayham who are the source of my inspiration too;

Most importantly, none of this would be possible without the love and patience of my dear friends in Iraq, Oman and Malaysia, I especially mention Mohamad Yahyaa, no amount of thanks can be said to express my appreciate for their support during my study.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

TP	Total number of documents correctly
FP	Refers to the total number of documents incorrectly
FN	Refers to the total number of documents ignored
TN	Total number of documents correctly rejected
MN	Min
MX	Max
S	Sum
S2	Sig. (2-tailed)
MD	Mean Difference
M1	Mode
M2	Mean
M3	Median
P	Percent
V.P	Valid Percent
C.P	Cumulative Percent
F	Frequency

LIST OF ABBREVIATIONS

EPSB	Electronic Personal Synthesis Behavior
NIST	National Institute of Standards and Technology
PaaS	Platform-as-a-Service
SaaS	Software as a Service
IaaS	Infrastructure-as-a-Service
BBS	British Broadcasting Corporation
MITMA	Man In The Middle Attacks
CSP	Cloud services provider
2FA	Two-Factor Authentication
MFA	Multi-Factor Authentication
PCC	Public Cloud Computing
OTP	One-Time Password
TOTP	Time-Based One-Time Password
OATH	Initiative for Open Authentication
KDC	Key Distribution Center
ZKP	Zero Knowledge Proof
TTP	Third Trusted Party
MCC	Mobile Cloud Computing
CCAF	Cloud Computing Adoption Framework
AS	Authentication Service
R	Range
PU	perceived usefulness
PE	Perceived Ease of Use
BI	Behavioral Intention to Use
AU	Actual System Use
TCR	Total Confidence range
CR	Confidence range
FSS	Feature selection method
TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action
QoE	Quality of Experience

LIST OF PUBLICATIONS

1. Mohanaad Shakir, Asmidar Bit Abubakar,Younus Bin Yousoff, Ali Makki Sagher, Hussam Alkialy,” Diagnosis Security Problems for Hybrid Cloud Computing in Business cloud”, Journal of Theoretical and Applied Information Technology, E-ISSN: 1817-3195,ISSN: 1992-8645,31 Aug 2016. Vol.90. No.2.

2. Mohanaad Shakir, Asmidar Bit Abubakar, Younus Bin Yousoff, Mohammed Waseem, Mostafa Al-Emran,” Model Of Security Level Classification For Data In Hybride Cloud Computing”, Journal of Theoretical and Applied Information Technology,15th Dec 2016, Vol94.No.1, Page 133-141, E-ISSN: 1817-3195,ISSN: 1992-8645.

3. Mohanaad Shakir, Asmidar Bit Abubakar, Younus Bin Yousoff, Mostafa Al-Emran , Maytham Hamood,” Application Of Confidence Range Algorithm In Recognizing User Behavior Through E-Fingerprinting In Cloud Computing “, Journal of Theoretical and Applied Information Technology, E-ISSN: 1817-3195,ISSN: 1992-8645.

4. Mohanaad Shakir, Maytham Hamood, & Ahmed Kh (2018). Literature review of security issues in SaaS for public cloud computing: a meta-analysis. International Journal of Engineering & Technology, 7 (3) (2018) 1161-1171.

5. Mohanaad Shakir, Asmidar Bit Abu Bakar , Yunus Bin Yusoff, and Mustefa Talal Sheker : Diagnosis Security Problems for Hybrid Cloud Computing in Medium Organizations, NIST2016-National Conference for talent of cloud computing, University of Nizwa,Oman.2016.

CHAPTER 1

INTRODUCTION

1.1 Research Background

Public cloud computing is one of the deployment services that can be accessed by all potential users through a website or program interface, at any time, from anywhere, and by using any device [1]. A public cloud is "based on shared physical hardware which is owned and operated by a third-party provider," where the infrastructure is shared by many clients[2]. Amazon Web Services, Microsoft Azure, and Google Cloud are examples of public clouds[3]. Some of the most common real-world examples of public cloud services include services such as cloud-based server hosting, storage services, webmail, and online office applications [1][3].

Public cloud computing is likely to be jeopardized by many security issues, such as false authentication and authorization, illegal access control on cloud data, threat detection, data deletion, and covert communication [4]. The issue of authentication in public cloud computing (PCC) has received considerable critical attention[5]. According to the National Institute of Standards and Technology (NIST), unauthorized access is considered one of the biggest challenges in authentication process in public cloud computing [2]. Besides, authentication accuracy in public cloud computing is crucial as it authenticates an authorized user and prevents unauthorized access to information resources [2]

There are four models of authentication; Ownership model, Inherent-based model, a mixed model, and Knowledge-based model[6]. Firstly, Ownership model requires users to constantly carry additional physical devices, such as a security token or smart card. Secondly, Inherent-based model has two sub-categories, which are physiological and behavioral. Thirdly, the mixed model has two or more authentication categories. Finally, the Knowledge-based model, it requires the knowledge of private information of an individual to prove that the person providing the identity information is the owner of the identity[6].

In the Knowledge-based model, the password is considered the cheapest and most popular and common used methods of computer authentication, in which 86% of U.S. companies use password authentication [7]. Passwords can be easily memorized and users at no cost can use them in their daily life[8]. However, users may forget their passwords when having too many for various accounts [9]. Furthermore, password leaks have been noted as one of the common problems around the world [10]. This problem threats customer's information, privacy and financial [10]. Password leaks have been recorded as one of the major problems in many famous organizations, such as iCloud and Apple Inc. [11][10]. Leaks happen via a wide range of threats, such as Stolen password attacks, Impersonations, Man In The Middle Attacks (MITMA), and Spoofing Attack. These threats influence negatively the process of authenticating the authorized user [12][13]. As time passes, different methods of authentication have gradually been introduced in the forms of biological and graphical passwords, such as password with Smart Card, SMS, Biometric, and Behavior recognition to avoid these threats. The new emerging trends of authentication systems combine two or more methods to successfully distinguish between authorized and unauthorized users.

However, passwords do have limitations. First, password with smart card has many limitations, such as offline guessing attack, stolen password attack, and impersonation [14][15]. Therefore, users must be made aware of the fact that their personal information can be lost, stolen, or shared. Second, password with SMS entails some disadvantages, such as expensive, smartphone battery can discharge in any instant of time, and if the smartphone is factory reset or lost, or authenticator application is accidentally deleted, the token would be lost, and its recovery is immensely difficult. Third, passwords with biometrics have the biggest downsides as they influence the authentication result of the system. Examples of their disadvantages are password cannot be changed, expensive, susceptible to forgery methods, unable to recognize users with surgery, scars, and sunglasses, and the risk of inaccurate recognition. Furthermore, password-based authentication with Biometric, SMS, and Smart card have other restrictions. For example is when a user has to memorize secret information used as a pass words, in which the user might forget when are rarely used. In addition, several authentication factors are utilized for users' authentication that increases the authentication procedure time and complicates the procedure of this authentication method [16][17][18]. Therefore, these restrictions have serious effects on the process of user authentication. To overcome these issues, several researchers have recommended the application of behavior recognition with a password to improve the authentication process [19][20][21][22][23][24].

Behavior recognition technique is considered as cheap “no need more hardware” and easy to use “no need to add any new authentication procedure”. Researchers have suggested authentication approach that uses behavioral recognition with human factor such as unique value, press on keyboard, and move mouse [25][26][27][28][29][30][31][32] [33][34]. Many researchers recognise the ability of the authentication model in dealing with human behavior when authenticating users[25][28][29][32]. Monrose et al. [28] proposed an authentication method that uniquely identifies users based on the analysis of keystrokes. The limitations to this model occur when the user is faced with environmental factors that affect their typing patterns, as well as when users are monitored with the web-based system only. Shen et al. [29] believe that this model is used to observe behavioral features in mouse movement to detect malicious users. The limitations of the model are: 1) behavioral variability; 2) the lacking in the integration and analysis of the user’s behavior background history. Therefore, any changes may identify the user as an impostor. Xie et al.[35] use a notable approach to identify legitimate users early when using online services by implementing a vouching process without the use of biometrics[32]. They introduce a technique, Souche, to monitor vouching via social communities (i.e., Twitter, Email). The limitation of Souche is that the effectiveness of such detection strategies is bound by the behavioral assumption of legitimate users who refuse to interact with unknown accounts. This was proven unrealistic by various experiments [36][37][38].

L.C. Leonard [25] proposed the web-based behavioral modelling for continuous user authentication (CUA). This technique can be used with web applications to provide reliable and secure authentication. The main limitation of this technique is the time required for analyzing the authenticating user when s/he logins into the system by comparing current and previous user behavior. This time gap enables an unauthorized user's illegal access to deal with data in the case of stolen password attacks.In addition, the monitoring of authenticity of the user interacting with a password, through behavior, is neglected.

Several studies have focused on the behavior of authorized user that interact with the web-based system. In a related context, most of these studies disregard behavior of an authorized user that interact with password-based authentication. In this thesis, we suggest an Electronic Personal Synthesis Behavior (EPSB) to fill this gap by transparently monitoring user's activities. This is to identify deviations from normal workflow patterns on password from three different perspectives: 1) Duration of input active password from an authorized user; 2) Password style; 3) Password Error. Besides, many researchers recommended to adopt intelligent model in the authentication process [19][20][21] [22][23][24]. The results of these studies, when embedded the human factor into the authentication process, lead to the improvement in its accuracy at authenticating an authorized user. The objective of this work is to improve the accuracy of user authentication through adopting intelligent behaviour recognition mechanism as a matching factor with a password during an authentication process.

1.2 Research Motivation

According to NIST [2], public cloud computing is suffering from weak confidentiality and integrity sureties. Insufficient security controls in the cloud provider's platform could affect negatively the confidentiality and privacy, or integrity of the system. For example, the use of an insecure method of remote access could allow intruders to gain unauthorized access, modify, or destroy the organization's information systems and resources; to deliberately introduce security vulnerabilities or malware into the system; or to launch attacks on other systems from the organization's network, perhaps making the organization liable for the damages incurred[2][39][40].

In the light of that, on September 1, 2014, foreign hackers used the disk system vulnerabilities of iCloud to steal the Hollywood actress private photos and they were released into the network by the British Broadcasting Corporation (BBS) - the Hollywood private-picture scandal event that shocked the world. Apple Inc. has noted that hackers did not directly intrude into the storage service system of iCloud; rather, it was an invasion of the actress' accounts from the terminal. With the popularity of smartphones and cloud computing, the cloud services bring great convenience to people, which allow them to share pictures, video, documents, applications, and other important data by the cross-platform in real time. However, if the cloud account is stolen, they will lose their data, which may cause huge losses[41][42]. The authentication process of an authorized user in public cloud computing needs to be improved by adding new tools or security level to enhance the accuracy of the authorized users[24][25].

1.3 Problem Statement

Insufficient password security controls in the public cloud computing could negatively affect the confidentiality and privacy of the system. For example, the use of the stolen password by remote access through authentication layer could allow an unauthorized user to gain unauthorized access, modify, or destroy an organization’s data[2]. In public cloud computing, the authentication is considered a millstone to allow an authorized user to deal with data saved in the cloud [2][43]. Authentication performance from an accuracy criterion is defined as the capability of the authentication system to correctly determine an authorized user [44][45]. Password-based authentication is still one of the most popular methods of all [8], as it is considered the cheapest and the most common methods of computer authentication. A number of researches have reported password leaks as major issues in many well-known organizations, such as iCloud and Apple Inc. [11]. However, these password leaks are having a serious effect on the accuracy of user authentication when facing stolen password attack [2][10][11][12][13]. Multi-factor authentication (MFA) model, such as a password with Smart card, SMS, and Biometric, is suggested by many researchers to avoid this problem [46]. The model of MFA is considered hard to break as compared to the use of password-based authentication alone. However, a set of deficiencies have been noted in the model of MFA such as high cost and stolen password attack which were discussed in details in section 1.1 above. Consequently, to improve the accuracy of user authentication, this thesis adopts the intelligent mechanisms to represent the user’s behavior as a matching factor with a password during an authentication process. The gaps identified from the literature are used to investigate any potential areas in the accuracy of user authentication in a public cloud that requires further enhancements and modifications. The points below are gathered and summarized from the literature review:

1. Most current authentication approaches[25][47][48][49][50][51][52][53][54][55] are weak when facing stolen password attack, which lead to negative effects on the accuracy of user authentication.

2. Most current studies have neglected or disregarded the presence of human behavior as a matching or complementing factor in authentication [24]. They also have neglected the fact that intelligent in password-based authentication is highly weak [22][56]. Therefore, when an unauthorized user trying to log into a cloud through an authorized password, device, and network on the first attempt, the original user's authority will grant the unauthorized users' access to data that are saved in the cloud.

3. Many researchers have recommended the application of intelligent mechanisms to represent human behavior in an authentication layer to improve the accuracy of user authentication[19][22][23] [24][56].

4. Previous studies of human behavior recognition have not dealt with monitoring user when interacting with a password before access into the system[26][29][30][33].

From reviewing the current state of the literature work, it was found that the accuracy of the current Multi-factor authentication in public cloud computing is deficient in dealing with the stolen of password attacks[57][58][59][60][61][62][63][64][65]. In line with the above, the purpose of this thesis is to fill in the gap related to the accuracy of user authentication. The weakness in most of the authentication process methods to face the stolen password attack affects negatively on the accuracy of user authentication [51][66][67][53][54][49][68][48][50][55](see Figure 1.1 below).This weakness is mainly due to its high cost of implementation and deployment. Besides, learnability from users behavior in authentication process is highly weak[21][56]. All in all, in multi-factor authentication within public cloud computing, the authentication process in password-based authentication process needs to move from traditional security process to intelligent security process [24] by developing an algorithm. This algorithm has an intelligent mechanism for representing an authorized user behavior that can prevent unauthorized user automatically[20][56]. Thus, this work adopts the intelligent mechanisms to represent the user's behavior as a matching factor with a password during an authentication process.

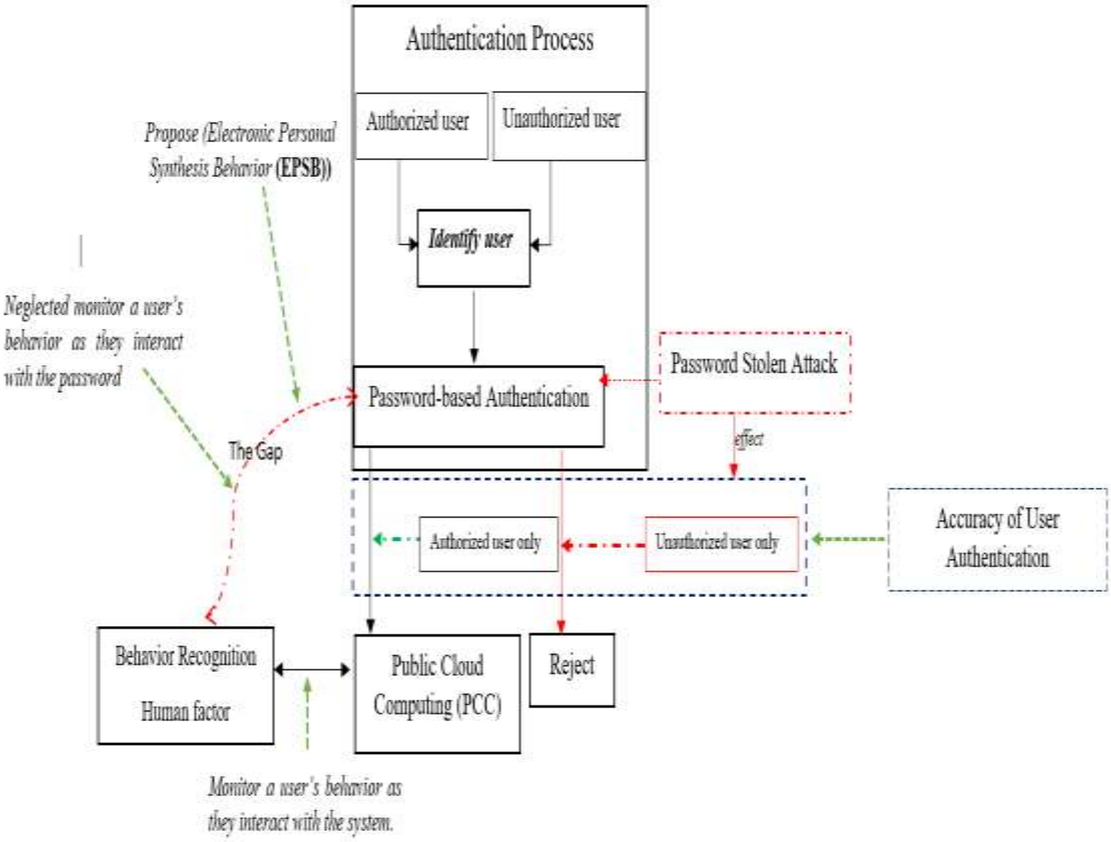

Authentication Process
Authorized user
Unauthorized user
Identify user
Password-based Authentication
Password Stolen Attack
effect
Propose (Electronic Personal Synthesis Behavior (EPSB))
Neglected monitor a user's behavior as they interact with the password
The Gap
Authorized user only
Unauthorized user only
Accuracy of User Authentication
Behavior Recognition
Human factor
Public Cloud Computing (PCC)
Reject
Monitor a user's behavior as they interact with the system.

Figure 1.1 Research Gap

1.4 Research Questions

The following research questions are used as a guide to conduct this research at various stages and to achieve the research objectives:

RQ1: What are the issues related to the accuracy of password-based authentication in public cloud computing?

RQ2: How is an algorithm designed to improve the accuracy of the authentication process in public cloud computing?

RO3: What is the required architecture to represent the behavior of the authorized user in password-based authentication in public cloud computing?

RQ4: How does the proposed algorithm improve the authentication process, and how does the validity of the proposed algorithm determined?

1.5 Objectives

1) To review the current authentication methods in public cloud computing focusing on the password-based authentication as follows:

   a. To point out the main processes of an authentication method that avoid unauthorized access.
   b. To highlight the strengths and weaknesses of the current authentication method in public cloud computing.

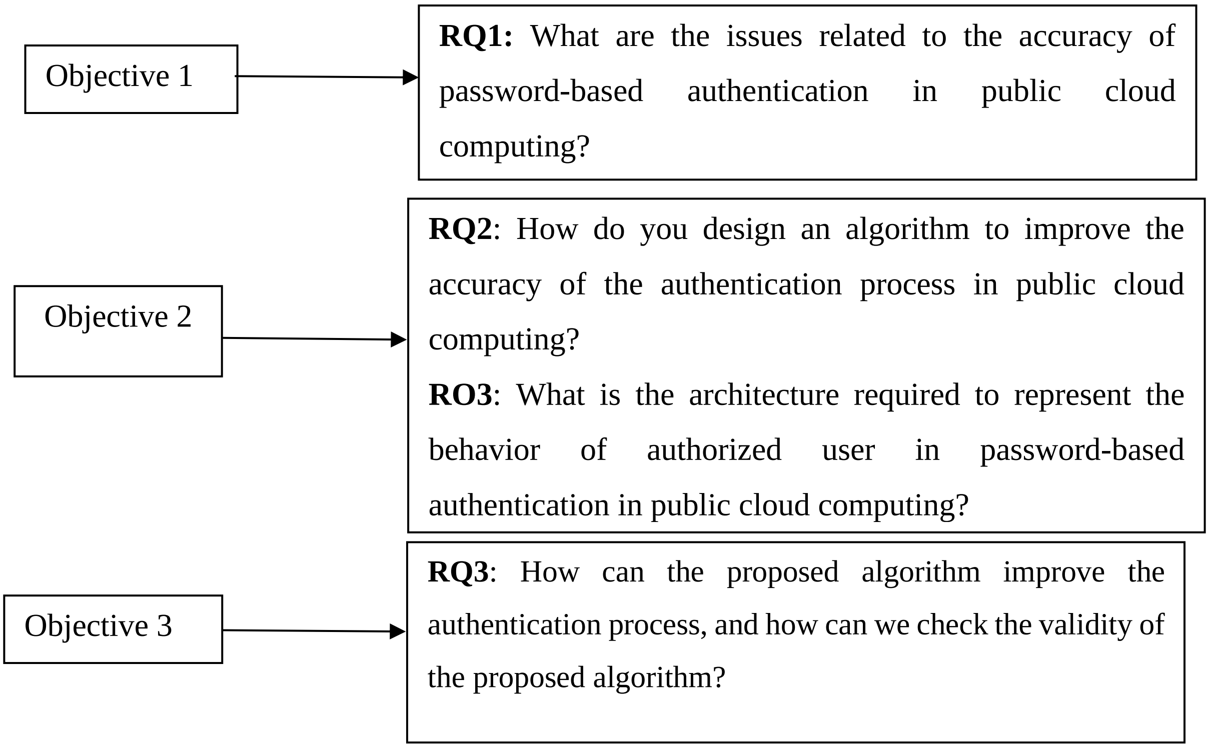
2) To develop an algorithm that incorporates user behaviour evaluation in order to improve the accuracy of user authentication in public cloud computing.

The algorithm can analyze authorized user behavior. This algorithm works to monitor and analyze all the authorized user activities associated with the authorization password duration, error, and style to recognize any suspicious activity. The expected outcomes are stated below:

   i. The identification of suitable processes to monitor and prevent any suspicious users.
   ii. The identification of the behavioral aspect of the authorized users; monitoring and analyzing each user’s behavior that is associated with the authorized user’s password. This algorithm works to fulfil the points below:
      a. Determine unauthorized users when they start to log on to the system in their first attempt.
      b. Determine an authorized user password error from an unauthorized user.
      c. Prevent any suspicious password changes.
      d. Prevent any suspicious user to deal with sensitive data.

3) To implement and validate the proposed algorithm.

Figure 1.2 shows directions for each objective, i.e. which objective will answer which research questions.



RQ1: What are the issues related to the accuracy of password-based authentication in public cloud computing?

RQ2: How do you design an algorithm to improve the accuracy of the authentication process in public cloud computing?

RO3: What is the architecture required to represent the behavior of authorized user in password-based authentication in public cloud computing?

RQ3: How can the proposed algorithm improve the authentication process, and how can we check the validity of the proposed algorithm?

Figure 1.2 Objectives to answer the Research Questions

1.6 Research Goal

The main goal of this thesis is to develop an authentication method for the public cloud that has the potential to analyze human behavior in authentication layer for improving the processes of password-based authentication for authenticating an authorized user, to enhance the authentication accuracy in public cloud computing in an organization.

1.7 The Expected Benefits

This research will raise the security of password-based authentication in public cloud computing, through adding new security layer with a password for determining an authorized user. This study is suggests electronic personal synthesis behavior (EPSB) for adding learnability into authentication layer. Thus, the authentication layer can learn from authorized user activities in password-based authentication. The main benefits of this study are listed below:

1. Authentication layer has learnability from an authorized user activity;

2. Low cost “no need additional hardware”;
3. Quick authentication for the authorized user;
4. Two factors authentication;
5. Easy to use;
6. Prevent sensitive data from suspicious users;
7. Prevent password change from suspicious users.

1.8 Proposed Methodology

The research work is divided into many phases as shown in Figure 1.2 to achieve the objectives listed in the objective section. The researcher will collect and investigate state-of-the-art works, and determine the pros and cons in the current authentication framework for public cloud computing. Consequently, the problem is made evident by critics and defects of the current approaches, and the list of research questions has been presented. Subsequently, after clearing the problem statement, the research objectives were drawn. It is an essential section, which represents the border of this research. Afterwards, the researcher conducts the research goal and lists the objectives of the proposed algorithm design.

The proposed algorithm approach has been divided into three main ideas, time to enter the password, password style, and password error, which have been tested individually and combined and evaluated in this thesis. The first idea is depending on a speed of click on the keyboard from start to input password till press on login from an authorized user. The researcher focuses on time to type the password for diagnosis of unauthorized user confidence range. This node works to monitor all authorised user activities associated with the password through recording and analysing and tries to find the confidence range for an authorized user. The second idea is password style; this node works on monitoring the user’s behavior in selecting the password through the analysis of previous historical passwords and tries to find the confidence range. The third idea is password error; there are some repetitive errors for the legitimate user such as: using an old password, repeating a particular character, using another account’s password, not paying attention to the enabled language, or writing the capital letters as small letters and vice-versa.

Electronic Personal Synthesis Behavior (EPSB) algorithm is suggested for authenticating authorized user behavior. It stands the electronic diagnostic process to agave out the manner of the authorized user. The purposes of this algorithm to analysis the human "behavior" on the authentication layer to improve the performance of passwords by improving the predictive layer. The main task of this algorithm is monitoring all the activities associated with the password on duration, error, and style to the authorized user.

This algorithm develops by using PHP and implement in a public cloud for checking the EPSB validation. Several experiments have been performed to empirically evaluate for recording and analysing an authorized user during s/he log in and logout in public cloud computing and then will generate numeric confidence range for all authorized user. Finally, the evaluation of the proposed authentication framework for public cloud computing process is conducted through preparing questionnaire according to the technology acceptance model (TAM). As the main step of the research work, the suggests authentication will compare with current authentication methods in public cloud computing is an essential part, and the result of the comparison will decide if the approach has a good contribution or still needs an enhancement. It’s normal for every research work to have defects and weaknesses, but still needs a solution to make the approach more effective**.**

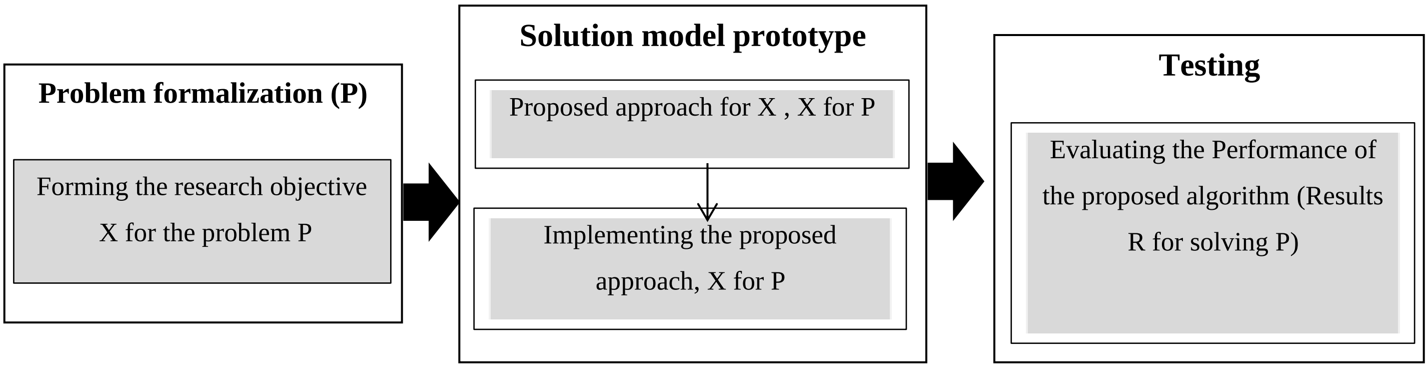

Problem formalization (P)
Forming the research objective X for the problem P
Solution model prototype
Proposed approach for X , X for P
Implementing the proposed approach, X for P
Testing
Evaluating the Performance of the proposed algorithm (Results R for solving P)

Figure 1.3: Research Work Methodology

1.9 Thesis Layout

In this thesis, the research discusses how to analyze user behavior in password-based authentication in public cloud computing. Hence, the research thesis will be divided into a set of chapters. Each chapter has satisfied a portion of the research works. Therefore, this section states the structure and organization of this thesis, and Table 1.1 briefly demonstrates the Structure as seen below:

Table 1.1: Thesis Layout

What?	Why?	How?
Introduction	Stating and highlighting the general cloud computing topic, and gives some background. Identifying the research problems, questions, and presetting the objectives. Highlighting the significance of the research. Providing the thesis layout.	a) Stating the researcher's statement. b) Writing the research objectives.
Literature Review	1) Reviewing related literature work. 2) Figuring out the strengths and defects of the related work. 3) Detecting the open research problem.	a) Criticizing the existing work. b) Linking the current work with the literature.
Research Methodology	1) Drawing the roadmap of this research work. 2) Providing the approach perspective of the proposed algorithm. 3) Explaining the evaluation work	a) Outlining the research methodology.
Proposed Algorithm	1) Generating Algorithm based on the approach perspective that is proposed on research methodology. 2) Explaining the algorithm functions.	a) Writing the algorithm pseudocode of the algorithm. b) Giving a demonstrative example.
Results and Discussion	1) Presenting the results of study. 2) Highlighting the strength of the proposed algorithms. 3) Analyzing the experimental results.	a) Empirical evaluation, drawing the results analysis. b) Comparing Password-based authentication with EPSB in public cloud computing with Password-based authentication without EPSB in public cloud computing.
Conclusion	1) Stating the contribution of the research work. 2) Explaining the work limitation and future work.	a) Answering the research questions. b) Confirming that research objectives were achieved.

This research is divided into six chapters. Following this introductory part is chapter 2: This chapter presents an overview of the public cloud computing and different authentication approaches in public cloud computing that have been developed to avoid an unauthorized access. Moreover, many current authentication approaches have been pointed out in in the investigation and a collection of the weaknesses of the state-of-the-art technique has been listed. Chapter 3 this chapter draws the direction of the research and clarifies the research roadmap. The direction of the research for this chapter is based on what is analysed in the literature works. In this chapter, we present the approach philosophy, which is based on the presented algorithm in Chapter 4. Finally, the evaluation method, used in chapter 5, is explained. Chapter 4: In this chapter, the proposed algorithm is presented. This chapter consists of many parts. The first one draws the flowchart of the proposed algorithm and architecture predictive behavior. And the second one contains the algorithm of the core of the proposed algorithm. Moreover, all the related functions used in this algorithm are discussed. Chapter5, the result of evaluating the algorithm and discussion is in this chapter. However, the experiments have been performed on a sets of future assumptions problems in password-based authentication in public cloud computing. Moreover, the result of the proposed algorithm is compared with current password-based authentication. Chapter 6: This chapter is the conclusion of this research thesis. Any suspected weaknesses are stated. Moreover, some proposals for future work are also suggested.

CHAPTER 2

LITERATURE REVIEW

2.1 Background

National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [69]. It is commonly broken down into three deployments: public, private, and hybrid [70].

Public cloud computing is weak when facing stolen password attack. For example, use of a stolen password of remote access through authentication layer could allow an unauthorised user to gain unauthorised access, and further, modify or destroy the organisation’s information systems and resources [2]. Authentication methods play a considerable in preventing unauthorized access to data that had been saved in public cloud [2]. It is classified into many types such as; Username and Password Authentication, Multifactor Authentication (MFA), Mobile Trusted, Single Sign-On, Public Key Infrastructure, Biometric Authentication and implicit authentication. In a related context, Multifactor Authentication (MFA) which has two or more sub-categories (physiological and behavioral) would be harder to break. MFA has many classical models such as a password with a smart card, pin, SMS, fingerprint, face recognition, and behavior recognition[71]. However, there are limitations to these models because the additional hardware that is needed to implement this technique would make it costly if an entire organisation is to use this feature to authenticate users, except behavior recognition.

In MFA, behavior recognition technique is considered cheap and easy to use. Many researchers recommend the current approaches of password-based user authentication research to be improved by incorporating behavior recognition in human cognitive factors both in design and run-time[25][72][27][28][29][73][74][32][33][75][76]. In addition, several current studies have focused on behavior of authorised users that interact with web-based software inside system when dealing with data, such as moving the mouse and clicking on keyboard [25][72][27][28][29][73][74][32][33][75]. However, this process has accentuated the problem of unauthorised users having a little time to deal with data which is saved in the public cloud until it is diagnosed. Moreover, previous studies of behavior recognition to authenticate an authorised user in public cloud computing have not dealt with the behavior of an authorised user that interacts with a password before accessing into the system. However, the literature has emphasised the importance of moving from traditional security processes to intelligent security processes[24].

Intelligent security is defined as the information relevant to protecting an organisation from external and internal threats, as well as the processes, policies and tools designed to gather and analyse that information [77]. There are many intelligent mechanism applications in authentication process such as Neural network in L.C. Leonard[25], Leaning Algorithm in Shi et al. [78], and agent in Mostafa et al. [79]. M. Hajivali & F. Zhang [79][80] have recommended for the intelligent actions of user authentication to be applied on public cloud computing. According to Russell et al. [81], the intelligent agent is divided into five classes, namely simple reflex, model-based reflex, goal-based, non-goal based and learning agent. In a related context, many studies[24][19][21][82] point out that learning process for simulating human behavior in authentication process is far more effective in cost and performance. Therefore, in this thesis, we work to apply a learning technique by suggesting an algorithm named Electronic Personal Synthesis Behavior (EPSB) to improve the accuracy of authenticating an authorised user by monitoring, recording and analysing a user's behavior as he interacts with the password in mitigating these problems.

An overview of the overall issues discussed in this chapter can be viewed using the conceptual framework presented in Figure 2.1 below. The framework discusses authentication in public cloud computing (PCC) concept such as the types of authentication in public cloud computing, authentication definitions, services, characteristics, authentication approaches features and also the limitation of current approaches. To know the areas of researches that are currently studied by researchers, reviews on areas of research in authentication in public cloud computing are also conducted and documented. This chapter aims to give the overall research overview in authentication in PCC and the current research areas that have been the focus of many researchers, such as multi-factor authentication in PCC, behavior recognition in authentication, and password-based authentication in PCC. The gaps from the literature are used to investigate any potential areas in authentication in PCC that require further enhancements or modifications.

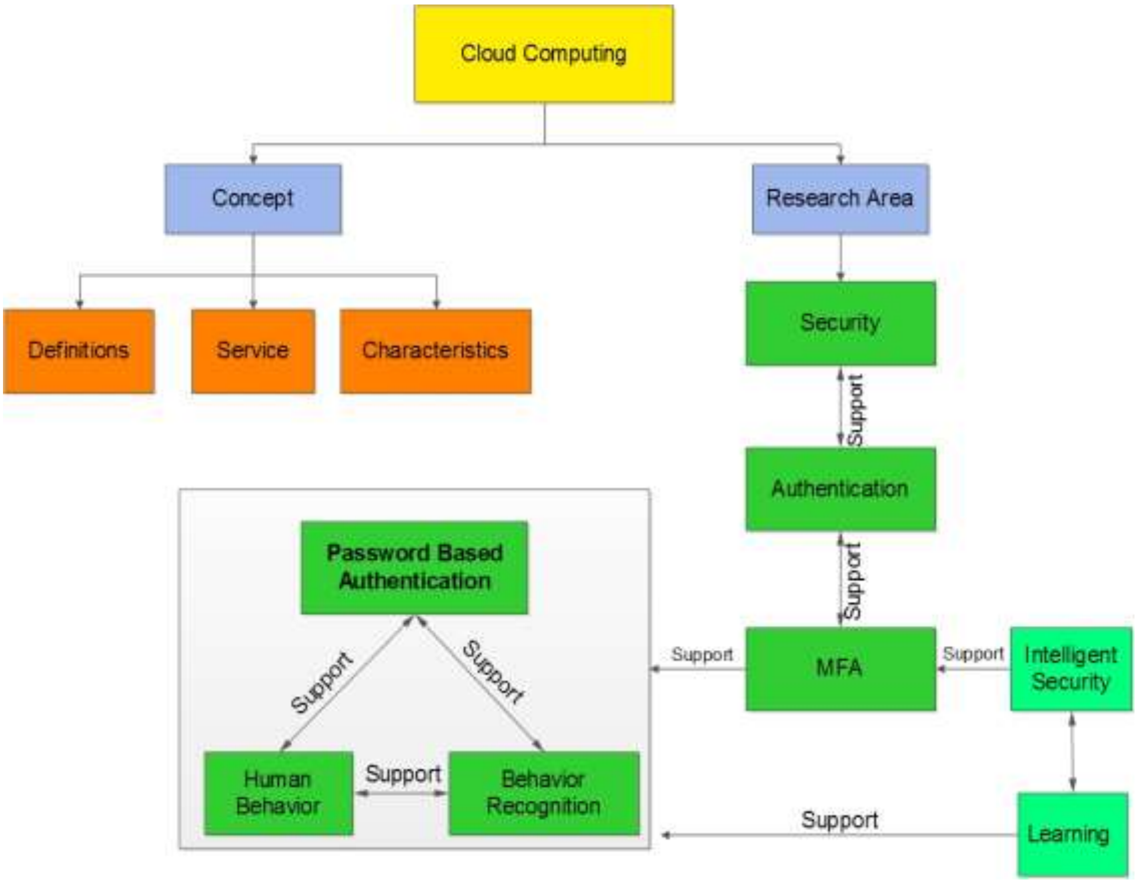


Figure 2.1 Overview of Areas of Research

2.2 Cloud Computing

National Institute of Standards and Technology (NIST), defines Cloud computing as *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [69]. It is generally divided into three; deployment, service and characteristics [70], as shown in Figure 2.2.

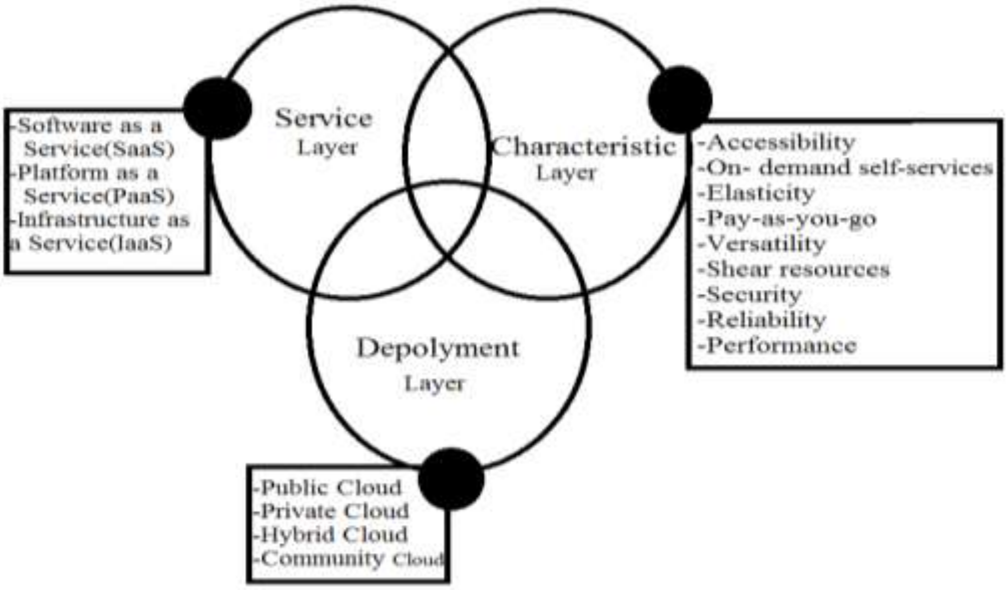


Figure 2.2 Cloud Computing Layers.

NIST classifies cloud computing based on four deployment models: public, private, hybrid and community [83]. Service models that NIST defines include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [84]. This section introduces the fundamental concepts in the field of cloud computing to provide better insights into the terminologies used for the study.

2.2.1 Cloud Service Models

A cloud service is a service which is made available to users on demand via the internet from a cloud computing provider's server as opposed to one supplied by a company's on-premise servers. Three main services are offered by cloud computing providers [69], and they are as follows :

a) IaaS (Infrastructure-as-a-Service)

Infrastructure-as-a-Service (IaaS), as its name suggests, comprises of basic storage, server, and network services for virtual use [70]. It can be used with any software chosen by the client, be it an application or operating system. Clients are in charge of maintaining the application or operating system in use, but IaaS providers are the ones that house, run, and sustain the resources that customers pay for[85].

b) PaaS (Platform-as-a-Service)

Platform-as-a-Service (PaaS), on the other hand, deals with the expansion, hosting, arrangement, employing development tools like databases, programming languages, and libraries. Clients take care of the applications, while the PaaS providers manage the storage, fundamental infrastructure and operating systems[70].

c) SaaS (Software-as-a-Service)

Software as a Service (SaaS) includes a group of software that can be used on Cloud computing, such as web conferencing, email, etc. SaaS providers extend on-demand applications to customer's usage [86].

2.2.2 Cloud Deployment Service

Cloud computing explains about the use of a network of remote servers hosted over the Internet, and there are many cloud deployments and service models available. Three main services offered by Cloud computing providers [69] are explained as follows:

a) Public Cloud

A public Cloud is most often presented as a service by a certain cloud provider, most often an organisation, which uses the Internet to make this service accessible to public users. The organisation is the owner and administrator of the infrastructure, and they have established it at its corporate premises. It extends its services on a pay-as-you-go basis. The installation, maintenance, and catering for the cloud services are performed by the cloud providers[69]. User data is accessible and operational within the cloud, which in some cases can result in privacy or security concerns [87]. Furthermore, public cloud computing is weak when facing stolen password attack. For example, use of a stolen password of remote access through authentication layer could allow an unauthorised user to gain unauthorised access, modify, or destroy the organization's information systems and resources [2]. Thus, this research sheds light on security issues in public cloud computing.

b) Private Cloud

Single company resources are, in most cases, attributed to a Private Cloud, with only internal personnel given access to them. Although the location of the cloud remains with the owner, i.e., the company, it can be hosted and administered by a cloud provider. The issues of privacy and security are the provider's responsibility. They are the ones controlling the maintenance and operational activities connected with the cloud use[70].

c) Hybrid Cloud

Undoubtedly, the hybrid cloud is a result of incorporating the previous three types – Public, Private, and Community Clouds. The availability of many resources in public is made available for the public. In this case, a hybrid cloud is addressed by keeping important data and processes within a limited group [88][69].

2.2.3 Characteristics of Cloud Computing

As a whole, cloud computing is characterised by the following features [89]:

i. **Accessibility**: Customers can use various platforms like mobile phones, laptops, tablets, or desktops to access cloud services through selected applications or browsers. A prerequisite for using cloud services is a working connection like a LAN, WAN, or the Internet.

ii. **On-demand self-service**: Cloud services are accessed instantly by users through a relatively simple process.

iii. **Elasticity**: Cloud services automatically evaluate the needs of the customer, decreasing or increasing the necessary capacity.

iv. **Pay-as-you-go**: A flexible payment schedule which allows users to pay only for the services they have used, such as storage, bandwidth, number of users, or computing power, which may cost them any flat rate or sometimes may be complimentary.

v. **Versatility**: Various applications can be used simultaneously by different service types like IaaS, SaaS, and PaaS, which can also be run at the same time.

vi. **Shared Resources**: Multiple customers (multi-tenant) share Cloud resources, for example, the infrastructure, platform, and software. This allows unused resources to serve different needs for different customers.

vii. **Security**: Theoretically speaking, cloud services should be relatively secure because the clouds and the data they store are administered centrally. In reality, however, certain scenarios including complex environments, present security concerns because different users share the same information, while the information itself is stored in an unknown physical location.

viii. **Performance**: Due to a large number of available computing resources, applications in cloud services work better and faster. This is also the main reason why cloud computing is very appropriate for applications characterised by excessive data.

Security represents one of the highest interests concerning the characteristics of public cloud computing. As Minhaj [42], Zissis et al. [90], Nalini[91], Harit[92], Mohammed[93], Akshita[94], Jayachander[95], Hao et al.[96], Ahmed et al. [97], and NIST [2] point out, the security issue is considered one of the main obstacles in public cloud computing. This issue is impacting the quality of service and the security of customers' data. Thus, our study means to clarify important security in public cloud computing. The security requirements in public cloud computing to determine the main security aspects in PCC will be presented in the next section.

2.3 Security Requirements in Public Cloud Computing

Security deals with informational privacy, integrity, and availability, and is additionally characterised by Authorisation, Authentication, and Access control (AAA), as shown in Figure 2.1.

Authentication
Access Control
Authorisation

Figure 2. 3 AAA Triangle.

Privacy, in turn, relates to the adherence to certain legal and functional requirements, including client agreements, personal identification, and legit usage, as well as purpose constraints. Additional norms are control, compliance, and clarity. When these requirements are met, the cloud arrangement is considered to be lawfully operating. ISO 7498 2 specifically concerns some supplementary specifications:

- *Identification and authentication management* applies to the functional checks for user identification and authentication that prevent antagonist malpractices within the cloud [98]. Therefore, CSPs are obliged to ensure that valid client credentials are used when users are logging into their accounts.

  In most cases, this process of verification is achieved through a username-password system, adopted during the browser or cloud login stage. An optimal identification solution involves a two-factor authentication (2FA), which adds the verification step. However, such a solution poses some access limitations to cloud services. Still, in order for client profiles to be safe and their information secure, authentication is an important part of the process.

- *Authorisation and access control* deals with the fact that various users are entitled to different prerogatives when using cloud services, especially in the case of public clouds. Their privileges depend on the account type they have purchased from the CSP. It is crucial that the CSP rightfully administers users' permissions, privileges, and claims over acquired information. Additionally, elite members of the cloud should abide by certain internal regulations as well [99]. Unauthorised users should furthermore be prevented from abusing the information of legit customers. Google and Apple are among the companies that have tried to solve this issue by functional account segregation, meaning that staff members are always monitoring elite user activities and administrators with extended data access in order to prevent data abuse and hacker attacks. It is of utmost importance for client security for clients to completely trust in the CSP and vice versa; the same is valid for the client-administrator and CSP-administrator relationships [99].

- *Confidentiality* involves numerous cloud access points and users, which makes it sensitive to illegitimate venues and pirate individuals. Clouds must ensure that only authorised users can access their data. Such precaution is especially mandatory for public clouds since they are most vulnerable. Software applications, shared information and profiles, information exposure; and weak user identifications are among the immediate threats concerning cloud storage. The cloud's multitenancy characteristics pose the threat of user data abuse since resource sharing between clients can expose private information. This is largely because a cloud separates its data assets only virtually. Information that has been deleted can be unlawfully retained and reconstructed because of the cloud's data remnants. Fraud protection should also be implemented because weak identification may result in illegitimate data access. It is mandatory that cloud service providers protect users from breaches coming from various software applications, which require access to the clients' information [90]. This data, although used by the application, must remain secure and unavailable to third parties. Privacy can be secured by popular techniques like 2FA [100] and encryption algorithms [101][102].

- *Security Plan:* Based on NIST, an organisation's security plan for public cloud computing must cover [103][104]:

  a) Policies: represent the standards and guidelines or procedures that are suggested to avoid any perceived threats.

  b) Roles and responsibilities: the purpose of this point is to determine the responsibility of tasks when implementing a security policy.

  c) Planning: the group of procedures that will be implemented for security during a system's lifecycle. These procedures are related to data in cloud storage. This point imposes stringent standards in security and privacy issues when dealing with data.

  d) Ensure: this point determines the safety range of cloud computing in its environment.

  e) Accreditation: verify the proposed system matches the core standards.

Moreover, there are more security specifications such as *Integrity*, *Non-repudiation* [105]. *Availability* [90]. *Compliance and audit*, *Transparency*, *Governance*

Accountability[106]. On the other hand, Nalini et al. [91] point out that public cloud computing is likely to be jeopardised by many security issues. In a similar context, Gartner points out top seven security issues that clients should take into considerations together with vendors before public cloud computing which is: 1) privileged user access, 2) regulatory compliance, 3) data location, 4) data segregation, 5) data recovery, 6) investigative support, and 7) long-term viability [107]. In addition, Carrol et al. [89] outline some concerns that are important in addressing public cloud computing security issues. These concerns include administration and control, data security, network security, physical security, logical access, compliance and virtualisation. In the same vein, Jin Li et al.[4] in his article "*Special Issue on Security in Cloud Computing"* note the top five current security issues in public cloud computing. These issues will be summarised in the next section.

2.4 Security Issues in Public Cloud Computing

Jin Li et al. determine five special issues on security in public cloud computing[4]: 1) Authentication and authorization; 2) Access control on cloud data; 3)Threat detection; 4) Data deletion; and 5) Covert communication. For authentication and authorisation, it is considered one of the important security issues and is still a highlighted factor[5][108] [109][110]. Authentication process in public cloud computing is a major consideration [2]. It works by granting authentication to an authorised user while preventing unauthorised access to information resources in the public cloud. In addition, another major feature of public cloud computing is multi-tenancy. It works by allowing one single instance of software to serve various clients. However, this will also lead to authentication and identification problems. Multi-tenancy may lead to different users using different identity tokens and negotiation protocols, which will cause interoperability defects. The complication that will arise from the data security protection mechanism will likely provide chances for malicious utilisation[98]. Access control, which is the second issue, concerns a system that controls access to services or resources made by cloud users based on authentication, authorisation attributes of subjects, attributes of objects or resources as well as system attributes which conforms to policies. Each entity, i.e. subject and object or resource is identified by its attributes. Subject's attributes are divided into two categories which are mutable and immutable[111]. The third issue, threat detection, is an effective means to guard against malicious attacks such as stolen password attack in public cloud computing[4]. For the fourth issue which is data deleting, data owners normally store their data on the remote cloud which helps in reducing the data owner's overhead as the cloud server maintains the data for them, e.g. in storing, updating and deleting. However, the data deletion that comes with it poses a security challenge as the data may not be deleted by the cloud server, for reasons such as financial incentives[112]. In the fifth issue which is covert communication, as a major approach to handle information leakage, covert channels are rapidly gaining popularity with the exponentially growing cloud computing and network resources. However, this brings a higher risk to the covert channels [53]. Overall, these studies highlight the special issues on security for public cloud computing. The issue of authentication in public cloud computing has received considerable critical attention. Therefore, in this thesis, we work to deal with this issue.

2.5 Authentication Method in Public Cloud

User authentication in public cloud computing involves the process of validating the identity of the user, ensuring that he is authorised to gain access to public cloud computing [54]. Being a critical aspect of security enforcement approaches in public computing, authentication is crucial in protecting users against present security and privacy issues by blocking unauthorised access to the public cloud user information [113][114]. According to the Correlation Matrix of Latent Variables (Security Risk Construct) on page 68, the author conducts a study to asses the risk in public cloud computing. The result of this study considers the diagnosis of the authorised user for access into the cloud as a top concerning issue among groups of security risk in cloud computing[115]. Authentication layer in cloud computing is established to authenticate an authorised user and grant him authority to access into data which is saved in cloud computing. Authentication in public cloud computing (PCC) is classified into seven types which are Username and Password Authentication (password-based Authentication), Multifactor Authentication; Mobile Trusted, Single Sign-On, Public Key Infrastructure, Biometric Authentication and Implicit Authentication as shown as in Table 2.1 below. Even with the increasing number of innovative ways to authenticate users, password-based authentication is still the favourite method chosen. [8].

Table 2.1 Authentication Types

Authentication Type	Description
Username and Password Authentication	Confidentiality and privacy can be maintained at some level in this authentication technique. For the information to be accessed in the CSP, the user needs to enter the username and password. As it is difficult to determine whether the request is from the authorised user, this technique does not seem to provide higher and reliable security. Moreover, very easy passwords chosen by the users make it easy for a machine to guess them. Even the best password can be stolen by brute force and dictionary attacks. In another case, the input constraints in a cloud computing environment make it hard for users to set a complex password which makes them use easy and short passwords. Users also reuse their passwords in many different servers, and this adds to the security risks of users' pooled information. Strong passwords protect by making it impossible for brute force and dictionary attacks to happen. The length of the password is said to determine the security it delivers. There have been various protocols presented in which a user can use a single password authentication that is recognised in numerous services securely [59]. They protect users from a dictionary attack, cross-site attack, malware and phishing. These proposed protocols work on the premise that the user's password is still secure even if the mobile device is stolen.
Multifactor Authentication (MFA)	Multi-factor authentication (MFA) method works by confirming a user's said identity in which access is granted only after the user presents two or more pieces of evidence (or factors) for a valid authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherent (something the user and only the user is)
Mobile Trusted	Trusted Computing Group (TCG) introduces a set of conditions that stores, measures and reports software and hardware integrity via a hardware root-of-trust (Mobile Trusted Module (MTM) and Trusted Platform Module (TPM). While TPM is for PCs, MTM security aspect is set in mobile devices [60]. With MTM, the integrity and reliability of a mobile platform is guaranteed [61]. There are three main issues that come with MTM. The first issue is the need to balance fairly distinct goals at the system-level designs. The second issue points to the cryptographic algorithms which MTM should be able to support, and the third issue is related to the application of cryptographic primitives.
Single Sign On (SSO)	Single Sign On (SSO) is a method of gaining access to multiple independent software systems in a way that a user is able to have access to all the systems without being required to re-login in each application [62]. Through this process, the user's access to numerous services is supported and the threat for the administrators to practically direct users is reduced. As it prevents the user from having to remember many passwords, user efficiency is improved and the amount of time spent on typing numerous passwords to login is decreased.
Public Key Infrastructure (PKI)	Traditional authentication method, such as RSA, is based on the secret key and primarily supports the placement of traditional asymmetric cryptographic algorithms. The identity of a user is proven using a private key. In security protocol designs for Secure Electronic Transactions (SET) and Secure Socket Layer (SSL/TLS) for example, authentication is handled by Public Key Infrastructure (PKI). Its mechanism manages data integrity, data confidentiality, non-repudiation, strong authentication and also authorisation. The proposed security characteristics of cloud environment use combination of SSO, Public Key Infrastructure, cryptography techniques and LDAP; to ensure the integrity, authentication and confidentiality of data and communications [33]. This model shows benefits of both single technologies and their combinations. PKI is an important feature in security and authentication of users in a distributed environment such as that of mobile cloud computing, cloud computing and wireless sensor network.
Biometric Authentication	The process of validation is considered complete if a user is indeed who he claims to be. The word "biometric" is derived from the Greek word "bios" meaning "life" and the word "metron" meaning "measure". In biometric authentication, there are three important factors of information security: identification, authentication and non-repudiation. This authentication technique is based on recognition of an individual's behavioral and physiological features. Its ability to provide the biological proof of what we are and what we know makes biometric authentication a strong authentication technique [63]. There are two types of biometric authentication which are behavioral and physiological. Behavioral biometric depends on the behaviors of the user where signatures, keystrokes and voice prints are identified. Physiological biometric, on the other hand, is based on physical characteristics and identifies features such as hands, faces, iris , fingerprints, palm-prints and retina.

Implicit authentication	This approach authenticates a user by observing his behavior and is suitable to be used in mobile devices as such devices are capable of collecting a rich set of user information - be it location, motion, communication or his usage of applications. A number of profiling techniques has been studied to determine a suitable service for user and personal profile information in the mobile cloud environment [64][65][66]. But to date, no formal model for this approach is realised and limited device resources still pose technical constraints that need to be overcome. There are still inadequate studies on intelligent mobile authentication service [67].

Multi-factor authentication (MFA) method that aims to enhance the security of different applications and websites has gained more popularity [116]. Its two sub-categories (physiological and behavioral) would be more difficult to break in, compared to Password-based authentication alone. In addition, its security is more guaranteed as it also requires another factor, instead of just validating the username and password pair [59]. It is also considered as among the most secure authentication techniques[59]. As Sumitra et al. [58], Alok Tripathi et al. [117], P. Ravi Kumar [109], Matthew et al. [118], Muhammad et al. [119], and Nalini et al. [91] state: there are many good reasons in MFA for it to be a suitable method to decrease authentication attacks in cloud. Thus, in this thesis we select MFA to improve the accuracy in authenticating an authorised user when facing stolen password attack [120][116].

2.5.1 Multi-Factor Authentication (MFA)

In ensuring information is more secure in cloud computing environment, there needs to be a combination of authentication techniques employed. This method would promise more security because it requires another factor, e.g. biometric authentication, as opposed to just validating the username and password pair. It proposes to be one of the stronger authentication techniques. There are various authentication methods present. Passwords, smart cards, digital certificates, Kerberos and biometrics are among the numerous authentication methods currently in use. There are three classical forms of authentication, and they are as follows: (1) something the user knows, e.g., password, pin; (2) something the user has, e.g., smart card, Yubikey [121]; and (3) something the user is, e.g., iris scan or fingerprint. In cases where additional factors are involved in the verification process, the expectation of authenticity rises exponentially. For cloud computing environment, a multifactor biometric authentication system that includes fingerprint and palm vein is proposed [4]. This is done with the aim to handle the biometric data in a protected fashion, by having the data of fingerprint kept in the central database of the cloud security server and the biometric data of palm vein kept in multi-component smart cards. Among the typical MFA scenarios are [77]:

a) Security tokens (Hardware) - smart cards or small devices with USB technology (password + smart card).

b) Security tokens (Software) - a single-use login PIN with device-based possession factor. For example, Google Authenticator (password + pin).

c) Mobile authentication - e.g. SMS or calls with one-time password (password+ SMS).

d) Biometric authentication method - fingerprint, facial recognition etc. which uses Inherence factor. For example, Dell Defender (password+ Face/ Voice/ Fingerprint).

i. *Password with Smart Card*

In this method, the authentication performance works according to two factors which are Password and smart card. More recent authentication methods on smart card-based password have also been proposed in [122][14][123][124]. Shoup-Rubin [125] suggest extension of Bellare-Rogaway model based on three-part key distribution protocol. A smartcard is used to store long-term secret key. Assuming the smartcard is not compromised, this method falls in one factor category (two factor methods can only be broken by compromising both the factors). Liao et al. [79][78] attempt to consolidate a number of passwords and smartcard-based properties and come up with two-factor smartcard and password authentication method. This method however, is still vulnerable to numerous attacks such as offline guessing attack, stolen password attack and impersonation[79][83]. The limitations of this method are presented below[126]:

1. Users must be educated in their use;
2. Cards along with any assigned PINs must be issued and tracked;
3. Cards can be lost, stolen, or shared;
4. Cards must be kept close at hand;
5. Problems can occur for users who forget their PINs or make typographical errors;
6. The method is not very robust and can be easily broken.

ii. *Password with SMS*

A worthy alternative to SMS codes are code generation apps. The most common application is the Google two-factor authentication solution- Google Authenticator. Its One-Time Password (OTP) tokens generate codes independently according to a particular algorithm or random sequence. The algorithms used for generating those one-time codes are the HOTP (Hash-based One Time Password, RFC6238) and OCRA OATH (OATH Challenge-Response Algorithm, RFC6287), developed and supported by the OATH (Initiative for Open Authentication) [85]. The limitations of this method are as follows:

1. Expensive (requires the use of smartphone or other similar device);
2. Risk of application being hacked;
3. Possibility of smartphone battery discharging;
4. The hassle of recovering lost token if the smartphone is lost or put in factory reset; or the authenticator application is accidentally deleted.

iii. *Password with Biometrics*

Facial recognition, voice recognition and fingerprints are some of the features under biometric authentication. The systems validate on biometric authentication when it is imperative that you really are who you say you are, especially in areas with security clearance (e.g. the government). The biggest downsides, and the reasons why it is not a popular two-factor method, are listed below:

1. Password can’t be changed if compromised;
2. Expensive (extremely high cost of implementation and deployment);
3. Forgery method
4. Man in the Medial (MITM) attack;
5. Accuracy issue;
6. Surgery and scars

To date, the risk of inaccurate recognition is still quite high, which means that the system can deny access when there is an erroneous determination of the user's biometric parameters. For example, common cuts can affect the fingerprint pattern. There are also people whose temperature and body moisture make it difficult to take the print.

iv. Password with User Behavior Recognition

Behavior recognition technique is considered a cheap technique that is easy to use, does not require more hardware and additional authentication procedure. Furthermore, many researchers recommend behavior recognition to be applied in authentication processes to improve its performance[19][20][21][22][23][24]. To avoid threats in authentication, user behavior recognition with password is recommended. Belk et al. [76] study the interactivity between humans, technology and user authentication. The study findings emphasise on the need to make current approaches of password-based user authentication research better by incorporating human cognitive factors in both design and run-time. It is according to the reasons above that we choose this method in this thesis. In the next section we need to shed light on password-based authentication and behavior recognition in understanding the link between password and human behavior to help deal with our research problem.

2.5.2 Password-based Authentication

Password-based authentication can be easily memorised and users are able to use them in their daily lives at no cost [58]. However, personal computer users witness an annual increase in motivated cyber-attacks from different unknown directions. Even governmental computers such as parliamentary computers of Australian federal ministers were reportedly compromised, along with many other examples [89]. In this case, a number of authentication systems recognisable in today's security engineering is susceptible to some attacks, namely denial-of-service, replay and deception attacks [90]. Traditional password-based authentications come with several problems, as shown in Campbell and Bryant research. They discover that a personal computer can guess common passwords in a week at approximately 80% [91]. Combining different symbols in a passphrase makes this task subsequently harder. In their study to understand users' habits in the web-based environment, Florencio and Herley find out that nearly half a million users tend to only use the lower-case password [92]. Password strength is also higher on websites such as Microsoft and PayPal in comparison to New York Times which has fewer rules to mandate password. Likewise, Cazier and Medlin have also analysed a dataset of passwords belonging to 500 people from an E-business website. They discover that for 60% of the users, the cracking time takes less than 10 hours, and only 38% takes longer than 10 hours. For the majority of the passwords that can be cracked in less than one hour, it is only the case of mixing the alpha or alphanumeric characters and only 0.8% of the passwords cannot be cracked because special symbols and alphanumeric characters are utilised [93]. The password-based authentication threats are listed in Table 2.2 below[127].

Table 2.2 Password-based Authentication Threats

Password-based Authentication Threat/Attack	**Description**	**Examples**
Duplication	The authenticator belonging to the subscriber is copied without their knowledge.	**1.** Passwords written on paper are disclosed. **2.** Passwords stored in an electronic file are copied.
Eavesdropping	As the subscriber is authenticating, the authenticator secret or authenticator output is disclosed to the attacker.	An attacker obtains and uses a hashed password for another authentication (p*ass- the hash-attack*).
Offline Cracking	The authenticator is revealed when analytical methods outside the authentication mechanism is used.	A dictionary attack is imposed on a software PKI authenticator in an effort to identify the correct password used to decrypt the private key.
Phishing or Pharming	The subscriber is fooled into thinking the attacker is a verifier or RP, enabling the authenticator output to be captured.	When a website impersonates as the verifier, a subscriber may accidentally reveal the password.
Social Engineering	The attacker convinces the subscriber to reveal their authenticator secret or authenticator output when there is a level of trust established.	The subscriber reveals a memorised secret to an officemate for example, who asks the password on behalf of the subscriber's boss.
Online Guessing	The attacker connects to the verifier online and tries to guess a valid authenticator output, looking at the context of that verifier.	Use of online dictionary attacks to guess memorised secrets.

Stolen password[128]	The attacker manually steals the active password.	1. Brute Force Attacks; 2. Spidering; 3. Keyloggers; 4. Shoulder Surfing[129].
Impersonation Attacks[130]	The attacker tries to log in as an authorised user.	Business Email Compromise (BEC) or "CEO fraud" manipulates companies through false identities, which can seriously damage a company's reputation. A blog from last year explains BEC in detail.
Man-In-The-Middle (MITM)[131]	A common type of cybersecurity attack that makes it possible for attackers to eavesdrop on the communication between two targets. The attack happens when two legitimate hosts are communicating, and the attacker "listens" to a conversation that he should normally not be able to listen to (hence the name "man-in-the-middle").	1. IP spoofing 2. DNS spoofing 3. HTTPS spoofing 4. SSL hijacking 5. Email hijacking 6. Wi-Fi eavesdropping 7. Stealing browser cookies

- ***Stolen password attack***: The most basic threat model that can occur to a user's accounts is the case in which an adversary directly obtains a user's login credentials or more specifically, his or her password[128]. This can be achieved using a number of well-known online and offline attacks, such as client-side malware, phishing using a spoofed site and eavesdropping on the password transmission. When used, these attack strategies can compromise a user's account for a given site, along with any associated personal information. According to Mark Zuckerberg[132], Facebook was caught up in an estimated 272 million stolen password attack in only one month. However, a number of defenses against this threat has risen in recent years. This includes the use of multiple factor authentication, such as SMS, Smartcard, and Biometric in addition to a password[133]. Nonetheless, limitations to these models exist because of the additional hardware that is needed to implement this technique which can become costly if an entire organisation is to use this feature to authenticate users. In addition, if both of the user's authentication factor and password are stolen at the same time, there is then no way to prevent an attacker from impersonating as the user[134]. In a related context, many researchers are recommended to apply behavior recognition as an authenticating factor with password during authentication process[25][72][27][28] [29][73][74][32][33][75]. Thus, in this thesis we select behavior recognition with password to improve the accuracy in authenticating an authorised user when facing stolen password attack [120][116].

2.5.3 Behavior Recognition with Human Factor in Authentication

Behavior recognition with human factor provides continuous authentication security for account access and transactions by continuously monitoring and scoring the way users interact with their computers and mobile devices via mouse movements, keystroke, and gesture dynamics in real-time. These actions, recorded and learned over time, are mapped to the returning user to generate a risk score. When the behavior of the user does not match the known user model when he tries to log in, the security platform can initiate a "stepped up" authentication. This can include requiring additional biometric authentication (i.e. face recognition or fingerprint scan), requesting correct response to a security question, or prompting a secure one-time password[25]. Achieving a strong security in this approach can be done through three simple steps: 1) Input Data: The behavioral authentication solution is fed with a constant stream of all common user behavior data including mouse movements, key strokes, swipe patterns and more; 2) Analyse Data: The platform is able to swiftly create an accurate behavioral model of each unique user; 3)Score Data: DIGIPASS for Apps behavioral authentication continuously compares the current behavior with the known user model to determine a "trust score"[135].

Many researchers have suggested authentication approach which uses behavioral recognition with human factor. Several studies have employed biometrics to continuously authenticate users through the use of cognitive fingerprints, eye scans, colour of user's clothing, and face tracking [26][27][136]. However, many of these techniques require additional hardware and higher cost in order to operate efficiently. Behavioral modelling addresses these limits by observing how users interact with the system. Evaluating mouse movement, assessing how users search for and select information, and figuring out the habitual typing rhythm of users are some of the measures used to continuously observe a user's behavior[29][28]. Although these approaches do not require special hardware, most of them require the installation of specialised monitoring software. Thus, in this thesis we adopt an implicit learning mechanism as a software for monitoring, recording, and analysing an authorised user behavior when interacting with password in authenticating PCC.

2.6 Authentication Methods in Public Cloud Computing

In order for a user to access cloud services over the Internet, he needs to enrol in Cloud Service Provider (CSP). After enrolment, the end user can gain access to any service remotely via the Web. CSP normally stores the secret information in the Key Distribution Center (KDC). A single point of comptonization may jeopardise the whole system, and it is also susceptible to online and offline dictionary attack. For example, existing approaches[137] [138][139] enroll an end user by requesting his username and password. The username is taken as the primary credential and later verified during user authentication. In actuality, a username alone is not sufficient for a strong private entity. It can result in an opponent easily incorporating different attacks. Some attacks can be in the form of impersonation attack and identity comptonisation attack, in which the "username" is sniffed from the insecure media. In addition, the existing password-based enrolment is also exposed to password-guessing (dictionary) attack, stolen-verifier attack and many others. The existing approaches [137][140] are also able to retrieve the client's secret key as the hash value of its password. Therefore, the key is most likely to remain the same until the client changes the current password. However, in changing the password, updates are needed in the enrolled data maintained by the KDC and this, subsequently, invites many key rollover problems [141].

Chang and Wu[142] propose a remote password authentication method with a smart card based on the Chinese Remainder Theorem (CRT). The method protects against attacks of replaying previously intercepted requests, and verification table does not need to be stored. Nevertheless, in this method the user cannot choose his password and the owner cannot freely change it. Some methods proposed by [143][144][145] also present similar problems. Chan et al. [146] 2003 and Shen et al. [144], respectively, indicate further that Hwang et al.'s method[143] is not safe. In [147], Yamaguchi et al. come up with an authentication system that is simple but efficient, SPLICE/AS. Later, Hwang et. al identify that SPLICE/AS system is vulnerable to guessing attack [117]. In [118], an efficient method based on the geometric Eucidean plane is proposed. The advantages of this method lie in its simplicity of geometry and the property that users can freely choose passwords of their choice. Still, this method is insecure as indicated in [119]. In [120], Jan and Chen present a new method without verification table. Users are free to choose and change their own passwords. However, the fact that it uses the public key cryptosystem makes it inefficient. Its computational cost is also very high. In addition, Yang and Shieh in [121] present methods that do not store passwords or verification tables in the servers, and users are free to change their own passwords. These two methods are chosen with the main purpose to prevent replay attack. Nevertheless, two researches [122][123] point out the setback in Yang and Shieh's methods, in which an intruder is able to impersonate a legal user by constructing a valid login request from an intercepted login request. As such, Yang and Shieh's methods are not able to prevent modification attack. Hwang et al. [124] and Chien et al. [78] come up with an efficient and practical smart card-based method according to a secure one-way hash function. Through their methods, the authors claim that the following characteristics can be achieved: 1) the verification or password tables are not required in the server; 2) the communication and computational costs are low; 3) the replay attack problem is completely solved; and 4) users are free to choose their passwords. Nonetheless, some limitations in these methods are going to affect authentication accuracy . In [13], mutual authentication cannot be achieved through their method. In [78], their method does not allow users to freely change their passwords.

Hao et al. [51]proposes a time-bound ticket-based mutual authentication method for cloud computing. The time-bound tickets are employed to enhance performance authentication. The proposed authentication method accomplishes mutual authentication between the server and the client. Using time-bound tickets also lessens the server's processing overhead efficiently. In addition, the corresponding relationship between the digital ticket and the client's smart card effectively prevents user masquerade attack. Unfortunately, Jaid-har [126] points out that Hao et al.'s method is not able to withstand denial-of-service attack during the password change phase and impersonation attacks [127]. Wazid et al. [128] also present a provably secure user authentication and key agreement method for cloud computing environment. Their methods defy the weaknesses the existing methods present and support extra functionality features such as user anonymity, and efficient password and biometric update phase in multi-server environment. Still, the greatest disadvantages of this method come in the forms of invasion of privacy, costs of implementation, long duration, problematic surgery and influence on the performance of the authentication [129][130].

Omri et al.[66], propose the use of user handwriting as an authentication factor in accessing the cloud securely, improving the performance of the authentication. The mobile user writes his password manually on his smartphone touch screen. The image is then sent to cloud server for the validity of the password to be checked. Two criteria are involved in checking authentication authentication of users in this manner: first the user's unique handwriting, and second the password. In this proposed method, a Hadoop server establishes the connection between the cloud and the mobile phone.The uniqueness of biometrics features helps in improving the security of different authentication methods. The limitations of this method, however, are its usability and privacy issues and the low accuracy of using handwriting. The implementation cost is also higher, plus it requires a long time. Low accuracy authentication metrics such as handwriting is recommended to be substituted with other methods, for example ID and Password together. If handwriting authentication fails, the system can ask for other methods.

In[67], Le proposes an authentic method called NemoAuth based on mnemonic multimodal approach to help improve on the performance of authentication. NemoAuth makes use of various mobile device sensors such as gyroscopic, gravity, orientation, proximity, pressure, ambient light, temperature, touch screen, and moisture sensor; as well as other facilities such as microphone and camera to determine and draw out the biometric features of a mobile device user. NemoAuth procedure is very much alike biometric based methods that pre-characterise and set user's signature profile during system setup step. The user's signatures consists of a set of multimodal signatures, and each signatures is made up of a set of mnemonic and atomic motions. The atomic actions related to the mnemonics assist users in memorising the secret keys more conveniently. Based on types of mobile device sensors, there are various types of atomic actions that can be used. For instance, the set of atomic actions for touch screen can be taped, lined, held, circled, and cross; plus a mobile user can use his fingertip to tap at specific position. He can also hold his fingertip for a certain duration on the mobile screen that shows the mnemonic image. In addition, the user can choose a desirable signature profile according to a preferable level of security and usability. Additionally, each signature profile comprises of a set of duple that displays the kind of authentication method and trigger time. The user can fix a signature profile to employ different authentication methods according to different period of the day. For instance, the mobile device can be instructed to automatically enable voice signature during non-bed time and use GPS authentication at home. The main objective of the NemoAuth is for different capabilities of the mobile device to be utilised in order to improve the usability of authentication by using mnemonic images. This method however, simplifies the need for users to remember password and provides different actions following the mobile device capacities. Among the limitations found in this method are:

1. In this study, the performance metrics such as False-Acceptance Rate (FAR), False-Rejection Rate (FRR), Relative Operating Characteristic (ROC), and Crossover Error Rate (CER) are not evaluated, which can affect the performance of authentication;
2. Sufficient processing and storage power are needed to apply a multi-modal method;
3. User authentication utilises several authentication factors, making authentication procedure time longer;
4. A lot of user's private information is used to process authentication;
5. User's private information is not protected as there is no privacy mechanism provided.

To improve performance, a suitable algorithm to transfer intensive processing phases to cloud can be designed. Finally, this method is more suitable for mobile cloud computing than computer cloud.

In Banyal et al.[53] the authors suggest that multi-factor authentication consists of three-layer key entities and key approaches use authentication according to secret key. The algorithm of this framework consists of Registration phase, Login Phase, Authentication Phase, Change Authentication and Secret Phase Change. The major drawback in this framework is user has to memorise complicated password [134], and the authentication procedure is made more complicated when several patterns such as SMS activities, calling patterns, location, and requirement of much computational power are processed. In addition, many devices such as PC, Smart phone and a server that leads to framework process are needed, making it costly. Finally, this framework is also vulnerable to impersonation and stolen password attack[148].

Yang and Lin [54] propose an ID-based user authentication method in a cloud environment. The proposed method consists of three rules: the user, the server and the ID provider. The authentication procedure is the responsibility of ID provider. This method is classified into two phases: registration phases and mutual authentication phases. However, in [47] Chen et al. identify the security risks present in Yang et al.'s method [54], stating that it is exposed to insider and impersonation attacks. In handling the security loopholes in Yang et al.'s method, Chen et al. then develops a dynamic ID-based authentication for cloud computing environment that is based on elliptic curve cryptography (ECC). After reviewing Chen et al.'s method, Wang et al. confirm that their method is susceptible to offline password guessing, together with impersonation and stolen attacks. Additionally, Chen et al.'s method is also found to not provide user anonymity and face problem with clock synchronization [47].

Cindhamani et al.[49]propose a security framework that consists of two stages: 1) How securely are we storing the data?; and 2) How securely are we retrieving the data by using encryption algorithm? The authentication in this algorithm is checked by sending the password to the owner with a security question. The main downside in this framework is that the procedure is made more difficult when the user has to memorise some secrets, and use both password and the secret question[50]. Furthermore, processing several parameters like ID/password,IMEI, IMSI as well as voice and face recognition leads to the authentication procedure being more complicated, costly, having problematic surgery and influencing the accuracy of the system[6].

Zhang et al. [149] suggest the use of fingerprint as an authentication algorithm. In this method, the existing mobile device camera captures the fingerprint image, which will not require sensors to be implemented in the mobile device. Taking all the benefits from cloud, the whole process of capturing and matching fingerprint is hosted on the cloud server. This method is similar to other normal finger recognition methods that use mobile device camera to capture fingerprint. Capturing the fingerprint image to be processed on the cloud server initiates the procedure. After that, the image is pre-processed to convert RGB to gray-scale image, and other steps for example reducing the blur effect, ridge enhancement and segmentation are also completed. The pre-processed image is then sent to feature extraction phase. In the final phase, the server examines the similarity of the extracted features before storing the information of the user's fingerprint. The privacy issues of using biometrics make the requirement of applying privacy preserving approaches necessary. In a similar situation, the captured image would go through some cryptographic algorithms in the mobile device before it is sent to cloud server. However, in this method, the fingerprint image is sent in plain text. The details of utilising MCC processing and storage resources are also not clearly explained in this approach. The fit utilisation framework for MCC is another aspect advised to be designed. Other than that, this method also does not clearly define the adaptability to MCC. Another fact to be considered is that the accuracy of fingerprint that is captured by mobile device camera is lower than using sensors to capture the finger print images. Therefore, it is recommended that other authentication factors such as using ID and Password be added to this method.

V. Chang et al. [48] propose Cloud Computing Adoption Framework (CCAF), a security framework for business cloud computing which comes in three layers. First, tasks for layer 1 include password protection, network, and IP-based firewall and access control. Second, tasks for layer 2 comprises of out-of-band authentication and openID serving for identity management; and the tasks for layer 3 are encryption and decryption for authentication file. In this framework there are 99.95% viruses and trojans detected and blocked, and 85% of blocking could be achieved for 100 hours of continuous attack. Detection and blocking take less 0.012 seconds per trojan or virus. Additionally, it could block all SQL (structured query language) injection, providing a real protection to data. The weakness in authentication with this framework comes from the fact that memorising some secrets makes the procedure more difficult to the user. Several authentication factors are also utilised for user authentication, which adds to the authentication procedure time. Lastly, this framework is also vulnerable to impersonation and stolen password attacks [97][95].

Table 2.3 Summary of Multifactor Authentication

Method	Threats	Drawbacks
Password-based authentication V. Chang et al. [48]	1. Stolen password attack; 2. Impersonation attack	- Procedure becomes more difficult for users as they have to memorise some secrets; - Authentication procedure time is increased when several authentication factors are utilised.
Cindhamani et al. [49] Password with security questions	1. Stolen password attack; 2. Impersonation attack	- Procedure becomes more difficult as users have to memorise some secrets; - Procedure becomes more difficult for users as they have to use both password and secret question; - Authentication procedure becomes more complicated as several parameters such as ID/password, IMEI, IMSI, voice and face recognition are processed; - High cost, surgery can be problematic and the accuracy of the system can be influenced.

Omri et al. [66] Password with biometric	1. MITM attack; 2. Replay attack	- Handwriting pattern is a method prone to errors as mobile users may use different styles to write the same digits; - Low accuracy of using handwriting; - More hardware required; - High cost; - Only suitable for mobile cloud compared to others; - Surgery and scars
Le et al.[67] Password with Mobile + biometric	1. MITM attack; 2. Replay attack	- More hardware required; - High cost; - Surgery and scars; - Only suitable for mobile cloud compared to others; - Procedure becomes more difficult for users as they have to memorise some secrets; - Authentication procedure time is increased as several authentication factors are utilised for user authentication.
Hao et al.[51] Password + smartcard	1. Denial-of-service attack during the password change phase; 2. Impersonation attacks; 3. Stolen password.	- Users have to memorise some secret information; - Authentication procedure time is increased as several authentication factors are utilised for user authentication.
Banyal et al. [53] Password + Smartphone	1. Stolen password attack; 2. Impersonation attack	- Users have to memorise complicated password; - Many computational powers are required because several patterns such as SMS activities, calling pattern and location are processed; - Many devices are required such as PC, smart phone and server; - High cost
Yang et al. [54] ID+ OTP	1. Impersonation attacks 2. Stolen password attack; 3. Offline password guessing.	- User anonymity is not guaranteed; - Clock synchronisation problem.
Zhang et al. [68] Password with biometric	1. Impersonation attacks 2. Stolen password attack; 3. Offline password guessing.	- No clear explanation on the details of utilising MCC processing and storage resources; - Lower accuracy of fingerprint captured by mobile device camera, as compared to using sensors to capture fingerprint images; - High cost.

All in all, most of the multi factor authentication methods in public cloud computing have high cost of implementation and deployment, and most of current authentication approaches are weak when facing stolen password attack, which then lead to negative effects on the accuracy of authenticating an authorised user[51][66] [67] [53] [54] [49] [68][48] [50] [55]. Still, many researchers have suggested authentication approach which use behavioral recognition with human factor [25][72][27][28][29][73][74] [32][33] [75]. Most current studies neglect the presence of human behavior recognition in authentication process as a factor in the performance of authenticating an authorised user in public cloud computing [21]. In addition, learnability in password-based authentication is highly weak[21][56]. Thus, in the next subsection the related works in behavior recognition with human in authentication area are presented.

2.6.1 Behavior Recognition Related work

Chow in[17] proposes an authentication method known as TrustCube[150] by integrating the implicit authentication [78] for mobile client authentication (the name TrustCube is featured in both the initial and extended method). TrustCube, a cloud-based authentication solution, is policy-based and employs an open standard. For its robustness and adaptability, it also supports the combination of different authentication methods. The policy-based authentication comes with some distinctive advantages, namely the utilisation of policies that are user-specific and finely grained, with the ability to be immediately updated based on users' preferences. Furthermore, it uses a framework with federated authentication, much like the OpenID, in which the algorithms of the implicit authentication is not specified and the top-level system description is provided. Developed with implicit authentication, it utilises mobile data like SMS messages, calling logs, location and website accesses in the existing public cloud environment.

However, it also has its limitations. Among them is, the public cloud constraints in input requirements will make it more difficult to use complicated passwords, and this in turn will lead to use of short password and PINs. Consequently, this poses higher security risks such as stolen password and impersonation attacks. Other than that, many computation powers are needed in order to process several patterns such as SMS activities, calling pattern and location, which makes the authentication procedure more complicated. Moreover, to improve the accuracy of TrustCube method, specific mobile data patterns are required. This will be inconvenient to the users and will affect approach usability. Using a lot of users' private information in processing authentication can also negatively affect privacy [130][128].

Niinuma et al. suggest a CUA framework that automatically registers a user's colour of clothing and face as soft biometric traits [26][27]. This method is able to authenticate users irrespective of their status in front of the workstation. It uses information about users' colour of clothing as an enrolment template in addition to their facial information. The system automatically registers this information each time the user logs in and integrate it with the conventional password identification system. From the results, it is indicated that the system can successfully authenticate the user, showing high tolerance to the user’s posture. Limitations in the study come from the additional hardware that needs to be implemented, as it can be costly should an entire organization decide to use this feature to authenticate users [25]**.**

Monrose et al. propose a unique authentication method that identifies users according to the analysis of keystrokes[28]. Keystroke dynamics analyses how you type vs what you type. The user’s habitual typing rhythm is a function of the user and their environment. When a person types, a unique structure (i.e. profile) for that individual can be constructed using the latencies between successive keystrokes, keystroke durations, finger placement and applied pressure on the keys. Farwell-known, regularly typed strings signatures can be quite consistent. A limitation to this approach only occurs when the user faces environmental factors that affect their typing patterns.

Altinok et al. suggest a continuous biometric authentic system that gives an estimation of authentication certainty at any given time, even when any biometric data is not present[73] . The study presents an initial approach for temporal integration depending on uncertain propagation over time to estimate channel output distribution from recent history, and classification with uncertainty. This technique, which operates on a continuous basis, computes expected values as a function of time differences. The results from the experiments show that temporal information helps to improve authentication accuracy. These empirical results show much potential and promote further investigation. Some of the limitations of this study includes the fact that the authentication uncertainty rises over time which will cause a decrease in system usability. This technique also requires hardware such as camera and scanner for fingerprints, which can become costly. Kang at el. present temporal integration of biometrics and behavioral features in order to authenticate users continuously [31] . To compute behavioral features, a face tracking system that uses colour and edge information is used.

Shen et al. employ mouse dynamics when carrying out continuous user authentication [9]. This technique is used to monitor behavioral features in mouse operations to recognise malicious users. Nevertheless, this emerging approach has some existing limitations. Behavioral variability is shaped by human or environmental factors. For instance, a user’s behavior will be modified significantly if he or she switches software environments or experiences biological or emotional change. Furthermore, this method deeply disregards the integrated and analysis of the user’s history. In this case, any changes would make the user identified as an impostor.

Xie et al. [32] use an extraordinary approach to recognise legitimate users early when they use online services, by implementing a vouching process without using biometrics. They come up with a technique called Souche that monitors vouching via social committee (i.e. Twitter, email). Additionally, early recognition helps in both usability and security. Souche brings advantages to social connections established over time. In this method, legitimate users help identify other legitimate users through an implicit vouching process, strategically controlled within vouching trees. Souche consists of two components. The first component sets a social graph and chooses vouchers by computing connected subgraphs. This approach is made possible by a key observation of real data; that there is only one huge connected subgraph of legitimate users, as opposed to malicious users that are mostly isolated nodes. The second component restricts the growth of the trusted user population according to community structures defined as a set of vouching trees. The use of vouching trees limits the impact of active adversaries to small local subgraphs, which then prevents the population of malicious users from expanding rapidly. Other than that, it allows for strong audit trails to be generated, which will permit reconsidering and invalidating vouching between accounts. Souche is lightweight and fully transparent to users. It is also efficient in identifying 85% of legitimate users and denying entry to malicious users. With Souche, its limitation lies on the idea that the effectiveness of such detection strategies depends on the behavioral assumption that legitimate users are not willing to interact with unknown accounts. This has been proven to be unrealistic by various experiments [36][37][38]. A large-scale social bot infiltration on Facebook reveals that over 20% of legitimate users accept friendship requests randomly, and over 60% accept requests from accounts with as little as one contact in common [36]. For other platforms like Twitter and Tumblr, one of its strong features is connecting and communicating with strangers. In these situations, the innocent-by-association paradigm yields high false-negative rates. Some authors notice the assumption of finding groups is limited to social bots or legitimate users only, whereas real platforms may contain various mixed groups of legitimate users who fall prey to some bots [151], and sophisticated bots may be able to perform large-scale infiltrations which makes it impossible for them to be detected solely from network structure information.

L.C Leonard [25] suggested a web-based behavioral modelling for Continuous User Authentication (CUA). The technique can go together with web applications for a reliable and secure authentication. There are challenges that occur when modelling the behavior of users that interact with web-based software. Other than that, an approach to address the need for web-based continuous user authentication is also presented. Statistical Language is applied to classify users according to document classification, information retrieval, machine translation and speech recognition. This model comprises of six internal techniques: Neural networks, Maximum entropy, Probabilistic context-free grammars, Decision trees, n-grams and Hidden Markov models. It helps in exploring various statistical language models. The authors make use of n-grams to capture user interaction with web-based software. N-grams are also used to model sequences and sub sequences of user actions, their orderings and the temporal relationships that make them unique. After the behavior is identified, authors illustrate the ability to classify the models using multiclass classification to identify role and/or individual user characteristics. Results indicate that model-specific differences in user behavior with performance are highly dependent on session and keyword size. Using the binary classification technique, outliers are identified in variable length keyword sequences. Results from this approach display the rate at which each model rejects uncharacteristic sequences and accepts valid sequences. This study establishes a novel keyword abstraction process to identify user activity for each system user. It also develops new techniques to observe users' web-based applications behavior using information that is already available to a system administrator. The main limitation of this technique is the time required for analyzing the authenticating user when s/he logins into the system by comparing current and previous user behavior. This time gap enables an unauthorized user's illegal access to deal with data in the case of stolen password attacks.In addition, the monitoring of authenticity of the user interacting with a password, through behavior, is neglected.

Table 2.4 Summary of Behavior Authentication

Terms		**Meanings**
Authentication Process	**Password**	Authentication process focuses on password only
	Interact with user behavior on system	Authentication process focuses on password + monitoring and record interact of user behavior with system only
Cost	**Extra H/W (High)**	Authentication process needs to add extra hardware such as camera, smartphone, smartcard, etc[6].
	Low	Authentication process no need extra hardware [6].

Current approaches	Authentication Process		Costly			Drawbacks
	Interact with user behavior on system	PW	Low	High	Extra H/W	
Chow in [17] TrustCube		√		√	√	1. Complicated passwords; 2. Requires many computational powers; 3. More complicated authentication procedure; 4. Accuracy of TrustCube method needs to be improved; 5. Utilises a lot of user’s private information.
Niinuma et al.[26] [27] CUA framework		√		√	√	The additional hardware that is needed to implement this technique can become costly if an entire organization uses this feature to authenticate users.
Monrose et al.[28] Analysis of Keystrokes	√		√			Environmental factors can affect user’s typing patterns.
Altinok et al. data [73] Continuous Biometric Authentic		√		√	√	1. The authenticity uncertainty rises over time which decreases system usability; 2. Hardware such as camera and scanner are required.
Shen et al. [29] Employ Mouse Dynamics	√		√			1.If there is a change in the user’s software environments, or if the user experiences biological and emotional change, the user’s behavior will be modified significantly; 2.This method deeply neglects the integrated and analysis of the user’s history; 3. Any changes can bring a risk of the user being identified as an impostor.
Xie et al.[32] Souche	√		√			The idea that the effectiveness of such detection strategies depends on the behavioral assumption that legitimate users are not willing to interact with unknown accounts. This has been proven to be unrealistic by various experiments [145][146][147].
L.C. Leonard [25] Continuous User Authentication (CUA)	√		√			This technique is the time required for analyzing the authenticating user when s/he logins into the system by comparing current and previous user behavior.

According to section 2.6.1 above, most of authentication methods that monitor an interacting user with password need extra hardware as an authentication tools in authentication process[17][26] [27][73].However, these methods are too expensive to be used for authentication in public cloud computing[6]. On the other hand, the cost of authentication methods that monitors an interacting user with system via applying extra software as an authentication tools during authentication process is low[28][29][32][25]. However, the main limitation in these methods is there is some time for the user to deal with data which is saved in public cloud till the user's legitimacy is determined. Furthermore, in most of these methods the monitoring of the user’s behavior when interacting with password has not been investigated sufficiently. To avoid these problems, the literature has emphasized the importance of moving from traditional security processes to intelligent security processes [24] through adapting intelligent mechanisms that represent an authorised user’s behavior, which can automatically prevent an unauthorised user [20][56]. There are many intelligent mechanism applications in authentication process such as Neural network in L.C. Leonard[25] , Leaning Algorithm in Shi et al. [78] , and agent in Mostafa et al [79].

Learning process is applied in our thesis, because we need to apply intelligent mechanisms that analysis an authorized user’s behavior in authentication process. These activities need perception of an authorised user, recording, update, and making a decision (action) when interacting with password. This process perfectly matches the principle of Learning process. In a related context, M. Hajivali & F. Zhang [79][80], have recommended for the learning process actions of user authentication on public cloud computing to be applied. Thus, in this thesis we apply learning process t to deal with this problem.

2.7 Learning Process

According to Tim. [152]Learning has an advantage as it permits the component to start operation in unknown environments and become more competent than if it is to operate on its initial knowledge alone. The most important features are the “learning element” that is responsible for making improvements, and the “performance element” that is responsible for choosing external actions. The learning element takes feedback from the “critic” on how the component is performing and sets how the performance elements are to be modified for better performance in the future. The performance element is what we have previously determined to be the entire component it takes in precepts and decides on actions. The last component of the learning process is the “problem generator”. It handles all the suggesting actions that will lead experiences that are new and informative as illustrated in Figure (2.4) below.

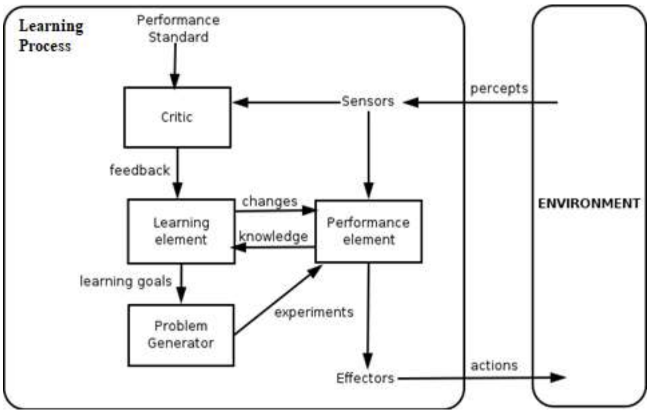


Figure 2.4 Learning Process

Many previous studies apply intelligent methods in authentication process such as Mostafa et al. [79], Elaine et al. [78], and Vadim. [82]. Mostafa et al. [79]. This study proposes a method named ACUA (Access Control and User Authentication) that utilises a cloud-based software-as-a service application depending on one client-based agent and four cloud-based agents (Authentication, Access control, Cryptography, and Cloud manager). In order to increase the rate of intelligence during cloud computing communications, authors apply agents. This study is conducted with the definite objective to establish a secure algorithm during processes, services and communications. However, this method increases the rate of reliability, security, efficiency and trust in cloud computing. In this method, the main limitation is compatibility of cloud manager agent with various public computing servers. Other than that, diving data in several parts and joining them to the main part in access control agent is time-consuming. Another limitation to this method is finding a suitable way to teach users to use the method without mistakes. Finally, this method does not fully represent the interaction among human factor with password and web-based system. Thus, it is weak when facing stolen password attack.

Elaine et al. [78] state in this study the authors suggest implicit authentication; authenticating users based on behavior patterns in cloud computing. This method consists of two major components. The first component is learning algorithm that works according to past behavior. The second component is user model that works by comparing between recent behavior with past behavior to generate authentication score. The first step learns about a user model through learning algorithm based on past users' behavior. In the second step, the user model characterises the user's behavioral patterns based on modelling independent features such as time elapsed since last good call, frequency of bad calls incidents per day and GPS coordinates. However, this algorithm is fairly robust to the pollution of a single feature. This algorithm has also introduced learning algorithm principle of a user's behavior as a new authentication factor. This method has proven the effectiveness of learning principle when it is embedded with authentication. As with many other methods, this method also suffers from many limitations and one example is the fact that it is suited for mobile devices rather than computers since it generates user behavior patterns according to mobile parameters (time calls, bad calls, and location). In addition, this method has not dealt with the way of determining an illegitimate user during cases of stolen password and when the user tries to log in through same time, device, and location. Finally, this method requires smart phones to generate users' behavior pattern which lead to high cost when applied in any organisation.

A recent study by Vadim [82] proposes learning method in authentication to improve the accuracy of user authentication. The researcher in this study tries to apply the intelligent principles in user authentication process. The specific objective of this study is to improve the performance user authentication by sharing a unique information knowledge between user and the system through intelligent software agents. The study explains about employing JADE agents to share knowledge in multi-agent system. This system can effectively learn a new activity and perform learned actions. This research defines three kinds of agent: Student, Teacher and Examiner. Student can receive messages from other agents and can choose to either adopt new knowledge or display the result of known action, but initially it does not know anything. The second type of agent is "Teacher". Initially, it knows something. In this case, it knows the mathematical operation of adding on two elements of either integer or fraction. Teacher can also pass this knowledge during communication act. Teacher is also able to identify any students before communication act happens because the only agent with the ability to learn in Student. The third type of agent, which is the Examiner, knows the same terms that the Teacher does, but it searches for the Student agent specifically to inspect their knowledge by sending special type of requests. The main limitations to this study are listed as follows:

1) The user needs to be monitored when interacting with password-based authentication;

2) In trust function, it is not defined which particular parameters that the method needs to measure in order to calculate authentication function. These parameters are application specific and depend on operational domain. For a working authentication system, application domain must be defined, notwithstanding designing principles that are general. Ontology elements are domain-specific.

Thus, in our thesis we apply learning tactic in authentication process for monitoring, recording and analysing the user password behavior when interacting with password-based authentication process. Nevertheless, in this method which particular parameter with human password behavior has to be defined in order to calculate the accuracy of authentication function. Thus, the next section sheds light on human password behavior to deal with this point.

2.7.1 Human Password Behavior

The specific objective of this section is to determine the particular parameters in human password behavior which can be used to improve the performance of user authentication. This section focuses on this aspect and brings into attention the most relevant findings in the fields of human password behavior in order to provide a clear understanding on the factors that generate various password behavioral patterns of an authorised user. First, there is a set of innate, unchangeable and context independent traits. Second, there is a set of features which are context-generated and variable in real-time. This understanding creates the starting point for answering research question 3, by establishing an algorithm as a relevant context for testing the assumptions made in this thesis.

Several recent studies investigating human behavior have been carried out on password such as P. Hoonakker et al.[153] and Mashael et al. [154]. Mashael et al.[154] present an analysis of a demographically-diverse password dataset. The aim of this analysis is to gain insights on how users from various groups incorporate their personal information (names, birthdays and phone numbers) into their passwords and display the extent to them doing this. The results of this study show that there is an unambiguous relationship between personal information and passwords in most users. In addition, the cultural linguistic backgrounds are a principal determining factor in creating passwords.

P.Hoonakker et al.[153] state that the study analyses the impact of human behavior on password. A large survey involving 836 (employees) end users is conducted to examine password behavior of end-users, with the main aim of investigating the relation between human factor and password. The results show that human factor is an important component in the authentication system, and it plays a key role in creating password. Additionally, this study distributes the interactions of users with password according to the points below:

1. Eighteen percent of the respondents opt for the same password to access different computer systems;

2. Fifty six percent of the respondents use a long password of more than 8 characters;

3. Seventy nine percent use a combination of upper and lower cases together with numbers;

4. Thirty eight percent use special characters such as #,*or ^ when they change to a new password;

5. When they change their passwords, 68% of the respondents re-use their old password (e.g. password2007 becomes password2008)

The important results in P.Hoonakker et al.[153] this study show that the human factor is an important component in the authentication system and that it plays a crucial role in creating a password. Therefore, in this thesis we work to analyse human factor in authentication process through several parameters in human password behavior namely the duration of entrance password, old password, password size, upper cases, lower cases, special character, numbers and password error; as shown in Figure (2.5) below.

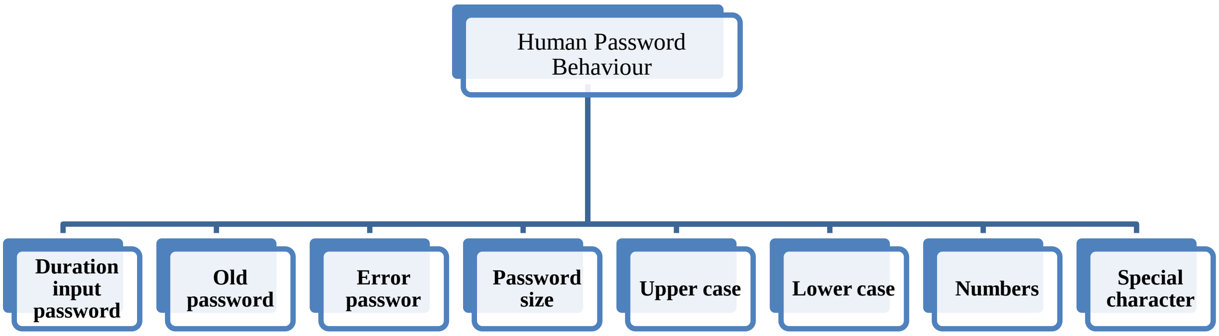


Figure 2.5 Human Password Behavior Parameters in EPSB

2.8 Chapter Summary

This chapter covers cloud computing as a whole. It covers cloud computing definition and services, as well as cloud characteristics. In cloud computing, public deployment supports many applications from military to commercial applications. In addition, an authorised user can access the public cloud at any time anywhere by using any device through the authentication layer.

In this chapter, reviews on current research areas in public cloud computing are also documented. Based on the reviews, it is discovered that security-related area is a research trend. Issues on security such as authentication are studied by many current researches. In the literature on the security of public cloud computing, the relative importance of authentication has been the subject to considerable discussions [4][42]. However, authentication is considered a milestone to allow only an authorised user to deal with the data saved in the cloud [43][2]. Authentication performance from an accuracy criterion defines the capability of the authentication system to correctly determine a user’s identity [44][45]. According to NIST, use of a stolen password by remote access through authentication layer in public cloud computing could allow unauthorised user to gain unauthorised access, modify and destroy the organisation’s information systems and resources [2]. Therefore, out of many security issues in public cloud computing we select authentication performance related area from accuracy criterion as a more specific research trend.

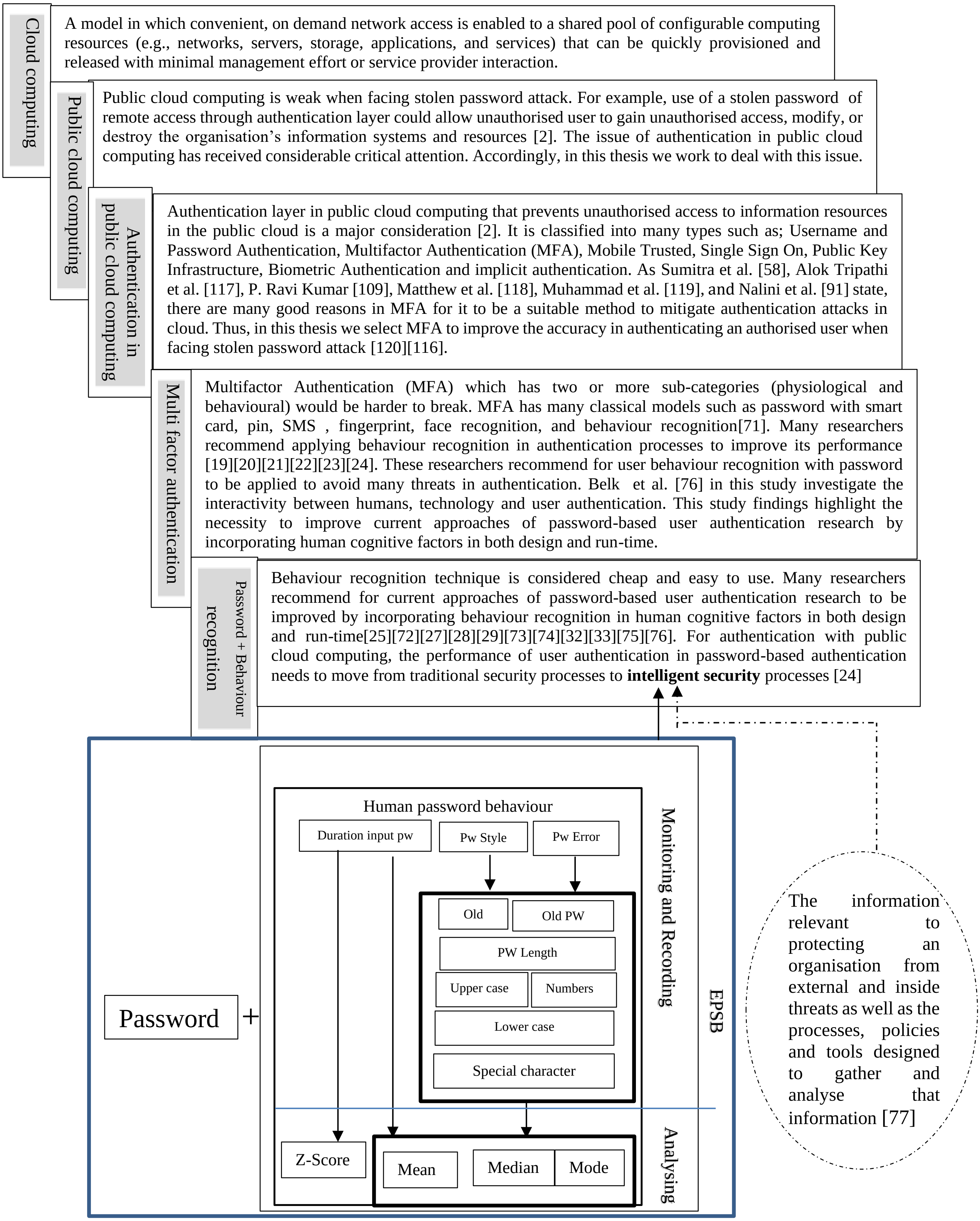
In our study, to narrow down in authentication accuracy, we must determine the current authentication method in public cloud computing to shed light on the pros and cons in those methods. However, there are many authentication methods in cloud computing such as password-based authentication, multifactor authentication, mobile trusted, single sign on, public key , biometric and implicit authentication. Password is considered the cheapest, the most popular and the most commonly used method of computer authentication. 86% of U.S. companies use password authentication [7]. Password-based authentication can be easily memorised and users are able to use them at no cost in their daily lives [8]. The majority of passwords that can be cracked in less than one hour are simple passwords that mix alpha or alphanumeric characters and only 0.8% of passwords cannot be cracked due to the utilisation of special symbols and alphanumeric characters. Passwords are also weak when facing impersonation and stolen password attack [155]. To avoid these problems, many studies propose multi-factor authentication (MFA) be applied. To avoid these problems, many studies propose applying multifactor authentication (MFA).

MFA is a method of confirming a user’s claimed identity. In this case, a user is granted access only after successfully presenting two or more factors to an authentication mechanism. It is considered a more popular method due to the exponential growth of new methods of cyber attacks [6]. There are many MFA methods such as password with smart card, SMS, biometric and security question. These methods are harder to break compared to password-based authentication[6]. However, most methods in the field of MFA only focus on adding extra hardware authentication factor which leads to high cost when applied in any organisation. In addition, most of these methods are weak when facing stolen password attack which causes a negative effect on the performance of user authentication. To avoid these problems, many researchers recommend behavior recognition to be applied as a factor in authentication processes with password to improve its performance, because this technique is considered cheap, easy to use, and there is no need for any extra hardware to be added [19][20][21] [22][23][24]. Behavior recognition technique is considered cheap as there is no need to add more hardware. It is also easy to use as there is no need to add any new authentication procedure technique. In section 2.5.1, many researchers have suggested authentication approach which uses behavioral recognition with human factor [25][72][27][28][29][73][74][32][33][75].

Currently, many researchers suggest that the representation of human behavior by only adopting software is far more cost-effective. Therefore, it is better adapted to improve the accuracy of user authentication [28][29] [32][25]. Monrose et al. [28] propose an authentication method that distinctively recognises users based on the analysis of keystrokes. The limitation to this model comes when the user is faced with environmental factors that change their typing patterns. Monitoring also connects users with a web-based system only. Shen et al [29] state that this model is used to monitor behavioral features in mouse operations in detecting malicious users. There are, however, two limitations to this model. First is its behavioral variability, and second is the fact that it deeply neglects the integrated and analysis of users' behavioral history. Thus, any changes could result in the user being identified as an impostor. Xie et al. use a distinguished approach to recognise legitimate users early when using online services by implementing a vouching process that does not use biometrics [32]. They come up with a technique called Souche to observe vouching via social communities (i.e., Twitter, Email). One limitation of Souche is that the effectiveness of such detection strategies is closely dependent on behavioral assumption that legitimate users are not willing to interact with unknown accounts, which is proven unrealistic by various experiments[36][37][38].

L. C. Leonard [25] proposed in this study for intelligent security applied in the authentication process by adopting neural network principles. It suggests a web-based behavioral modelling for continuous user authentication (CUA). Web applications can be used in this technique to administer and reliable and secure authentication. The main limitation to this technique is it analyses and authenticates users when he or she logs in to the system comparing between current and previous behavior analysis results. That leads to an authorised user being granted some time to deal with data in case of stolen password attacks. Besides, during the authentication process, the monitoring of user interacting with password-based authentication is also neglected. Likewise, Vadim. [82] suggests for intelligent security to be applied in the authentication process, but instead of the neural network, learning techniques are applied. In this study, the main contribution is this method has the ability to learn a new activity and perform learned actions. However, this method suffers from many limitations. One of the important limitations is it needs to determine particular parameters for improving authentication performance during the authentication process. Furthermore, P. Hoonakker et al.[153], draw on an extensive range of human parameters such as upper case, lower case, number, special character, password size, and old password to assess human behavior with the password. The authors distribute a huge survey among 836 (employees) end-users in examining human behavior with the password. The results of this study reveal that the human factor plays a key role in creating a password in the authentication process. Thus, in this thesis, we work to analysis human factor in authentication process through duration of input password, old password, password size, upper cases, lower cases, special character, numbers, and password error as particular parameters in human password behavior.

Several studies have focused on behavior of authorised users that interact with the web-based software system. In a related context, most of these studies neglect behaviors of authorised users that interact with the password when trying to access the system. In addition, it needs to determine particular parameters to improve the authentication process. Furthermore, many researchers recommend for machine learning to be adapted in authentication process[19][20][21] [22][23][24]. The results of these studies show that when human factors are embedded in authentication, it leads to improved performance in authenticating users. Despite this finding, very few studies have adopted the behavior recognition in password-based authentication in the public cloud. In this thesis, we suggest an Electronic Personal Synthesis Behavior (EPSB) fill this gap through transparent monitoring of user activity in an effort to identify deviations from normal workflow patterns on password-based on three parameters: 1) Duration of input active password from an authorised user; 2) Password style, and 3) Password Error. Therefore, the objective of this study is to improve accuracy in authenticating users by adopting learning tactic for password human behavior as a matching factor with a password during the authentication process. EPSB is adopting authentication layer in public cloud computing to add learnability option into the authentication process. See a summary of literature review in our thesis in Figure (2.6) below.



A model in which convenient, on demand network access is enabled to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or service provider interaction.

Public cloud computing is weak when facing stolen password attack. For example, use of a stolen password of remote access through authentication layer could allow unauthorised user to gain unauthorised access, modify, or destroy the organisation's information systems and resources [2]. The issue of authentication in public cloud computing has received considerable critical attention. Accordingly, in this thesis we work to deal with this issue.

Authentication layer in public cloud computing that prevents unauthorised access to information resources in the public cloud is a major consideration [2]. It is classified into many types such as; Username and Password Authentication, Multifactor Authentication (MFA), Mobile Trusted, Single Sign On, Public Key Infrastructure, Biometric Authentication and implicit authentication. As Sumitra et al. [58], Alok Tripathi et al. [117], P. Ravi Kumar [109], Matthew et al. [118], Muhammad et al. [119], and Nalini et al. [91] state, there are many good reasons in MFA for it to be a suitable method to mitigate authentication attacks in cloud. Thus, in this thesis we select MFA to improve the accuracy in authenticating an authorised user when facing stolen password attack [120][116].

Multifactor Authentication (MFA) which has two or more sub-categories (physiological and behavioural) would be harder to break. MFA has many classical models such as password with smart card, pin, SMS , fingerprint, face recognition, and behaviour recognition[71]. Many researchers recommend applying behaviour recognition in authentication processes to improve its performance [19][20][21][22][23][24]. These researchers recommend for user behaviour recognition with password to be applied to avoid many threats in authentication. Belk et al. [76] in this study investigate the interactivity between humans, technology and user authentication. This study findings highlight the necessity to improve current approaches of password-based user authentication research by incorporating human cognitive factors in both design and run-time.

Behaviour recognition technique is considered cheap and easy to use. Many researchers recommend for current approaches of password-based user authentication research to be improved by incorporating behaviour recognition in human cognitive factors in both design and run-time[25][72][27][28][29][73][74][32][33][75][76]. For authentication with public cloud computing, the performance of user authentication in password-based authentication needs to move from traditional security processes to **intelligent security** processes [24]

The information relevant to protecting an organisation from external and inside threats as well as the processes, policies and tools designed to gather and analyse that information [77]

Figure 2.6 Summary of Literature Review

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Scientific Approach in the Thesis

This chapter explains the research methodology that is suitable for achieving the stipulated objectives of this thesis. From the literature, the research works in this domain are conducted using both qualitative and quantitative data gathering. For the qualitative part, the research study is based on collecting data in order to determine the scope of the work and to find the research gap. For quantitative part, there are two reasons for using such method. The first one is the statistical purpose, which is used to generate results for the proposed algorithm. The second reason is to carry out some of the experimental studies using the proposed algorithm and to compare the authentication accuracy between with and without an algorithm.

3.2 Research Methodology

The research methodology is designed based on the research objectives. It is divided into four stages as shown in Figure 3.1 below. Section 3.3 is the first part of the methodology, which reviews the current state of the multi-factor authentication in public cloud computing. Section 3.4 explained the method choice, the implementation of the algorithm is presented in section 3.5. The fourth part of the evaluation will be presented in section 3.6.

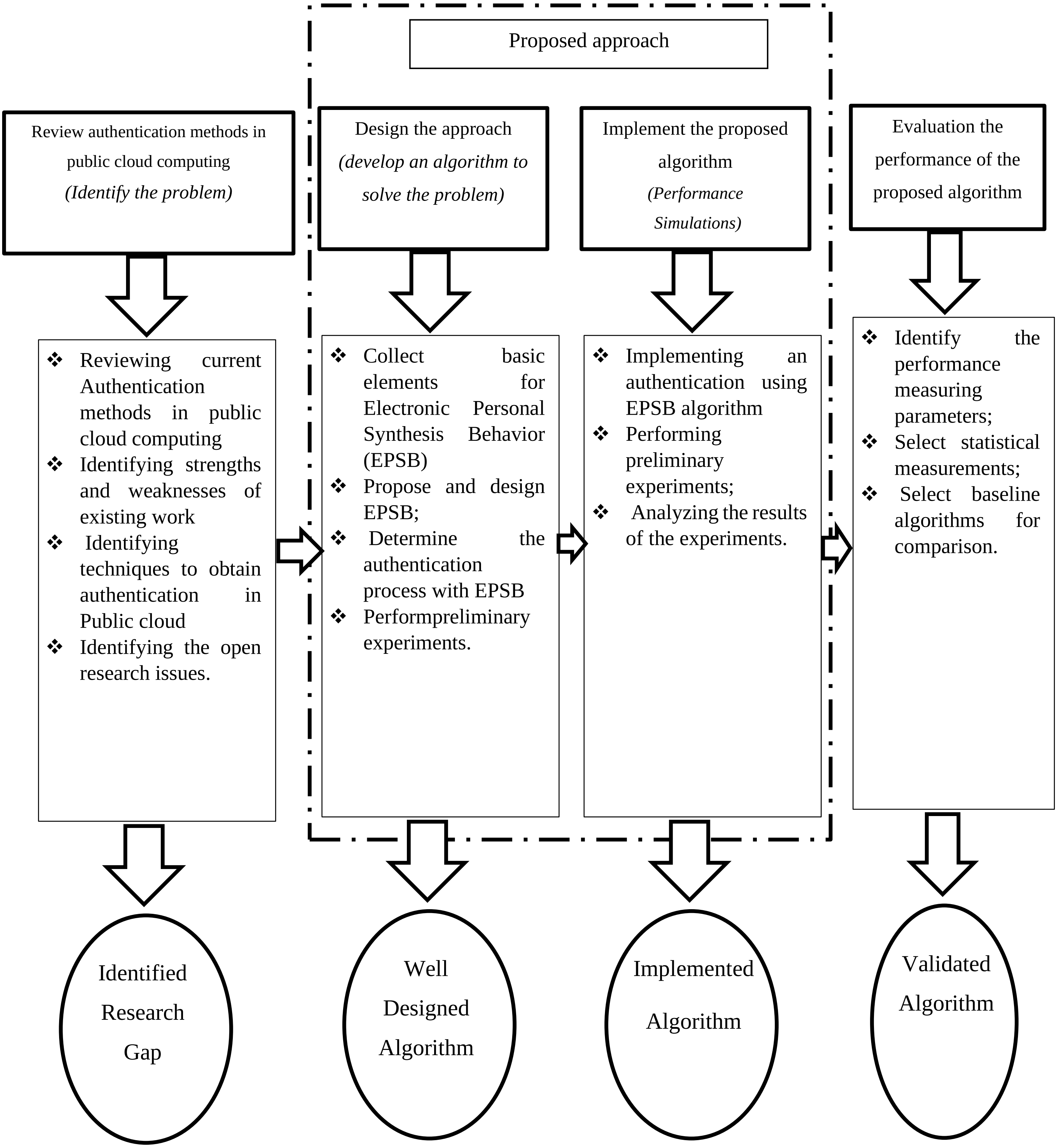

Proposed approach
Review authentication methods in public cloud computing
(Identify the problem)
Design the approach
(develop an algorithm to solve the problem)
Implement the proposed algorithm
(Performance Simulations)
Evaluation the performance of the proposed algorithm
❖ Reviewing current Authentication methods in public cloud computing
❖ Identifying strengths and weaknesses of existing work
❖ Identifying techniques to obtain authentication in Public cloud
❖ Identifying the open research issues.
❖ Collect basic elements for Electronic Personal Synthesis Behavior (EPSB)
❖ Propose and design EPSB;
❖ Determine the authentication process with EPSB
❖ Performpreliminary experiments.
❖ Implementing an authentication using EPSB algorithm
❖ Performing preliminary experiments;
❖ Analyzing the results of the experiments.
❖ Identify the performance measuring parameters;
❖ Select statistical measurements;
❖ Select baseline algorithms for comparison.
Identified Research Gap
Well Designed Algorithm
Implemented Algorithm
Validated Algorithm

Figure 3.1: Proposed Research Methodology

3.3 Reviewing Related Works

Reading and reviewing the existing works is like a bridge between the proposed work and the literature[156]. As a prerequisite of research work, we conducted a review of the state-of-the-art published works on authentication methods in public cloud computing. One of the aims of reviewing related works is to collect strong points and identify the weaknesses of the existing works on current authentication methods in public cloud computing. The investigation shows that there are many multi-factor authentication methods for obtaining the authentication in public cloud computing[157]. The top three methods are password with a smartcard, password with SMS or Mobile, and finally password with biometric[71]. Many researchers have suggested authentication framework in public cloud computing using these methods. However, all these methods have suffered from many drawbacks and threats[157]. The major problems are listed as follows:

1. Most of the current authentication methods in public cloud computing are suffering from weaknesses in dealing with stolen password attacks;
2. Most of previous studies of authentication methods in public cloud computing have not applied intelligent authentication operations;
3. Most studies in the field of authentication methods in public cloud computing have focused only on external authentication factors, such as mobile, SMS, smartcard, security question, or biometric as extra factors for an authentication process that lead to being more expensive;
4. Most of previous studies of authentication methods in public cloud computing have not dealt with learning mechanisms for user behavior recognition in the password as a matching factor with password.

From reviewing the current state of the literature work, we find that the accuracy of the current Multi-factor authentication in public cloud computing is deficient in dealing with the stolen of password attacks[57][58][59][60][61][62][63][64][65]. The best method to improve authentication accuracy is to obtain the intelligent authentication operations [24] by adapting learning mechanisms for behavior recognition that can provide mitigation to threats, automatically[20]. Consequently, the Electronic Personal Synthesis Behavior (EPSB) is suggested by this research, which is built to improve authentication accuracy in diagnosis of an authorized user.

3.4 Design of the Proposed Algorithm

The main objective of EPSB algorithm is to analysis the human "behavior" with the password in authentication process on public cloud computing. Thus, this algorithm has been designed according to five components Time, Password style, Password Error, and Decsion for analysis user behavior (all EPSB design details has been shown in chapter four).The benefits of analysis user behavior to add a new security level for avoiding any unauthorized password change and avoid or stop temporary login, based on the previous error and time (duration) of password entry. Report Identification (RID) service layer is adapted for censorship on all user activities (time (duration), password, error) as shown in Figure 3.2 below.

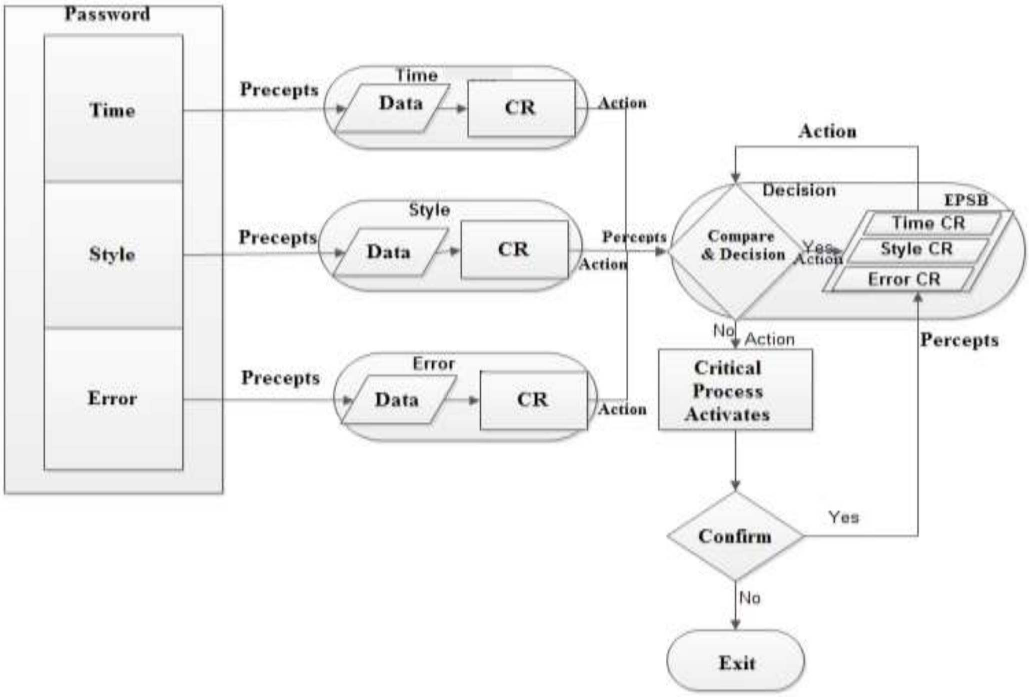


Figure 3.2 EPSB Design

3.5 Implement the Proposed Algorithm

The implementation layer in this work was conducted according to three main phases, implementing an authentication using EPSB algorithm, performing preliminary experiments, and analysing the results of the experiments. Firstly, the authentication using EPSB algorithm is developed by using PHP and JavaScript (see Figure 3.3 and for full interface, see Appendix C). These languages were selected for inclusion and verification in a web domain. The main algorithm components work together to get the required and necessary data for generating the confidence range. In the algorithm, the preliminary experiments were applied two times in Al-Buraimi University College (BUC), Oman for ten working days. The first application was from 17/12 to 29/12/2016 on 12 students from IT, English, Law, and Business departments. The second application was from 18/12/2018 till 03/1/2019 on 22 students from IT, and Business departments only[158]. Finally, the last phase controls the user's behavior, records all the activities completed by the user, analyses them statistically, and sends the results periodically to the decision component. This allows to compare the new entry with the previous confidence range results in order to determine the identification percentage and whether the data could benefit the layer's data integration or not

3.6 Evaluation of the Proposed Approach

The evaluation study for this research can be divided into two parts[159][160][161]. The first part looks at the experimental result of the simulation on the stolen password attacks to examine the accuracy of diagnosis an authorized user according to the EPSB approach. The first objective of this method is to examine the accuracy of user authentication in the proposed algorithm. The second one is to prepare a questionnaire for the samples were used the proposed algorithm in the experimental stage from 18/12/2018 till 3/1/2019. The specific objective of this questionnaire is to examine the acceptance, and ease of use, and analyze the results through statistical tools. Finally, the implemented algorithm will be tested by comparing the performance of the current authentication framework with and without an algorithm. The evaluation methodology is illustrated in Figure 3.3 below.

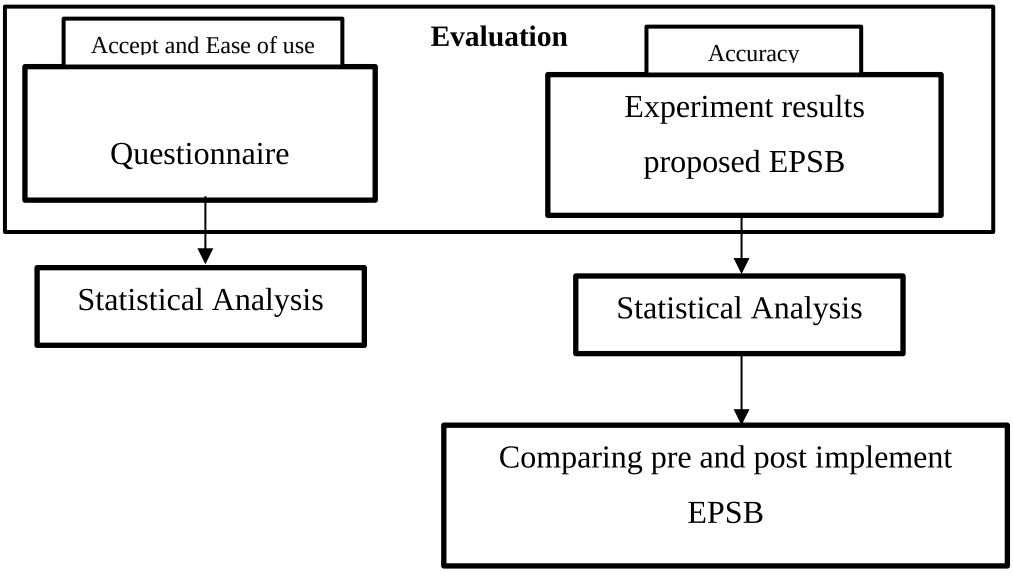


Figure 3.3 Evaluation Methodology

3.6.1 Experimental Result

For the evaluation and validation study of the implemented algorithm, a set of experiments is applied to the proposed algorithm. The problem of this research, which is the authentication in public cloud, is very weak when dealing stolen password attacks. The criteria that are used to evaluate EPSB are discussed. This research focuses on four critical criteria in evaluating the Electronic Personal Synthesis Behavior algorithms (EPSB), including accuracy and security [162][16]. Furthermore, each criterion is defined based on different sub-criteria for precise evaluation. The authentication methods presented in this research are evaluated based on the criteria explained as follows;

a) Accuracy

Accuracy is a criterion that has multiple meanings as a metric. In the world of authentication, accuracy may be referred to as the“degree of match”, which is often characterized by false rejection and false acceptance error rates [44]. However, it is necessary to have a more exact perspective for accuracy because a single user identity is either accepted by a system, or rejected[163]. A binary statistical classification from the world of multivariate statistics is a more appropriate perspective on accuracy[164].With this, there are four possible outcomes for user authentication to a system; a correct user who is granted access (true positive), an incorrect user who is granted access (false positive), a correct user who is denied access (false negative), and an incorrect user who is denied access (true negative)[45]. The accuracy of a user authentication system can be defined as the correct determination of a user’s identity[165]. An accuracy rate is summarized mathematically as the number of correct determinations of a user’s identity, both valid and invalid users, divided by the total number of authentication attempts[165].

b) Accept and Use

Accept and use in authentication refers to “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”[166]. Many information systems (IS) theories/models have been developed to assess the acceptance of the new algorithm in technology. Technology Acceptance Model (TAM) is one of these theories developed by Davis in 1989[167]. TAM has been developed based on the Theory of Reasoned Action (TRA) [168]. The evaluation criteria in this study was conducted according to the TAM model. Accordingly, several criteria are introduced to evaluate the use of existing authentication schemes, such as effortless memorization, fine-grained protection, and easy-to-learn[169][170][171]. The effortless memorization means that there is no need for the user to remember any secrets and the procedure of authentication is made clear and easy for users, which means the authentication method is easy-to-learn[16]. In addition, the security level of authentication procedure is tenable based on the user's preferences in fine-grained protection. The usability as one of the most important criteria of authentication can be preserved to increase the acceptance rate of the method by end-users[172].

c) Security

Security metrics are highly important criteria to evaluate the authentication methods[173]. These criteria show the strength and weakness of the algorithm under different attacks in various situations[174]. Privacy is a significantly critical requirement in authentication methods to ensure that the user is known only to legitimate entities[175]. The authentication method should protect the private information of users from impersonal and stolen password attacks during the authentication procedure. Moreover, anonymity is one of the best approaches to preserve both user and server privacy[176][142].

According to our review, EPSB security criteria must have resistant ability against attacks such as impersonation and stolen password. Therefore, the experiment analysis for evaluated security is focused on four important assumptions related to impersonation and stolen password in authentication algorithms, as listed below:

Assumptions 1: Unauthorized user logs into the authentication layer through an authorized password, network, and device on the first attempt.

Authorized password: Available.

Descriptions: The Unauthorized user has active password through a stolen password and Impersonations attacks.

Assumptions 2: Unauthorized user tries to change the authorized password in the authentication layer.

Authorized password: Available.

Descriptions: The Unauthorized user has active password through a stolen password and Impersonations attacks.

Assumptions 3: Unauthorized user tries to guess the authorized password in the authentication layer.

Authorized password: Unavailable.

Descriptions: Password guessing attacks.

Assumptions 4: Authorized user tries to log into the authentication layer using wrong password.

Authorized password: Available.

Descriptions: The authorized user may be using old password, another language active in PC, forget the current active password, and wrong in few active PW letters.

3.6.2 Distributed Questionnaire

In this study, a questionnaire was prepared to examine the acceptance and use of authentication in the public cloud with EPSB [177][178]. The focused experiment samples are participants who have an image about EPSB in public cloud computing practically for evaluating proposed authentication process. The questionnaire consists of two phases of data collection. The first phase includes the background information of the participants while the second phase sheds light on the process of authentication framework in public cloud computing. The participants were evaluated according to accept and use criterion (see Appendix A).

3.6.3 Statistical Function

The statistical study of this research focused on some values related to the performance of diagnosis the authorized in the authentication process. In the experimental analysis, three statistical functions were selected; the minimum, the maximum, and the average of the results. In this research, the focus was on the performance of diagnosis an authorized user against stolen password attack through examining the accuracy of authenticating an authorized user. In the interview analysis, eight statistical functions were selected: mode, mean, median, Cronbach's alpha, variance, composite reliability, std. deviation, and average to analyze the results gathered from the questionnaire.

3.7 Chapter Summary

This chapter explained the adopted research methodology that organized the research path of this study, where the research objectives were described and discussed accordingly. Moreover, the proposed algorithm named electronic personal synthesis behavior EPSB was explained. The implementation and more details about the approach will be introduced in chapter 4, which is entitled implementation.

This chapter is organized into six sections. The first one is the introduction to the chapter. The second one is the research methodology, which explains the main phases of the research study. The third section explains the review of related works. The fourth section presents the philosophy of the proposed approach, the fifth section explains the implement the proposed algorithm, and the sixth section explains the evaluation method.

The implementation of the proposed approach, which is called EPSB, will be introduced in Chapter 4. Chapter 5 consists of the results and discussions, which represent the evaluation. The last chapter contains the limitation of the research and future works.

CHAPTER 4

ELECTRONIC PERSONAL SYNTHESIS BEHAVIOR (EPSB) FRAMEWORK STRUCTURE AND IMPLEMENTATION

4.1 Electronic Personal Synthesis Behavior Algorithm (EPSB$_{\text{algorithm}}$)

The purpose of this chapter is to present EPSB$_{\text{algorithm}}$. This algorithm aims to improve the authentication process in public cloud computing by dealing directly with behavior recognition, confidence range, and finally generate the electronic personal synthesis behavior (EPSB). Moreover, the learning process of the proposed algorithm is to enable behavior recognition as a matching factor with a password during the authentication process. The main purpose of the proposed algorithm is to analyze human behavior in the authentication layer for improving the authentication process of password-based authentication in authenticating an authorized user. The proposed algorithm tackles not only mitigate the effect of stolen password attacks but also tackles the problem of traditional security strategies by moving into intelligent security operations. This algorithm provides some creative solutions for improving the authentication process in a public cloud computing problem. However, in the previous chapter, they showed that current approaches have some defects. One of the primary weaknesses is that the current methods are weak when dealing with stolen password attacks. Another thing is that the previous studies of the authentication process in public cloud computing have not dealt with learning mechanisms for user behavior recognition in the password as a matching factor with a password, and highly expensive as well. Therefore, we propose the Electronic Personal Synthesis Behavior (EPSB) algorithm to deal with these problems. In the next section, the concept of the proposed approach is stated. In this section, there are sub-sections. The first one presents the time component for the proposed method. The second sub-section describes the password style component. The third sub-section describes the password error component. The fourth sub-section presented the decision component and introduced the approach’s flow chart. The third section of this chapter describes the implementation and test. The first one in this section represents the implementation time(duration) component with decision component. The second on in this section describes the implementation of password style component with decision component, and the third on in this section, describes the implementation of password style component with decision component. The following section discusses the analysis of the results for time, password style, and password error components. The fourth section discusses the analysis of the results for classifying data component. The last section is the conclusion. An overview of the overall topics presented in this chapter can be viewed in Figure 4.1 below.

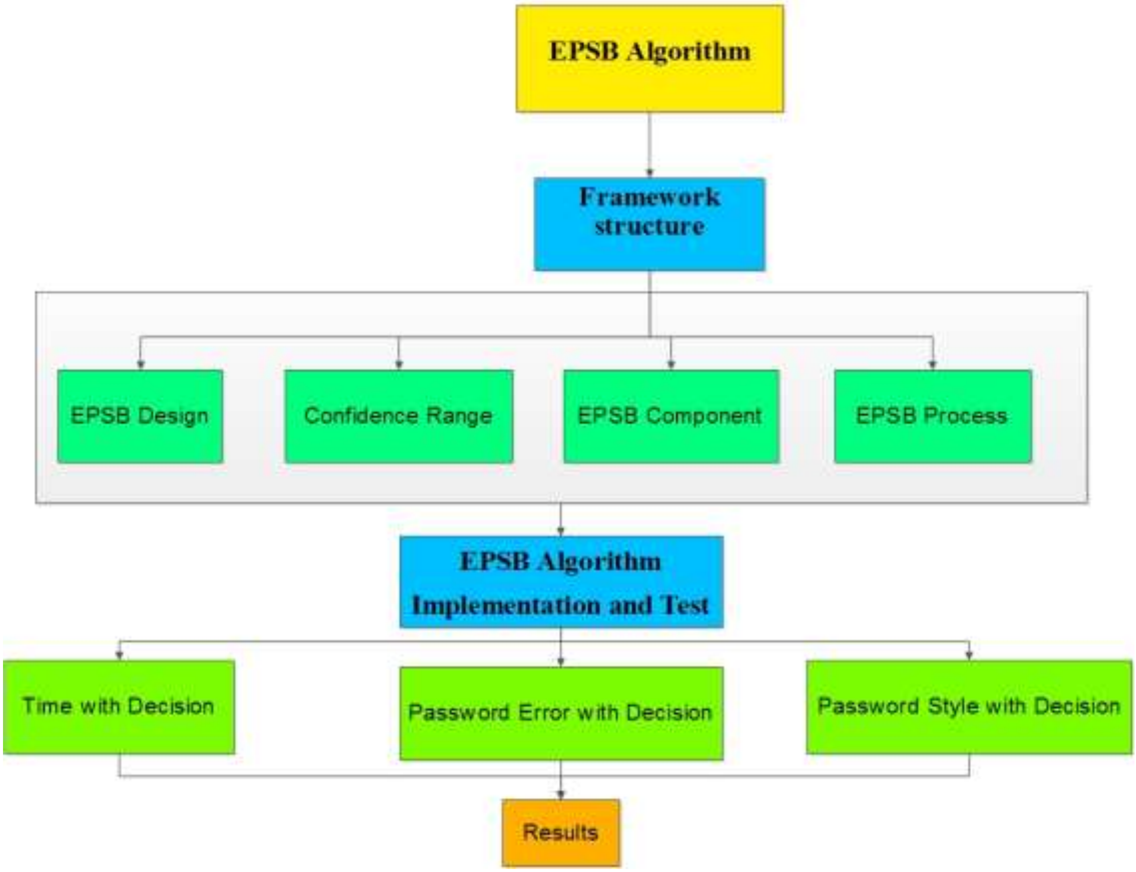


Figure 4.1 Overview of Topic Covered in Chapter Four

4.2 The EPSB Algorithm Framework Structure and Implementation

EPSB is an algorithm created for generating the behaviour of the authorized user when interacting with password numerically. This algorithm has the potential to adapt in any authentication process in public cloud computing, which is applied password with any factor. This algorithm aims to improve the accuracy of user authentication in a public cloud by dealing directly with authorized user behavior. The main body of this algorithm consists of four components; Password Time(Pd), Password Style(PS), Password Error (Pe), and Decision (D). These components will present in the next sub-section.

4.2.1 Design of the EPSB Algorithm

In this study, the main parameters taken from the previous research conducted by P.Hoonakker et al.[153], which explained in details in chapter two, section 2.7.1. The main parameters are Password Style(PS), Password Error(Pe), Password Time(Pd) and Decision (D). Using these parameters allowed to record and analyse most of the users' activities depending on the style of the password, time to typing the password, and the most of frequent error in password location by using statistical tools. The EPSB$_{\text{algorithm}}$ design, as shown in Figure 4.2 below.

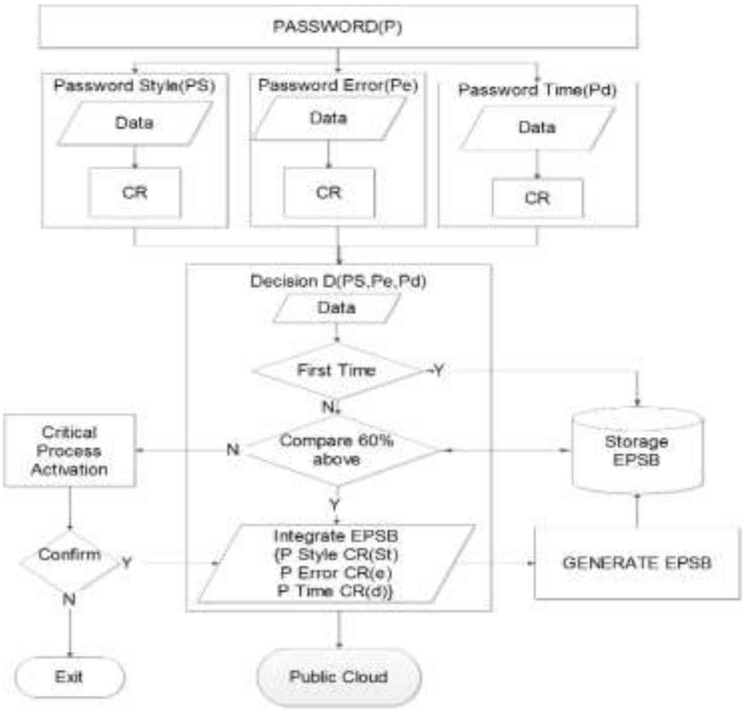


Figure 4.2 EPSB Algorithm Design.

4.2.2 Confidence Range (CR)

The algorithm determines the lowest and highest confidence range values that relate to each user's account. In this stage, it required to know all about each user's behavior that accompanied all associated password processes, including creating and entering the password. Statistically, the descriptive statistics of Mode, Mean, Median, and Range allow to compute and describe the nature of data numerically[179]. Thus, the descriptive statistics in EPSB algorithm adapted to analyse the entered values for each period of typing password, error accompanied by typing the password and password style.

a) Mode

The number that appears most often in a set of numbers. It is the value x at which its probability mass function takes its maximum value. The mode is a way of expressing, in a (usually) single number, relevant information about a random variable or a population. The mode is the most frequently occurring score in distribution and used as a measure of central tendency. The advantage of the mode as a measure of central tendency is that its meaning is obvious. The equation of Mode is shown as follows[179].

$$Mode = \mathrm{L} + \mathrm{h}\frac{\mathrm{fm}-\mathrm{f1}}{(2\mathrm{fm}-\mathrm{f1}-\mathrm{f2})} \qquad \textit{(Equations 4.1)}$$

Where

L=lower boundary modal class

h=size of modal class

fm=frequency corresponding to the modal class

f1=frequency preceding to modal class

f2= frequency proceeding to modal class

b) Mean

The **Mean** (or average) is the most commonly used method of describing central tendency. The Mean calculated from the sum of all the values divided by the total number of values. The mean can be used for both continuous and discrete numeric data. The equation of Mean, as shown as follows[179].

$$Mean = \frac{\sum fx}{\mathrm{n}} \qquad (Equations\ 4.2)$$

Where

x= data value

n= number of items

c) Median

The median is the middle score for a set of data that has been arranged in order of magnitude. The median is less affected by outliers and skewed data. The median is a good measure of the average value when the data include exceptionally high or low values because these have little influence on the outcome. The median is the most suitable measure of average for data classified on an ordinal scale. The equation of Median is shown as follows[179].

$$Median = L + \frac{h1}{f}((n/2)\text{-}C \qquad (Equations\ 4.3)$$

Where

L=lower boundary modal class

h1=size of the median class interval

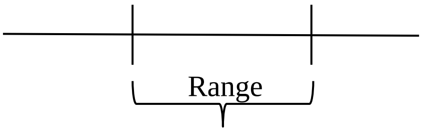
f= frequency corresponding of median class

C= cumulative frequency preceding the median class

n= number of items

d) Range

The range is everything between specified limits or a series of numbers that includes the highest and lowest possible amounts[179].



e) Z-Score

Z-Score can determine the abnormal from the normal value. A Z-score can be calculated using the following formula [180]:

$$\mathbf{Z = (X - \mu) / \sigma} \qquad (Equations\ 4.4)$$

z= is the value on the standard normal distribution

x=is the value on the original distribution

$\boldsymbol{\mu}$= mean

$\boldsymbol{\sigma}$= standard deviation

In this study, the above descriptive statistics of Mode, Mean, Median, and Range are used as one formula to generate electronic behavior print of the authorized user. The user's EPSB generates user's personal behaviour based on the statistical analysis for the confidence range, which works according to the application of the following statistical formula.

$$\text{Confidence Range (CR)}=\mathrm{L}+\mathrm{h}\,\frac{\mathrm{fm}-\mathrm{f1}}{(2\mathrm{fm}-\mathrm{f1}-\mathrm{f2})},\ \sum_i \frac{xi}{n},\ L+\frac{h1}{f}((\mathrm{n}/2)\text{-C} \qquad (Equations\ 4.5)$$

Where

L=lower boundary modal class

h=size of modal class

fm=frequency corresponding to the modal class

f1=frequency preceding to modal class

f2= frequency proceeding to modal class

x= data value

n= number of items

h1=size of the median class interval

f= frequency corresponding of median class

C= cumulative frequency preceding the median class

4.2.3 EPSB Algorithm Components

In this section, the predictive user behavior in a password (EPSB) is used by applying statistical analysis according to the learning principles. User behavior in passwords has many parameters, such as time (duration), password style, and password error [153]. Therefore, the use of passwords (P) in organizations or institutions may pose many security problems in availability, such as unauthorized user login through active P, unauthorized password changes, and restricted temporary logins. To avoid these problems, the EPSB Algorithm was firstly proposed, which includes four components; Password time(Pd), Password style (PS), Password error(Pe), and decision (see Figure 4.3 below).

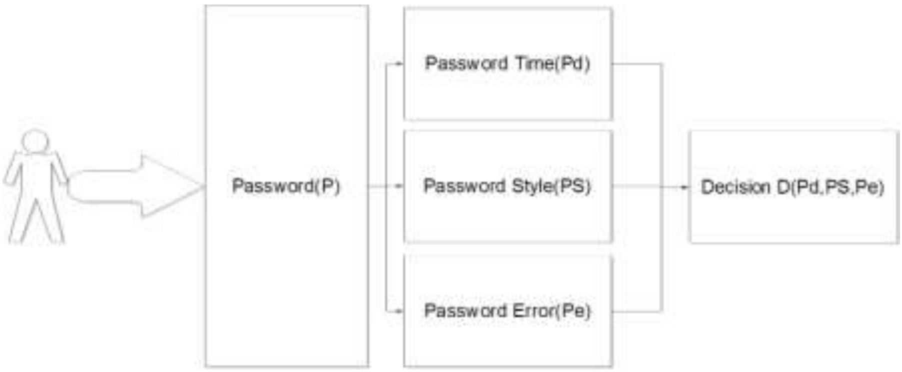


Figure 4.3 EPSB Algorithm Components

Each component is responsible for following up, registering, and analyzing the intended data via following up the legitimate user's behavior in terms of different factors. The main EPSB algorithm components are listed below:

a) Password Time(Pd)

This component describes and represents the time required to type the password. Its main task is to generate an EPSB$_{time}$ based on the CR for any user. The results of CR$_{Pd}$ are genrtated depending on analyse the speed of the click on the keyboard starting from the input of password until login key is pressed. The Pd focuses on determining the unauthorized users according to time (duration) confidence range (CR$_{Pd}$). The following pseudocode captures the Pd for EPSB$_{Time}$. Finally, Pd send the final results to decision(D) component for compare as shown as in Figure 4.4 below.

```
Algorithm: Electronic Personal Synthesis Behavior (EPSB)$_{Time}$
Input: Pd (float) {duration Typed password}
Output: Confidence range (CR$_{Pd(1-3)}$)
If $d$ start
Do
Count $d$
While (press enter)
Recorded $d$
Calculate CR$_{Pd}$
$d=d+1$
```

```
if $d>30$
Del old $d$
Integrated $d$ Value
if $d<=30$
Output:
Confidence range ($CR_{Pd1}, CR_{Pd2}, CR_{Pd3}$)
Send Output to Decision (D)
```

Figure 4.4 Electronic Personal Synthesis Behavior $EPSB_{Time}$

b) Password Style (PS)

In this component, the approach tries to determine an $EPSB_{Style}$ for the user behavior in creating the style of password for determining the authorized user manner in selecting the password (P). The purpose of PS is to prevent any suspicious password changes.

PS works to monitor, record, and analyse the user's behavior as they select passwords through analysis of passwords and tries to find the CR_{PS} for the authorized user based on the following parameters:

1. The number of capital letters used in the password (U).
2. The number of small letters used in the password (l).
3. The overall used letters(T).
4. The number of numeric values used in the password(N).
5. The number of special characters used in the password(E).
6. The length of the password (the number of the overall characters)(L).

Then PS stores all these data points and performs a statistical analysis process to generate the confidence range(CR_{PSN},CR_{PSU},CR_{PSL},CR_{PSE},CR_{PSl}, CR_{PST}) through the use of the $EPSB_{style}$ algorithm in Figure 4.5 below. Finally, PS send the final results to decision(D) component for compare

Algorithm: Electronic Personal Synthesis Behavior $(EPSB)_{Style}$

Input:

N:Number (Integer), U:Upper case (Integer), l:lower case (Integer), L:Length of password (Integer), E: Special character (Integer), T:The overall used letters.

{password characters}

Output:

Confidence range $(CR_{PSN(1-3)})$ Confidence range $(CR_{PSU(1-3)})$ Confidence range $(CR_{PSl(1-3)})$ Confidence range $(CR_{PSL(1-3)})$ Confidence range $(CR_{PSE(1-3)})$ Confidence range $(CR_{PST(1-3)})$

```
If Password started
Do
Count N,U,l,L,E,T
While (Empty)
Recorded N,U,l,L,E,T
Calculate $(CR_{PSN})$, $(CR_{PSU})$, $(CR_{PSl})$, $(CR_{PSL})$, $(CR_{PSE})$, $(CR_{PST})$
$N=N+1, U=U+1, l=l+1, L=L+1, E=E+1, T=T+1$
if  N (or) U (or) l(or) L(or) E (or) T >30
Del old N (or) U (or) l(or) L(or) E (or) T
Integrated N (or) U (or) l(or) L(or) E (or) T Value
if N (or) U (or) l(or) L(or) E (or) T <=30
Output:
($CR_{PSN1}$, $CR_{PSN2}$ , $CR_{PSN3}$ , $CR_{PSU1}$, $CR_{PSU2}$, $CR_{PSU3}$, $CR_{PSL1}$, $CR_{PSL2}$,$CR_{PSL3}$,
$CR_{PSE1}$, $CR_{PSE2}$, $CR_{PSE3}$, $CR_{PSl1}$, $CR_{PSl2}$, $CR_{PSl3}$, $CR_{PST1}$,$CR_{PST2}$, $CR_{PST3}$)
Send Output to Decision (D)
```

Figure 4.5 Electronic Personal Synthesis Behavior $EPSB_{style}$

c) Password Error (Pe)

This component tries to determine an $EPSB_{Error}$ from the errors and categorize them according to whether they are authenticated based on monitoring and recoding the user’s behavior while entering the password wrongly. In most cases, there are some repetitive errors for the authorized users, such as using an old password, repeating a particular character, using another account’s password, not paying attention to the enabled language, or writing the capital letters as small letters and vice versa. In such cases, most systems deactivate the account for a temporary period and then the account will be re-activated after a particular period has passed.

Pe works to monitor, record, and analyse the user's behavior as they select wrong passwords through analysis of error passwords and tries to find the CR_{Pe} for that user based on the following parameters:

1. The number of capital letters used in the password (U).
2. The number of small letters used in the password (l).
3. The overall used letters(T).
4. The number of numeric values used in the password(N).
5. The number of special characters used in the password(E).
6. The length of the password (the number of the overall characters)(L).

Then the Pe stores all these data points and performs a statistical analysis process to generate the confidence range(CR_{PeN},CR_{PeU},CR_{PeL},CR_{PeE},CR_{Pel}, CR_{PeT})through the use of the $EPSB_{Error}$ algorithm in Figure 4.6 below. Finally, Pe send the final results to decision(D) component for compare.

Algorithm: Electronic Personal Synthesis Behavior $(EPSB)_{Error}$

Input:

N:Number (Integer), U:Upper case (Integer), l:lower case (Integer), L:Length of password (Integer), E: Special character (Integer), T:The overall used letters. {password characters}

Output:

Confidence range ($CR_{PeN(1-3)}$) Confidence range ($CR_{PeU(1-3)}$) Confidence range ($CR_{Pel(1-3)}$) Confidence range ($CR_{PeL(1-3)}$) Confidence range ($CR_{PeE(1-3)}$) Confidence range ($CR_{PeT(1-3)}$)

```
If Password started
Do
Count N,U,l,L,E,T
While (Empty)
Recorded N,U,l,L,E,T
Calculate ($CR_{PeN}$), ($CR_{PeU}$), ($CR_{Pel}$), ($CR_{PeL}$), ($CR_{PeE}$), ($CR_{PeT}$)
$N=N+1, U=U+1, l=l+1, L=L+1, E=E+1, T=T+1$
if  N (or) U (or) l(or) L(or) E (or) T >30
Del old N (or) U (or) l(or) L(or) E (or) T
Integrated N (or) U (or) l(or) L(or) E (or) T Value
if N (or) U (or) l(or) L(or) E (or) T <=30
```

```
    Output:
        ($CR_{PeN1}, CR_{PeN2}, CR_{PeN3}, CR_{PeU1}, CR_{PeU2}, CR_{PeU3}, CR_{PeL1}, CR_{PeL2}, CR_{PeL3},$
         $CR_{PeE1}, CR_{PeE2}, CR_{PeE3}, CR_{PeI1}, CR_{PeI2}, CR_{PeI3}, CR_{PeT1}, CR_{PeT2}, CR_{PeT3}$)
Send Output to Decision (D)
```

Figure 4.6 Electronic Personal Synthesis Behavior $EPSB_{Error}$

d) Decision (D)

This component monitors and follows up the new user behavior to determine whether s/he is the authorized user. The component records and stores the $EPSB_{Time,Style,Error}$ which is generated from Pd, PS, Pe for the current user and works to compare it with the previous $EPSB_{Time,Style,Error}$. Then the component extracts the $EPSB_{Time,Style,Error}$ for the current user and compares it with the approved $EPSB_{Time,Style,Error}$ in all related issues as shown as in Figure 4.7 below.

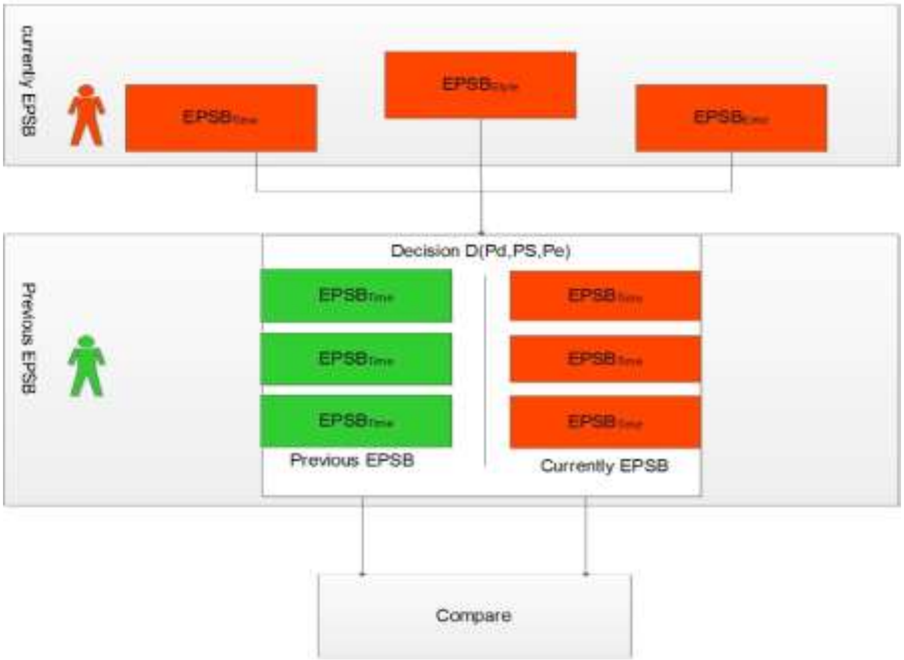


Figure 4.7 Decision Component Tasks

If the rate is < = 60%, then it will send the data, as it will be considered approved for all the related parties for confirmation to integrate the personal data for each user. Otherwise (i.e., the rate is > 60 %), it will activate the critical security procedures. The following pseudocode captures the decision component for the proposed algorithm.

```
    Algorithm: Electronic Personal Synthesis Behavior (EPSB) Decision Component
    Input: EPSB$_{Time}$, EPSB$_{Style}$, EPSB$_{Error}$
    Output:
    Last EPSB$_{Time}$, EPSB$_{Style}$, EPSB$_{Error}$ , Active critical security procedure,
    Block or unlock on Data high level security
    Login public cloud
    ------------------------------------------------------------
    Stored EPSB$_{Time}$, EPSB$_{Style}$, EPSB$_{Error}$
    Similarity between current EPSB$_{Time}$, EPSB$_{Style}$, EPSB$_{Error}$ and stored
    EPSB$_{Time}$, EPSB$_{Style}$, EPSB$_{Error}$
            Rate of compare:
            If rate >= 60
                Integrate EPSB$_{Time, Style, Error}$
                Update current EPSB $_{Time, Style, Error}$
                Login public cloud
            Else
             Active critical security procedure
             Block on Data high-level security
        For I = 2
             If confirm
                      Unlock Data
                      Integrate EPSB $_{Time, Style, Error}$
                      Update current EPSB $_{Time, Style, Error}$
                      Login public cloud
              Else
              Deactivate account
              Send active code into Authentication user
              Send active code into Administration
```

Figure 4.8 Electronic Personal Synthesis Behavior (EPSB)$_{Decision}$

4.2.4 The EPSB Algorithm Process

We analyze how login data from the authentication layer in the public cloud can be used to predict user behavior. The EPSB$_{algorithm}$ process captures all requests made to the authorized user such as time(Pe), password style(PS), and password error(pe). For many authentication systems, these activities are not fully utilized. These data include historical information about the activities performed by users. In addition to improving user interaction with the password can be used to trace patterns of behavior. The patterns can then be used with statistical language models, such as CR, to predict user behavior. The EPSB$_{\text{algorithm}}$ would determine which CR should be idled and which one should be active according to the user activities with the authentication layer.

The EPSB$_{\text{algorithm}}$ has four components including Password Time(Pd), Password style (PS), Password error(Pe), and decision(D) for generating EPSB$_{\text{Time}}$, EPSB$_{\text{Style}}$, EPSB$_{\text{Error}}$, EPSB$_{\text{D}}$ respectively. Each component is responsible for following up, registering, and analyzing the intended data via following up the authorized user's behavior in terms of different factors. The EPSB$_{\text{algorithm}}$ works to analyse human factor in authentication process through several parameters in human password behaviour namely duration of typing password(CR$_{\text{Pd}}$) EPSB$_{\text{Time}}$, Password Style(CR$_{\text{PS}}$) EPSB$_{\text{Style}}$, Password error(Pe) EPSB$_{\text{Error}}$, and then send all results to Decision (D) component, as shown as in Figure 4.9 below.

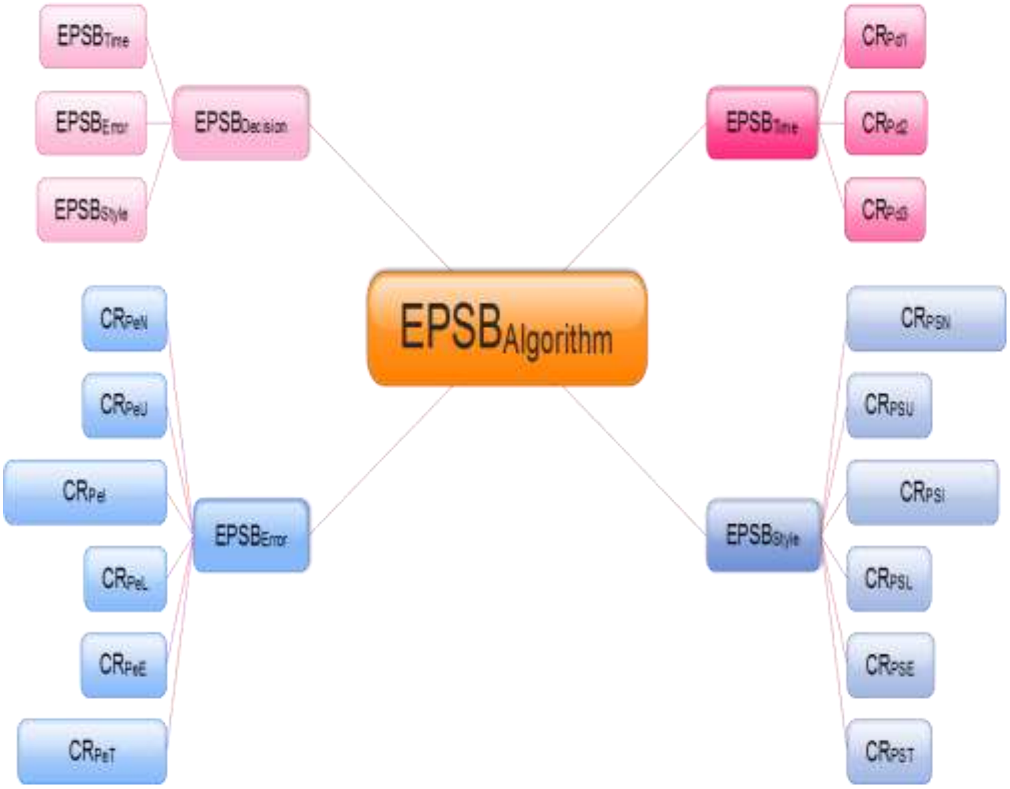


Figure 4.9 EPSB$_{\text{algorithm}}$ Parameters

The following Four components process shows how EPSB$_{\text{Algorithm}}$ may be used in typical settings.

a) The $\text{EPSB}_{\text{Time}}$ Process

The process of authentication in EPSB involves many steps that are intimately linked and completely interdependent. The initial steps, the component Pd is working to monitor, record and analyse the time required from the authorized user to type the password. The task of these steps to generate the $\text{EPSB}_{\text{Time}}$ ($\text{EPSB}_{\text{Time}}$= CRP_{d1}, CR_{Pd2},CR_{Pd3}) according to Confidence range(CR) formula in section 4.2.2 above. depending on the speed of the click on the keyboard starting from the input of password until the login key is pressed and then send the results to the Decision (D) component. Figure 4.10 and Table 4.1 below explain the process of generating $\text{EPSB}_{\text{Time}}$.

Table 4.1 Process of $\text{EPSB}_{\text{Time}}$.

Steps	Processes
Step1	Monitoring and recording the time required from the user to type the password (Data). (**Input**: the duration from user starting to input his/her password until login button is pressed)
Step2	Analysing the recording data by using confidence range (C_{Pd})
Step3	Generating confidence range (CR_{Pd}) **Output:** **$\text{EPSB}_{\text{Time}}$=** ($\text{CR}_{\text{Pd1}}$, CR_{Pd2}, CR_{Pd3})
Step4	Send the **$\text{EPSB}_{\text{Time}}$** as input into the Decision(D) component

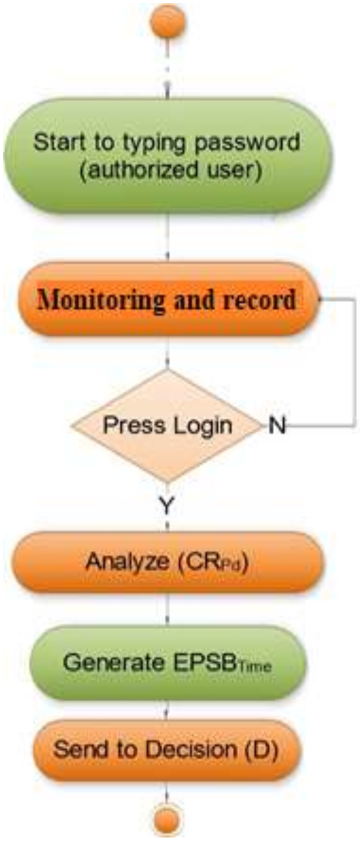


Figure 4.10 EPSB$_{Time}$ Process

Normally, the speed of using the keyboard is different from user to the user according to the location of keys, using two or one hands, time of using PC, using keyboard directly, and a familiar keyboard. The purpose of this component is to determine the authorized user according to the speed of the click on the keyboard. Later, these logins will be saved internally under Decision (D) control, and a set of statistical analysis processes will be performed to generate an approved confidence range (CR$_{Pd1}$,CR$_{Pd2}$,CR$_{Pd3}$) based on the user's timely behavior. This component aims at finding the authorized user behavior when typing his/her password to detect any suspicious logins even if the intrusive person has the real password (stolen password attack).

b) The EPSB$_{style}$ Process

The PS component is working to monitor, record, and analyse the authorized user's behaviour as they select or change passwords. The task of these steps to generate the EPSB$_{style}$ according to the Confidence range(CR) formula in section 4.2.2 above. The CR$_{PS}$ will be generated depending on the analyses of the current and old password aspects such as Number (N), Upper case (U), Lower case (l), Especial character(E), Length of password(L), Number of letters(T) and then send the results to Decision (D) component. The EPSBstyle is defined as:

$\mathrm{EPSB}_{\mathrm{style}}$=($\mathrm{CR}_{\mathrm{PSN1}}$, $\mathrm{CR}_{\mathrm{PSN2}}$, $\mathrm{CR}_{\mathrm{PSN3}}$, $\mathrm{CR}_{\mathrm{PSU1}}$, $\mathrm{CR}_{\mathrm{PSU2}}$, $\mathrm{CR}_{\mathrm{PSU3}}$, $\mathrm{CR}_{\mathrm{PSl1}}$, $\mathrm{CR}_{\mathrm{PS12}}$, $\mathrm{CR}_{\mathrm{PS3}}$, $\mathrm{CR}_{\mathrm{PSE1}}$, $\mathrm{CR}_{\mathrm{PSE2}}$, $\mathrm{CR}_{\mathrm{PSE3}}$, $\mathrm{CR}_{\mathrm{PSL1}}$, $\mathrm{CR}_{\mathrm{PSL2}}$, $\mathrm{CR}_{\mathrm{PSL3}}$, $\mathrm{CR}_{\mathrm{PST1}}$, $\mathrm{CR}_{\mathrm{PST2}}$, $\mathrm{CR}_{\mathrm{PST3}}$.

The $\mathrm{EPSB}_{\mathbf{style}}$ tries to determine the user behavior in creating the style of password to prevent any suspicious password changes. The Figure 4.11 and Table 4.2 below explain the process of generate $\mathrm{EPSB}_{\mathrm{style}}$.

Table 4.2 Process of $\mathrm{EPSB}_{\mathrm{style}}$.

Steps	**Processes**
Step 1	User chooses his/her password;
Step2	**Input**: Monitoring and recording the new and old password structure (Data).
Step3	Analysing password structure by using confidence range ($\mathrm{CR}_{\mathrm{PS}}$) according to the aspects below (Data): a) Number (N), b) Upper case (U) c) Lower case (l) d) Especial character(E), e) Length of password(L), f) Number of letters(T)
Step4	Generating confidence range ($\mathrm{CR}_{\mathrm{PS}}$) **Output:** **$\mathbf{EPSB}_{\mathbf{Style}}$=**($\mathrm{CR}_{\mathrm{PSN1}}$, $\mathrm{CR}_{\mathrm{PSN2}}$, $\mathrm{CR}_{\mathrm{PSN3}}$, $\mathrm{CR}_{\mathrm{PSU1}}$, $\mathrm{CR}_{\mathrm{PSU2}}$, $\mathrm{CR}_{\mathrm{PSU3}}$, $\mathrm{CR}_{\mathrm{PSL1}}$, $\mathrm{CR}_{\mathrm{PSL2}}$, $\mathrm{CR}_{\mathrm{PSL3}}$, $\mathrm{CR}_{\mathrm{PSE1}}$, $\mathrm{CR}_{\mathrm{PSE2}}$, $\mathrm{CR}_{\mathrm{PSE3}}$, $\mathrm{CR}_{\mathrm{PSl1}}$, $\mathrm{CR}_{\mathrm{PSl2}}$, $\mathrm{CR}_{\mathrm{PSl3}}$, $\mathrm{CR}_{\mathrm{PST1}}$, $\mathrm{CR}_{\mathrm{PST2}}$, $\mathrm{CR}_{\mathrm{PST3}}$)
Step5	Send the **$\mathbf{EPSB}_{\mathbf{Style}}$** as input into the Decision (D) component

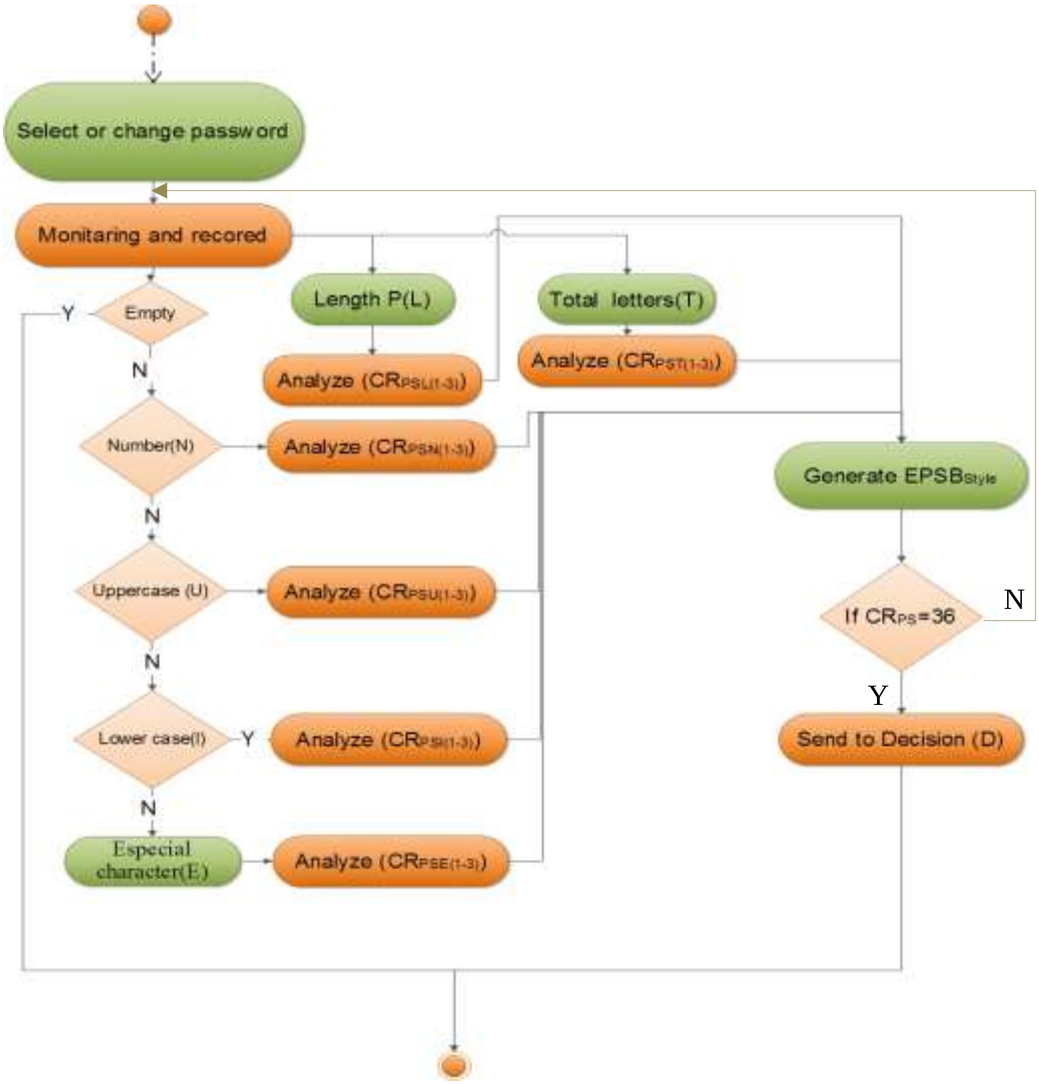


Figure 4.11 EPSB$_{\text{Style}}$ Process

c) The EPSB$_{\text{Error}}$ Process

The Pe component is working to monitor, record, and analyse the authorized user's behaviour when they typing error passwords. The task of these steps to generate the EPSB$_{\text{Error}}$ according to the Confidence range(CR) formula in Equation 4.5 above. The CR$_{\text{Pe}}$ will be generated depending on the analyses of the error password aspects such as Number (N), Upper case (U), Lower case (l), Especial character(E), Length of password(L), Number of letters(T) and then send the results to Decision (D) component. The EPSB$_{\text{Error}}$ is defined as:

EPSB$_{\text{Error}}$=(CR$_{\text{PeN1}}$, CR$_{\text{PeN2}}$, CR$_{\text{PeN3}}$, CR$_{\text{PeU1}}$, CR$_{\text{PeU2}}$,CR$_{\text{PeU3}}$, CR$_{\text{PeL1}}$, CR$_{\text{PeL2}}$, CR$_{\text{PeL3}}$, CR$_{\text{PeE1}}$, CR$_{\text{PeE2}}$, CR$_{\text{PeE3}}$, CR$_{\text{Pel1}}$, CR$_{\text{Pel2}}$, CR$_{\text{Pel3}}$, CR$_{\text{PeT1}}$, CR$_{\text{PeT2}}$, CR$_{\text{PeT3}}$).

The EPSB$_{\textbf{Error}}$ tries to determine the authorized user behavior when typing the wrong password. Figure 4.12 and Table 4.3 below explain the process of generating EPSB$_{\text{Error}}$.

Table 4.3 Process of EPSB$_{\text{Error}}$.

Steps	**Processes**
Step 1	User typing error password
Step2	**Input**: Monitoring and recording the error passwords typed
Step3	Analysing error password structure by using confidence range (CR$_{\text{Pe}}$) according to the aspects below (Data): a) Number (N) b) Upper case (U) c) Lower case (l) d) Especial character(E), e) Length of password(L), f) Number of letters(T)
Step4	Generating confidence range (CR$_{\text{Pe}}$) **Output:** **EPSB$_{\textbf{Error}}$=**(CR$_{\text{PeN1}}$,CR$_{\text{PeN2}}$,CR$_{\text{PeN3}}$, CR$_{\text{PeU1}}$, CR$_{\text{PeU2}}$,CR$_{\text{PeU3}}$, CR$_{\text{PeL1}}$, CR$_{\text{PeL2}}$, CR$_{\text{PeL3}}$, CR$_{\text{PeE1}}$,CR$_{\text{PeE2}}$, CR$_{\text{PeE3}}$, CR$_{\text{Pel1}}$, CR$_{\text{Pel2}}$, CR$_{\text{Pel3}}$, CR$_{\text{PeT1}}$, CR$_{\text{PeT2}}$, CR$_{\text{PeT3}}$).
Step5	Send the **EPSB$_{\textbf{Error}}$** as input into the Decision(D) component.

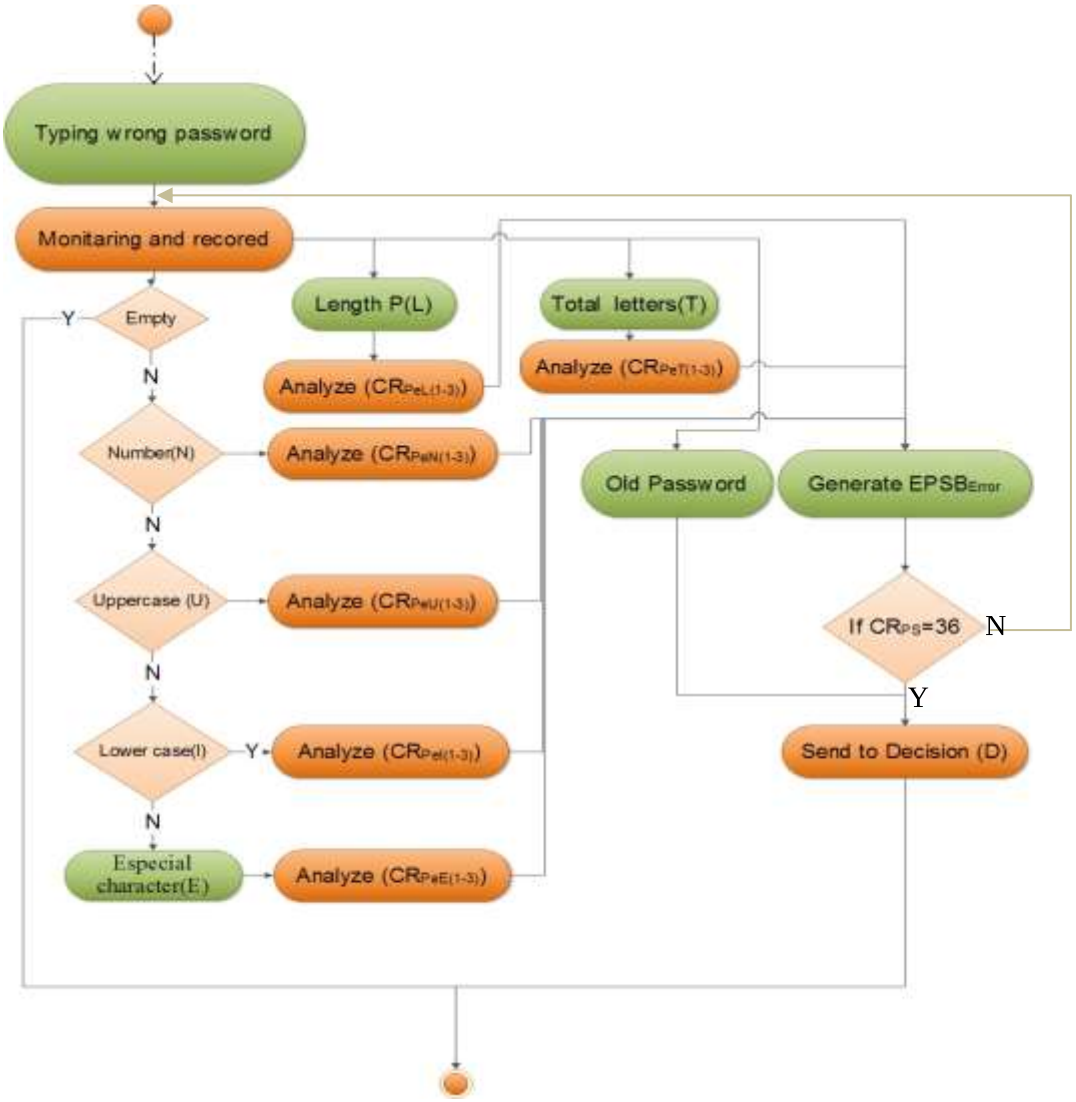


Figure 4.12 EPSB$_{Error}$ Process

d) Decision(D) process

The decision(D) component works on receiving the results from other components (EPSB$_{Time}$,EPSB$_{Style}$,EPSB$_{Error}$) and determines the rate similarity between the current and previous Electronic Personal Synthesis Behavior (EPSB$_{Time}$, EPSB$_{Style}$, EPSB$_{Error}$) for the authorized user. If the entire identical rate is more or equal to sixty percent (>= 60 %), then it is within the authentic range. Otherwise, a confirmation e-mail will be sent to the authorized user for confirmation. If the authorized user confirms the e-mail, the user will be considered as an authorized user. In case the user does not confirm the e-mail within 3 minutes, the link will be deactivated, and another link will be sent to the same e-mail. If the user does not confirm the new link, the account will be deactivated permanently, and an e-mail will be sent to both the authorized user and the admin to re-register along with the details showing the time and IP address of the person who tried to log in.

Sometimes an authorized user has been confirmed as being of extreme value. This activity affects negatively on the CR_{Pd} and in avoiding this weakness, these two steps must be followed:

1. Determine the extreme value in the duration component;
2. An active account of the user without an effect on confidence range values.

To achieve what has been applied as the Z Score function, a diagnosis of extreme values is crucial to avoid integration with previous values. Figure 4.13 and Table 4.4 below explain the process of generating $EPSB_D$.

Table 4.4 Process of $EPSB_D$

Steps	Processes
Step 1	**Input:** Current $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$
Step2	**If first time:** 2.1: Records all current $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$; 2.2: Go to step8 **Else** Step3
Step3	Stores current $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$;
Step4	Compares between current $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$ and previous $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$ **Output**: $EPSB_{DStyle}$, $EPSB_{DError}$, $EPSB_{DTime}$
Step5	**If the** $EPSB_{DStyle}$, $EPSB_{DError}$, $EPSB_{DTime}$ **similarity up to 60% :** 4.1: Integrated with previous $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$ 4.2: Generated new $EPSB_{Style}$, $EPSB_{Error}$, $EPSB_{Time}$ 4.3: Go to step 9 **Else** Step6

Step6	5.1: Active critical process activities; 5.2:Verification process; 5.2.1: **If EPSB$_{Style}$, EPSB$_{Error}$, verified**: Go to step6 5.2.2: **If EPSB$_{Time}$ verified:** Go to step 8 **Else** Go to step10
Step7	6.1 Integrated with previous EPSB$_{Style}$, EPSB$_{Error}$ 6.2 Generated and stored new EPSB$_{Style}$, EPSB$_{Error}$; 6.3 Deactivate critical process activities; 6.4 Go to step 9
Step8	7.1 Active z score 7.1.1: **If extremely anomalous:** a) Deactivate critical process activities; b) Logs in a public cloud **Else** a) Integrated with previous EPSB$_{time}$ b) Generated and stored new EPSB$_{time}$ c) Deactivate critical process activities; 7.1.2: Go to step 9
Step9	Login into Public cloud
Step10	Exit

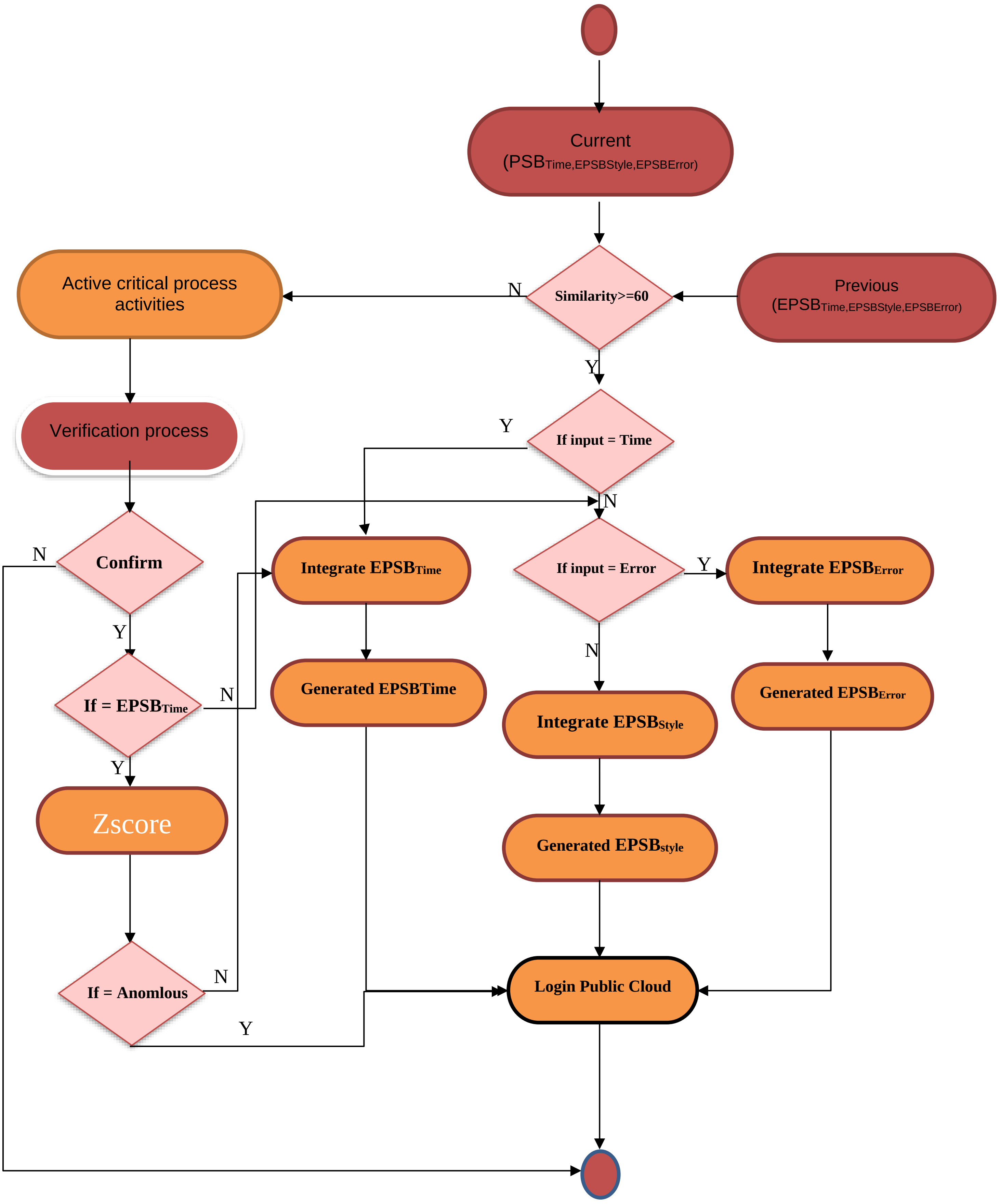


Figure 4.13 EPSB$_D$ Process

4.3 Implement and Test

The layer is improved by using PHP and JavaScript (see Appendix C). These languages were selected for inclusion and verification in a web domain. The components work together to get the required and necessary data for generating the confidence range(CR). The $\text{EPSB}_{\text{algorithm}}$ is monitoring the authorized user's behavior, recording all the activities completed by the authorized user, analyzing them statistically, and sending the results periodically to the decision (D) component for comparison to the current with the previous $\text{EPSB}_{\text{Time}}$,$\text{EPSB}_{\text{Style}}$,$\text{EPSB}_{\text{Error}}$, to determine the identification percentage and whether the data could benefit the layer's data integration. Figure 4.14 shows the component activities.

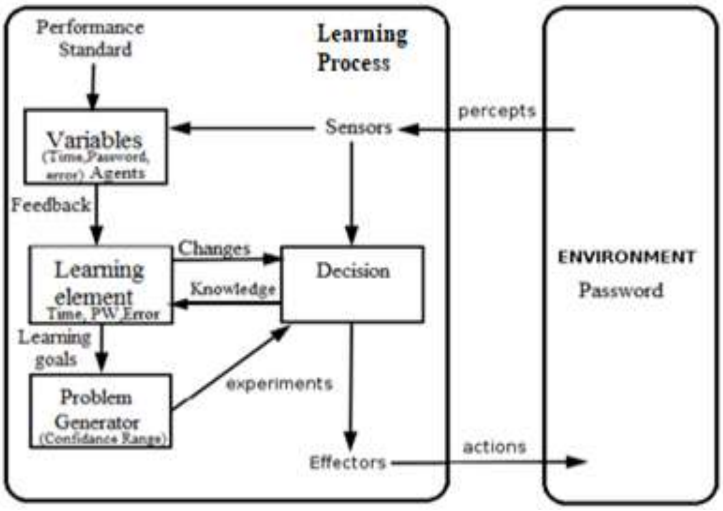


Figure 4.14 Learning Activities.

4.3.1 The EPSB Algorithm Scenarios

This study explores how user behavior affects system security in public cloud when using authentication layer. The following Three scenarios show how $\text{EPSB}_{\text{Algorithm}}$ may be used in typical settings.

Scenario 1: Alice usually uses her laptop to log in her public cloud from the university campus to perform her tasks. She types her password directly and easily as she daily uses the same password. One day, while Alice closed her public cloud to get a rest, Bob (as an unauthorized user) try to access into her public cloud illegally using an active password to perform actions on the corporate site and maliciously merge and change sensitive records. Unbeknown to the Bob, the unauthorized user, the website is equipped with $EPSB_{Time}$ that automatically detects the deviated behavior and subsequently locks the authorized user's system.

The $EPSB_{Time}$ is monitoring and recording the time required from the authorized user to type the active password. Its main task is to generate an $EPSB_{Time}$ based on the CR_{Pd} for any user. $EPSB_{Time}$ works as follows: It monitors all user actions with password and builds, for each user, an $EPSB_{Time}$, a mathematical representation of how the user typically interacts with the password. The $EPSB_{DTime}$ determines, in real time, whether the user is deviating from expected behavior, signalling the possible presence of an unauthorized user. Because this instance of $EPSB_{Time}$ is based solely on analysis of web logs, it is extremely fast and it requires no special hardware or changes to the system.

Scenario 2: Alice uses her laptop to telework from a University lab. She uses his web browser to login to her public cloud and perform her daily tasks. She writes an inactive password such as using an old password, repeating a particular character, using another account's password, not paying attention to the enabled language, or writing the capital letters as small letters and vice versa. The website is equipped with our $EPSB_{Error}$, that automatically detects deviations from normal behavior and subsequently locks her public cloud.

The $EPSB_{Error}$ works by monitoring, recording, and analysing the Alice's behavior when she type wrong passwords through analysis of wrong passwords and tries to find the CR_{Pe} for that user based on the number of capital letters used in the password (U), the number of small letters used in the password (l), the overall used letters(T), the number of numeric values used in the password(N), the number of special characters used in the password(E). the length of the password (the number of the overall characters) (L). Its main task is to generate an $EPSB_{Error}$ based on the CR_{Pe} for any user for the purpose of recognizing the authorized user error. when she closed her public cloud, an unauthorized person (Bob) attempt to accesses to her public cloud through guessing active password. The $EPSB_{Error}$ works as follows: It monitors all users actions with the wrong password typed and builds, for each user, an $EPSB_{Error}$, a mathematical representation of how the user typically typing wrong password. The $EPSB_{DError}$ determines, whether the user is deviating from expected behavior, signalling the possible presence of an unauthorized user. The purpose of

$EPSB_{Error}$ to determine Alice's action when typing her error password. Because this instance of $EPSB_{Error}$ is based solely on analysis of password structure by using confidence range (CR_{Pe}), it is extremely fast and it requires no special hardware or changes to the system.

Scenario 3: Alice uses her laptop to telework from a local coffee shop. She uses her web browser to login to her public cloud and perform her daily tasks. She has chosen her password when she registered as an authorized user in her company. During three months, she has changed her password many times. The $EPSB_{Style}$ works to monitoring, recording, and analysing the user's behaviour when they select passwords through analysis of passwords and tries to find the CR_{PS} for that user based on the number of capital letters used in the password (U), the number of small letters used in the password (l), the overall used letters(T), the number of numeric values used in the password(N), the number of special characters used in the password(E). the length of the password (the number of the overall characters)(L). Its main task is to generate an $EPSB_{Style}$ based on the CR_{PS} for any user for the purpose of recognizing the authorized user style when his/her choses the password. As she steps away from her laptop to get a refill of coffee, an unauthorized person accesses her laptop to change her system password. The unauthorized user has a current active password through stolen password attack. Unbeknownst to the "unauthorized user," the website is equipped with our $EPSB_{Style}$, that automatically detects deviations from normal behavior and subsequently locks her public cloud. The $EPSB_{Stley}$ works as follows: It monitors all user actions with the style of password and builds, for each user, an $EPSB_{syle}$, a mathematical representation of how the user typically chosen his/her password. The $EPSB_{DStley}$ determines, whether the user is deviating from expected behavior, signalling the possible presence of an unauthorized user. Because this instance of $EPSB_{Style}$ is based solely on analysis of password structure by using confidence range (CR_{PS}), it is extremely fast and it requires no special hardware or changes to the system. The component will be activated as shown as in Table 4.5 below.

Table 4.5 Actions between Scenarios and EPSB Components Processes

Scenarios	EPSB Components Processes			
	Password Time (Pd)	Password Style (PS)	Password Error (Pe)	Decision(D)
1	Active	Inactive	Inactive	Active
2	Inactive	Inactive	Active	Active
3	Inactive	Active	Inactive	Active

4.3.2 Implementation of $\text{EPSB}_{\text{Time}}$ and $\text{EPSB}_{\text{Decision}}$

We will now show, via an example, how $\text{EPSB}_{\text{algorithm}}$ works when authorized user interact with password in public cloud. Assume that, over time, authentication behavior have been collected for users of public cloud. ID has been developed, for each user, an $\text{EPSB}_{\text{Time}}$ component, essentially representing the user's typical behavior. According to scenario 1, Alice, an employee, typically starts from her user profile page to connect to the public cloud. She is using her password daily. Thus, she types her password directly and easily. The $\text{EPSB}_{\text{Time}}$ is used to moniter , record, and analyse the time required from Alice to type the password. The task of these steps to generate the $\text{EPSB}_{\text{Time}}$ for Alice as shown below:

$$(\text{EPSB}_{\text{Time}}= \text{CR}_{\text{Pd1}}, \text{CR}_{\text{Pd2}},\text{CR}_{\text{Pd3}}).$$

The implementation of $\text{EPSB}_{\text{Time}}$ is based on the mechanism below:

If the Alice correctly enters password from the first attempt to the system many time during one week, then the component that is monitoring the Alice would be the *Pe* component only. The other components will be inactived because the user's operation would be out of the components' scope of interest, as there are no wrong entries or changes to the passwords. In such a way, the *Pd* component will generate a new $\text{EPSB}_{\text{Time}}$ as shown as in the Table 4.6 below:

Table 4.6 Process of Generate EPSB$_{Time}$

Attempt	Input	Process					
	Activites	EPSB$_{Time}$				EPSB$_{Style}$	EPSB$_{Error}$
1	Alice started to typing active password till press login. The period of typing password=3.3s	**Step1**	Data	3.3		Inactive	Inactive
			Record	3.3			
		Step2	Analysis				
		Step2.1	CR$_{Pd1}$	Min	Max		
				3.3	3.3		
		Step2.2	CR$_{Pd2}$	Min	Max		
				3.3	3.3		
		Step2.3	CR$_{Pd3}$	Min	Max		
				3.3	3.3		
		Step3	Generated EPSB$_{Time}$= 3.3 - 3.3 , 3.3 - 33, 3.3 - 3.3				
		Step4	Send EPSB$_{Time}$ to Decision (D)				
	Activites	EPSB$_{Time}$				EPSB$_{Style}$	EPSB$_{Error}$
2	Alice started to typing active password till press login. The period of typing password = 3.1 s	**Step1**	Data	3.1		Inactive	Inactive
			Record	3.3			
				3.1			
		Step2	Analysis				
		Step2.1	CR$_{Pd1}$	Min	Max		
				3.2	3.3		
		Step2.2	CR$_{Pd2}$	Min	Max		
				3.2	3.3		
		Step2.3	CR$_{Pd3}$	Min	Max		
				3.2	3.3		
		Step3	Generated EPSB$_{Time}$= 3.2 - 3.3 , 3.2 - 33, 3.2 - 3.3				
		Step4	Send EPSB$_{Time}$ to Decision (D)				
	Activites	EPSB$_{Time}$				EPSB$_{Style}$	EPSB$_{Error}$
3	Alice started to typing active password till press login. The period of typing password =3s	**Step1**	Data	3.3		Inactive	Inactive
			Record	3.3			
				3.1			
				3			
		Step2	Analysis				
		Step2.1	CR$_{Pd1}$	Min	Max		
				3.13	3.3		
		Step2.2	CR$_{Pd2}$	Min	Max		
				3.13	3.3		
		Step2.3	CR$_{Pd3}$	Min	Max		
				3.1	3.3		
		Step3	Generated EPSB$_{Time}$= 3.13 - 3. 3 , 3.13 - 33, 3.1 - 3.3				
		Step4	Send EPSB$_{Time}$ to Decision (D)				

In Table 4.7 below explain the EPSB$_{Time}$ the cumulative results after 13 attempt to typing active password till press login from Alice.

Table 4.7 EPSB$_{\text{Time}}$ Cumulative Results

Attempt	**Pd**		Min M1	Max M1	Min M2	Max M2	Min M3	Max M3
1	**3.3**	**TCR**	3.3	3.3	3.3	3.3	3.3	3.3
2	**3.1**	**TCR**	3.2	3.3	3.2	3.3	3.2	3.3
3	**3**	**TCR**	3.1	3.3	3.1	3.3	3.1	3.3
4	**3.4**	**TCR**	3.1	3.3	3.1	3.3	3.1	3.3
5	**3.4**	**TCR**	3.1	3.4	3.1	3.3	3	3.35
6	**3.6**	**TCR**	3.1	3.4	3.1	3.3	3	3.4
7	**3.8**	**TCR**	3.1	3.4	3.1	3.37	3	3.4
8	**3.4**	**TCR**	3.1	3.4	3.1	3.37	3	3.4
9	**3.9**	**TCR**	3.1	3.4	3.1	3.43	3	3.4
10	**3.9**	**TCR**	3.1	3.4	3.1	3.48	3	3.4
11	**3.8**	**TCR**	3.1	3.4	3.1	3.5	3	3.4
12	**4.2**	**TCR**	3.1	3.4	3.1	3.56	3	3.5
13	**3.2**	**TCR**	3.1	3.4	3.1	3.56	3	3.5
EPSB$_{\text{Time}}$			3.1	3.4	3.12	3.39	3	3.4
			CR$_{\text{Pd1}}$		**CR$_{\text{Pd2}}$**		**CR$_{\text{Pd3}}$**	

After some time,, Alice closed her public cloud to get a rest, an unauthorized person (Bob) attempt accesses to her public cloud through active password to perform actions on the corporate site, maliciously merging and changing sensitive records. Unbeknownst to the “unauthorized user,” the website is equipped with our EPSB$_{\text{Time}}$, that automatically detects deviations from normal behavior and subsequently locks her system. For the Bob, in comparison to the current EPSB$_{\text{Time}}$ to determine the extent of the similarity what extent the Alice and Bob EPSB$_{\text{Time}}$ are the same. The decision(D) component will accept and integrate the EPSB$_{\text{Time}}$ if the similarity is more than 60% or will activate the critical security procedure if the similarity is less than 60%. The Pd component will start considering the time operation from the second character of the password to obtain the closest estimated corrected range when it generates the EPSB$_{\text{Time}}$ (see Table 4.8).

Table 4.8 Process of Generate EPSB$_{\text{DTime}}$

Attempt	**1**				
Scenario	**1**	Bob started to typing active password till press login. The period of typing password=**4.3s**			
EPSB$_{\text{Time}}$				EPSB$_{\text{Style}}$	EPSB$_{\text{Error}}$
Step1	Data	4.3		Inactive	Inactive
	Record	4.3			
Step2	Analysis				
Step2.1	CR$_{\text{Pd1}}$	Min	Max		
		4.3	4.3		
Step2.2	CR$_{\text{Pd2}}$	Min	Max		
		4.3	4.3		

Step2.3	CR_{Pd3}	Min	Max			
		4.3	4.3			
Step3	Generated $EPSB_{Time}$= 4.3 -4.3 , 4.3 - 4.3, 4.3 - 4.3					
Step4	Send $EPSB_{Time}$ to Decision (D)					
	$EPSB_{D}$					
Step1	Input Data	$EPSB_{Time}$	4.3 -4.3 , 4.3 - 4.3, 4.3 - 4.3			
Step2	Records	$EPSB_{Time}$	4.3 -4.3 , 4.3 – 4.3, 4.3 - 4.3			
Step3	Compare					
	Current			Historical $EPSB_{Time}$		
Step3.1	CR_{Pd1}	Min	Max	Min	Max	Results
		4.3	4.3	3.2	4.2	Pass
Step3.2	CR_{Pd2}	Min	Max	Min	Max	
		4.3	4.3	3.4	4.034	Pass
Step3.3	CR_{Pd3}	Min	Max	Min	Max	
		4.3	4.3	3.4	3.8	Pass
Step3.4	$EPSB_{D}$	0.0%				
Step4	0.0% <60%					
Step5	Active critical process activities					
Step5.1	Verification Process					
	a) Lock Public cloud b) Send verified email to Alice					

4.3.3 Implementation $EPSB_{Error}$ and $EPSB_{Decision}$

In this section , we will show via example, how $EPSB_{Error}$ works when Alice typing wrong password in public cloud. The $EPSB_{Error}$ will monitor and track Alice if she fails to enter the password from one to three times. Hence, these components will generate a new $EPSB_{Error}$ based on analyse the error password aspects such as Number (N), Upper case (U),Lower case (l), Especial character(E), Length of password(L), Number of letters(T) and then send the results to Decision (D) component. All these characters inside the error password will be examined and then will generate a new $EPSB_{Error}$ according to these characters.

Based on scenario 2, Alice may type an inactive password either by using an old password, repeating a particular character, using another account's password, not paying attention to the enabled language, or writing the capital letters as small letters if not the other way round. In any of these cases, the main task of the EPSB algorithm is to generate an EPSB error based on the CRPe to recognize the authorized user error based on her previous errors. The EPSB error works as follows: it monitors all user actions with the wrong typing password and builds, for each user, an EPSB error, a mathematical representation of how the user typically typing the wrong password. The EPSBDError determines whether the user is deviating from expected behavior, signalling the possible presence of an unauthorized user. The purpose of EPSBError is to determine Alice when typing her error password. In such a way, the Pe component will generate a new EPSBError, as shown in Table 4.9 below:

Table 4.9 Process of Generate EPSB$_{Error}$

Attempt	**Input**	**Process**									
	Activates	EPSB$_{Error}$									
1	Alice started to typing Error password. Shy typing: **@@@1976m1976###**	**Step1**	Type	Uppercase		Type	Lowercase		Type	Number	
			Data	0		Data	1		Data	8	
			Record	0		Record	1		Record	8	
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR$_{PeU1}$	Min M1	Max M1	CR$_{PeI1}$	Min M1	Max M1	CR$_{PeN1}$	Min M1	Max M1
				0	0		1	1		8	8
		Step2.2	CR$_{PeU2}$	Min M2	Max M2	CR$_{PeI2}$	Min M2	Max M2	CR$_{PeN1}$	Min M2	Max M2
				0	0		1	1		8	8
		Step2.3	CR$_{PeU3}$	Min M3	Max M3	CR$_{PeI3}$	Min M3	Max M3	CR$_{PeN1}$	Min M3	Max m3
				0	0		1	1		8	8
		Step4	CR$_{PeU1}$ = 0.0 – 0.0, CR$_{PeU1}$ = 0.0 – 0.0 CR$_{PeU1}$ = 0.0 – 0.0			CR$_{PeI1}$ =1 – 1, CR$_{PeI1}$ =1 - 1 CR$_{PeI1}$ =1 - 1			CR$_{PeN1}$ = 8 – 8, CR$_{PeN2}$ = 8 - 8 CR$_{PeN3}$= 8 - 8		
		Step1	Type	Especial character(E)		Type	Length of password(L)		Type	Number of letters(T)	
			Data	6		Data	15		Data	1	
			Record	6		Record	15		Record	1	
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR$_{PeU1}$	Min M1	Max M1	CR$_{PeI1}$	Min M1	Max M1	CR$_{PeN1}$	Min M1	Max M1
				6	6		15	15		1	1
		Step2.2	CR$_{PeU2}$	Min M2	Max M2	CR$_{PeI2}$	Min M2	Max M2	CR$_{PeN1}$	Min M2	Max M2
				6	6		15	15		1	1
		Step2.3	CR$_{PeU3}$	Min M3	Max M3	CR$_{PeI3}$	Min M3	Max M3	CR$_{PeN1}$	Min M3	Max m3
				6	6		15	15		1	1
		Step4	CR$_{PeU1}$ = 6 – 6, CR$_{PeU1}$ = 6 – 6 CR$_{PeU1}$ = 6 – 6			CR$_{PeI1}$ =15 – 15, CR$_{PeI1}$ =15 - 15 CR$_{PeI1}$ =15 - 15			CR$_{PeN1}$ = 1 – 1, CR$_{PeN2}$ = 1 - 1 CR$_{PeN3}$= 1 - 1		
		Step 5	EPSB$_{Error}$ = 0.0 – 0.0 , 0.0 – 0.0, 0.0 - 0.0, 1-1, 1-1,1-1, 8 – 8, 8 – 8, 8 – 8, 6 – 6, 6 – 6, 6 – 6, 15 – 15, 15 – 15, 15 – 15, 1 – 1, 1 – 1, 1 - 1								
		Step 6	Send EPSB$_{Error}$ to Decision (D)								
Attempt	**Input**	**Process**									
	Activates	EPSB$_{Error}$									
2		**Step1**	Type	Uppercase		Type	Lowercase		Type	Number	

	Alice started to typing Error password. Shy typing **@@@1976M 1976##**		Data	1		Data	0		Data	8	
			Record	0	1	Record	1	0	Record	8	8
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR_{PeU1}	Min M1	Max M1	CR_{Pel1}	Min M1	Max M1	CR_{PeN1}	Min M1	Max M1
				0	0.5		0.5	1		8	8
		Step2.2	CR_{PeU2}	Min M2	Max M2	CR_{Pel2}	Min M2	Max M2	CR_{PeN1}	Min M2	Max M2
				0	0.5		0.5	1		8	8
		Step2.3	CR_{PeU3}	Min M3	Max M3	CR_{Pel3}	Min M3	Max M3	CR_{PeN1}	Min M3	Max m3
				0	0.5		0.5	1		8	8
		Step4	CR_{PeU1} = 0.0 – 0.5, CR_{PeU1} = 0.0 – 0.5, CR_{PeU1} = 0.0 – 0.5			CR_{Pel1} =0.5 – 1, CR_{Pel1} =0.5 – 1 , CR_{Pel1} = 0.5 - 1			CR_{PeN1} = 8 – 8, CR_{PeN2} = 8 - 8 CR_{PeN3}= 8 - 8		
		Step1	Type	Especial character(E)		Type	Length of password(L)		Type	Number of letters(T)	
			Data	5		Data	15		Data	1	
			Record	6	5	Record	15	14	Record	1	1
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR_{PeU1}	Min, M1	Max M1	CR_{Pel1}	Min M1	Max M1	CR_{PeN1}	Min M1	Max M1
				5.5	6		14.5	15		1	1
		Step2.2	CR_{PeU2}	Min, M2	Max M2	CR_{Pel2}	Min M2	Max M2	CR_{PeN1}	Min M2	Max M2
				5.5	6		14.5	15		1	1
		Step2.3	CR_{PeU3}	Min, M3	Max M3	CR_{Pel3}	Min M3	Max M3	CR_{PeN1}	Min M3	Max m3
				5.5	6		14.5	15		1	1
		Step4	CR_{PeU1} = 5.5 – 6, CR_{PeU1} = 5.5 – 6, CR_{PeU1} = 5.5 – 6			CR_{Pel1} =14.5 – 15, CR_{Pel1} =14.5 – 15, CR_{Pel1} =15 - 15			CR_{PeN1} = 1 – 1, CR_{PeN2} = 1 - 1 CR_{PeN3}= 1 - 1		
		Step 5	$EPSB_{Error}$ = 0.0 – 0.5 , 0.0 – 0.5, 0.0 - 0.5, 0.5-1, 0.5 - 1,0.5 - 1, 8 – 8, 8 – 8, 8 – 8, 5.5 – 6, 5.5 – 6, 5.5 – 6, 14.5 – 15, 14.5 – 15, 14.5 – 15, 1 – 1, 1 – 1, 1 - 1								
		Step 6	Send $EPSB_{Error}$ to Decision (D)								

In Table 4.10 below explain the $EPSB_{Error}$ the cumulative results after 5 attempt to typing active password till press login from Alice.

Table 4.10 $EPSB_{Error}$ Cumulative Results

Attempt	**TCR**	**Upper case**	**Min M1**	**Max M1**	**Min M2**	**Max M2**	**Min M3**	**Maxi M3**
@@@1976m1976###	**TCR**	0	0	0	0	0	0	0
@@@1976M197###	**TCR**	1	0	1	0	0.5	0	0.5
@@@1976M1976##	**TCR**	1	0	1	0	0.7	0	1
@@1976M1976###	**TCR**	1	0	1	0	0.75	0	1
@@@1976m1967###	**TCR**	0	0	1	0	0.6	0	1
If min Rounded into min values **If max Rounded into max values**			**0**	**1**	**0**	**0.6**	**0**	**1**
		L. case	**CR_{PeU1}**		**CR_{PeU2}**		**CR_{PeU3}**	
@@@1976m1976###	**TCR**	1	1	1	1	1	1	1
@@@1976M197###	**TCR**	0	0	1	0.5	1	0.5	1
@@@1976M1976##	**TCR**	0	0	1	0.33	1	0	1
@@1976M1976###	**TCR**	0	0	1	0.25	1	0	1
@@@1976m1967###	**TCR**	1	0	1	0.25	1	0	1
If min Rounded into min values			**0**	**1**	**0.25**	**1**	**0**	**1**

If max Rounded into max values								
		Number	**CR$_{Pel1}$**		**CR$_{Pel2}$**		**CR$_{Ple3}$**	
@@@1976m1976###	**TCR**	8	8	8	8	8	8	8
@@@1976M197###	**TCR**	7	7	8	7.5	8	7.5	8
@@@1976M1976##	**TCR**	8	7	8	7.5	8	7	8
@@1976M1976###	**TCR**	8	7	8	7.5	8	7	8
@@@1976m1967###	**TCR**	8	7	8	7.5	8	7	8
If min Rounded into min values **If max Rounded into max values**			**7**	**8**	**7.5**	**8**	**7**	**8**
		Length	**CR$_{PeN1}$**		**CR$_{PeN2}$**		**CR$_{PeN3}$**	
@@@1976m1976###	**TCR**	15	15	15	15	15	15	15
@@@1976M197###	**TCR**	14	14	15	14.5	15	14.5	15
@@@1976M1976##	**TCR**	14	14	15	14.3	15	14	15
@@1976M1976###	**TCR**	14	14	15	14.25	15	14	15
@@@1976m1967###	**TCR**	15	14	15	14.25	15	14	15
			14	**15**	**14.25**	**15**	**14**	**15**
		Symbols	**CR$_{PeL1}$**		**CR$_{PeL2}$**		**CR$_{PeL3}$**	
@@@1976m1976###	**TCR**	6	6	6	6	6	6	6
@@@1976M197###	**TCR**	6	6	6	6	6	6	6
@@@1976M1976##	**TCR**	5	5	6	5.6	6	6	6
@@1976M1976###	**TCR**	5	5	6	5.5	6	5.5	6
@@@1976m1967###	**TCR**	6	5	6	5.5	6	5.5	6
			5	**6**	**5.5**	**6**	**5.5**	**6**
		T. Letter	**CR$_{PeE1}$**		**CR$_{PeE2}$**		**CR$_{PeE3}$**	
@@@1976m1976###	**TCR**	1	1	1	1	1	1	1
@@@1976M197###	**TCR**	1	1	1	1	1	1	1
@@@1976M1976##	**TCR**	1	1	1	1	1	1	1
@@1976M1976###	**TCR**	1	1	1	1	1	1	1
@@@1976m1967###	**TCR**	1	1	1	1	1	1	1
			1	**1**	**1**	**1**	**1**	**1**
			CR$_{PeT1}$		**CR$_{PeT2}$**		**CR$_{PeT3}$**	

As she closed her public cloud, an unauthorized person (Bob) attempt to accesses to her public cloud through guessing active password , he chose ***Alice88#@*** as a password. All these characters inside the error password will be examined and then will generate a new EPSB$_{Error}$ according to these characters. This newly generated EPSB$_{Error}$ will be compared with the Historical EPSB$_{Error}$. The EPSB$_{Decision(D)}$ component will accept and integrate the EPSB$_{Error}$ if the similarity is more than 60% or will activate the critical security procedure if the similarity is less than 60%. The EPSB$_{DError}$ will start considering the time operation from the second character of the password to obtain the closest estimated corrected range when it generates the EPSB$_{Error}$ according to the Table 4.11 below.

Table 4.11 Process of Generate $EPSB_{DError}$

Attempt	Input	Process						
	Activates	$EPSB_{Error}$						
1	Bob started to gussing active password till press login. The typing password= **Alice88#@**	**Step1**	Type	Uppercase	Type	Lowercase	Type	Number
			Data	1	Data	4	Data	2
			Record	1	Record	4	Record	2
		Step2	Analysis		Analysis		Analysis	
		Step2.1	CR_{PeU1}	Result 1	CR_{Pel1}	Result 4	CR_{PeN1}	Result 7
				1		4		2
		Step2.2	CR_{PeU2}	Result 2	CR_{Pel2}	Result 5	CR_{PeN1}	Result 8
				1		4		2
		Step2.3	CR_{PeU3}	Result 3	CR_{Pel3}	Result 6	CR_{PeN1}	Result 9
				1		4		2
		Step4	CR_{PeU1} = 1, CR_{PeU1} =1 CR_{PeU1} = 1		CR_{Pel1} =4, CR_{Pel1} =4 CR_{Pel1} =4		CR_{PeN1} =2 , CR_{PeN2} = 2 CR_{PeN3}= 2	
		Step1	Type	Especial character(E)	Type	Length of password(L)	Type	Number of letters(T)
			Data	2	Data	9	Data	5
			Record	2	Record	9	Record	5
		Step2	Analysis		Analysis		Analysis	
		Step2.1	CR_{PeE1}	Result 10	CR_{PeL1}	Result 13	CR_{PeT1}	Result 16
				2		9		5
		Step2.2	CR_{PeE2}	Result 11	CR_{PeL2}	Result 14	CR_{PeT1}	Result 17
				2		9		5
		Step2.3	CR_{PeE3}	Result 12	CR_{PeL3}	Result 15	CR_{PeT1}	Result 18
				2		9		5
		Step4	CR_{PeU1} = 2, CR_{PeU1} =2 CR_{PeU1} = 2		CR_{Pel1} =9, CR_{Pel1} =9 CR_{Pel1} =9		CR_{PeN1} = 5, CR_{PeN2} = 5 , CR_{PeN3}= 5	
		Step 5	$EPSB_{Error}$ = 1 , 1 , 1 , 4, 4, 4, 2, 2, 2, 2, 2, 2, 9, 9, 9, 5, 5, 5					
$EPSB_D$								
Step1	Input Data	$EPSB_{Error}$	1 , 1 , 1 , 4, 4, 4, 2, 2, 2, 2, 2, 2, 9, 9, 9, 5, 5, 5					
Step2	Recods	$EPSB_{recods}$	1 , 1 , 1 , 4, 4, 4, 2, 2, 2, 2, 2, 2, 9, 9, 9, 5, 5, 5					
Step3	Compare							
	Current		Historical $EPSB_{Error}$					
Step3.1	CR_{PeU1}	Result 1	Min M1	Max M1	Similarity			
		1	0	1	Fail			
Step3.2	CR_{PeU2}	Result 2	Min M2	Max M2				
		1	0	0.6	Pass			
Step3.3	CR_{PeU3}	Result 3	Min M3	Max M3				
		1	0	1	Fail			
Step3.3	CR_{Pel1}	Result 4	Min M1	Max M1				
		4	0	1	Pass			
Step3.3	CR_{Pel2}	Result 5	Min M2	Max M2				
		4	0.25	1	Pass			
Step3.3	CR_{Pel3}	Result 6	Min M3	Max M3				

		4	0	1	Pass
Step3.3	CR_{PeN1}	Result 7	Min M1	Max M1	
		2	7	8	Pass
Step3.3	CR_{PeN1}	Result 8	Min M2	Max M2	
		2	7.5	8	Pass
Step3.3	CR_{PeN1}	Result 9	Min M3	Max M3	
		2	7	8	Pass
Step3.3	CR_{PeE1}	Result 10	Min M1	Max M1	
		2	5	6	Pass
Step3.3	CR_{PeE2}	Result 11	Min M2	Max M2	
		2	5.5	6	Pass
Step3.3	CR_{PeE3}	Result 12	Min M3	Max M3	
		2	5.5	6	Pass
Step3.3	CR_{PeL1}	Result 13	Min M1	Max M1	
		9	14	15	Pass
Step3.3	CR_{PeL2}	Result 14	Min M2	Max M2	
		9	14.5	15	Pass
Step3.3	CR_{PeL3}	Result 15	Min M3	Max M3	
		9	14	15	Pass
Step3.3	CR_{PeT1}	Result 16	Min M1	Max M1	
		5	1	1	Pass
Step3.3	CR_{PeT1}	Result 17	Min M2	Max M2	
		5	1	1	Pass
Step3.3	CR_{PeT1}	Result 18	Min M3	Max M3	
		5	1	1	Pass
Step3.4	EPSB_{D}	11.11%			
Step4	11.11 % < 60 %				
Step5	Active critical process activities				
Step5.1	Verification Process				
	a) Lock Public cloud b) Send verified email to Alice				

4.3.4 Implementation $\text{EPSB}_{\text{Style}}$ and $\text{EPSB}_{\text{Decision}}$

In this section, we will show via example, how $\text{EPSB}_{\text{Style}}$ works when Alice chose her password in public cloud. The PS component is activated only when the user changes the password for preventing any suspicious password change. The $\text{EPSB}_{\text{Style}}$ will monitor and track Alice behavior when she selects her password. The PS component will generate the $\text{EPSB}_{\text{Style}}$ based on analyse the password aspects such as Number (N), Upper case (U),Lower case (l), Especial character(E), Length of password(L), Number of letters(T) and then send the results to Decision (D) component. All these characters inside the password will be examined and then will generate a new $EPSB_{Style}$ according to these characters.

Based on scenario 3, Alice has been chosen her password when she registered as an authorized user in her company. During three months, she has been changed her password many times. The $EPSB_{Stley}$ works as follows: It monitors all user actions with the style of password and builds, for each user, an $EPSB_{syle}$, a mathematical representation of how the user typically chosen his/her password. The final results will be send to $EPSB_{DStley}$ for the next process. The $EPSB_{DStley}$ determines, whether the user is deviating from expected behavior, signalling the possible presence of an unauthorized user. Because this instance of $EPSB_{Style}$ is based solely on analysis of password structure by using confidence range (CR_{PS}) as shown in the Table 4.12 below.

Table 4.12 Process of Generate $EPSB_{Style}$

Attempt	**Input**	**Process**									
	Activates	$EPSB_{Style}$									
1	Alice has been chosen her password. Password = **@@@1976 M1976###**	**Step1**	Type	Uppercase		Type	Lowercase		Type	Number	
			Data	1		Data	0		Data	8	
			Record	1		Record	0		Record	8	
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR_{PSU1}	Min M1	Max M1	CR_{PSI1}	Min M1	Max M1	CR_{PSN1}	Min M1	Max M1
				1	1		0	0		8	8
		Step2.2	CR_{PSU2}	Min M2	Max M2	CR_{PSI2}	Min M2	Max M2	CR_{PSN1}	Min M2	Max M2
				1	1		0	0		8	8
		Step2.3	CR_{PSU3}	Min M3	Max M3	CR_{PSI3}	Min M3	Max M3	CR_{PSN1}	Min M3	Max m3
				1	1		0	0		8	8
		Step4	CR_{PSU1} = 1 – 1, CR_{PSU1} = 1 – 1 CR_{PSU1} = 1 – 1			CR_{PSI1} =0 – 0, CR_{PSI1} =0 - 0 CR_{PSI1} =0 - 0			CR_{PSN1} = 8 – 8, CR_{PSN2} = 8 - 8 CR_{PSN3}= 8 - 8		
		Step1	Type	Especial character(E)		Type	Length of password(L)		Type	Number of letters(T)	
			Data	6		Data	15		Data	1	
			Record	6		Record	15		Record	1	
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR_{PSU1}	Min M1	Max M1	CR_{PSI1}	Min M1	Max M1	CR_{PSN1}	Min M1	Max M1
				6	6		15	15		1	1
		Step2.2	CR_{PSU2}	Min M2	Max M2	CR_{PSI2}	Min M2	Max M2	CR_{PSN1}	Min M2	Max M2
				6	6		15	15		1	1
		Step2.3	CR_{PSU3}	Min M3	Max M3	CR_{PSI3}	Min M3	Max M3	CR_{PSN1}	Min M3	Max m3
				6	6		15	15		1	1
		Step4	CR_{PSU1} = 6 – 6, CR_{PSU1} = 6 – 6 CR_{PSU1} = 6 – 6			CR_{PSI1} =15 – 15, CR_{PSI1} =15 - 15 CR_{PSI1} =15 - 15			CR_{PSN1} = 1 – 1, CR_{PSN2} = 1 - 1 CR_{PSN3}= 1 - 1		

		Step 5	$EPSB_{Style}$ = 1 – 1, 1 – 1, 1 - 1, 0 – 0, 0 – 0,0 – 0, 8 – 8, 8 – 8, 8 – 8, 6 – 6, 6 – 6, 6 – 6, 15 – 15, 15 – 15, 15 – 15, 1 – 1, 1 – 1, 1 - 1								
		Step 6	Send $EPSB_{Style}$ to Decision (D)								
Attempt	**Input**	**Process**									
	Activates	$EPSB_{style}$									
2	Alice has been changed her password. Password = **1976m1976###**	**Step1**	Type	Uppercase		Type	Lowercase		Type	Number	
			Data	0		Data	1		Data	8	
			Record	1	0	Record	0	1	Record	8	8
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR_{PSU1}	Min M1	Max M1	CR_{PSl1}	Min M1	Max M1	CR_{PSN1}	Min M1	Max M1
				0.5	1		0	0.5		8	8
		Step2.2	CR_{PSU2}	Min M2	Max M2	CR_{PSl2}	Min M2	Max M2	CR_{PSN1}	Min M2	Max M2
				0.5	1		0	0.5		8	8
		Step2.3	CR_{PSU3}	Min M3	Max M3	CR_{PSl3}	Min M3	Max M3	CR_{PSN1}	Min M3	Max m3
				0.5	1		0	0.5		8	8
		Step4	CR_{PSU1} = 0.5 – 1, CR_{PSU1} = 0.5 – 1, CR_{PSU1} = 0.5 – 1			CR_{PSl1} =0 – 0.5, CR_{PSl1} =0 – 0.5 , CR_{PSl1} = 0 - 0.5			CR_{PSN1} = 8 – 8, CR_{PSN2} = 8 - 8 CR_{PSN3}= 8 - 8		
		Step1	Type	Especial character(E)		Type	Length of password(L)		Type	Number of letters(T)	
			Data	3		Data	15		Data	1	
			Record	6	3	Record	15	12	Record	1	1
		Step2	Analysis			Analysis			Analysis		
		Step2.1	CR_{PSU1}	Min, M1	Max M1	CR_{PSl1}	Min M1	Max M1	CR_{PSN1}	Min M1	Max M1
				4.5	6		13.5	15		1	1
		Step2.2	CR_{PSU2}	Min, M2	Max M2	CR_{PSl2}	Min M2	Max M2	CR_{PSN1}	Min M2	Max M2
				4.5	6		13.5	15		1	1
		Step2.3	CR_{PSU3}	Min, M3	Max M3	CR_{PSl3}	Min M3	Max M3	CR_{PSN1}	Min M3	Max m3
				4.5	6		13.5	15		1	1
		Step4	CR_{PSU1} = 4.5 – 6, CR_{PSU1} = 4.5 – 6, CR_{PSU1} = 4.5 – 6			CR_{PSl1} =13.5 – 15, CR_{PSl1} =13.5 – 15, CR_{PSl1} =13.5 - 15			CR_{PSN1} = 1 – 1, CR_{PSN2} = 1 - 1 CR_{PSN3}= 1 - 1		
		Step 5	$EPSB_{Style}$ = 0.0 – 0.5 , 0.0 – 0.5, 0.0 - 0.5, 0.5-1, 0.5 - 1,0.5 - 1, 8 – 8, 8 – 8, 8 – 8, 5.5 – 6, 5.5 – 6, 5.5 – 6, 14.5 – 15, 14.5 – 15, 14.5 – 15, 1 – 1, 1 – 1, 1 - 1								
		Step 6	Send $EPSB_{Style}$ to Decision (D)								

In Table 4.13 below explain the $EPSB_{style}$ the cumulative results after 5 attempt to change her password from Alice.

Table 4.13 $EPSB_{style}$ Cumulative Results

Attempt	**TCR**	**Upper case**	**Min M1**	**Max M1**	**Min M2**	**Max M2**	**Min M3**	**Max M3**
@@@1976M1976###	**TCR**	1	1	1	1	1	1	1
1976m1976###	**TCR**	0	0	1	0	1	0.5	1
7905781614mOH@	**TCR**	2	0	2	0	1.5	0.5	1
M1976@1976moh	**TCR**	1	0	2	0	1.5	0.5	1
Lkikh1##1976	**TCR**	1	0	2	0	1.5	0.5	1
If min Rounded into min values **If max Rounded into max values**			**0**	**2**	**0**	**2**	**0**	**1**
		L. case	**CR_{PSU1}**		**CR_{PSU2}**		**CR_{PSU3}**	
@@@1976M1976###	**TCR**	0	0	0	0	0	0	0
1976m1976###	**TCR**	1	0	1	0	0.5	0	0.5
7905781614mOH@	**TCR**	1	0	1	0	0.75	0	1
M1976@1976moh	**TCR**	3	0	3	0	1.875	0	1
Lkikh1##1976	**TCR**	4	0	4	0	2.94	0	1
If min Rounded into min values **If max Rounded into max values**			**0**	**4**	**0**	**3**	**0**	**1**
		Number	**CR_{PSl1}**		**CR_{PSl2}**		**CR_{PSl3}**	
@@@1976M1976###	**TCR**	8	8	8	8	8	8	8
1976m1976###	**TCR**	8	8	8	8	8	8	8
7905781614mOH@	**TCR**	10	8	10	8	9	8	8
M1976@1976moh	**TCR**	8	8	10	8	9	8	9
Lkikh1##1976	**TCR**	5	5	10	7	9	8	9
If min Rounded into min values **If max Rounded into max values**			**5**	**10**	**7**	**9**	**8**	**9**
		Length	**CR_{PSN1}**		**CR_{PSN2}**		**CR_{PSN3}**	
@@@1976M1976###	**TCR**	15	15	15	15	15	15	15
1976m1976###	**TCR**	12	12	15	13.5	15	13.5	15
7905781614mOH@	**TCR**	14	12	15	13.5	15	13.5	15
M1976@1976moh	**TCR**	13	12	15	13.4	15	13.5	15
Lkikh1##1976	**TCR**	12	12	15	12.7	15	13	15
			12	**15**	**12**	**15**	**13**	**15**
		Symbols	**CR_{PSL1}**		**CR_{PSL2}**		**CR_{PSL3}**	
@@@1976M1976###	**TCR**	6	6	6	6	6	6	6
1976m1976###	**TCR**	3	3	6	4.5	6	4.5	6
7905781614mOH@	**TCR**	1	1	6	3.33	6	3	6
M1976@1976moh	**TCR**	1	1	6	2.75	6	2	6
Lkikh1##1976	**TCR**	2	1	6	2.6	6	2	6
			1	**6**	**2**	**6**	**2**	**6**
		T. Letter	**CR_{PSE1}**		**CR_{PSE2}**		**CR_{PSE3}**	
@@@1976M1976###	**TCR**	1	1	1	1	1	1	1
1976m1976###	**TCR**	1	1	1	1	1	1	1
7905781614mOH@	**TCR**	3	1	3	1	1.7	1	1
M1976@1976moh	**TCR**	3	1	3	1	2	1	2
Lkikh1##1976	**TCR**	5	1	5	1	2.6	1	3
			1	**5**	**1**	**3**	**1**	**3**
			CR_{PST1}		**CR_{PST2}**		**CR_{PST3}**	

Alice steps away from her laptop to get a refill of coffee, an unauthorized person(Bob) accesses her laptop to change her system password for control on it. Bob has a current active password through stolen password attack. Unbeknownst to the "unauthorized user,” the website is equipped with our $EPSB_{Style}$, that automatically detects deviations from normal behavior and subsequently locks her public cloud. All these characters inside password will be examined and then will generate a new $EPSB_{Style}$ according to these characters. This newly generated $EPSB_{Style}$ will be compared with the Historical $EPSB_{Style}$. The $EPSB_{Decision(D)}$ component will accept and integrate the $EPSB_{DStyle}$ if the similarity is more than 60% or will activate the critical security procedure if the similarity is less than 60%. The $EPSB_{Style}$ will start considering the time operation from the second character of the password to obtain the closest estimated corrected range when it generates the $EPSB_{Style}$ according to the Table 4.14 below.

Table 4.14 Process of Generate $EPSB_{DStyle}$

Attempt	**Input**	**Process**						
	Activates	$EPSB_{Style}$						
1	Bob started to change active password. The chose password= **BobBob123@**	**Step1**	Type	Uppercase	Type	Lowercase	Type	Number
			Data	2	Data	4	Data	3
			Record	2	Record	4	Record	3
		Step2	Analysis		Analysis		Analysis	
		Step2.1	CR_{PSU1}	Result 1	CR_{PSl1}	Result 4	CR_{PSN1}	Result 7
				2		4		3
		Step2.2	CR_{PSU2}	Result 2	CR_{PSl2}	Result 5	CR_{PSN1}	Result 8
				2		4		3
		Step2.3	CR_{PSU3}	Result 3	CR_{PSl3}	Result 6	CR_{PSN1}	Result 9
				2		4		3
		Step4	CR_{PSU1} = 2, CR_{PSU1} =2 CR_{PSU1} = 2		CR_{PSl1} =4, CR_{PSl1} =4 CR_{PSl1} =4		CR_{PSN1} =3,CR_{PSN2} = 3 CR_{PSN3}= 3	
		Step1	Type	Especial character(E)	Type	Length of password(L)	Type	Number of letters(T)
			Data	1	Data	10	Data	3
			Record	1	Record	10	Record	3
		Step2	Analysis		Analysis		Analysis	
		Step2.1	CR_{PSE1}	Result 10	CR_{PSL1}	Result 13	CR_{PST1}	Result 16
				1		10		3
		Step2.2	CR_{PSE2}	Result 11	CR_{PSL2}	Result 14	CR_{PST1}	Result 17
				1		10		3
		Step2.3	CR_{PSE3}	Result 12	CR_{PSL3}	Result 15	CR_{PST1}	Result 18
				1		10		3
		Step4	CR_{PSU1} = 1, CR_{PSU1} =1 CR_{PSU1} = 1		CR_{PSl1} =10, CR_{PSl1} =10 CR_{PSl1} =10		CR_{PSN1} = 3, CR_{PSN2} = 3 , CR_{PSN3}= 3	
		Step 5	$EPSB_{Style}$ = 2 , 2 , 2, 4, 4, 4, 3, 3, 3, 1, 1, 1, 10, 10, 10, 3, 3, 3					
$EPSB_D$								

Step1	Input Data	EPSB$_{Style}$	2 , 2 , 2, 4, 4, 4, 3, 3, 3, 1, 1, 1, 10, 10, 10, 3, 3, 3		
Step2	Recods	EPSB$_{recods}$	2 , 2 , 2, 4, 4, 4, 3, 3, 3, 1, 1, 1, 10, 10, 10, 3, 3, 3		
Step3	Compare				
	Current		Historical EPSB$_{Style}$		
Step3.1	CR$_{PSU1}$	Result 1	Min M1	Max M1	Similarity
		2	0	2	Fail
Step3.2	CR$_{PSU2}$	Result 2	Min M2	Max M2	
		2	0	2	Fail
Step3.3	CR$_{PSU3}$	Result 3	Min M3	Max M3	
		2	0	1	Pass
Step3.3	CR$_{PSI1}$	Result 4	Min M1	Max M1	
		4	0	4	Fail
Step3.3	CR$_{PSI2}$	Result 5	Min M2	Max M2	
		4	0	3	Pass
Step3.3	CR$_{PSI3}$	Result 6	Min M3	Max M3	
		4	0	1	Pass
Step3.3	CR$_{PSN1}$	Result 7	Min M1	Max M1	
		3	5	10	Pass
Step3.3	CR$_{PSN1}$	Result 8	Min M2	Max M2	
		3	7	9	Pass
Step3.3	CR$_{PSN1}$	Result 9	Min M3	Max M3	
		3	8	9	Pass
Step3.3	CR$_{PSE1}$	Result 10	Min M1	Max M1	
		1	1	6	Fail
Step3.3	CR$_{PSE2}$	Result 11	Min M2	Max M2	
		1	2	6	Pass
Step3.3	CR$_{PSE3}$	Result 12	Min M3	Max M3	
		1	2	6	Pass
Step3.3	CR$_{PSL1}$	Result 13	Min M1	Max M1	
		10	12	15	Pass
Step3.3	CR$_{PSL2}$	Result 14	Min M2	Max M2	
		10	12	15	Pass
Step3.3	CR$_{PSL3}$	Result 15	Min M3	Max M3	
		10	13	15	Pass
Step3.3	CR$_{PST1}$	Result 16	Min M1	Max M1	
		3	1	5	Fail
Step3.3	CR$_{PST1}$	Result 17	Min M2	Max M2	
		3	1	3	Fail
Step3.3	CR$_{PST1}$	Result 18	Min M3	Max M3	
		3	1	3	Fail
Step3.4	EPSB$_{D}$	11.11%			
Step4	38.88 % < 60 %				
Step5	Active critical process activities				
Step5.1	Verification Process				
	a) Lock Public cloud b) Send verified email to Alice				

4.4 Chapter Summary

Authentication is considered a core layer in public cloud computing. The password is one of the most significant mechanisms in authentication, which works to diagnose the authorized user from others. Performance enhancement in authentication is considered one of the important tasks through adopting an algorithm, as proposed here in this chapter. The suggested algorithm is called Electronic Personal Synthesis Behavior (EPSB). However, the current authentication schemes commonly use mechanisms that face many problems, such as stolen password attacks. Such the unauthorized user would be able to access data and change the active password which in turn causes a significant loss in efforts and cost.

Similarly, a hacker who does not have a password also attempts to penetrate the system by predicting a set of words. Both authorized users and hackers input a wrong password. However, authorized users may have only one or two wrong characters in the password whereas hackers input a completely wrong password. Thus, adopting an algorithm under the name of Electronic Personal Synthesis Behavior (EPSB) is crucial. The first main task of this algorithm is monitoring all the activities associated with password duration, Time , Error, and Style for the authorized user in order to recognize any suspicious activity. The second basic task is generating an $EPSB_{Time,Error,Style}$ for the authorized user by the application of the $EPSB_{algorithm}$ in the authentication layer for recognizing any suspicious activity. A whole system may be damaged if the unauthorized or non-privileged user attempts to enter a system either directly or through websites. The current study suggests an algorithm to improve the performance of the authentication layer through improving the accuracy of determining on the authorized user according to the many parameters adopted that are related to the behavior of the authorized user. The created blocks protect data and prevent suspicious users from logging into the entire data.

.

CHAPTER 5

EVALUATION

5.1 EPSB$_{algorithm}$ Evaluation

In this chapter, the evaluation criteria conducted according to security, accuracy, acceptance and use. In this chapter, we will present the work outcome and effects, which are made possible by the proposed algorithm with many experiments performed. The first part is the experimental results, which show the improvement made by the proposed algorithm on the accuracy in authenticating an authorized user and acceptance and use. The second part of this chapter provides a statistical study to check the validity of the proposed approach. The third features comparison between before and after adopting the proposed algorithm on the authentication accuracy when facing stolen password attacks on the public cloud field.

This chapter contains four sections. This section is the introduction of the chapter. The second section is the EPSB algorithm results analysis that explains the EPSB experiment to examine the accuracy of authenticating an authorized user. Section 5.3 discusses the results and analysis of the examination on the acceptance and the use of EPSB. Technology Acceptance Model (TAM), one of the information system theories developed by Davis in 1989[167], was used for assessing EPSB acceptance and use level. The comparison focuses on the accuracy of authenticating an authorized user, cost, intelligent authentication, and the presence of human factors, as enhancing authentication accuracy is considered the main objective of this thesis, as is seen in the literature.

5.2 EPSB Algorithm Results Analysis

This section evaluates the EPSB results. The evaluation criteria were conducted according to the algorithm’s accuracy, acceptance and use. In the first part, the results on the accuracy of authenticating an authorized user in the proposed algorithm are presented. Results are valid when the algorithm worked as expected through testing across a range of assumptions inputs. All assumptions are built and constructed according to two inputs; the first one is the authorized user, and the second one is unauthorized user behavior with stolen password attacks. Normally, the unauthorized user of the stolen password tries to log in as an authorized user and changes the password to dominate the system authority.

On the other hand, authorized user sometimes tries logging in using an old password, repeating a particular character, using another account's password, not paying attention to the enabled language, or writing the capital letters as small letters and vice versa.

The sample users divided into three groups in which each one has four users[158] [181]. This layer implemented on 12 students from IT, English, Law, and Business departments, at Al-Buraimi University College, Oman for ten working days from 17th to 29th of July 2016. A heterogeneous sample was selected, such as four females and eight male. In a related context, three whose first language is Arabic, nine bilinguals (Arabic, English), three who have high computer skills proficiency, six who have intermediate computer skills proficiency, and three who have basic computer skills proficiency.

5.2.1 EPSB Accuracy Test - Results and Analysis

This section presents the results and analysis of the $\text{EPSB}_{\text{Time}}$ accuracy test. Users selected their passwords in authentication pre and post Electronic personal synthesis behavior ($\text{EPSB}_{\text{Time}}$), signed in and out. They used the authentication layer for login public cloud for ten (10) days, at least one hour per day. The period that students used the $\text{EPSB}_{\text{algorrithm}}$ was at least one hour per day[181][161].

During the last day, users substituted, as each user had used another user's password to check the algorithm's ability in authenticating the right user according to the below security assumptions:

a) Assumptions 1:

Unauthorized user logs in to the authentication layer through an authorized password, network, and device on the first attempt.

Authorized password: Available.

Descriptions: The Unauthorized user has active password through a stolen password and Impersonations attacks.

The description of the first experiments with $\text{EPSB}_{\text{Time}}$ according to test idea framework as shown as in table 5.1 below[182].

Table 5.1 Assumptions 1 Test Idea Framework

<table>
<tr><th>Phases</th><th colspan="2">Questions</th><th colspan="7">Answers</th></tr>
<tr><td>1.</td><td colspan="2"><b>What problems are we trying to solve?</b></td><td colspan="7">1. Authentication in public cloud computing dealing with Stolen password attacks;
2. Previous studies of the authentication framework in public cloud computing have not applied intelligent authentication operations;
3. Previous studies of the authentication framework in public cloud computing have not dealt with learning mechanisms for user behavior recognition in the password as a matching factor with the password.</td></tr>
<tr><td>2.</td><td colspan="2"><b>Top metric</b></td><td colspan="7"><b>Pass:</b> Diagnosis and Prevent Unauthorized user<b>;</b>
<b>Fail:</b> Unauthorized user access into the public cloud<b>.</b></td></tr>
<tr><td>3.</td><td colspan="2"><b>Test location</b></td><td colspan="7">Alburaimi university College, Oman</td></tr>
<tr><td>4.</td><td colspan="2"><b>Number of Samples</b></td><td colspan="7">12 users</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"><b>4.1</b></td><td rowspan="2"><b>Samples description</b></td><td><b>Male</b></td><td><b>Female</b></td><td><b>One language</b></td><td><b>Two languages</b></td><td><b>High computer skills</b></td><td><b>intermediate computer skills</b></td><td><b>Basic computer skills</b></td></tr>
<tr><td>8</td><td>4</td><td>3</td><td>9</td><td>3</td><td>6</td><td>3</td></tr>
<tr><td>5.</td><td colspan="2"><b>Proposed change</b></td><td colspan="7">Analysis human behavior in the authentication process</td></tr>
<tr><td>6.</td><td colspan="2"><b>Hypothesis</b></td><td colspan="7">Applying behavior recognition in the authentication process in public cloud computing lead to mitigating stolen password effects.</td></tr>
<tr><td>7.</td><td colspan="2"><b>Secondary metrics</b></td><td colspan="7">Data security level</td></tr>
<tr><td>8.</td><td colspan="2"><b>Targeting</b></td><td colspan="7">Prevent unauthorized user to log in public cloud computing with an active password</td></tr>
<tr><td>9.</td><td colspan="2"><b>Duration</b></td><td colspan="7">Ten days</td></tr>
<tr><td>10.</td><td colspan="2"><b>Ideal results</b></td><td colspan="7">Diagnose all unauthorized user for improving the accuracy of user authentication</td></tr>
</table>

Without adopting EPSB$_{\text{Time}}$ in authentication layer in the public cloud, all unauthorized users logged in public cloud computing directly and deal with data that saved in the public cloud. The accuracy determined according to the formula below[180]:

$$\boldsymbol{Accuracy\ Rate} = \frac{\boldsymbol{pass\ attempts}}{\boldsymbol{total\ attempts}} * \mathbf{100} \qquad \text{…. } \textit{Equation (5.1)}$$

$$\boldsymbol{Pre\ Accuracy\ Rate}\ = \frac{\mathbf{0}}{\mathbf{12}} * \mathbf{100} = \mathbf{00\%}$$

When the authentication layer is adopted the EPSB$_{\text{Time}}$, that automatically detects deviations from normal behavior and subsequently prevent the unauthorized user from login public cloud. The Pd task is to generate an EPSB$_{\text{Time}}$ based on the CR$_{\text{Pd}}$ for any user. The EPSB$_{\text{Time}}$ works as follows: It monitors all user actions with a password and builds, for each user, an EPSB$_{\text{Time}}$, a mathematical representation of how the user typically interacts with the password. The results are shown in Table 5.2 below:

Table 5.2 the EPSB$_{DTime}$ Results

Current users	EPSB$_{Time}$ Current user	EPSB$_{DTime}$ Authorized user range	Decision
1	3.45	3.12 - 4.55	Fail
2	5.46	3.23 - 4.35	Pass
3	6.35	2.55 – 4.2	Pass
4	4.19	3.56 - 5.4	Fail
5	7.13	4.32 – 5.42	Pass
6	6.17	4.2 – 5.13	Pass
7	5.56	4.35 – 5.47	Pass
8	4.12	3.11 – 5.1	Fail
9	6.15	4.27 – 5.30	Pass
10	5.55	3.54 – 4.6	Pass
11	5.34	4.3 – 6.2	Fail
12	6.38	3.5 1– 5.43	Pass

According to the above table, The authentication process in public cloud computing determined 8 unauthorized users out of 12 password entries. In this test, the EPSB$_{Time}$ prevent 66.66% from unauthorized users to login in the public cloud, although they have an active password. Thus, they could consider as accepted results.

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{8}}{\mathbf{12}} * \ \mathbf{100} = \mathbf{66.6\%}$$

b) Assumptions 2:

Unauthorized user tries to change the authorized password in the authentication layer.

Authorized password: Available.

Descriptions: The Unauthorized user has active password through a stolen password and Impersonations attacks.

The description of the second experiments with EPSB$_{Style}$ is following the test idea framework in Table 5.3 below[182].

Table 5.3 Assumptions 2 Test Idea Framework

<table>
<tr><th>Phases</th><th>Questions</th><th colspan="7">Answers</th></tr>
<tr><td>1.</td><td><b>What problems are we trying to solve?</b></td><td colspan="7">1. Authentication in public cloud computing dealing with Stolen password attacks;
2. Previous studies of the authentication framework in public cloud computing have not applied intelligent authentication operations;
3. Previous studies of the authentication framework in public cloud computing have not dealt with learning mechanisms for user behavior recognition in the password as a matching factor with password</td></tr>
<tr><td>2.</td><td><b>Top metric</b></td><td colspan="7"><b>Pass:</b> Prevent unauthorized user to change password<b>;</b>
<b>Fail:</b> Unauthorized user has the potential to change the password<b>.</b></td></tr>
<tr><td>3.</td><td><b>Test location</b></td><td colspan="7">Alburaimi university College, Oman</td></tr>
<tr><td>4.</td><td><b>Number of Samples</b></td><td colspan="7">12 users</td></tr>
<tr><td rowspan="2"><b>4.1</b></td><td rowspan="2"><b>Samples description</b></td><td>Male</td><td>Female</td><td>One language</td><td>Two language</td><td>High computer skills</td><td>intermediate computer skills</td><td>Basic comput er skills</td></tr>
<tr><td>8</td><td>4</td><td>3</td><td>9</td><td>3</td><td>6</td><td>3</td></tr>
<tr><td>5.</td><td><b>Proposed change</b></td><td colspan="7">Analysis human behavior in the authentication process</td></tr>
<tr><td>6.</td><td><b>Hypothesis</b></td><td colspan="7">Applying behavior recognition in the authentication process in public cloud computing lead to mitigating stolen password effects.</td></tr>
<tr><td>7.</td><td><b>Secondary metrics</b></td><td colspan="7">Data security level</td></tr>
<tr><td>8.</td><td><b>Targeting</b></td><td colspan="7">Prevent unauthorized user to change the password</td></tr>
<tr><td>9.</td><td><b>Duration</b></td><td colspan="7">Ten days</td></tr>
<tr><td>10.</td><td><b>Ideal results</b></td><td colspan="7">Diagnose all unauthorized user when tries to change the password</td></tr>
</table>

The experiment, without the adoption of $\text{EPSB}_{\text{Style}}$ in the authentication layer, the unauthorized users changed the active password directly and dealt with saved data.

$$\boldsymbol{Pre\ Accuracy\ Rate\ = \frac{0}{12} * \ 100 = 00\%}$$

When the authentication layer is adopted the $\text{EPSB}_{\text{Style}}$, that automatically detects deviations from normal behavior and subsequently determine the unauthorized user. The $\text{EPSB}_{\text{Stley}}$ works as follows: It monitors all user actions with the style of password and builds, for each user, an $\text{EPSB}_{\text{syle}}$, a mathematical representation of how the user typically has chosen his/her password. The PS component will generate the $\text{EPSB}_{\text{Style}}$ based on analyse the password aspects such as Number (N), Upper case (U), Lower case (l), Especial character(E), Length of password(L), Number of letters(T) and then send the results to Decision (D) component. All these characters inside the password will be examined and then will generate a new $\text{EPSB}_{\text{Style}}$ according to these characters. The final results will be sent to EPSB$_{\text{DStley}}$ for the next process. The EPSB$_{\text{DStley}}$ determines whether the user is deviating from expected behavior, signalling the possible presence of an unauthorized user. The EPSB$_{\text{DStley}}$ results, as shown in Table 5.4 below:

Table 5.4 the EPSB$_{\text{DStley}}$ Results

Current users	**EPSB$_{\text{style}}$ Current user**						**EPSB$_{\text{Dstyle}}$ Authorized user range**						**Decision**
	PSN	PSU	PSI	PSL	PSE	PST	PSN	PSU	PSI	PSL	PSE	PST	
1	3	2	5	10	1	6	**1.2–2.3**	**1.2- 3.4**	**3.2-4.1**	**7.9 – 9.4**	**1.1 – 2.1**	**3.3 – 6.9**	Pass
2	5	3	3	12	2	6	**2.2– 5.1**	**2.2– 4.3**	**4.3– 5.2**	**6.3 – 7.8**	**1.5 – 2.6**	**3.7 – 7.5**	Fail
3	3	1	3	7	0	4	**1.2 – 2.8**	**2.2– 5.1**	**1.3 -3.2**	**6.8 – 8.4**	**1.2 – 2.3**	**2.4 – 6.3**	Pass
4	2	1	5	10	2	6	**2.3 – 4.3**	**1.1 - 3.5**	**4.4 – 6.8**	**7.3 – 12-.5**	**1.5 – 1.9**	**2.6 – 5.5**	Pass
5	6	2	3	11	0	5	**3.1 - 5**	**2.3 – 4**	**2.4 – 4.6**	**8.6 – 12.7**	**1.2 – 2.6**	**3.1 – 6.1**	Pass
6	3	3	2	9	1	5	**2.2- 3.5**	**1.3-3.3**	**3.2 – 4.5**	**7.9 – 13.2**	**1.6- 3.1**	**4.4 – 7.9**	Fail
7	1	2	3	8	2	5	**3.2 – 5.8**	**3.4 – 5.3**	**4.2 – 6.6**	**9.9 – 14.5**	**1.4 – 2.5**	**3.9 – 7.1**	Pass
8	2	1	2	9	4	3	**4.6 – 5.9**	**1.6 – 3.2**	**5.3 – 7.4**	**10.3 – 13.4**	**1.7 – 2.8**	**6.6 – 9.1**	Pass
9	1	0	3	6	2	3	**3.7 – 6.8**	**2.1- 2.8**	**4.8 – 5.4**	**10.7 – 12.4**	**1.8 – 3.2**	**5.9 – 8.4**	Pass
10	0	2	6	10	2	8	**3.5 – 6.3**	**2.2 – 3.9**	**2.3 – 3.5**	**9.9 – 11.4**	**2.2 – 4.5**	**7.2 – 9.7**	Pass
11	3	3	5	13	2	8	**2.1 – 4.6**	**2.3 – 3.6**	**4.7 – 6.9**	**8.7 – 12.2**	**1.1 – 3.7**	**6.3 – 9.1**	Fail
12	4	3	5	15	3	8	**1.3 – 3.2**	**1.2- 2.3**	**4.3 -5.7**	**6.8– 10.1**	**1.2 – 2.1**	**4.6 – 7.8**	Pass

According to the above table, the results show that the authentication process in public cloud computing determined that 9 unauthorized users out of 12 have their password changed. In these assumptions, the EPSB$_{\text{style}}$ determine 75% from unauthorized users to change the active password in the authentication layer. Thus, they could be considered as accepted results. The accuracy is determined according to the formula below:

$$\boldsymbol{Post\ Accuracy\ Rate = \frac{9}{12} * \ 100 = 75\%}$$

c) Assumptions 3:

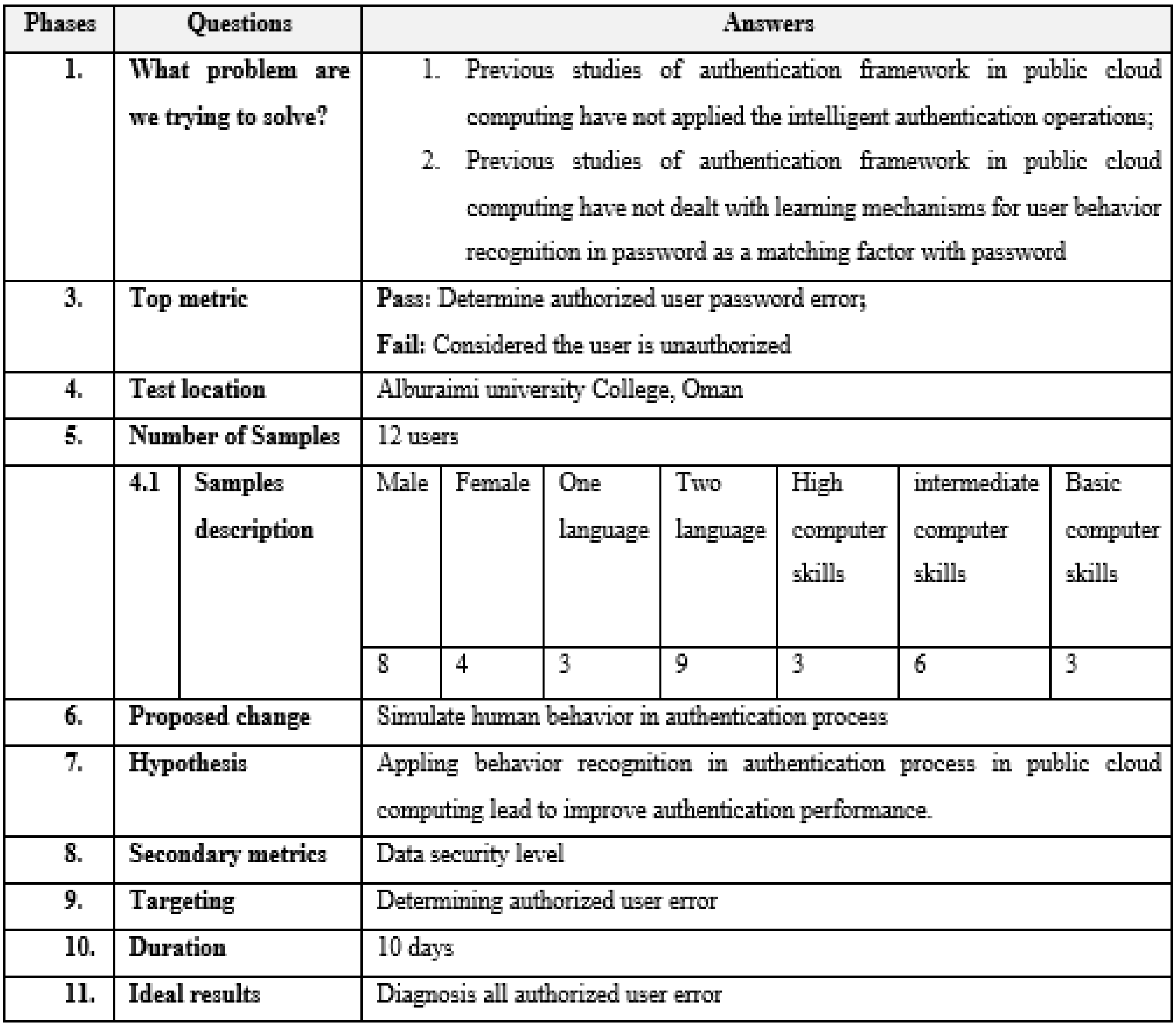
Authorized user tries to log in to the authentication layer using the wrong password.

Authorized password: Available.

Descriptions: The authorized user may be using old password, another language active in PC, forget the current active password, and wrong in a few active PW letters.

The description of the third experiment with EPSB is accordance to the test idea framework in Table 5.5 below[182].

Table 5.5 Assumptions 3 Test Idea Framework



<table>
<tr><th>Phases</th><th colspan="2">Questions</th><th colspan="7">Answers</th></tr>
<tr><td>1.</td><td colspan="2">What problem are we trying to solve?</td><td colspan="7">1. Previous studies of authentication framework in public cloud computing have not applied the intelligent authentication operations;
2. Previous studies of authentication framework in public cloud computing have not dealt with learning mechanisms for user behavior recognition in password as a matching factor with password</td></tr>
<tr><td>3.</td><td colspan="2">Top metric</td><td colspan="7">Pass: Determine authorized user password error;
Fail: Considered the user is unauthorized</td></tr>
<tr><td>4.</td><td colspan="2">Test location</td><td colspan="7">Alburaimi university College, Oman</td></tr>
<tr><td>5.</td><td colspan="2">Number of Samples</td><td colspan="7">12 users</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">4.1</td><td rowspan="2">Samples description</td><td>Male</td><td>Female</td><td>One language</td><td>Two language</td><td>High computer skills</td><td>intermediate computer skills</td><td>Basic computer skills</td></tr>
<tr><td>8</td><td>4</td><td>3</td><td>9</td><td>3</td><td>6</td><td>3</td></tr>
<tr><td>6.</td><td colspan="2">Proposed change</td><td colspan="7">Simulate human behavior in authentication process</td></tr>
<tr><td>7.</td><td colspan="2">Hypothesis</td><td colspan="7">Appling behavior recognition in authentication process in public cloud computing lead to improve authentication performance.</td></tr>
<tr><td>8.</td><td colspan="2">Secondary metrics</td><td colspan="7">Data security level</td></tr>
<tr><td>9.</td><td colspan="2">Targeting</td><td colspan="7">Determining authorized user error</td></tr>
<tr><td>10.</td><td colspan="2">Duration</td><td colspan="7">10 days</td></tr>
<tr><td>11.</td><td colspan="2">Ideal results</td><td colspan="7">Diagnosis all authorized user error</td></tr>
</table>

Without adopting $EPSB_{Error}$, the result shows that all users who printed the wrong password considered as unauthorized. Besides, the chance of input password fixed according to system requirement.

$$\boldsymbol{Pre\ Accuracy\ Rate\ = \frac{0}{12} * 100 = 00\%}$$

With $EPSB_{Error}$, the result shows an authentication process in public cloud computing. In most cases, there are some repetitive errors for the authorized users, such as using an old password, repeating a particular character, using another account’s password, not paying attention to the enabled language, or writing the capital letters as small letters and vice-versa. The task of Pe to generate the $EPSB_{Error}$ according to apply the Confidence range(CR). The CR_{Pe} will be generated depending on analyse the error password aspects such as Number (N), Upper case (U), Lower case (l), Especial character(E), Length of password(L), Number of letters(T) and then send the results to Decision (D) component. The EPSB$_{\text{DError}}$ results as shown as in Table 5.6 below:

Table 5.6 the EPSB$_{\text{DError}}$ Results

Current users	**EPSB$_{\text{Error}}$ Current user**						**EPSB$_{\text{DError}}$ Authorized user range**						**Decision**
	PeN	PeU	PeI	PeL	PeE	PeT	PeN	PeU	PeI	PeL	PeE	PeT	
1	3	2	5	11	1	7	**2.2–3.3**	**1.2- 4.3**	**3.2-5.7**	**8.3 – 11.2**	**1.1 – 2.1**	**5.2 – 8.4**	Pass
2	4	2	6	14	2	8	**2.5– 4.8**	**1.6– 3.3**	**3.8– 6.2**	**9.3 – 12.2**	**1.2 – 2.7**	**5.7 – 8.3**	Pass
3	5	3	3	13	2	6	**1.2 – 4.9**	**2.4– 3.6**	**1.4 -3.8**	**6.8 – 9.2**	**1.7 – 2.9**	**2.1 – 7.2**	Pass
4	3	3	4	13	3	7	**2.4 – 4.8**	**1.9 - 4.2**	**3.8 – 8.6**	**6.9 – 14.5**	**1.6 – 3.1**	**3.9 – 8.4**	Pass
5	5	3	6	14	0	9	**2.1 – 6.2**	**1.2 – 2.3**	**2.6 – 7.2**	**9.4 – 15.1**	**1.1 – 2.3**	**4.5 – 9.1**	Pass
6	2	4	2	11	2	6	**2.3- 3.7**	**1.3 - 4.7**	**4.8 – 6.9**	**8.1 – 13.5**	**1.8- 2.6**	**5.3 – 7.9**	Pass
7	1	7	2	10	0	8	**1.2 – 3.9**	**2.9 – 7.3**	**4.2 – 8.1**	**9.9 – 12.5**	**0 – 2**	**3.9 – 9.1**	Pass
8	3	1	3	7	0	4	**1.6 – 3.2**	**0.5 – 3.1**	**4.3 – 8.2**	**6.3 – 10.2**	**1 – 2.1**	**2.7 – 5.7**	Pass
9	4	2	2	9	1	4	**5.1 – 6.7**	**2.7- 4.5**	**5.7 – 6.3**	**10.1 – 12.1**	**0.5 – 1.7**	**7.2 – 9.1**	Fail
10	3	7	1	13	2	8	**2.2 – 4.1**	**4.9 – 8.2**	**2.2 – 4.2**	**8.2 – 14.2**	**1.5 – 3.2**	**7.2– 11.3**	Pass
11	4	3	6	14	1	9	**3.1 – 4.2**	**3.7 – 4.9**	**5.2 – 7.6**	**9.2 – 14.3**	**1.8 – 2.4**	**4.2– 8.5**	Fail
12	4	2	5	13	2	7	**2.2 – 4.8**	**1.7- 2.5**	**5.3 -6.1**	**8.9– 14.3**	**1.2 – 2.5**	**6.1 – 9.1**	Pass

According to the above table, the authentication with EPSB$_{\text{Error}}$ has been determined 10 authorized password errors out of 12. The EPSB$_{\text{DError}}$ is determined 83.3% from the authorized users to typing error password in the authentication layer. Thus, they could be considered as accepted results. The accuracy is determined according to the formula below:

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{10}}{\mathbf{12}} * \ \mathbf{100} = \mathbf{83.3\%}$$

d) Assumptions 4:

Unauthorized user tries to guess the authorized password in the authentication layer.

Authorized password: Unavailable.

Descriptions: Password guessing attacks.

The description of the fourth experiments with EPSB$_{\text{Error}}$ according to test idea framework, as shown in Table 5.7 below[182].

Table 5.7 Assumptions 4 Test Idea Framework

<table>
<tr><th>Phases</th><th>Questions</th><th colspan="7">Answers</th></tr>
<tr><td>1.</td><td><b>What problems are we trying to solve?</b></td><td colspan="7">1. Previous studies of the authentication framework in public cloud computing have not applied intelligent authentication operations;
2. Previous studies of the authentication framework in public cloud computing have not dealt with learning mechanisms for user behavior recognition in the password as a matching factor with the password.</td></tr>
<tr><td>2.</td><td><b>Top metric</b></td><td colspan="7"><b>Pass:</b> Determine unauthorized user password error from the first attempt<b>;</b>
<b>Fail:</b> the user has more chance to input password</td></tr>
<tr><td>3.</td><td><b>Test location</b></td><td colspan="7">Alburaimi University College, Oman</td></tr>
<tr><td>4.</td><td><b>Number of Samples</b></td><td colspan="7">12, and 22 users</td></tr>
<tr><td rowspan="2">4.1</td><td rowspan="2"><b>Samples description</b></td><td>Male</td><td>Female</td><td>One language</td><td>Two language</td><td>High computer skills</td><td>intermediate computer skills</td><td>Basic computer skills</td></tr>
<tr><td>8</td><td>4</td><td>3</td><td>9</td><td>3</td><td>6</td><td>3</td></tr>
<tr><td>5.</td><td><b>Proposed change</b></td><td colspan="7">Analysis of human behavior in the authentication process</td></tr>
<tr><td>6.</td><td><b>Hypothesis</b></td><td colspan="7">Applying behavior recognition in the authentication process in public cloud computing lead to improving authentication accuracy.</td></tr>
<tr><td>7.</td><td><b>Secondary metrics</b></td><td colspan="7">Data security level</td></tr>
<tr><td>8.</td><td><b>Targeting</b></td><td colspan="7">Determining unauthorized user error directly</td></tr>
<tr><td>9.</td><td><b>Duration</b></td><td colspan="7">Ten days</td></tr>
<tr><td>10.</td><td><b>Ideal results</b></td><td colspan="7">Diagnose all unauthorized user error from the first attempt</td></tr>
</table>

Without adopting EPSB$_{\text{Error}}$, the result of this experiment showed that all users who printed the wrong password are considered as unauthorized while the authentication process still grants them more chance to type the password.

$$\boldsymbol{Pre\ Accuracy\ Rate} = \frac{\mathbf{0}}{\mathbf{12}} * \mathbf{100} = \mathbf{00\%}$$

With EPSB$_{\text{Error}}$, the result of the experiment, as shown in Table 5.8 below:

Table 5.8 the $\text{EPSB}_{\text{DError}}$ Results

Current users	$\text{EPSB}_{\text{Error}}$ Current user						$\text{EPSB}_{\text{DError}}$ Authorized user range						Decision
	PeN	PeU	PeI	PeL	PeE	PeT	PeN	PeU	PeI	PeL	PeE	PeT	
1	5	1	6	14	2	7	2.2–3.3	1.6- 4.4	3.8-5.1	8.5 – 11.3	1.1 – 2.1	2.3 – 5.4	Pass
2	2	1	6	10	1	7	2.1– 4.1	2.6– 5.3	3.3– 5.6	7.3 – 9.8	1.2 – 2.3	4.7 – 8.2	Pass
3	3	2	4	12	3	6	1.4 – 2.9	2.1– 3.3	1.4 -3.8	7.8 – 10.2	1.6 – 2.2	2.4 – 6.3	Pass
4	3	2	5	11	2	7	2.1 – 4.7	1.5 - 4.5	4.8 – 7.6	6.3 – 11.5	1.5 – 1.7	2.9 – 7.5	Fail
5	6	1	3	12	2	4	3.4 – 5.6	2.2 – 4.3	2.2 – 5.6	7.4 – 11.7	1.2 – 2.6	3.1 – 6.1	Pass
6	1	3	5	12	3	7	2.1- 3.8	1.6 - 3.2	4.2 – 6.5	8.7 – 12.5	1.4- 3.6	5.2 – 7.7	Fail
7	7	2	7	19	3	8	2.7 – 7.8	3.9 – 6.6	5.2 – 6.4	10.9 – 13.5	1.7 – 2.9	4.9 – 7.1	Pass
8	7	1	1	9	0	2	2.6 – 4.6	1.7 – 4.2	5.3 – 7.4	8.3 – 12.6	1.1 – 2.3	4.7 – 7.3	Pass
9	0	8	1	9	0	9	4.7 – 7.8	1.7- 3.5	5.2 – 7.8	10.4 – 13.8	1.6 – 3.7	7.5 – 9.3	Pass
10	9	0	0	10	1	0	2.5 – 4.7	2.8 – 4.2	2.1 – 3.2	8.7 – 12.7	2.3 – 3.1	5.6– 10.2	Pass
11	3	0	3	7	1	3	3.2 – 4.8	2.1 – 4.7	2.7 – 5.4	7.2 – 11.3	1.3 – 3.1	5.1 – 7.5	Pass
12	4	1	8	15	2	9	1.2 – 4.2	1.3- 3.6	6.3 -8.1	7.6– 13.2	1.5 – 2.7	5.1 – 8.3	Pass

According to the above table, the $\text{EPSB}_{\text{DError}}$ determined 10 unauthorized password errors out of 12, and the password field prevented any other chances to print the password. The accuracy determined according to the formula below:

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{10}}{\mathbf{12}} * \mathbf{100} = \mathbf{83.3\%}$$

According to the results of the above experiment, the proposed algorithm performance had not dealt with determining and ignoring the abnormal value in time component performance.

To overcome this obstacle, we adopted the z-score formula to determine and exclude the integration of abnormal value in $\text{EPSB}_{\text{Time}}$ results. The experiments repeated with adoption z score. This layer was implemented on 22 students in from IT, and Business departments, at Al-Buraimi University College, Oman for ten working days from 18/12/2018 till 3/1/2019. The number of users divided into three groups. Two groups have eight users in two groups, and one with six users[158]. A heterogeneous sample, such as 14 females and eight males were selected, nine with the Arabic language as his/her first language, 13 who are bilingual (Arabic, English), 11 users have high computer skills proficiency, eight users have intermediate computer skills proficiency, and three users have basic computer skills proficiency.

All experiments were conducted according to the same previous security assumptions for testing accuracy and distribute a questionnaire to examine the acceptance and use level. The results of experiments accuracy, according to security assumptions, are listed below:

Assumptions 1: Unauthorized user logs into the authentication layer through an authorized password, network, and device on the first attempt.

Without adopting EPSB$_{\text{Time}}$, the result of this experiment showed the authentication process determined 0 users out of 22 password entries.

$$\boldsymbol{Pre\ Accuracy\ Rate} = \frac{\mathbf{0}}{\mathbf{22}} * \mathbf{100} = \mathbf{00\%}$$

With EPSB$_{\text{Time}}$, the result of the experiment, as shown in Table 5.9 below:

Table 5.9 the EPSB$_{\text{DTime}}$ Second Results

Current users	EPSB$_{\text{Time}}$ Current user	EPSB$_{\text{DTime}}$ Authorized user range	Decision
1	6.3	3.5 – 4.6	Pass
2	5.2	3.7 – 5.8	Fail
3	4.7	3.1 – 5.1	Fali
4	7.5	3.6 – 4.8	Pass
5	6.3	4.1 – 6.2	Pass
6	6.8	3.8 – 5.7	Pass
7	6.4	3.9 – 5.9	pass
8	5.4	3.2 – 5.5	Fail
9	5.3	2.3 – 4.6	Pass
10	5.9	3.2 – 4.9	Pass
11	6.8	3.6 – 5.8	Pass
12	7.3	2.9 – 4.8	Pass
13	6.4	3.6 – 7.2	Fail
14	5.8	3.7 – 6.2	Fail
15	6.1	2.8 – 5.3	Pass
16	8.2	3.4 – 6.3	Pass
17	5.3	3.6 – 5.8	Fail
18	7.6	3.5 – 5.5	Pass
19	7.3	4.5 – 7.4	Fail
20	5.7	3.1 – 4.8	Pass
21	6.4	4.1 – 7.1	Fail
22	7.2	3.7 – 5.7	Pass

According to the table above, the EPSB$_{\text{Time}}$ determined 14 users out of 22 password entries. In this test, the EPSB$_{\text{Time}}$ prevent 63.6% from unauthorized users to login in the public cloud, although they have an active password. Thus, they could consider as accepted results, the accuracy determined according to the formula below:

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{14}}{\mathbf{22}} * \mathbf{100} = \mathbf{63.6\%}$$

Assumptions 2: The results of this experiment without EPSB$_{\text{Style}}$ will show that all unauthorized users change the active password directly and deal with saved data.

Without the adoption of EPSB$_{\text{Style}}$, the authentication process in public cloud computing was determined 0 users out of 22 password change.

$$\boldsymbol{Pre\ Accuracy\ Rate} = \frac{\mathbf{0}}{\mathbf{22}} * \mathbf{100} = \mathbf{00\%}$$

On the other hand, the result of this experiment with the adoption of EPSB$_{\text{Style}}$ as shown in Table 5.10 below:

Table 5.10 the EPSB$_{\text{Dstyle}}$ Second Results

Current users	**EPSB$_{\text{style}}$ Current user**						**EPSB$_{\text{Dstyle}}$ Authorized user range**						**Decision**
CR	PSN	PSU	PSI	PSL	PSE	PST	PSN	PSU	PSI	PSL	PSE	PST	
1	2	4	4	10	0	8	**1.4–2.7**	**1.8- 3.7**	**4.2-6.1**	**7.6 – 12.3**	**2.1 – 3.5**	**5.3 – 7.4**	Pass
2	1	5	5	12	1	10	**2.1– 4.2**	**2.6– 5.3**	**5.3– 7.1**	**7.3 – 10.8**	**0.5 – 2.1**	**2.5 – 6.5**	Pass
3	3	2	3	9	1	5	**1.2 – 2.8**	**2.2– 5.1**	**1.3 -3.2**	**6.8 – 9.4**	**0.5 – 2.3**	**2.4 – 6.3**	Fail
4	2	3	3	10	2	6	**1.5 – 4.3**	**1.6 - 3.2**	**5.3 – 7.5**	**8.1 – 13.5**	**2.1 – 3.4**	**6.3 – 8.5**	Pass
5	5	3	6	15	1	9	**3.3 – 4.2**	**3.3 – 5.8**	**2.4 – 4.6**	**8.9 – 11.7**	**1.4 – 3.6**	**6.1 – 9.1**	Pass
6	3	3	4	12	2	7	**2.1- 3.7**	**1.2 - 3.5**	**3.1 – 5.5**	**8.2 – 11.8**	**1.3- 1.8**	**4.4 – 6.9**	Pass
7	4	0	4	8	0	4	**3.6 – 6.9**	**2.4 – 4.5**	**4.1 – 7.2**	**10.9 – 13.5**	**1.5 – 2.2**	**3.9 – 7.1**	Pass
8	2	5	3	10	0	8	**4.2 – 6.4**	**1.2 – 3.1**	**3.3 – 5.3**	**10.3 – 13.4**	**1.2 – 2.4**	**6.6 – 9.1**	Pass
9	5	1	5	11	0	6	**3.1 – 5.3**	**2.5 - 3.5**	**4.1 – 7.8**	**9.9 – 11.4**	**1.5 – 3.6**	**5.9 – 8.4**	Fail
10	6	2	2	10	0	4	**2.5 – 5.1**	**2.1 – 3.5**	**3.3 – 5.7**	**8.7 – 12.2**	**2.1 – 3.5**	**7.2 – 9.7**	Pass
11	3	3	5	11	0	8	**2.6 – 5.6**	**2.5 – 3.8**	**4.3 – 7.6**	**6.8– 10.1**	**1.3 – 2.7**	**6.3 – 9.1**	Fail
12	2	4	4	10	0	8	**2.3 – 4.2**	**1.6 - 2.9**	**3.3 - 6.4**	**7.2 – 11.3**	**1.3 – 2.4**	**4.6 – 7.8**	Pass
13	3	3	5	11	0	8	**1.3-3.3**	**3.6 – 6.9**	**3.6 – 5.6**	**10.7 – 12.4**	**1.1 - 3.5**	**4.2 – 6.7**	Pass
14	4	2	2	10	2	4	**3.4 – 5.3**	**2.1 – 3.1**	**4.6 – 8.6**	**8.3 -12.6**	**1.2 – 3.2**	**6.3 – 8.9**	Pass
15	0	5	0	6	1	5	**1.6 – 3.2**	**2.4 – 4.3**	**3.3 – 5.4**	**6.7 – 10.2**	**1.5 – 3.6**	**5.5 – 7.8**	Pass
16	5	0	4	10	1	4	**2.1- 2.8**	**2.2 – 3.6**	**3.5 – 6.2**	**8.2 – 11.2**	**0.5 – 4.3**	**3.5 – 6.5**	Fail
17	3	2	3	8	0	5	**2.2 – 3.9**	**3.2 – 5.2**	**3.6 – 5.3**	**7.3 – 10.5**	**0.5 – 2.5**	**5.5 – 8.6**	Pass
18	5	0	4	11	2	4	**2.3 – 3.6**	**2.4 – 4.3**	**4.5 – 6.5**	**9.5 – 13.5**	**00 – 00**	**5.7 – 8.7**	Pass
19	7	0	0	8	1	0	**1.2- 2.3**	**2.6 – 5.2**	**4.1 - 6.5**	**7.4 – 10.8**	**0.5 – 2.1**	**4.4 – 8.2**	Pass
20	3	4	4	11	0	8	**2.1 – 4.2**	**3.1 – 5.7**	**3.1 – 5.3**	**8.3 – 11.7**	**1.2 – 3.2**	**4.6 – 8.3**	Fail
21	2	2	3	8	0	5	**3.2 – 4.5**	**2.6 – 5.3**	**4.1 – 6.7**	**5.3 – 7.9**	**1.3 – 3.5**	**3.5 – 7.5**	Pass
22	3	2	2	9	0	4	**4.2 – 6.6**	**3.1 – 6.1**	**3.6 – 6.9**	**7.3 – 10.3**	**00 – 00**	**5.7 – 9.3**	Pass

According to the above table, the authentication process in public cloud computing shows that 17 unauthorized users out of 22 password change were determined. In this test, the EPSB$_{\text{style}}$prevent 77.27% from unauthorized users to change the active password in the public cloud, although they have the active password. Thus, they could consider as accepted results, the accuracy rate determined according to the formula below:

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{17}}{\mathbf{22}} * \mathbf{100} = \mathbf{77.27\%}$$

Assumptions 3: The results of this experiment show that without EPSB$_{\text{Error}}$, all users who printed the wrong password considered as unauthorized. Besides, the chance of input password fixed according to system requirement.

The result of this experiment without the adoption of EPSB$_{\text{Error}}$ in the authentication process in public cloud computing shows that the authentication was determined 0 authorized password errors out of 22.

$$\boldsymbol{Pre\ Accuracy\ Rate}\ = \frac{\mathbf{0}}{\mathbf{22}} *\ \mathbf{100} = \mathbf{00\%}$$

The result of this experiment with the adoption of EPSB$_{\text{Error}}$ in the authentication process in public cloud computing, as shown in Table 5.11 below:

Table 5.11 the EPSB$_{\text{DError}}$ Second Results

Current users	**EPSB$_{\text{Error}}$ Current user**						**EPSB$_{\text{DError}}$ Authorized user range**						**Decision**
CR	PeN	PeU	PeI	PeL	PeE	PeT	PeN	PeU	PeI	PeL	PeE	PeT	
1	3	3	5	14	3	8	**2.1–3.4**	**2.2- 4.5**	**4.2-6.7**	**7.3 – 14.2**	**2.1 – 3.1**	**6.2 – 9.4**	Pass
2	3	0	5	8	1	5	**1.5– 3.5**	**1.5– 3.5**	**4.5– 6.7**	**8.2 – 12.7**	**0.5 – 1.5**	**4.9 – 9.3**	Pass
3	3	2	4	9	0	6	**1.5 – 3.5**	**2.1– 3.5**	**3.4 -5.3**	**6.5 – 7.2**	**1.5 – 2.5**	**3.1 – 6.4**	Fail
4	2	1	5	10	2	6	**2.4 – 4.5**	**1.5 - 4.5**	**4.5 – 7.5**	**7.6 – 12.5**	**1.5 – 3.1**	**4.5 – 9.5**	Pass
5	1	2	5	9	1	7	**2.2 – 5.6**	**1.5 – 3.3**	**4.5 – 7.3**	**8.5 – 11.1**	**0.5 – 2.5**	**3.5 – 8.1**	Pass
6	1	2	6	10	2	8	**3.5- 5.5**	**2.5 – 4.5**	**5.6 – 8.8**	**6.5 – 10.9**	**1.5 – 2.5**	**2.5 – 8.5**	Pass
7	2	4	5	12	1	9	**1.5 – 4.5**	**3.5 – 5.5**	**4.5 – 6.5**	**5.5 – 9.5**	**2.0 – 3.1**	**4.6 – 9.5**	Pass
8	2	1	4	7	0	5	**1.5 – 3.5**	**2.5 – 3.5**	**5.5 – 7.5**	**3.5 – 8.5**	**0.5 - 1.5**	**5.5 – 8.5**	Fail
9	6	3	5	15	1	8	**5.1 – 6.7**	**2.5 – 4.5**	**4.5 – 6.5**	**6.5 – 11.5**	**0.5 – 2.5**	**3.5 – 6.5**	Pass
10	3	2	5	10	0	7	**2.5 – 4.5**	**0.5 – 3.5**	**3.5 – 6.5**	**5.5 – 12.5**	**1.0 – 2.5**	**4.5 – 9.5**	Pass
11	2	2	4	9	0	6	**2.5 – 3.5**	**1.5 – 4.5**	**5.5 – 6.8**	**6.5 – 10.8**	**0.0 – 0.0**	**3.5 – 8.5**	Pass
12	4	3	3	11	1	6	**3.5 – 5.5**	**2.5 – 5.5**	**2.5 – 5.5**	**7.5 – 12.5**	**0.5 – 1.5**	**5.5 – 7.5**	Pass
13	5	2	5	12	0	7	**1.2- 4.3**	**1.3 - 4.7**	**4.8 – 6.9**	**8.1 – 13.5**	**1.8- 2.6**	**5.3 – 7.9**	Pass
14	6	0	6	12	0	6	**1.5– 3.5**	**2.5 – 5.5**	**4.6 – 5.1**	**7.9 – 10.5**	**1.5 – 2.5**	**4.2 – 6.1**	Fail
15	4	2	7	13	0	9	**2.4– 3.6**	**0.5 – 3.5**	**4.3 – 8.5**	**7.5 – 13.2**	**1.5– 2.1**	**5.7 – 9.7**	Pass
16	5	3	6	10	1	9	**1.9 - 4.2**	**2.7- 4.5**	**5.7 – 6.3**	**9.1 – 12.1**	**0.5 – 1.7**	**7.2 – 9.1**	Pass
17	3	4	1	10	2	5	**2.5– 4.8**	**4.9 – 8.2**	**2.2 – 4.2**	**8.2 – 14.2**	**1.5 – 3.2**	**7.2– 11.3**	Pass
18	1	4	6	13	2	10	**1.2 – 4.9**	**3.7 – 4.9**	**5.2 – 7.6**	**9.2 – 14.3**	**1.8 – 2.4**	**6.2– 10.5**	Pass
19	4	4	5	13	0	9	**2.4 – 4.8**	**1.7- 2.5**	**5.3 -6.1**	**8.9– 14.3**	**0.0 – 0.0**	**6.1 – 9.1**	Pass
20	2	2	6	11	1	8	**2.1 – 6.2**	**1.3 - 4.7**	**4.8 – 6.9**	**8.1 – 13.5**	**1.8- 2.6**	**5.3 – 8.9**	Pass
21	4	3	3	10	0	6	**2.5– 4.8**	**2.9 – 7.3**	**4.2 – 8.1**	**9.9 – 12.5**	**0.0 – 0.0**	**3.9 – 9.1**	Pass
22	2	2	5	12	2	7	**1.2 – 4.9**	**1.5 – 2.5**	**4.5 – 7.5**	**8.5 – 13.5**	**0.5 – 1.5**	**6.5 – 8.5**	Pass

According to the above table, the authentication process in public cloud computing shows that 19 authorized users out of 22 password error were determined. In this test, the $\text{EPSB}_{\text{Error}}$ determined 86.54% password error from the authorized users in the public cloud. Thus, they could consider as accepted results, the accuracy rate determined according to the formula below:

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{19}}{\mathbf{22}} * \mathbf{100} = \mathbf{86.54}\%$$

Assumption 4: The results of this experiment without $\text{EPSB}_{\text{Error}}$ show that all users who printed the wrong password considered as unauthorized but the authentication process granted them more chance to type the password.

The result of this experiment without the adoption of $\text{EPSB}_{\text{Error}}$ in the authentication process in public cloud computing show that the authentication was determined 0 unauthorized password errors out of 22 and password field was still active that led to the authentication process granting them more chance to print password.

$$\boldsymbol{Pre\ Accuracy\ Rate}\ = \frac{\mathbf{0}}{\mathbf{22}} * \mathbf{100} = \mathbf{00}\%$$

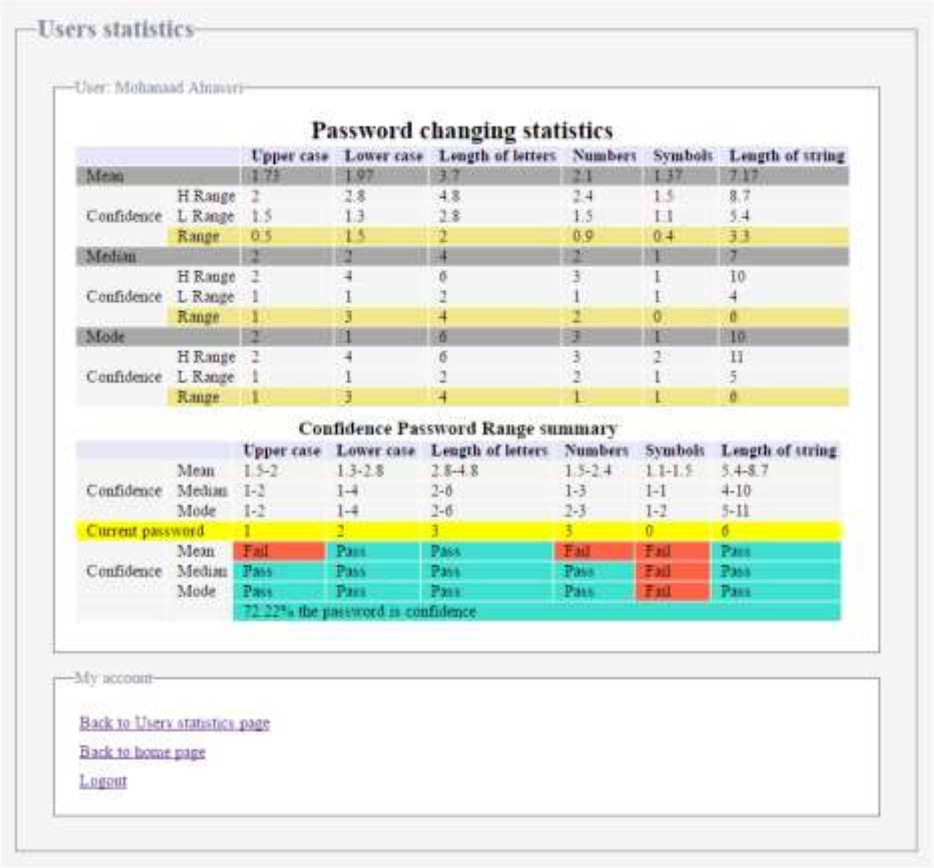
The result of this experiment with the adoption of $\text{EPSB}_{\text{Error}}$ in the authentication process in public cloud computing. The $\text{EPSB}_{\text{DError}}$ determined 18 unauthorized password errors out of 22, and the password field was inactive without more input chance. The accuracy determined according to the table formula below:

$$\boldsymbol{Post\ Accuracy\ Rate} = \frac{\mathbf{18}}{\mathbf{22}} *\ \mathbf{100} = \mathbf{81.81}\%$$

The layer recorded and analyzed all the activities of each user. Generally, the layer produces three $\text{EPSB}_{\text{Time,Style,Error}}$ based on confidence ranges for each part used in the analysis. The total experiments result summarized in Table 5.12, and Figure 5.1 is a snapshot from the password component. See Appendix D for the sample from the results test.

Table 5.12 Total Experiments Results

	Assumption 1 $\text{EPSB}_{\text{Time}}$	**Assumption 2** $\text{EPSB}_{\text{Style}}$	**Assumption 3** $\text{EPSB}_{\text{Error}}$	**Assumption 4** $\text{EPSB}_{\text{Error}}$
Scenario 1	63.6%	Inactive	Inactive	Inactive
Scenario 2	Inactive	77.27%	Inactive	Inactive
Scenario 3	Inactive	Inactive	86.54%	81.81%



Password changing statistics

		Upper case	Lower case	Length of letters	Numbers	Symbols	Length of string
Mean		1.73	1.97	3.7	2.1	1.37	7.17
Confidence	H Range	2	2.8	4.8	2.4	1.5	8.7
	L Range	1.5	1.3	2.8	1.5	1.1	5.4
	Range	0.5	1.5	2	0.9	0.4	3.3
Median		2	2	4	2	1	7
Confidence	H Range	2	4	6	3	1	10
	L Range	1	1	2	1	1	4
	Range	1	3	4	2	0	6
Mode		2	1	6	3	1	10
Confidence	H Range	2	4	6	3	2	11
	L Range	1	1	2	2	1	5
	Range	1	3	4	1	1	6

Confidence Password Range summary

		Upper case	Lower case	Length of letters	Numbers	Symbols	Length of string
Confidence	Mean	1.5-2	1.3-2.8	2.8-4.8	1.5-2.4	1.1-1.5	5.4-8.7
	Median	1-2	1-4	2-6	1-3	1-1	4-10
	Mode	1-2	1-4	2-6	2-3	1-2	5-11
Current password		1	2	3	3	0	6
Confidence	Mean	Fail	Pass	Pass	Fail	Fail	Pass
	Median	Pass	Pass	Pass	Pass	Fail	Pass
	Mode	Pass	Pass	Pass	Pass	Fail	Pass
		72.22% the password is confidence					

Figure 5.1 Snapshot Password Component.

5.2.2 Discussion and Analysis

According to the above results, the adopting of $\text{EPSB}_{\text{algorithm}}$ in authentication layer in public cloud computing leads to the increase in the performance of authentication through improving the accuracy of authorized user authentication. In $\text{EPSB}_{\text{Time}}$, there is a possibility of the unauthorized user diagnosis even if their password is correct, and they used the correct user's laptop based on the time taken during typing password. Table 5.13 as show the total experiment results $\text{EPSB}_{\text{Time}}$ based on scenario 1.

Table 5.13 Experiment Results for $\text{EPSB}_{\text{Time}}$

	Assumption 1 (12 samples) **$\text{EPSB}_{\text{Time}}$**	**Assumption 1 (22 samples)** **$\text{EPSB}_{\text{Time}}$**
Scenario 1	66.6%	63.6%

In addition, $\text{EPSB}_{\text{Style}}$ will add a new security level for the user. It will also strengthen the unauthorized user's password change diagnosis based on the Password Style (PS) Component. Thus, the closest reliable range can be determined while choosing the password; if the change is not included in this range, it will not be changed until all critical security procedures have been followed. Table 5.14 as show the total experiment results for the $\text{EPSB}_{\text{Style}}$ based on scenario 2.

Table 5.14 Experiment Results for $\text{EPSB}_{\text{Style}}$

	Assumption 2 (12 samples) **$\text{EPSB}_{\text{Time}}$**	**Assumption 2 (22 samples)** **$\text{EPSB}_{\text{Time}}$**
Scenario 2	75%	77.27 %

Additionally, the $\text{EPSB}_{\text{Error}}$ also could diagnose the ultimate amount of reliable errors made by the authorized user, depending on saving the authorized user's previous errors and differentiating them from the unauthorized user's entries; consequently, the algorithm prevents the temporary blocks and strengthens the availability. Table 5.15 as show the total experiment results for the $\text{EPSB}_{\text{Error}}$ based on scenario 3,4.

Table 5.15 Experiment Results for $\text{EPSB}_{\text{Error}}$

	Assumption 3 (12 samples) $\text{EPSB}_{\text{Time}}$	**Assumption 3 (22 samples) $\text{EPSB}_{\text{Time}}$**	**Assumption 4 (12 samples) $\text{EPSB}_{\text{Time}}$**	**Assumption 4 (22 samples) $\text{EPSB}_{\text{Time}}$**
Scenario 3	83.3%	86.54 %	83.3%	81.81%

The adopting of $\text{EPSB}_{\text{algorithm}}$ in authentication is enhancing the accuracy of user authentication in a public cloud. In a related context, applying $\text{EPSB}_{\text{algorithm}}$ while authenticating any suspicious activity of the user results in reducing possible impact has a significant effect on the system to strengthen and therefore reduce the harmful effects of stolen password attacks. As a result, the adopting of $\text{EPSB}_{\text{algorithm}}$ in authentication process lead to the mitigation of stolen password attacks' effects through the shift from traditional authentication strategies to intelligent authentication operations.

5.2.3 EPSB Accept and Use Test Results and Analysis

The user test or questionnaire designed to determine how usable the authentication systems with EPSB$_{\text{algorithm}}$ and how the participants evaluated accept, use, and perceive security. In this research, a security procedure suggested for improving the authentication accuracy when facing stolen password attacks. It was of particular interest to determine the effects of security procedure on accepting and use level[159]. The validation structure was prepared based on the Technology Acceptance Model (TAM). The accept and use structure questionnaires in this section were conducted based on adoption some of previously used in many studies to be fitting with proposed algorithm evaluations [16][183]. Besides, this questionnaire was sent to a native speaker expert who is an assistant professor in the field of software engineering for language and content validation. In addition, three experts in information technology have checked the criterion-related and approved this questionnaire with some modifications (see Appendix A). The questions are listed in Table 5.16 below.

Table 5.16 Accept and Use Questionnaire

No.	**Perceived Usefulness**
PU1	The EPSB enhances my authentication efficiency.
PU2	The EPSB algorithm enhances authentication productivity.
PU3	The EPSB algorithm enables me to accomplish authentication tasks quickly.
PU4	The EPSB algorithm improves authentication accuracy .
PU5	The EPSB algorithm saves my time.
PU6	The EPSB algorithm doesn't have any distinctive useful features.
PU7	The EPSB algorithm is not applicable to all authentication process
Perceived Ease of Use	
PE1	The EPSB algorithm in authentication is easy to use.
PE2	The EPSB algorithm enables me to access the data which saved in public cloud computing smoothly.
PE3	The EPSB algorithm is convenient and user-friendly.
PE4	The user should memorize complicated password in EPSB algorithm process.
PE5	The EPSB algorithm is needed to memorize some secrets procedures
PE6	The EPSB authentication procedure is complicated to the user
PE7	The EPSB algorithm requires no training.

Behavioral Intention to Use	
BI1	I intend to increase my use of the EPSB algorithm.
BI2	It is worth to recommend the EPSB algorithm for other organizations.
BI3	I am interested in using the EPSB algorithm more frequently in the future.
Actual System Use	
AU1	I use the EPSB algorithm on a daily basis.
AU2	I use the EPSB algorithm frequently.

This section contains eight subsections. This section shows the introduction to usability. The second subsection presents the theoretical framework and research hypotheses of this study. The third subsection shows the study participants. The fourth subsection shows the research's pilot study. The fifth subsection presents the context and subjects and followed by data collection instrument and data analysis and results. Finally, this section closes with a discussion and conclusion.

Figure 5.2 Snapshot During Distribute Questionnaire

a) Theoretical Framework and Research Hypotheses

Many information systems (IS) theories/models were developed to assess the acceptance of the new algorithm in technology. Technology Acceptance Model (TAM) is one of the theories that were developed by Davis in 1989[167]. TAM has been prepared based on the Theory of Reasoned Action (TRA) [168]. TAM suggests that the user's behavioral intention to use the EPSB algorithm is determined by two main beliefs; perceived usefulness (PU) and perceived ease of use (PEOU). PU refers to the degree to which a person believes that using a particular system would enhance his/her job performance, whereas, PEOU denotes to the degree to which user believes that using a specific system would be free from efforts (see Figure 5.3 below). Various studies have adopted the TAM to study technology acceptance and usage. For instance, it has been successfully adopted in studies with similar objectives to the present research[184][185][186]. In this study, the TAM [167] is adopted for measuring the users' acceptance of the EPSB algorithm as technology in their authentication accuracy in public cloud computing. In this respect, TAM provides a solid background for the effectiveness of new technology. Besides, TAM also suggests that when users are exposed to new technology, many factors can influence their acceptance decision. Accordingly, many researchers have suggested groups of hypotheses[177]. In this thesis, the hypotheses used for this study were adopted from M. Al-Emran et al. [177]. Thus, this thesis is interested in testing the following hypotheses:

H1: Perceived ease of use positively influences the perceived usefulness of EPSB.
H2: Perceived ease of use positively influences the behavioral intention to use EPSB.
H3: Perceived usefulness positively influences the behavioral intention to use EPSB.
H4: Behavioral intention to use influences the actual use of EPSB.

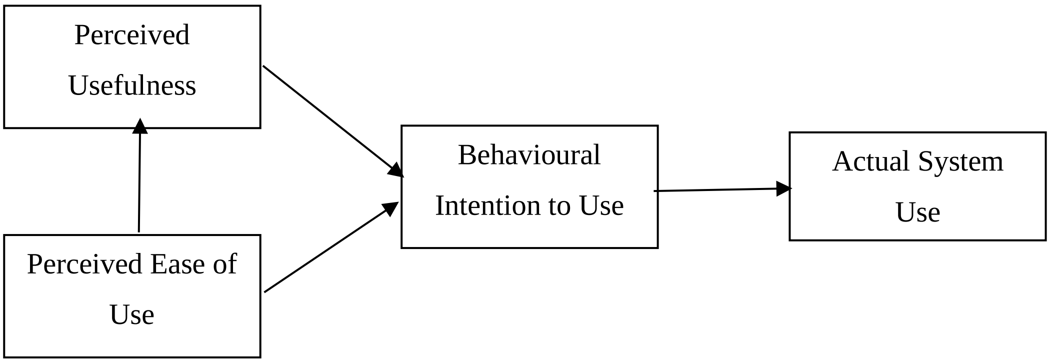


Figure 5.3 Technology Acceptance Model (TAM)

b) Participants

The total number of participants is twenty-two (22) [158]. The same experiments test participants were chosen because they had already used the authentication system with EPSB 10 days during the accuracy test. Thus, all the participants have an idea about the manner of using the proposed algorithm. Of the 22 students, 14 were female, and all details have been shown in the earlier sections (3.5 and 5.2.1).

c) Pilot test

As explained by Creswell [187], pilot testing of research instruments provides researchers with an idea of whether the respondents were able to complete the questionnaire and understand the questions. More importantly, the appropriateness of the operational definitions and research methodology can be ascertained[188]. The aim of the pilot study is to assess the acceptance and use and acceptability of receiving the EPSB questionnaire questions. It was also of interest to assess whether the questions in the questionnaire are clear and are comprehended by most of the students. In the case of the current study, a pilot study which was conducted involving four students, two from both of female and male, two were monolinguals, and two were bilinguals, and two have high computer skills, and one in both of intermediate and basic computer skills. The pilot study was also carried out as a way of familiarizing with the data collection procedures. The pilot study generally revealed that changes only on the two deep technical questions, thus these questions were cancelled. In order to assess the reliability of the items of the questionnaire, composite reliability and average variance extracted (AVE) measures were utilized. Value of 0.7 and greater for composite reliability and value of 0.5 and greater for AVE were suggested by Hair et al. [189] for the factor to be considered as reliable. In this research, composite reliability values for all questions were well above the 0.9 and the AVE for all questions were above the 0.55(see Table 5.17 below). These two results were very close to the recommended cut-off points of 0.7 and 0.5 respectively; therefore, they considered as valid. By taking into consideration composite reliability and average variance extracted values, it can be concluded that questionnaire constructs were found to be reliable. Besides, the Cronbach's Alpha was used to test the reliability of the questionnaire as well. The results are presented in Table 5.18

below. The results of PU, PE, BI, and AU around 89% are considered acceptable rates (see appendix B).

Table 5.17 Reliability Statistics.

TAM	**Cronbach's Alpha**
PU	0.897
PE	0.748
BI	0.917
AU	0.84
Total	0.899

Table 5.18 Average Variance Extracted.

	Variance(y)	$\mathbf{y^2}$	$\boldsymbol{\epsilon}$
PU1	0.667	0.444889	0.555111
PU2	0.917	0.840889	0.159111
PU3	0.917	0.840889	0.159111
PU4	0.917	0.840889	0.159111
PU5	0.667	0.444889	0.555111
PU6	0.667	0.444889	0.555111
PU7	0.917	0.840889	0.159111
PE1	0.250	0.0625	0.9375
PE2	0.917	0.840889	0.159111
PE3	0.917	0.840889	0.159111
PE4	0.917	0.840889	0.159111
PE5	0.917	0.840889	0.159111
PE6	0.917	0.840889	0.159111
PE7	0.667	0.444889	0.555111
BI1	0.667	0.444889	0.555111
BI2	0.250	0.0625	0.9375
BI3	0.250	0.0625	0.9375
AU1	0.667	0.444889	0.555111
AU2	0.250	0.0625	0.9375
N			19
Average Variance Extracted			0.551965
Composite Reliability			0.953788

d) Context and Subjects

The study was conducted at Al Buraimi University College (BUC) in Oman. By the end of 2018, we have evolved the initiative of implementing the EPSB algorithm in authentication on a virtual authentication layer in the public cloud. The sample of this study consists of the same students who have used the EPSB in above accuracy experimental. A total of 22 valid responses were received from a total of 22 questionnaires administrated, which shows a response rate of 100%.

c) Data Collection Instrument

A questionnaire was distributed to all the enrolled students on this experiment for data collection. The questionnaire consists of 2 different parts. The first part aims to collect the students' demographic information. The second part is devoted to collect data regarding the Technology Acceptance Model (TAM) factors. These factors include the perceived usefulness (PU), the perceived ease of use (PEOU), the behavioral intention (BI), and the actual use (AU). The items used for this study were adopted from M. Al-Emran et al. and other [177] with a further adjustment to fit the scope of this study. The passed value according to cumulative percentage value is supposed to be equal or greater than 80%. This rate covered strongly agree and agree in the questionnaire. Appendix A shows the construct items. The data collection was conducted by distributing the questionnaire and collecting the feedback from students directly. Table 5.19 shows the five-level Likert scale that was used in the questionnaire.

Table 5.19 Five-Level Likert Scale

Mark Range	90-100	89.99- 80	79.99-75	74.99 – 65	64.99 - 0
Grade Points	4	3.5	3.12	2.7	0
Grade	A	B	C	D	F
Meaning	Outstanding	Very good	Marginal Pass	Marginal Pass	Fail
Statistical denote	1	2	3	4	5
	Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

e) Data Analysis and Results

In this section, we present four factors, according to TAM. These factors include the perceived usefulness (PU), the perceived ease of use (PEOU), the behavioral intention (BI), and the actual use (AU). The items used for this study were adopted by M. Al-Emran et al. [177]. The statistical analysis and evaluation of the data in this study were done by using the average mean, average median, mode, average std. Deviation, average variance, and final percentages. SPSS was used for statistical relation analysis. There are many types of averages in statistics, and one of those averages is the mean and the median, which is the mid-value. The recurring values are called mode. The standard deviation is a statistical dimension or appraisal of the dispersion of a set of data from its mean. The more spread the data is, the higher the deviation. Standard deviation is calculated as the square root of the variance. The variance is the measure of the spreading set of data that points around their mean value. Variance is a mathematical prospect of the average squared divergences from the mean. Moreover, finally, the percentage is presenting the highest one chosen from five-levels Likert scale.

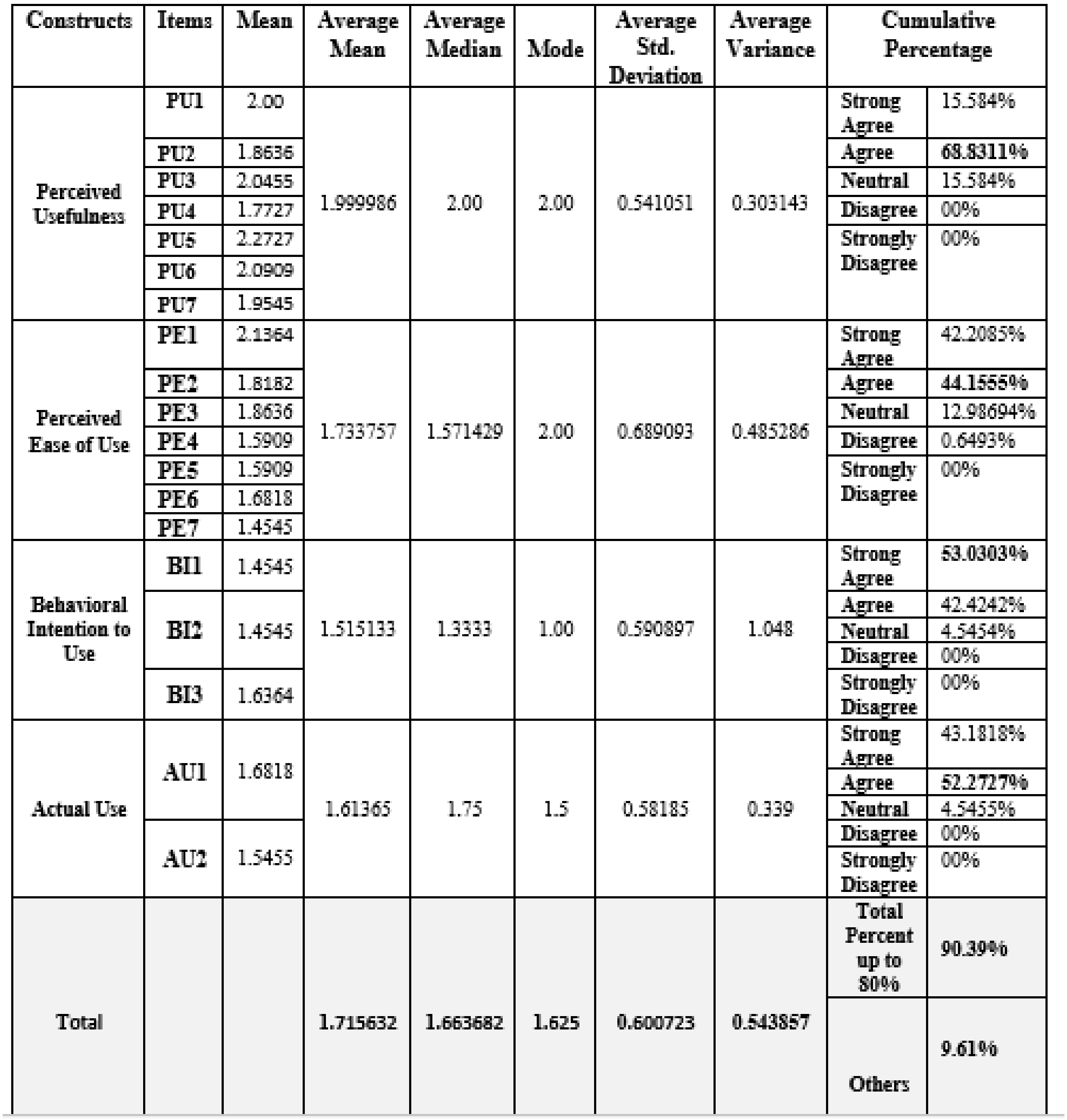
f) Descriptive statistics

The data demonstrates the responses collected from samples which were 22 in total. Table 5.9 shows the demographic information of the participants. We can observe that females constitute 63.63% of the collected data, while only 36.37% are males. Furthermore, all of the users are aged between 18 and 23 years, which represent the sample population. In terms of the department, 32% of the students are from the Business Administration & Accounting; this is followed by 13% from the English Language, 42% from the Information Technology, and 13% from the Law, respectively. With regard to the computer skills, it is clearly shown that 50% of the participants have high computer skills proficiency, followed by 36.36% have intermediate computer skills proficiency,13.63% have basic computer skills proficiency. Table 5.13 below is an explanation of the analysis for TAM.

g) Discussion and Conclusion

In order to measure the validity of each item, the factor’s total percent up to 80% should be measured. The data collection instrument is assumed as valid when the threshold value is of equal or greater than 70% for each item, and the cumulative percentage value is of equal or greater than 80%. In addition, the average mean and median, and mode values should be equal or greater than 2.00. Based on Table 5.20 below, we can observe the first construct of the questionnaire (PU) is near to agree on category (Average Mean = 1.999). Since this value is between 80 and 89 range in the five-level Likert scale, it could be considered as an acceptable value. However, the values of the questions respectively from PE, BI, and AU (Average Mean= 1.733757, 1.515133, 1.61365) are near to Agree as well. In addition, the cumulative percentage results up to 80% of PU, PE, BI, and AU are 84.4151%, 86.364%, 95.4542%, and 95.4545%, respectively. Accordingly, they could be considered as highly accepted results.

Table 5.20 Descriptive Statistical for TAM



Constructs	Items	Mean	Average Mean	Average Median	Mode	Average Std. Deviation	Average Variance	Cumulative Percentage	
Perceived Usefulness	PU1	2.00	1.999986	2.00	2.00	0.541051	0.303143	Strong Agree	15.584%
	PU2	1.8636						Agree	**68.8311%**
	PU3	2.0455						Neutral	15.584%
	PU4	1.7727						Disagree	00%
	PU5	2.2727						Strongly Disagree	00%
	PU6	2.0909							
	PU7	1.9545							
Perceived Ease of Use	PE1	2.1364	1.733757	1.571429	2.00	0.689093	0.485286	Strong Agree	42.2085%
	PE2	1.8182						Agree	**44.1555%**
	PE3	1.8636						Neutral	12.98694%
	PE4	1.5909						Disagree	0.6493%
	PE5	1.5909						Strongly Disagree	00%
	PE6	1.6818							
	PE7	1.4545							
Behavioral Intention to Use	BI1	1.4545	1.515133	1.3333	1.00	0.590897	1.048	Strong Agree	**53.0303%**
	BI2	1.4545						Agree	42.4242%
								Neutral	4.5454%
								Disagree	00%
	BI3	1.6364						Strongly Disagree	00%
Actual Use	AU1	1.6818	1.61365	1.75	1.5	0.58185	0.339	Strong Agree	43.1818%
								Agree	**52.2727%**
								Neutral	4.5455%
	AU2	1.5455						Disagree	00%
								Strongly Disagree	00%
Total			**1.715632**	**1.663682**	**1.625**	**0.600723**	**0.543857**	**Total Percent up to 80%**	**90.39%**
								Others	**9.61%**

In this study, four hypotheses were listed in theoretical framework section and the research hypotheses are above the correlation coefficient results according to Spearman's[190] . In terms of path analysis, Figure 5.4 and Table 5.21 demonstrate the path coefficients and *p*-values for each hypothesis. It can be noticed that all the hypotheses are supported, which in turn indicates that all the paths are significant between the independent and dependent variables. **H**1 (B = 0.225, p < 0.05) describes the path between perceived ease of use and perceived usefulness; indicating that the perceived ease of use enhances the perceived usefulness of EPSB. **H2** (*B* = 0.292, $p < 0.05$) shows the path between perceived ease of use and behavioral intention; representing that the perceived ease of use leverages the behavioral intention to use EPSB. **H3** (B = 0.320, p < 0.05) demonstrates the path between perceived usefulness and behavioral intention; revealing that perceived usefulness positively influences the behavioral intention to use EPSB. **H4** (B = 0.250, p < 0.05) describes the path between behavioral intention and actual usage; indicating that behavioral intention is significantly affecting the actual usage of EPSB. The results of this section suggest that both PEOU and PU positively affect the behavioral intention by users who perceive the use of EPSB as easy and useful.

Table 5.21 Hypotheses Results

Hypotheses	Path	Path Coefficient	P-Value	Remarks
H1	**PE ⟶ PU**	**0.225**	**0.002**	Supported
H2	**PE⟶ BI**	**0.292**	**0.001**	Supported
H3	**PU ⟶ BI**	**0.320**	**0.001**	Supported
H4	**BI ⟶ AU**	**0.250**	**0.001**	Supported

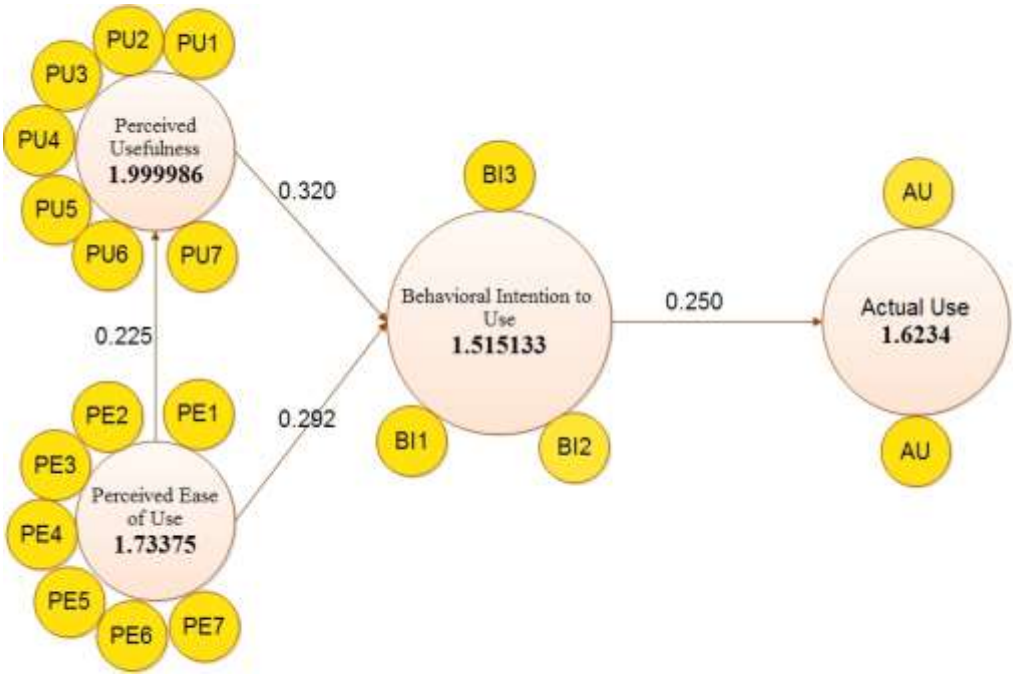


Figure 5.4 Path Analysis Results

5.3 Approaches Comparison

A comparative study in this section looks at the authentication accuracy before and after adopting the proposed algorithm with authentication. The finding of this comparison is that the adopting of the EPSB algorithm leads to improving the performance of authenticating an authorized user in public cloud authentication.
Finally, the summary of comparison is listed below:

A) According to section 2.6 (conclusion), most of the current multi-factor authentication methods have extremely high cost of implementation and deployment, and Oracle is recommended to move from traditional authentication strategies to intelligent authentication operations[24]. On the other hand, the proposed algorithm add new factor has security, easy to use, and cheap. In addition, the adopting EPSB in authentication leads to a shift from traditional authentication strategies to intelligent authentication operations through adapting learning mechanisms for behavior recognition that can provide mitigation to threats automatically.

B) Also, according to section 2.6 (Conclusion), most of the current studies neglected the presence of the human factor in password-based authentication, and learnability in password-based authentication is highly weak. Thus, the proposed algorithm is monitoring, recording, and analyzing all user activities with password-based authentication and has learnability based on user behavior.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Introduction

As one of the most important research fields in public cloud computing security, authentication aims to allow authorized user only to login into data saved in public cloud computing. The current authentication methods are suffering a drawback in dealing with stolen password attacks. However, to find the high authentication accuracy in determine an authorized user in public cloud computing when an unauthorized user has an active password "stolen password attacks" is where the challenge lies. In addition, there are some repetitive errors for legitimate users, such as using an old password, repeating a particular character, using another account's password, not paying attention to the enabled language, or writing the capital letters as small letters and vice versa. In these cases, the diagnosis of an authorized user is more difficult to accomplish.

This research has reviewed the existing works of those that tackle the authentication accuracy in public cloud computing from password-based authentication, especially the two factors techniques. As an output of the literature study, a set of defects was detected, which make the processing less efficient, less accurate, and very costly. Even if the side effect of these defects is insignificant, we have to improve them. These challenges in the cloud computing authentication generally come from the unauthorized diagnosis user whose first attempt logging into public cloud computing via authorized password, device, or network. Also, previous studies of authentication framework in public cloud computing have not dealt with learning mechanisms "intelligent authentication operations" for user behavior recognition in the password as a matching factor with a password.

To solve these research issues through improving the authentication accuracy, we have proposed a new approach to deal with the behavior recognition in order to raise the accuracy of authenticating authorized user, especially when an unauthorized user has the active password. The proposed algorithm updates the authentication accuracy through simulating the human "behavior" on the authentication layer to improve the performance of passwords by improving its predictability. The proposed approach is an enhancement to the authentication process in the public cloud computing field, which is the EPSB Algorithm. The main tasks of this algorithm are monitoring, recording and analyzing all the activities associated with the password on duration, error, and style to the authorized user. Furthermore, the approach was implemented, and the algorithm was coded. Moreover, we have evaluated the performance of the $\text{EPSB}_{\text{algorithm}}$ in practical applications by carrying out experiments.

6.2 Contribution

This thesis contributes significantly to the development of authentication accuracy in public cloud computing. First of all, the proposed algorithm is considered a key advantage that adds a new security level to monitor then identify any unauthorized user when the active password is stolen by using the previous behavior of the authorized user. Besides, the proposed algorithm does not only tackle the accuracy of authenticating authorized user with stolen password problems, but it has also improved the intelligent authentication operations that come from learnability of previously authorized user behavior with a password (behavior recognition). Although the problem of authentication accuracy has been investigated previously and many approaches have been proposed to deal with this problem, most of these approaches have only focused on external authentication factors, such as mobile, SMS, smart card, security question, and biometric which are considered very expensive. However, the previous studies didn’t examine empirically the represented of human behavior (behavior recognition) internally which comes from the password. The behavior recognition approach has many features such as being the cheapest approach on the security field generally, and on the authentication field particularly since it does not need for more authentication hardware to be added[19][24]. Furthermore, the present study suggested that it can deal with learning mechanisms that consider user behavior recognition as a matching factor to the password. The contributions of the present thesis are listed below.

6.2.1 An Improved Algorithm

The main contribution of this study is the proposed algorithm which is named EPSB. This algorithm is an enhancement to one of the authentications in the public cloud area. The proposed algorithm improves the authentication accuracy and helps to deal with stolen password attacks by adding the predictability node. This node is moving password-based authentication performance from traditional security strategies to intelligent security operations via analysing human behavior in the authentication process. The design of the proposed algorithm solves many defects and stolen password attack problems, which have been discussed in the literature review section.

6.2.2 Raising Accuracy of Authentication

Highly accuracy in authenticating the authorized user is one of the most important aspects of the authentication process that has been studied very well in the public cloud field and computer science in general. More specifically, a stolen password attack is one of the popular challenges that encounter the current authentication process. According to the results of this study, the proposed $\text{EPSB}_{\text{Algorithm}}$ is demonstrated as a significant contribution to the enhancement of the accuracy rate in authentication process.

6.2.3 Reduce Temporary Ban for Authorized User

Generally, in most cases, there are some repetitive errors for authorized users, such as using an old password, repeating a particular character, using another account’s password, not paying attention to the enabled language, and writing the capital letters as small letters and vice versa. In such cases, most of the authentication approaches work by deactivating the account for a temporary period and then the account will be re-activated after a particular period has passed. Nevertheless, the proposed algorithm contributes significantly to monitor, record, and analyze the errors of the authorized user of the current and old passwords to authenticate the errors of the authorized user and to avoid temporary pending.

6.2.4 Reduce Unauthorized User Password Change

In stolen password attacks, the common behavior of the unauthorized user is to change the current password to dominate and control the authentication process in the public cloud. This gap impacted on the authentication accuracy in public cloud computing. Hence, the proposed algorithm bridges this gap by building $\text{EPSB}_{\text{style}}$ to prevent any unauthorized password change.

6.2.5 Speed of Click on Keyboard When Input Password

Commonly, the speed of using the keyboard has been differing from user to another according to the location of keys, using two or one hands, time of using PC, using keyboard directly and spontaneously, and familiar keyboard. Besides, the authorized user uses an active password many times. Thus, the duration of typing the password from the authorized user is faster than the unauthorized user. According to the previous studies, the authentication framework in public cloud computing has not dealt with the speed of click on the keyboard when enter password. In this sense, the proposed algorithm deals with this point by building $\mathrm{EPSB}_{\mathrm{time}}$ to prevent any unauthorized password. The purpose of $\mathrm{EPSB}_{\mathrm{time}}$ is to monitor the duration of the user behavior by recording the required time for password entrance for all successful logins. Then, these logins will be saved and analyzed for generating an approved $\mathrm{EPSB}_{\mathrm{time}}$ based on the duration of user behavior. The $\mathrm{EPSB}_{\mathrm{time}}$ aims to find a relationship between the time and the password for detecting any suspicious login to improve the authentication accuracy level.

6.3 Summary of Results

In this section, the research questions, which stated in Chapter One, will be reassessed based on this outline of the research. By reviewing the questions, we can confirm if the research results answered the research questions.

Questions One: What are the issues related to the accuracy of password-based authentication in public cloud computing?

By reviewing the authentication approaches in public cloud computing research field, several issues have been found that they are requiring to improve authentication accuracy such as dealing with stolen password attacks, intelligent authentication operations, high cost of external authentication factor, and learning mechanisms for the user by recognition in authentication framework. More details regarding the stolen password attacks issue and current authentication approaches in the field of public cloud are stated in the literature review (Chapter Two).

Question Two: How to design an algorithm that improves the accuracy of the authentication process in public cloud computing?

During the review of existing authentication approaches in public cloud computing field, we find many critical issues in the authentication process when facing stolen password attacks, such as login inside public cloud from unauthorized user via active password, unauthorized password change, diagnose the errors of authorized user to avoid temporary pending, applied traditional authentication process, and classify data according to multi-security level for protecting a sensitive data. Every authentication in the public cloud area should take these things into consideration to obtain high accuracy authentication in diagnosis of an authorized user when dealing with stolen password attacks. The process of the proposed algorithm consists of three phases. The first one is monitoring all users activities to generate the related $EPSB_{style}$, $EPSB_{style}$, $EPSB_{error}$, which is called electronic personal synthesis behavior, which the input parameter entered according to user behavior with a password. The second phase of the process tests the current user $EPSB_c$ for determining whether s/he is the legitimate user or not. The last phase divided into two parts according to second phases, the first one if the output of the second phase is yes, then integrate last EPSB and gave user authority to deal with data which saved in public cloud. The second one, if the output of the second phase is not, block data which has a high-security level, and activation the critical procedures activities.

Question Three: What is the required architecture to represent the behavior of the authorized user in password-based authentication in public cloud computing?

This study shows that the human factor is a key component in the authentication system in the public cloud as it plays a crucial role in creating the password. Therefore, we suggest the EPSB algorithm to analyze human factor in authentication process through the main parameters which are Password Style(PS), Password Error(Pe), Password Time(Pd) and Decision (D). The design of the proposed algorithm was discussed in detail in Chapter Three section 3.4, and in Chapter Four, section 4.2.1 as well.

Question Four: How does the proposed algorithm improve the authentication process, and how to check the validity of the proposed algorithm?

From the study of popular works in the authentication approaches in public cloud computing, we find two important things. The first one is the most secure approaches in the public authentication field, multi-factor authentication, particularly password with an authentication factor. The second step is to review the works thoroughly, looking for defects in existing works. Consequently, the research provides a potential enhancement for the authentication accuracy in public cloud computing when facing stolen password attacks. This work proposed a new algorithm named EPSB. In designing the solution, the defects of existing approaches are taken into consideration. The proposed algorithm is tested by carrying out many experiments. The results of this experiment shows the high ability of the proposed algorithm to diagnose an unauthorized user of the stolen password. Results and discussions were covered in Chapter Four and Five.

6.4 Achievements of Objectives

This section reviews the research objectives, which are stated in Chapter One. Then it checks if the research work has achieved the target objectives. The research objectives stated below:

Objective one: To review the current authentication methods in public cloud computing focusing on the password-based authentication as following.

The research thesis covers the most popular published work in the authentication in public cloud area, especially those techniques that build password-based authentication from multi-factor authentication in the public cloud. The research focuses on password with authentication factor techniques, where the password is the baseline for the proposed approach.

Objective Two: To develop an algorithm that incorporates user behaviour evaluation in order to improve the accuracy of user authentication in public cloud computing.

Reviewing the literature helps the research to identify the essential elements of the algorithm that should present in the authentication approaches. Also, reviewing helps to figure out the manner of authenticating an authorized user in the authentication process in the public cloud field. The proposed algorithm works by analyzing an authorized user behavior in the authentication layer through monitoring, recording and analyzing all the authorized user activities associated with the authorization password time, error, and style. Consequently, the research journey leads to the design of a new approach, which described in Chapter Four of this thesis.

Objective Three: To implement and validate the proposed algorithm.

The approach in this work was implemented and the algorithm's pseudocode was discussed in Chapter Three. However, many experiments were done on many users. The proposed EPSB algorithm shows a good improvement for the authentication process, and it helped to raise the security through improving the accuracy of authenticating an authorized user without effecting the usability.

6.5 Future Works

This study recommended further experimental investigation into the EPSB time since it has only six points (three ranges) which influenced negatively on the level of usability. Therefore, it is suggested to expand the points of EPSB time to more than six points by using algebraic theories or numerical analysis.

It is recommended that the classification be improved with encryption layers by adding the potential of classifying and encrypt the image, video, and audio. Besides, this framework can be used to improve the security level in any mobile application, website, and system. Finally, it is recommended that an improved new information hiding mechanism that has the potential to hide text, video, audio, and image before uploading data inside cloud computing.

REFERENCES

[1] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, “Multilevel classification of security concerns in cloud computing,” *Appl. Comput. Informatics*, vol. 13, no. 1, pp. 57–65, 2016.

[2] W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” *NIST Spec. Publ. 800-144*, p. 80, 2011.

[3] Ben Snedeker, “Pros and Cons of Cloud Computing for Small Business,” *INFUSION SOFT*, 2017. [Online]. Available: https://www.infusionsoft.com/business-success-blog/growth/planning-strategy/the-pros-and-cons-of-public-and-private-clouds%0D.

[4] J. Li, A. Castiglione, and C. Dong, “Special issue on security in cloud computing,” *J. Netw. Comput. Appl.*, vol. 110, pp. 97–98, 2018.

[5] T. Mahboob, M. Zahid, and G. Ahmad, “Adopting Information Security Techniques for Cloud Computing – A Survey,” pp. 7–11, 2016.

[6] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, “Authentication systems: A literature review and classification,” *Telematics and Informatics*, vol. 35, no. 5. pp. 1491–1511, 2018.

[7] J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer, “Improving multiple-password recall: an empirical study,” *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 165–176, 2009.

[8] C. Shen, T. Yu, H. Xu, G. Yang, and X. Guan, “User practice in password security: An empirical study of real-life passwords in the wild,” *Comput. Secur.*, vol. 61, pp. 130–141, 2016.

[9] J. Nicholson, L. Coventry, and P. Briggs, “Faces and Pictures: Understanding age differences in two types of graphical authentications,” *Int. J. Hum. Comput. Stud.*, vol. 71, no. 10, pp. 958–966, 2013.

[10] M. Farcasin, A. Guli, and E. Chan-Tin, “Fluid Passwords-Mitigating the effects of password leaks at the user level,” *arXiv Prepr. arXiv1708.09333*, 2017.

[11] R. K. L. Ko *et al.*, “TrustCloud: A framework for accountability and trust in cloud computing,” in *Services (SERVICES), 2011 IEEE World Congress on*, 2011, pp. 584–588.

[12] D. Jefferson, A. D. Rubin, B. Simons, and D. Wagner, “Analyzing internet voting security,” *Commun. ACM*, vol. 47, no. 10, pp. 59–64, 2004.

[13] S. Subashini and V. Kavitha, “A survey on security issues in service delivery

models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[14] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, 2006.

[15] G. Yang, D. S. Wong, H. Wang, and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," *J. Comput. Syst. Sci.*, vol. 74, no. 7, pp. 1160–1172, 2008.

[16] M. Alizadeh, S. Abolfazli, M. Zamani, and S. Baharun, "Authentication in mobile cloud computing : A survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 59–80, 2016.

[17] R. Chow *et al.*, "Authentication in the clouds: a framework and its application to mobile users," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*, 2010, pp. 1–6.

[18] S.-N. Cheong, H.-C. Ling, and P.-L. Teh, "Secure encrypted steganography graphical password scheme for near field communication smartphone access control system," *Expert Syst. Appl.*, vol. 41, no. 7, pp. 3561–3568, 2014.

[19] W. Paper and W. Paper, "ADAPTIVE AUTHENTICATION SUPERIOR USER EXPERIENCE AND GROWTH THROUGH INTELLIGENT."

[20] J. Oeltjen, "Authentication and Machine Learning: Taking Behavior Recognition to a New Level," *RSA Identity Reimagined*. [Online]. Available: https://www.csoonline.com/article/3209917/identity-management/article.html.

[21] V. Jayawardana, "Adaptive Authentication And Machine Learning," *Towards Data Science*, 2017. [Online]. Available: https://towardsdatascience.com/adaptive-authentication-and-machine-learning-1b460ae53d84.

[22] J. Shepherd, "Duo + OneLogin: Adaptive Authentication," *product and technology, security & compliance*, 2016. [Online]. Available: https://www.onelogin.com/blog/what-is-adaptive-authentication.

[23] A. Ferdowsi and W. Saad, "Deep Learning for Signal Authentication and Security in Massive Internet of Things Systems," pp. 1–30, 2018.

[24] Oracle Corporation, "Machine learning-based adaptive intelligence : The future of cybersecurity Executive summary," no. January, 2018.

[25] L. C. Leonard, *Web-Based Behavioral Modeling for Continuous User Authentication (CUA)*, 1st ed., vol. 105. Elsevier Inc., 2017.

[26] K. Niinuma and A. Jain, “Continuous user authentication using temporal information,” *SPIE Defense, Secur. …*, vol. 7667, p. 11, 2010.

[27] K. Niinuma, U. Park, and A. K. Jain, “Soft biometric traits for continuous user authentication,” *IEEE Trans. Inf. forensics Secur.*, vol. 5, no. 4, pp. 771–780, 2010.

[28] F. Monrose and A. D. Rubin, “Keystroke dynamics as a biometric for authentication,” *Futur. Gener. Comput. Syst.*, vol. 16, no. 4, pp. 351–359, 2000.

[29] C. Shen, Z. Cai, and X. Guan, “Continuous authentication for mouse dynamics: A pattern-growth approach,” in *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, 2012, pp. 1–12.

[30] A. Altinok and M. Turk, “Temporal integration for continuous multimodal biometrics,” in *Proceedings of the Workshop on Multimodal User Authentication*, 2003, no. 1.

[31] H.-B. H. Kang and M. M.-H. Ju, “Multi-modal feature integration for secure authentication,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4113 LNCS, pp. 1191–1200, 2006.

[32] Y. Xie *et al.*, “Innocent by Association : Early Recognition of Legitimate Users,” *ACM Conf. Comput. Commun. Secur. (CCS ’12)*, pp. 353--364, 2012.

[33] J. Zhu, P. Wu, X. Wang, and J. Zhang, “Sensec: Mobile security through passive sensing,” in *2013 International Conference on Computing, Networking and Communications (ICNC)*, 2013, pp. 1128–1133.

[34] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, “Continuous user authentication using multi-modal biometrics,” *Comput. Secur.*, vol. 53, pp. 234–246, 2015.

[35] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and privacy in cloud computing: A survey,” in *Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on*, 2010, pp. 105–112.

[36] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, “Design and analysis of a social botnet,” *Comput. Networks*, vol. 57, no. 2, pp. 556–578, 2013.

[37] A. Elyashar, M. Fire, D. Kagan, and Y. Elovici, “Homing socialbots: intrusion on a specific organization’s employee using Socialbots,” in *Advances in Social Networks Analysis and Mining (ASONAM), 2013 IEEE/ACM International Conference on*, 2013, pp. 1358–1365.

[38] G. Stringhini, C. Kruegel, and G. Vigna, “Detecting spammers on social

networks," in *Proceedings of the 26th annual computer security applications conference*, 2010, pp. 1–9.

[39] P. Dubey, V. Tiwari, S. Chawla, and V. Chauhan, "Authentication Framework for Cloud Machine Deletion," in *Information and Communication Technology for Sustainable Development*, Springer, 2018, pp. 199–206.

[40] H. Karajeh, M. Maqableh, and R. Masa�deh, "Privacy and Security Issues of Cloud Computing Environment," in *Proceedings of the 23rd IBIMA Conference Vision*, 2020, pp. 1–15.

[41] P. Kalagiakos and P. Karampelas, "Cloud computing learning," in *Application of Information and Communication Technologies (AICT), 2011 5th International Conference on*, 2011, pp. 1–4.

[42] M. A. Khan, "A survey of security issues for cloud computing," *J. Netw. Comput. Appl.*, vol. 71, pp. 11–29, 2016.

[43] F. Information and P. Standards, "Standards for security categorization of federal information and information systems," no. February, 2004.

[44] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, 2002.

[45] M. Golfarelli, D. Maio, and D. Malton, "On the error-reject trade-off in biometric verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 19, no. 7, pp. 786–796, 1997.

[46] R. Nikam and M. Potey, "Cloud storage security using Multi-Factor Authentication," *2016 Int. Conf. Recent Adv. Innov. Eng. ICRAIE 2016*, 2017.

[47] T.-H. Chen, H. Yeh, and W.-K. Shih, "An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing," in *Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on*, 2011, pp. 155–159.

[48] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," *Futur. Gener. Comput. Syst.*, vol. 57, pp. 24–41, 2016.

[49] J. Cindhamani, N. Punya, R. Ealaruvi, and L. D. Dhinesh, "An enhanced data security and trust management enabled framework for cloud computing systems," 2014.

[50] S. Dey, S. Sampalli, and Q. Ye, "Message digest as authentication entity for

mobile cloud computing," in *Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International*, 2013, pp. 1–6.

[51] Z. Hao, S. Zhong, and N. Yu, "A time-bound ticket-based mutual authentication scheme for cloud computing," *Int. J. Comput. Commun. Control*, vol. 6, no. 2, pp. 227–235, 2011.

[52] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Futur. Gener. Comput. Syst.*, vol. 68, pp. 74–88, 2017.

[53] R. K. Banyal, P. Jain, and V. K. Jain, "Multi-factor authentication framework for cloud computing," *Proc. Int. Conf. Comput. Intell. Model. Simul.*, pp. 105–110, 2013.

[54] J. H. Yang and P. Y. Lin, "An ID-based user authentication scheme for cloud computing," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*, 2014, pp. 98–101.

[55] S. Grzonkowski, "Sedici: an authentication service taking advantage of zero-knowledge proofs," in *International Conference on Financial Cryptography and Data Security*, 2010, p. 426.

[56] S. Y. Lim, M. L. Mat Kiah, and T. F. Ang, "Security issues and future challenges of cloud service authentication," *Acta Polytech. Hungarica*, vol. 14, no. 2, pp. 69–89, 2017.

[57] N. Fisher, "5 Identity Attacks That Exploit Your Broken Authentication," *Product Marketing Manager, Security*, 2018. [Online]. Available: https://www.okta.com/security-blog/2018/03/5-identity-attacks-that-exploit-your-broken-authentication/%0D. [Accessed: 06-Oct-2018].

[58] B. Sumitra, C. R. Pethuru, and M. Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 2, no. 10, pp. 6245–6253, 2014.

[59] H. Farooq, "A Review on Cloud Computing Security Using Authentication Techniques," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 2, pp. 19–22, 2017.

[60] M. H. Eldefrawy and J. F. Al-Muhtadi, "Cryptanalysis and enhancement of a password-based authentication scheme," *Proc. - IEEE 7th Int. Conf. Cloud Comput. Technol. Sci. CloudCom 2015*, pp. 548–551, 2016.

[61] A. Kaushik, H. O. Awashti, K. Goel, and S. Goel, "Secure Authentication with Encryption Technique for Mobile on Cloud Computing," vol. 1, no. 5, pp. 28–33,

2012.

[62] A. Bennett, “8 Public Cloud Security Threats to Enterprises in 2018,” *DELL EMC, IT security, networking and cloud technology*, 2018. [Online]. Available: https://www.comparethecloud.net/articles/8-public-cloud-security-threats-to-enterprises-in-2017/. [Accessed: 06-Oct-2018].

[63] Chris Fuller, “Complying with NIST Guidelines for Stolen Passwords,” *Security Bloggers Network*. [Online]. Available: https://securityboulevard.com/2018/03/complying-with-nist-guidelines-for-stolen-passwords/. [Accessed: 06-Oct-2018].

[64] S. Ruoti, J. Andersen, and K. Seamons, “Strengthening Password-based Authentication,” *Twelfth Symp. Usable Priv. Secur. (SOUPS 2016)*, 2016.

[65] John Killoran, “4 Password Authentication Vulnerabilities & How to Avoid Them,” *Swoop founders and Matt Custer*, 2018. .

[66] F. Omri, R. Hamila, S. Foufou, and M. Jarraya, “Cloud-ready biometric system for mobile security access,” in *International Conference on Networked Digital Technologies*, 2012, pp. 192–200.

[67] Z. Le, X. Zhang, and Z. Gao, “NemoAuth: a mnemonic multimodal approach to mobile user authentication,” in *TENCON 2013-2013 IEEE Region 10 Conference (31194)*, 2013, pp. 1–6.

[68] I. Al Rassan and H. AlShaher, “Securing mobile cloud computing using biometric authentication (SMCBA),” in *Computational Science and Computational Intelligence (CSCI), 2014 International Conference on*, 2014, vol. 1, pp. 157–161.

[69] V. Kundra, “Federal cloud computing strategy,” 2011.

[70] P. Mell, T. Grance, and others, “The NIST definition of cloud computing,” 2011.

[71] S. Ziyad and A. Kannammal, “A multifactor biometric authentication for the cloud,” in *Computational Intelligence, Cyber Security and Computational Models*, Springer, 2014, pp. 395–403.

[72] K. Niinuma and A. K. Jain, “Continuous user authentication using temporal information,” in *Biometric Technology for Human Identification VII*, 2010, vol. 7667, p. 76670L.

[73] A. Altinok and M. Turk, “Temporal integration for continuous multimodal biometrics,” *Multimodal User Authentication, 2003*, no. 1, pp. 11–12, 2003.

[74] H.-B. Kang and M.-H. Ju, “Multi-modal feature integration for secure

authentication," in *International Conference on Intelligent Computing*, 2006, pp. 1191–1200.

[75] H. Saevanee, N. Clarke, S. Furnell, and V. Biscione, "Continuous user authentication using multi-modal biometrics," *Comput. Secur.*, vol. 53, pp. 234–246, 2015.

[76] M. Belk, C. Fidas, P. Germanakos, and G. Samaras, "The interplay between humans, technology and user authentication: A cognitive processing perspective," *Comput. Human Behav.*, vol. 76, pp. 184–200, 2017.

[77] Margaret Rouse, "security intelligence (SI)," *TechTarget network*. [Online]. Available: https://whatis.techtarget.com/definition/security-intelligence-SI.

[78] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *International Conference on Information Security*, 2010, pp. 99–113.

[79] M. Hajivali, M. T. Alrashdan, F. Fatemi Moghaddam, and A. Z. M. Alothmani, "Applying an agent-based user authentication and access control model for cloud servers," *Int. Conf. ICT Converg.*, no. October 2013, pp. 807–812, 2013.

[80] F. Zhang and D.-Y. Han, "Applying agents to the data security in cloud computing," in *Computer Science and Information Processing (CSIP), 2012 International Conference on*, 2012, pp. 1126–1128.

[81] S. J. Russell and P. Norvig, "A rtificial intelligence: a modern approach." Pearson Education, Inc, 2003.

[82] V. Kimlaychuk, "Authentication using shared knowledge: Learning agents," *Adv. Intell. Syst. Comput.*, vol. 194 AISC, no. VOL. 2, pp. 523–531, 2013.

[83] P. Jadhwani, J. Mackinnon, and M. Elrefal, "Cloud Computing Building a Framework for Successful Transition," *GTSI, North. Virginia*, 2009.

[84] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 50–55, 2008.

[85] S. A. Hussain, M. Fatima, A. Saeed, I. Raza, and R. K. Shahzad, "Multilevel classification of security concerns in cloud computing," *Appl. Comput. Informatics*, vol. 13, no. 1, pp. 57–65, 2016.

[86] S. A. Mertz, C. Eschinger, T. Eid, H. H. Huang, C. Pang, and B. Pring, "Market trends: Software as a service, worldwide, 2008-2013," *Gartner, Stamford, CT*, 2009.

[87] R. V. Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Comput. Sci.*, vol. 48, pp. 204–209, 2015.

[88] M. Shakir, A. B. Abubakar, Y. Bin Yousoff, A. M. Sagher, and H. Alkayali, "DIAGNOSIS SECURITY PROBLEMS IN CLOUD COMPUTING FOR BUSINESS CLOUD," *J. Theor. Appl. Inf. Technol.*, vol. 90, no. 2, p. 151, 2016.

[89] M. Carroll, A. Van Der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls," in *Information Security South Africa (ISSA), 2011*, 2011, pp. 1–9.

[90] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[91] N. Subramanian and A. Jeyaraj, "Recent security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 71, no. July 2017, pp. 28–42, 2018.

[92] H. Shah and S. S. Anandane, "Security Issues on Cloud Computing," vol. 11, no. 8, pp. 1602–1606, 2013.

[93] M. M. Dawoud, G. A. Ebrahim, and S. A. Youssef, "A Cloud Computing Security Framework Based on Cloud Security Trusted Authority," *Proc. 10th Int. Conf. Informatics Syst. - INFOS '16*, pp. 133–138, 2016.

[94] A. Bhandari, "A framework for Data Security and Storage in Cloud Computing," no. March, pp. 430–436, 2016.

[95] J. Surbiryala, C. Li, and C. Rong, "A framework for improving security in cloud computing," in *2017 IEEE 2nd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, 2017, pp. 260–264.

[96] H. Li, C. Yang, and J. Liu, "A novel security media cloud framework," *Comput. Electr. Eng.*, no. 1, pp. 0–1, 2018.

[97] A. E. Youssef and M. Alageel, "A Framework for A Framework for Secure Cloud ure Cloud ure Cloud Computing Computing Computing," vol. 9, no. 4, pp. 487–501, 2012.

[98] Z. Wang, "Security and privacy issues within the Cloud Computing," in *Computational and Information Sciences (ICCIS), 2011 International Conference on*, 2011, pp. 175–178.

[99] E. Mathisen, "Security challenges and solutions in cloud computing," in *Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on*, 2011, pp. 208–212.

[100] D. Abraham, "Why 2FA in the cloud?," *Netw. Secur.*, vol. 2009, no. 9, pp. 4–5,

2009.

[101] F. Scott, M. Itsik, and S. Adi, “Weakness in the key scheduling algorithm of RC4,” in *Proceedings of the 8 Annual Workshop on SAC*, 2001.

[102] S. Ramgovind, M. M. Eloff, and E. Smith, “The management of security in cloud computing,” in *Information Security for South Africa (ISSA), 2010*, 2010, pp. 1–7.

[103] A. Sedgewick, “Framework for Improving Critical Infrastructure Cyber-security,” *NIST*, 2014.

[104] M. Basso and J. Mann, “MarketScope for Enterprise File Synchronization and Sharing,” *Gartner*, 2013.

[105] A. Youssef and M. Alaqeel, “Security Issues in Cloud Computing.,” *GSTF J. Comput.*, vol. 1, no. 3, 2011.

[106] E. C. Amazon, “Amazon elastic compute cloud (Amazon EC2),” *Amaz. Elastic Comput. Cloud (Amazon EC2)*, 2010.

[107] J. Brodkin, “Gartner: Seven cloud-computing security risks,” *InfoWorld*, vol. July, pp. 2–3, 2008.

[108] H. Dey, R. Islam, and H. Arif, “An Integrated Model To Make Cloud Authentication And Multi-Tenancy More Secure,” in *2019 International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST)*, 2019, pp. 502–506.

[109] P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring Data Security Issues and Solutions in Cloud Computing,” *Procedia Comput. Sci.*, vol. 125, no. 2009, pp. 691–697, 2018.

[110] A. Sharma, B. Keshwani, and P. Dadheech, “Authentication Issues and Techniques in Cloud Computing Security: A Review,” *SSRN Electron. J.*, pp. 2305–2307, 2019.

[111] S. Mudgil and S. Singh, “An Access Control Framework for Grid Environment,” no. June, 2014.

[112] C. Yang, X. Chen, and Y. Xiang, “Blockchain-based publicly verifiable data deletion scheme for cloud storage,” *J. Netw. Comput. Appl.*, vol. 103, pp. 185–193, 2018.

[113] E.-Y. Jang, H.-J. Kim, C.-S. Park, J.-Y. Kim, and J. Lee, “The study on a threat countermeasure of mobile cloud services,” *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 21, no. 1, pp. 177–186, 2011.

[114] H. Suo, Z. Liu, J. Wan, and K. Zhou, "Security and privacy in mobile cloud computing," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*, 2013, pp. 655–659.

[115] L. Bernard, "A Risk Assessment Framework for Evaluating Software-as-a-Service (SaaS) Cloud Services Before Adoption," *ProQuest Diss. Theses*, pp. 129-n/a, 2011.

[116] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Comput. Secur.*, vol. 63, pp. 85–116, 2016.

[117] A. Tripathi and A. Mishra, "Cloud computing security considerations," in *Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on*, 2011, pp. 1–5.

[118] M. Metheny, *Chapter 9 - The FedRAMP Cloud Computing Security Requirements*. 2013.

[119] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, no. September 2016, pp. 38–54, 2017.

[120] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva, and J.-J. Quisquater, "Authentication protocols for ad hoc networks: taxonomy and research issues," in *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, 2005, pp. 96–104.

[121] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *IEEE Trans. parallel Distrib. Syst.*, vol. 25, no. 2, pp. 384–394, 2014.

[122] H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Comput. Secur.*, vol. 21, no. 4, pp. 372–375, 2002.

[123] E. Yoon, E. Ryu, and K. Yoo, "Efficient remote user authentication scheme based on generalized elgamal signature scheme," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 568–570, 2004.

[124] E.-J. Yoon and K.-Y. Yoo, "New Authentication Scheme Based on a One-Way Hash Function and {Diffie}-{Hellman} Key Exchange," *CANS 05\ifnum\shortbib=0{: 4th }\fi\ifnum\shortbib=0{International Conference on Cryptology and Network Security}\fi*, vol. 3810. pp. 147–160, 2005.

[125] V. Shoup and A. Rubin, “Session key distribution using smart cards,” in *International Conference on the Theory and Applications of Cryptographic Techniques*, 1996, pp. 321–331.

[126] H. Abie, “Different Ways to Authenticate Users with the Pros and Cons of each Method,” 2006.

[127] P. A. Grassi *et al.*, “NIST Special Publication 800-63B,” *Digit. Identity Guidel. Authentication Lifecycle Manag.*, 2018.

[128] “Stolen password lets hackers into Deloitte’s systems,” *Industry News*, 2017. [Online]. Available: https://www.securenvoy.com/en-gb/blog/stolen-password-lets-hackers-deloittes-systems.

[129] “4 Ways Hackers Can Steal Your Password,” *Diverge IT*, 2017. [Online]. Available: https://www.divergeit.com/4-ways-hackers-can-steal-password/%0D.

[130] Kanika Sharma, “How Dangerous are Impersonation Attacks,” *AT&T Completes Acquisition of AlienVault*, 2018. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/how-dangerous-are-impersonation-attacks.

[131] Symantec employee, “Man-in-the-Middle (MITM) Attacks,” *Norton by Symantec*, 2018. [Online]. Available: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

[132] L. Leigh, “Cloud security provider MailGuard partners with Southern Cross Protection to enhance cyber safety,” *Startup daily., Insights and Stories from the Australian and New Zealand tech ecosystem.*, 2016. [Online]. Available: https://www.startupdaily.net/2016/06/mailguard-partnership-sxp/.

[133] G. Chen, “Convenience over safety : How authentication cookies compromise user account security on the Web,” 2014.

[134] Y. An, “Security Weaknesses of a Biometric-Based Remote User Authentication Scheme Using Smart Cards,” vol. 4, no. 3, pp. 21–28, 2012.

[135] “Behavioral Authentication,” *Open Span*, 2017. [Online]. Available: https://www.vasco.com/behavioral-authentication.html.

[136] DARPA, “Active authentication,” *Authentication*, 2013. [Online]. Available: http://www.darpa.mil/program/active.

[137] J. Kohl and C. Neuman, “The Kerberos network authentication service (V5),” 1993.

[138] R. M. Needham and M. D. Schroeder, “Using encryption for authentication in

large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, 1978.

[139] L. O'gorman, A. Bagga, and J. Bentley, "Query-directed passwords," *Comput. Secur.*, vol. 24, no. 7, pp. 546–560, 2005.

[140] B. C. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Commun. Mag.*, vol. 32, no. 9, pp. 33–38, 1994.

[141] X. Yi, S. Ling, and H. Wang, "Efficient two-server password-only authenticated key exchange," *IEEE Trans. Parallel Distrib. Syst.*, no. 9, pp. 1773–1782, 2013.

[142] C.-C. Chang, C.-Y. Lee, and Y.-C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks," *Comput. Commun.*, vol. 32, no. 4, pp. 611–618, 2009.

[143] M.-S. Hwang and L.-H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 1, pp. 28–30, 2000.

[144] J.-J. Shen, C.-W. Lin, and M.-S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 49, no. 2, pp. 414–416, 2003.

[145] H.-M. Sun, "An efficient remote use authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 4, pp. 958–961, 2000.

[146] C.-K. Chan and L.-M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. Consum. Electron.*, vol. 46, no. 4, pp. 992–993, 2000.

[147] S. Yamaguchi, K. Okayama, and H. Miyahara, "Design and implementation of an authentication system in WIDE Internet environment," in *Computer and Communication Systems, 1990. IEEE TENCON'90., 1990 IEEE Region 10 Conference on*, 1990, pp. 653–657.

[148] K. Sharma, "How Dangerous are Impersonation Attacks?," *ALIENVAULT IS NOW AN AT&T COMPANY*, 2018. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/how-dangerous-are-impersonation-attacks%0D.

[149] Z. Zhang, "Design and implementation of dual-factor authentication file encryption system based on smart-phone," in *2012 IEEE Symposium on Electrical & Electronics Engineering (EEESYM)*, 2012, pp. 678–681.

[150] Z. Song, J. Molina, S. Lee, H. Lee, S. Kotani, and R. Masuoka, "Trustcube: An infrastructure that builds trust in client," in *Future of Trust in Computing*,

Springer, 2009, pp. 68–79.

[151] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, “Sok: The evolution of sybil defense via social networks,” in *Security and Privacy (SP), 2013 IEEE Symposium on*, 2013, pp. 382–396.

[152] Tim French, “Algorithms, Agents and Artificial Intelligence,” 2016.

[153] P. Hoonakker, N. Bornoe, and P. Carayon, “Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users,” *Hum. Factors Ergon. Soc.*, vol. 53, pp. 459–463, 2009.

[154] M. AlSabah, G. Oligeri, and R. Riley, “Your culture is in your password: An analysis of a demographically-diverse password dataset,” *Comput. Secur.*, vol. 77, pp. 427–441, 2018.

[155] J. A. Cazier and B. D. Medlin, “Password security: An empirical investigation into e-commerce passwords and their crack times,” *Inf. Syst. Secur.*, vol. 15, no. 6, pp. 45–55, 2006.

[156] G. A. Bowen, “Preparing a qualitative research-based dissertation: Lessons learned,” *Qual. Rep.*, vol. 10, no. 2, pp. 208–222, 2005.

[157] I. Velásquez, A. Caro, and A. Rodríguez, “Authentication schemes and methods: A systematic literature review,” *Inf. Softw. Technol.*, vol. 94, no. September 2016, pp. 30–37, 2018.

[158] J. Nielsen, “How Many Test Users in a Usability Study?,” *World Leaders in Research-Based User Experience*, 2012. [Online]. Available: https://www.nngroup.com/articles/how-many-test-users/. [Accessed: 03-Nov-2016].

[159] M. Mihajlov, B. J. Blažič, and S. Josimovski, “Quantifying usability and security in authentication,” *Proc. - Int. Comput. Softw. Appl. Conf.*, no. July, pp. 626–629, 2011.

[160] S. C. Way and Y. Yuan, “Criteria for Evaluating Authentication Systems,” *AMCIS 2009 Proc.*, p. 338, 2009.

[161] R. S. Sollie, “Security and usability assessment of several authentication technologies,” 2005.

[162] T. Grance, M. Stevens, and M. Myers, “Guide to Selecting Information Technology Security Products,” p. 67, 2003.

[163] A. Darabseh and A. S. Namin, “The accuracy of user authentication through keystroke features using the most frequent words,” *Proc. 9th Annu. Cyber Inf.*

Secur. Res. Conf. - CISR '14, pp. 85–88, 2014.

[164] A. J. Izenman, "Modern multivariate statistical techniques," *Regression, Classif. manifold Learn.*, 2008.

[165] S. C. Way and S. C. Way, "Criteria for Evaluating Authentication Systems Criteria for Evaluating Authentication Systems," 2009.

[166] E. Din, "9241-11. Ergonomic requirements for office work with visual display terminals (VDTs)--Part 11: Guidance on usability," *Int. Organ. Stand.*, 1998.

[167] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, pp. 319–340, 1989.

[168] M. Fishbein and I. Ajzen, *Belief, attitude, intention and behavior: An introduction to theory and research*. 1975.

[169] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Comput. Secur.*, vol. 39, pp. 127–136, 2013.

[170] C. Braz and J.-M. Robert, "Security and usability: the case of the user authentication methods," in *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, 2006, pp. 199–203.

[171] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*, 2012, pp. 553–567.

[172] K. Sacha, "Evaluation of Software Quality," *Conf. Softw. Eng. Evol. Emerg. Technol. CCIA2005*, pp. 381–388, 2005.

[173] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 215–230, 2006.

[174] B. Biggio, Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET biometrics*, vol. 1, no. 1. IET, pp. 11–24, 2012.

[175] P. Zeng, Z. Cao, K.-K. Choo, and S. Wang, "On the anonymity of some authentication schemes for wireless communications," *IEEE Commun. Lett.*, vol. 13, no. 3, pp. 170–171, 2009.

[176] S. Kim, H. S. Rhee, J. Y. Chun, and D. H. Lee, "Anonymous and traceable authentication scheme using smart cards," in *Information Security and Assurance, 2008. ISA 2008. International Conference on*, 2008, pp. 162–165.

[177] R. A. S. Al-Maroof and M. Al-Emran, “Students acceptance of google classroom: An exploratory study using PLS-SEM approach,” *Int. J. Emerg. Technol. Learn.*, vol. 13, no. 6, pp. 112–123, 2018.

[178] M. Q. Patton, “Qualitative Research & Evaluation Methods: Integrating Theory and Practice [Kindle DX version](p. 255, 286).” SAGE Publications. Kindle Edition, 2015.

[179] D. R. Anderson, D. J. Sweeney, and T. A. Williams, *Essentials of statistics for business and economics, revised*. Cengage Learning, 2011.

[180] W. J. Dixon, F. J. Massey, and others, *Introduction to statistical analysis*, vol. 344. McGraw-Hill New York, 1969.

[181] G. Chief and I. Officer, “GUIDELINES FOR APPLICATION SOFTWARE TESTING,” no. May, 2018.

[182] “Test Idea Framework,” *optimizely testing toolkit*, 2016. [Online]. Available: https://files.mtstatic.com/site_6806/4102/0?Expires=1563460895&Signature=MX0RoYGedorfK3BaebD5xcELQsDii30f4m1qLFabmc4b33XAs2AxqUZ6BnVG1HOfdYdFsvNVxa2eufQMmAH45qdYFNQSW5pubRRrnJIucVzrzFZtInPxHDWRloWJR3NwhzWKYh1KJa8MtIotYmA-CjLGpI01OkgeWYeg~P-mkks_&Key-Pair-Id=APKAJ5Y6AV4GI7A555NA.

[183] C. Borysowich, “Sample Website Usability Questionnaire,” *TOOLBOX TECHNOLOGY*. [Online]. Available: https://it.toolbox.com/blogs/craigborysowich/sample-website-usability-questionnaire-072407. [Accessed: 12-Dec-2017].

[184] T. Almarabeh, “Students’ Perceptions of E-learning at the University of Jordan,” *Int. J. Emerg. Technol. Learn.*, vol. 9, no. 3, pp. 31–35, 2014.

[185] M. Al-Emran, H. M. Elsherif, and K. Shaalan, “Investigating attitudes towards the use of mobile learning in higher education,” *Comput. Human Behav.*, vol. 56, pp. 93–102, 2016.

[186] N. Polk, “Adoption of Cloud Computing Services in an Illinois-Based Insurance Company,” Walden University, 2019.

[187] J. W. Creswell, *Education Research planning, conduction, and evaluation quantitative and qualtative research*, vol. 39, no. 5. 2008.

[188] A. R. Donald Ary, Lucy Cheser Jacobs, Chris Sorensen, *Introduction to research in education*, Eight Edit., vol. 39, no. 5. Ary, Jacobs, Razavieh and Sorensen 2006, USA: WADSWORTH CENGAE Learning, 2008.

[189] J. Hair, R. Anderson, R. Y. Tatham, and W. Black, “Multivariate data analysis with readings. New Jersey: Prentice Hall,” 1998.

[190] J. M. G. Taylor, “Kendall’s and Spearman’s correlation coefficients in the presence of a blocking variable,” *Biometrics*, pp. 409–416, 1987.

[191] S. Bakshi, “Portfolio, Program and Project Management Using COBIT 5,” *Cybersecurity Nexus*, 2017. [Online]. Available: https://www.isaca.org/pages/default.aspx. [Accessed: 25-Feb-2019].

Appendix A

PARTICIPANT INFORMATION SHEET

Title: Examine the Accept and Use of Authentication Framework in Public Cloud with EPSB

To participants:

My name is Mohanaad Talal Shakir, I am an Instructor in Information technology department at al Buraimi university college, Oman, and I am PhD student at UNITEN, Malaysis. I am conducting research into authentication accuracy in public cloud computing. We are investigating how computers can support people's needs for examine the usability of authentication with a part of exploring these ideas is involving potential 'ordinary' users in the design, usability testing and evaluation of the prototype applications. In this questionnaire we need to examine the effects of security procedures in EPSB on usability of system.

You are invited to participate in our research and we would appreciate any assistance you can offer us, although you are under no obligation to do so.

Participation involves one visit to our laboratory at Alburaimi University College (BUC), for approximately 60 minutes daily. If you agree to participate, you may be asked to perform a number of tasks on paper or using a computer. The tasks will be fully explained and demonstrated. You will be asked to login and using our public cloud computing. The activities you undertake and the time you spend working on each task will be recorded together with authentication system. You will be asked fill in a short questionnaire on your experience.

All the questionnaire information you provide will remain anonymous. The digital recordings, with your specific consent, may be used in research reports on this project. You choose whether your recordings are used or not on the consent form. Your consent form will be held in a secure file for 6 years, at the end of this time it will be properly disposed of. Your name will not be used in any reports arising from this study. The information collected during this study may be used in future analysis and publications and will be kept indefinitely. When it is no longer required all copies of the data will be destroyed. At the conclusion of the study, a summary of the findings will be available from the researchers upon request.

If you don't want to participate, you don't have to give any reason for your decision. If you do participate, you may withdraw at any time during the session and you can also ask for the information you have provided to be withdrawn at any time until one week after the conclusion of your session, without explanation and without penalty, by contacting me (details below). If you are a student at Alburaimi University College (BUC) choosing not to participate, or to withdraw yourself or your information, your grades or academic relationships with the University or members of staff will not be affected.

If you agree to participate in this study, please first complete the consent form attached to this information sheet. Your consent form will be kept separately from your questionnaire data so that no-one will be able to identify your answers from the information you provide.

Thank you very much for your time and help in making this study possible. If you have any questions at any time you can phone me (0096891990794) or the Head of Department, Professor Sohail Iqbal (+968 9267 9362), or you can write to us at email: **mohanaad@buc.edu.om**

Questionnaire Objectives: Examine security, accept and use in the authentication process.

INTRODUCTION

This questionnaire is conducted by a Mohanaad Talal Shakir for gathering information about validating an authentication system in cloud computing. To ensure the validity, we are taking some experts opinion in some aspects to examine usability, security, efficiency, and privacy of the system.

System's features:

- Prevent data which have been classified, sensitive, very high, high, intermediate from suspicious users;
- Prevent whole data from unauthorized users;
- Upload data safely in cloud computing;
- Monitoring whole system accounts;

The system provides some mechanisms that enhance authority performance on the system side, such as data uploading on the public cloud, determining and saving keys and a mechanism for active penetration accounts. On the user's hand, the system classifies data into three main types which are: sensitive, semi- sensitive and normal. The core of authority is to divide users also into three classifications according to data levels. Each user has some boundaries to data according to its level in the system. They also classified as legal, illegal and suspicious so the system can take the right procedure to the actions of each one of them.

Mohanaad Talal Shakir

This questionnaire has been approved by Alburaimi University College, Information technology

Associated Professor
Dr. Bahaaeddin Ali
Head of English Dept.
Linguistic Expert

Associated Professor
Dr. Sohail Iqbal
Head of Information
Technology Dept.
Information Technology Expert

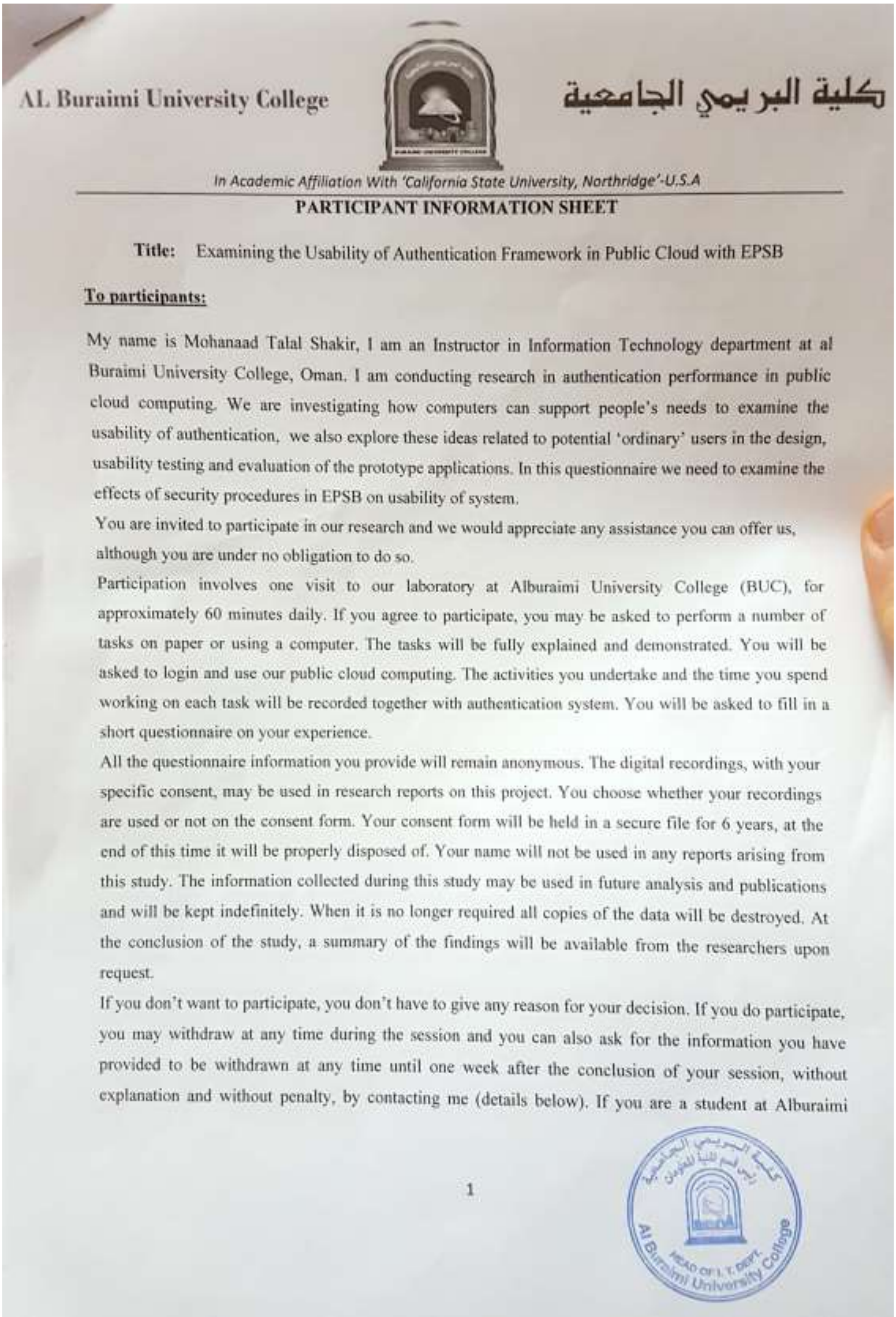
Associated Professor
Dr. Roy Mathew
Coordinator of Software
Engineering
Information Technology Expert

Associated Professor
Dr. Mohammed Al Kaabi
Information Technology
Dept.
Information Technology

No.	**Perceived Usefulness**			
PU1	The EPSB enhances my authentication efficiency.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PU2	The EPSB algorithm enhances authentication productivity.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PU3	The EPSB algorithm enables me to accomplish authentication tasks quickly.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PU4	The EPSB algorithm improves authentication accuracy .			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PU5	The EPSB algorithm saves my time.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PU6	The EPSB algorithm has many distinctive useful features.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PU7	The EPSB algorithm is applicable with authentication process			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
	Perceived Ease of Use			
PE1	The EPSB algorithm in authentication is easy to use.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PE2	The EPSB algorithm enables me to access the data which saved in public cloud computing smoothly.			

Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PE3	The EPSB algorithm is convenient and user-friendly.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PE4	User no need to memorize complicated password in EPSB algorithm process.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PE5	The EPSB algorithm is no needs to memorize some secrets procedures			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PE6	The EPSB authentication procedure is not complicated to the user			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
PE7	The EPSB algorithm requires no training.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Behavioral Intention to Use				
BI1	I intend to increase my use of the EPSB algorithm.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
BI2	It is worth to recommend the EPSB algorithm for other organizations.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
BI3	I’m interested to use the EPSB algorithm more frequently in the future.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**

Actual System Use				
AU1	I use the EPSB algorithm on daily basis.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
AU2	I use the EPSB algorithm frequently.			
Strongly agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**



AL Buraimi University College

كلية البريمي الجامعية

In Academic Affiliation With 'California State University, Northridge'-U.S.A

PARTICIPANT INFORMATION SHEET

Title: Examining the Usability of Authentication Framework in Public Cloud with EPSB

To participants:

My name is Mohanaad Talal Shakir, I am an Instructor in Information Technology department at al Buraimi University College, Oman. I am conducting research in authentication performance in public cloud computing. We are investigating how computers can support people's needs to examine the usability of authentication, we also explore these ideas related to potential 'ordinary' users in the design, usability testing and evaluation of the prototype applications. In this questionnaire we need to examine the effects of security procedures in EPSB on usability of system.

You are invited to participate in our research and we would appreciate any assistance you can offer us, although you are under no obligation to do so.

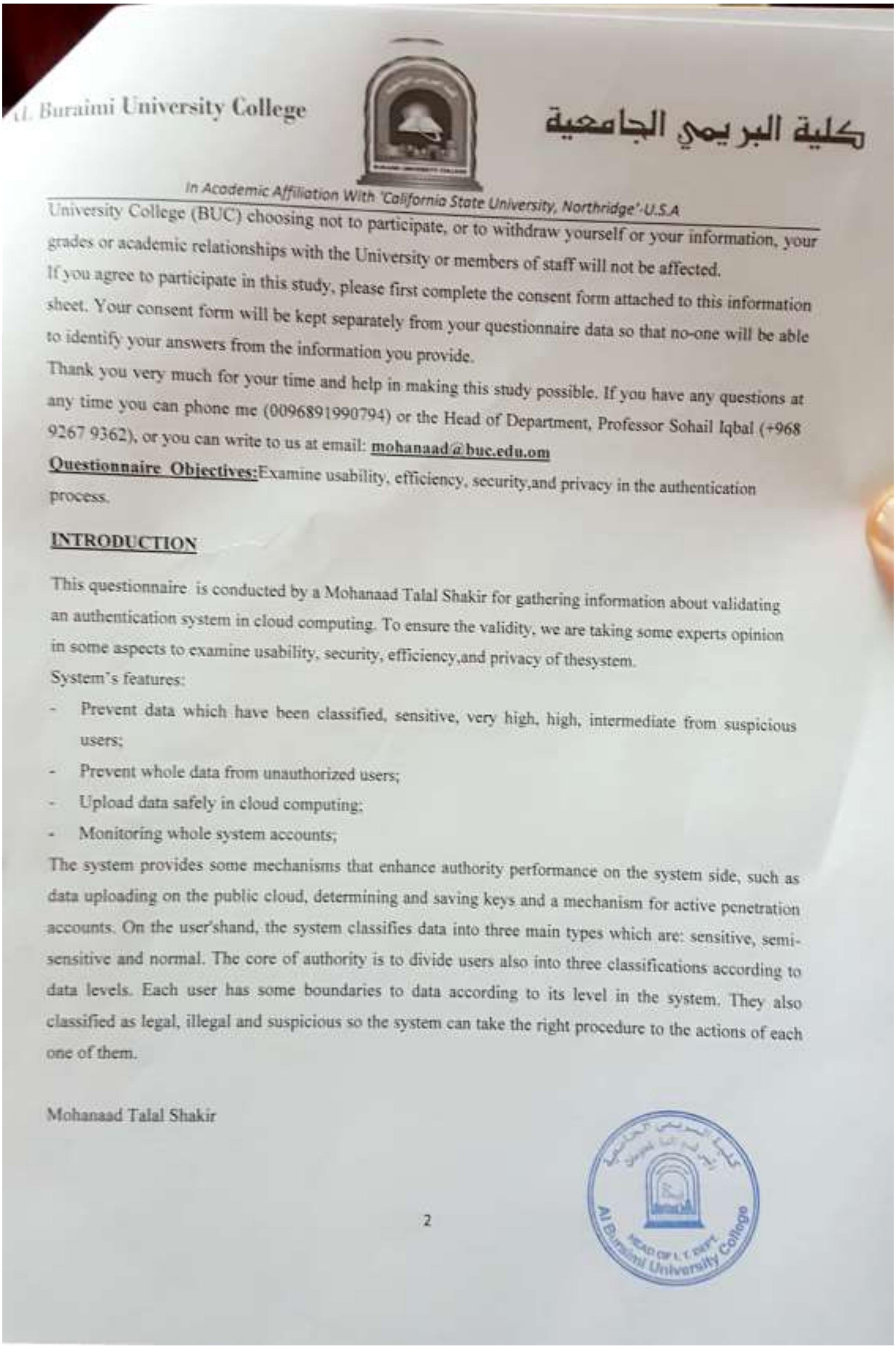
Participation involves one visit to our laboratory at Alburaimi University College (BUC), for approximately 60 minutes daily. If you agree to participate, you may be asked to perform a number of tasks on paper or using a computer. The tasks will be fully explained and demonstrated. You will be asked to login and use our public cloud computing. The activities you undertake and the time you spend working on each task will be recorded together with authentication system. You will be asked to fill in a short questionnaire on your experience.

All the questionnaire information you provide will remain anonymous. The digital recordings, with your specific consent, may be used in research reports on this project. You choose whether your recordings are used or not on the consent form. Your consent form will be held in a secure file for 6 years, at the end of this time it will be properly disposed of. Your name will not be used in any reports arising from this study. The information collected during this study may be used in future analysis and publications and will be kept indefinitely. When it is no longer required all copies of the data will be destroyed. At the conclusion of the study, a summary of the findings will be available from the researchers upon request.

If you don't want to participate, you don't have to give any reason for your decision. If you do participate, you may withdraw at any time during the session and you can also ask for the information you have provided to be withdrawn at any time until one week after the conclusion of your session, without explanation and without penalty, by contacting me (details below). If you are a student at Alburaimi

1

كلية البريمي الجامعية
رئيس قسم تقنية المعلومات
HEAD OF I.T. DEPT.
Al Buraimi University College



Al Buraimi University College

كلية البريمي الجامعية

In Academic Affiliation With 'California State University, Northridge'-U.S.A

University College (BUC) choosing not to participate, or to withdraw yourself or your information, your grades or academic relationships with the University or members of staff will not be affected.

If you agree to participate in this study, please first complete the consent form attached to this information sheet. Your consent form will be kept separately from your questionnaire data so that no-one will be able to identify your answers from the information you provide.

Thank you very much for your time and help in making this study possible. If you have any questions at any time you can phone me (0096891990794) or the Head of Department, Professor Sohail Iqbal (+968 9267 9362), or you can write to us at email: **mohanaad@buc.edu.om**

Questionnaire Objectives: Examine usability, efficiency, security,and privacy in the authentication process.

INTRODUCTION

This questionnaire is conducted by a Mohanaad Talal Shakir for gathering information about validating an authentication system in cloud computing. To ensure the validity, we are taking some experts opinion in some aspects to examine usability, security, efficiency,and privacy of thesystem.

System's features:

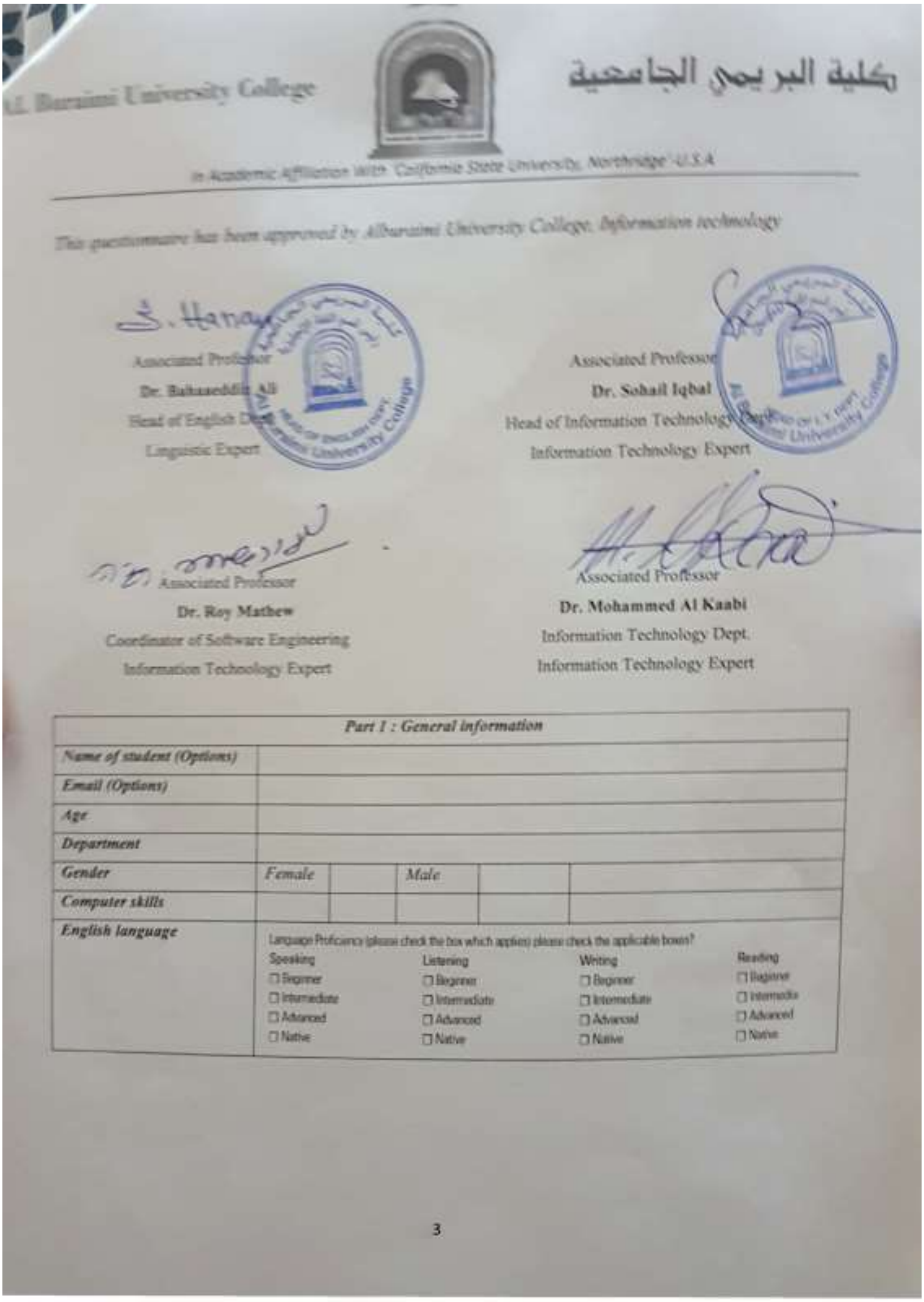
- Prevent data which have been classified, sensitive, very high, high, intermediate from suspicious users;
- Prevent whole data from unauthorized users;
- Upload data safely in cloud computing;
- Monitoring whole system accounts;

The system provides some mechanisms that enhance authority performance on the system side, such as data uploading on the public cloud, determining and saving keys and a mechanism for active penetration accounts. On the user'shand, the system classifies data into three main types which are: sensitive, semi-sensitive and normal. The core of authority is to divide users also into three classifications according to data levels. Each user has some boundaries to data according to its level in the system. They also classified as legal, illegal and suspicious so the system can take the right procedure to the actions of each one of them.

Mohanaad Talal Shakir

HEAD OF I.T. DEPT.
Al Buraimi University College

2



Al Buraimi University College

كلية البريمي الجامعية

In Academic Affiliation With "California State University, Northridge"-U.S.A

This questionnaire has been approved by Alburaimi University College, Information technology

Associated Professor
Dr. Bahaaeddin Ali
Head of English Dept.
Linguistic Expert

HEAD OF ENGLISH DEPT.
Al Buraimi University College

Associated Professor
Dr. Sohail Iqbal
Head of Information Technology Dept.
Information Technology Expert

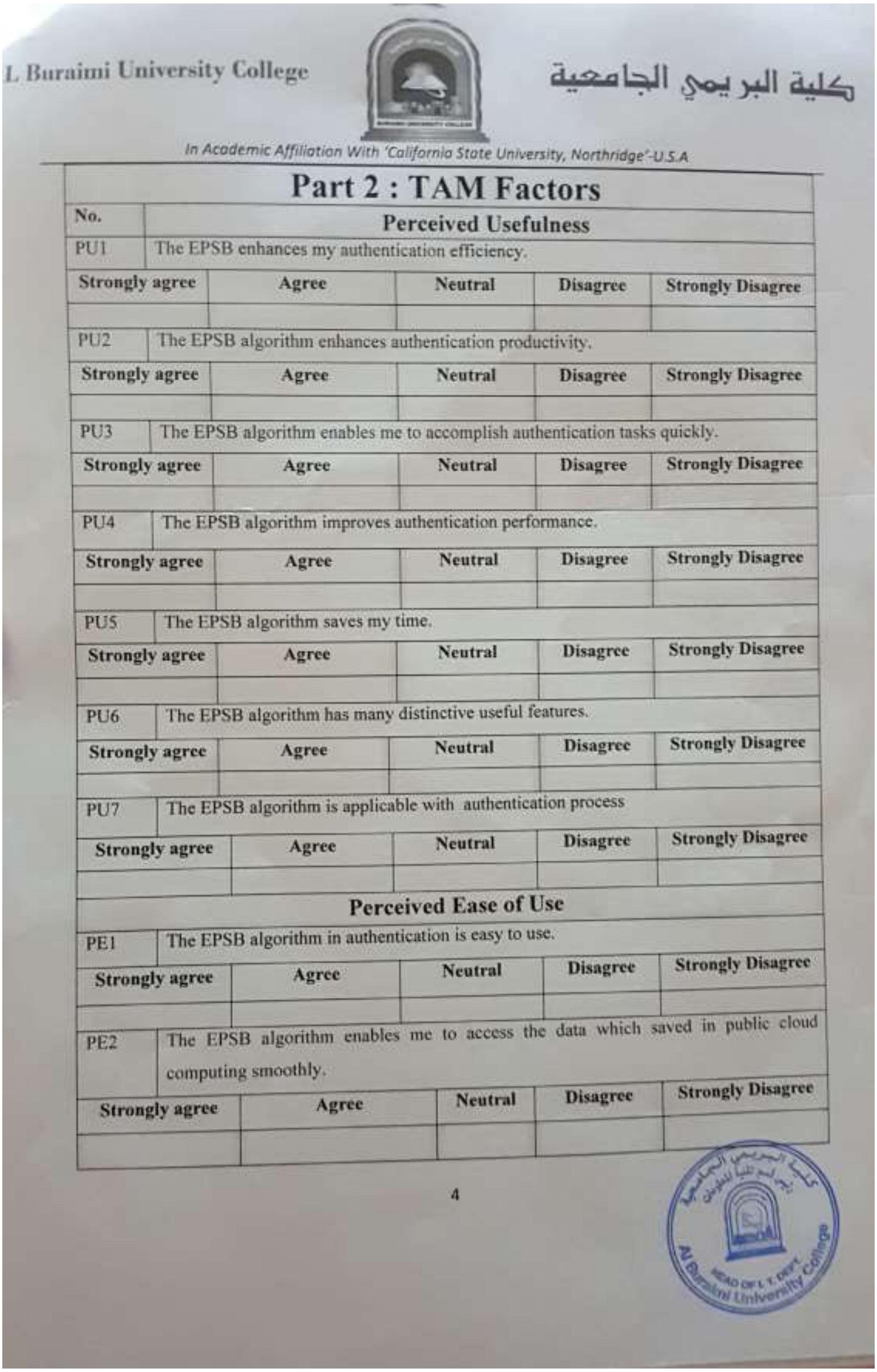
HEAD OF I.T. DEPT.
Al Buraimi University College

Associated Professor
Dr. Roy Mathew
Coordinator of Software Engineering
Information Technology Expert

Associated Professor
Dr. Mohammed Al Kaabi
Information Technology Dept.
Information Technology Expert

Part 1 : General information					
Name of student (Options)					
Email (Options)					
Age					
Department					
Gender	*Female*		*Male*		
Computer skills					
English language	Language Proficiency (please check the box which applies) please check the applicable boxes? Speaking □ Beginner □ Intermediate □ Advanced □ Native	Listening □ Beginner □ Intermediate □ Advanced □ Native		Writing □ Beginner □ Intermediate □ Advanced □ Native	Reading □ Beginner □ Intermedia □ Advanced □ Native

3



L Buraimi University College كلية البريمي الجامعية

In Academic Affiliation With 'California State University, Northridge'-U.S.A

Part 2 : TAM Factors

No.	Perceived Usefulness
PU1	The EPSB enhances my authentication efficiency.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PU2	The EPSB algorithm enhances authentication productivity.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PU3	The EPSB algorithm enables me to accomplish authentication tasks quickly.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PU4	The EPSB algorithm improves authentication performance.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PU5	The EPSB algorithm saves my time.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PU6	The EPSB algorithm has many distinctive useful features.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PU7	The EPSB algorithm is applicable with authentication process

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

	Perceived Ease of Use
PE1	The EPSB algorithm in authentication is easy to use.

Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

PE2	The EPSB algorithm enables me to access the data which saved in public cloud computing smoothly.

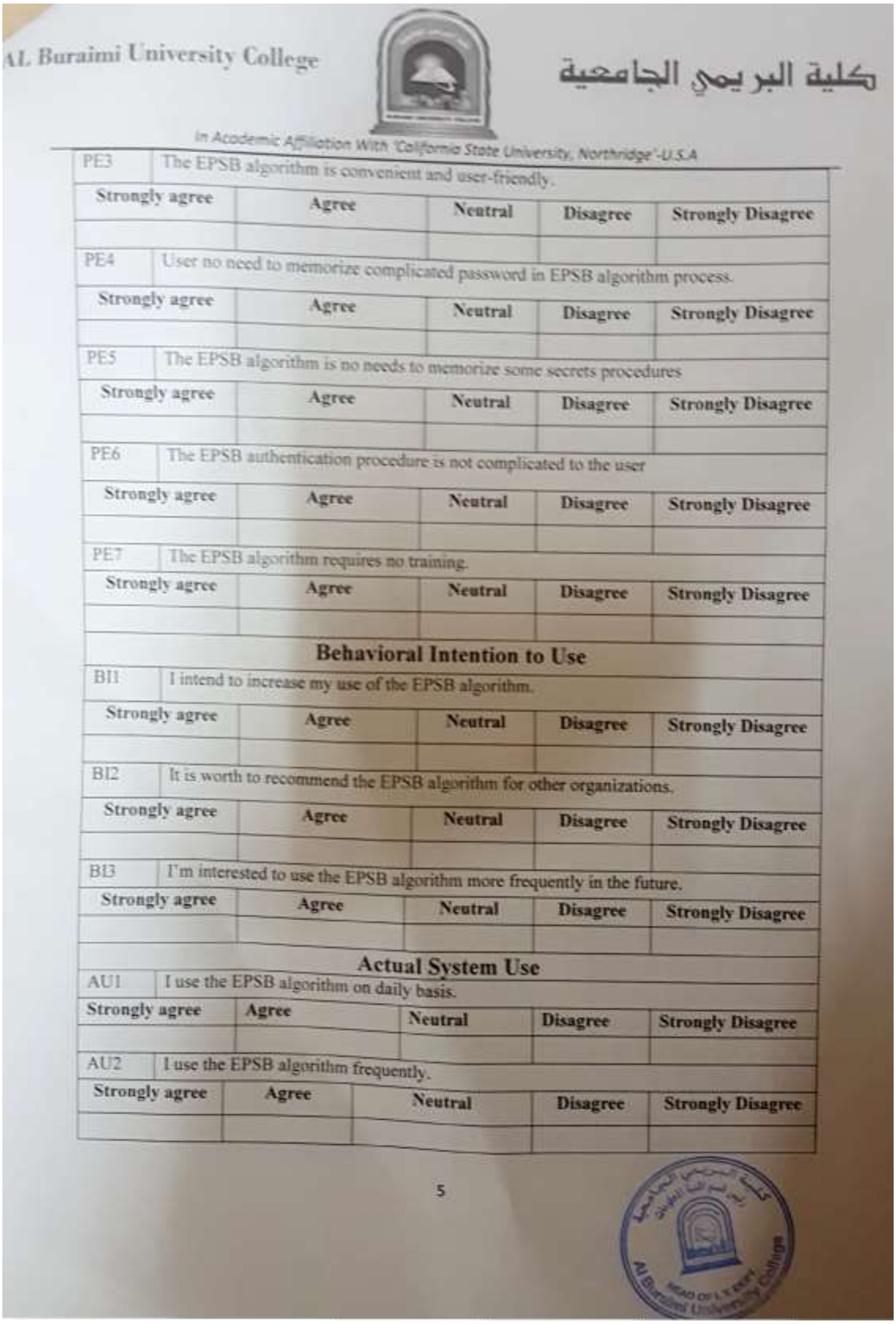
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

4

كلية البريمي الجامعية

HEAD OF I.T. DEPT.

Al Buraimi University College



PE3	The EPSB algorithm is convenient and user-friendly.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
PE4	User no need to memorize complicated password in EPSB algorithm process.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
PE5	The EPSB algorithm is no needs to memorize some secrets procedures			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
PE6	The EPSB authentication procedure is not complicated to the user			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
PE7	The EPSB algorithm requires no training.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
	Behavioral Intention to Use			
BI1	I intend to increase my use of the EPSB algorithm.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
BI2	It is worth to recommend the EPSB algorithm for other organizations.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
BI3	I'm interested to use the EPSB algorithm more frequently in the future.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
	Actual System Use			
AU1	I use the EPSB algorithm on daily basis.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree
AU2	I use the EPSB algorithm frequently.			
Strongly agree	Agree	Neutral	Disagree	Strongly Disagree

5

كلية البريمي الجامعية
HEAD OF I.T. DEPT
Al Buraimi University College

Appendix B

Accept and Use Results

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	4	100.0
	Excluded[a]	0	.0
	Total	4	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.727	.732	2

Inter-Item Correlation Matrix

	AU1	AU2
AU1	1.000	.577
AU2	.577	1.000

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
AU1	1.7500	.250	.577	.333	.
AU2	1.5000	.333	.577	.333	.

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	4	100.0
	Excluded[a]	0	.0
	Total	4	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.875	.884	3

Inter-Item Correlation Matrix

	BI1	BI2	B13
BI1	1.000	.577	.577
BI2	.577	1.000	1.000
B13	.577	1.000	1.000

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
BI1	3.5000	1.000	.577	.	1.000
BI2	3.2500	.917	.870	.	.727
B13	3.2500	.917	.870	.	.727

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	4	100.0
	Excluded[a]	0	.0
	Total	4	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.739	.741	5

Inter-Item Correlation Matrix

	PE2	PE3	PE4	PE6	PE7
PE2	1.000	.000	-.577	.000	.577
PE3	.000	1.000	.577	1.000	.577
PE4	-.577	.577	1.000	.577	.333
PE6	.000	1.000	.577	1.000	.577
PE7	.577	.577	.333	.577	1.000

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PE2	6.0000	3.333	.000	.	.867
PE3	6.0000	2.000	.816	.	.556
PE4	6.2500	2.917	.293	.	.762
PE6	6.0000	2.000	.816	.	.556
PE7	5.7500	2.250	.778	.	.593

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	4	100.0
	Excluded[a]	0	.0
	Total	4	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.833	.834	7

Inter-Item Correlation Matrix

	PU1	PU2	PU3	PU4	PU5	PU6	PU7
PU1	1.000	.000	.577	1.000	.577	.577	.577
PU2	.000	1.000	.577	.000	.577	.577	-.577
PU3	.577	.577	1.000	.577	1.000	1.000	-.333
PU4	1.000	.000	.577	1.000	.577	.577	.577
PU5	.577	.577	1.000	.577	1.000	1.000	-.333
PU6	.577	.577	1.000	.577	1.000	1.000	-.333
PU7	.577	-.577	-.333	.577	-.333	-.333	1.000

Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
PU1	10.0000	4.667	.802	.	.771
PU2	10.0000	6.000	.236	.	.867
PU3	9.7500	4.917	.827	.	.773
PU4	10.0000	4.667	.802	.	.771
PU5	9.7500	4.917	.827	.	.773
PU6	9.7500	4.917	.827	.	.773
PU7	9.7500	6.917	-.063	.	.896

Appendix C

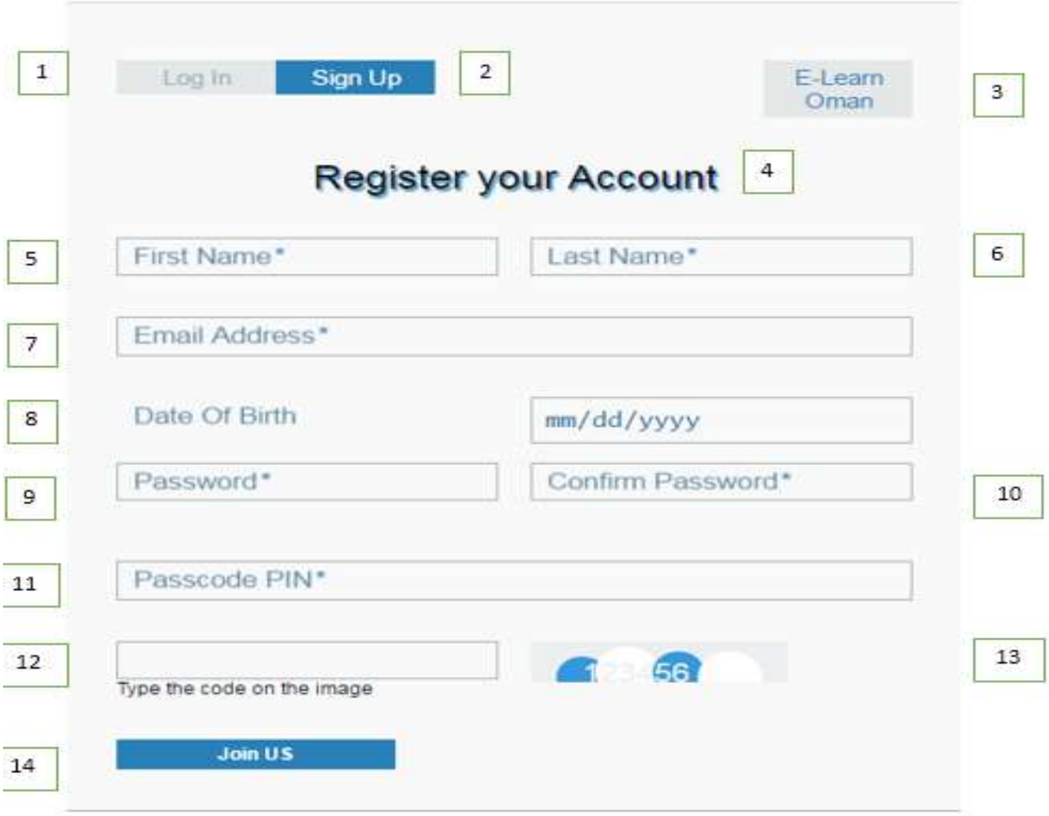
Authentication Interface

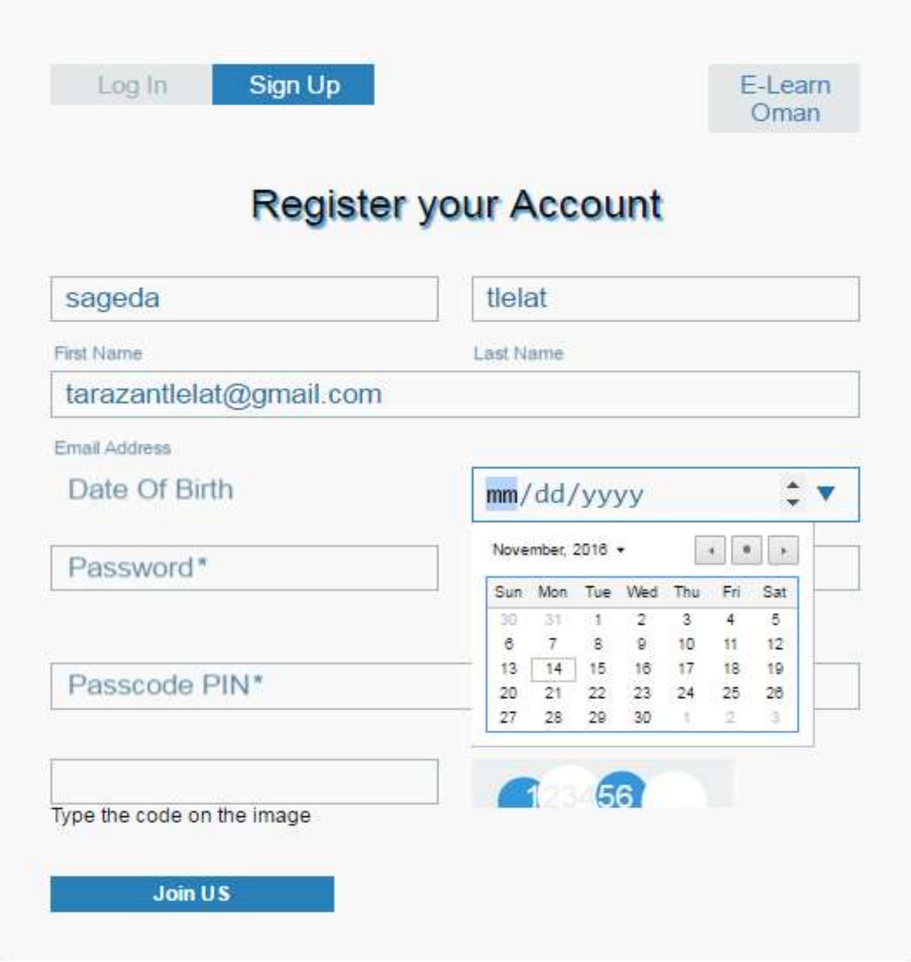
Screen shots

The main sign up page

The first page is for sign up it contain many label which can help you to create new account. By going in detail we will note the following things:

1. Login icon become in dark which tell us it’s not the correct page you are in
2. Sign up icon in blue which is the certain page
3. Logo of system “E-learn oman “
4. Title of page
5. Label which request from user to enter first name
6. Label which request from user to enter last name
7. Label which request from user to enter email address
8. Label which request from user to date of birth
9. Label which request from user to enter password the size is from 6 to 12 and should contain small and capital letter and symbols and number
10. Label which request from user to confirm password
11. Label which request from user to enter passcode pin it should be number from 6 to 8
12. Label which request from user to enter the code in the image beside
13. Label which include code that request from user to enter it to make sure that you are the person how write
14. Input submit button , submit user email and password
15. Input join us button , submit user information





First Name: sageda

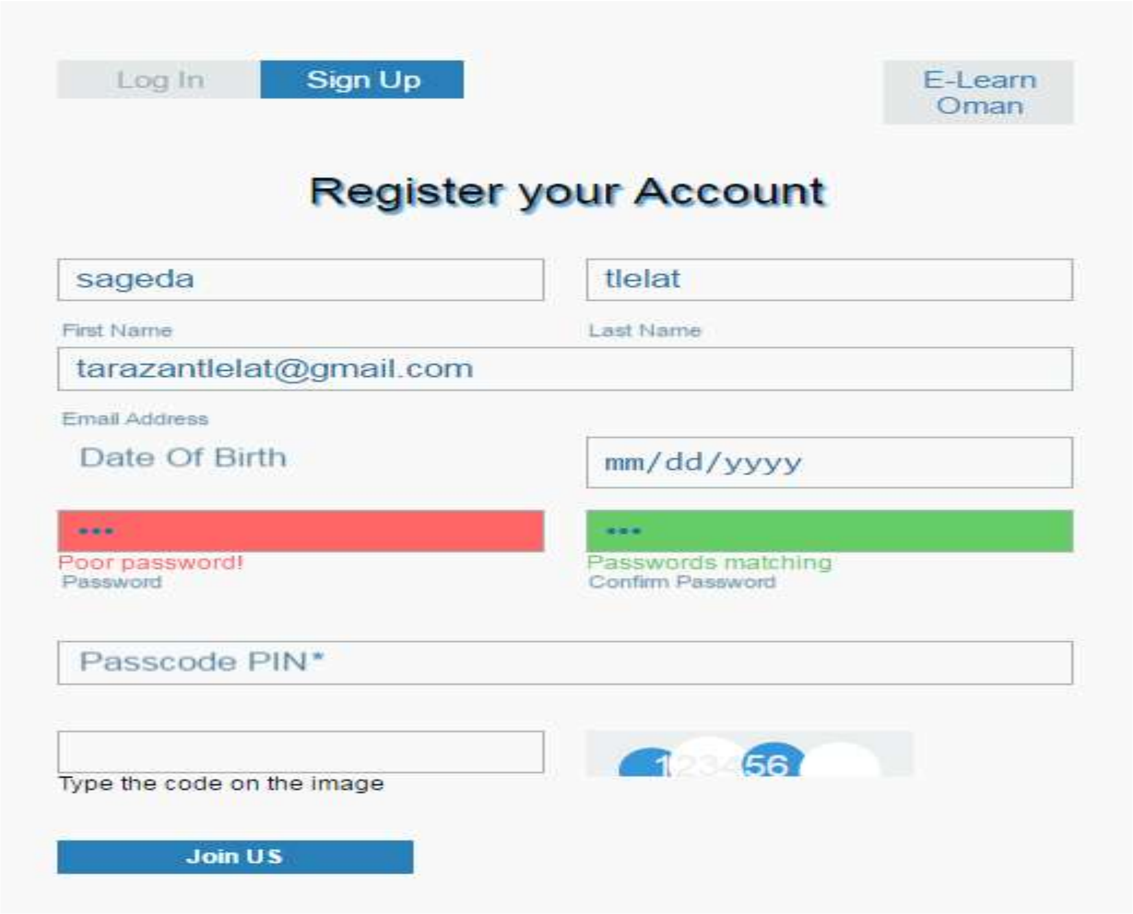
Last Name: tlelat

Email Address: tarazantlelat@gmail.com

Date Of Birth: mm/dd/yyyy

November, 2016

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3



Register your Account

sageda

First Name

tlelat

Last Name

tarazantlelat@gmail.com

Email Address

Date Of Birth

mm/dd/yyyy

•••

Poor password!

Password

•••

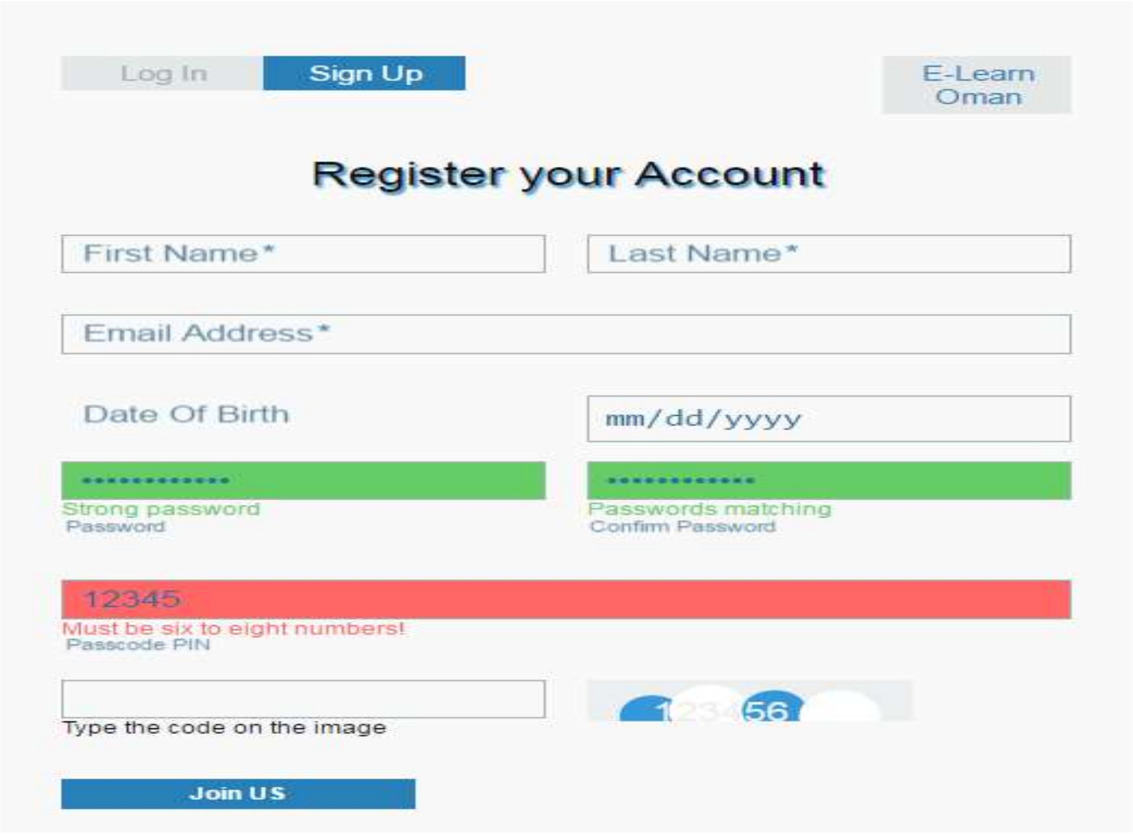
Passwords matching

Confirm Password

Passcode PIN*

Type the code on the image

123456



Register your Account

First Name*

Last Name*

Email Address*

Date Of Birth

mm/dd/yyyy

•••••••••••••

Strong password

Password

••••••••••••

Passwords matching

Confirm Password

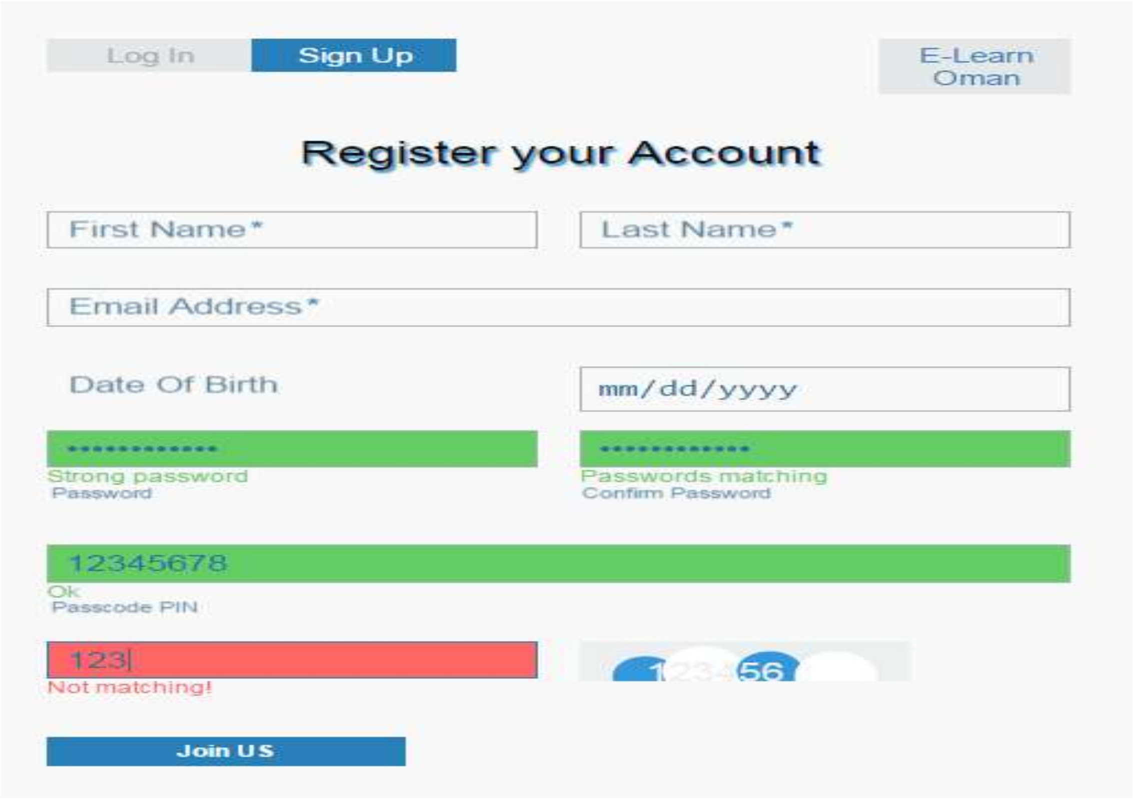
12345

Must be six to eight numbers!

Passcode PIN

Type the code on the image

123456



Register your Account

First Name*

Last Name*

Email Address*

Date Of Birth

mm/dd/yyyy

••••••••••••
Strong password
Password

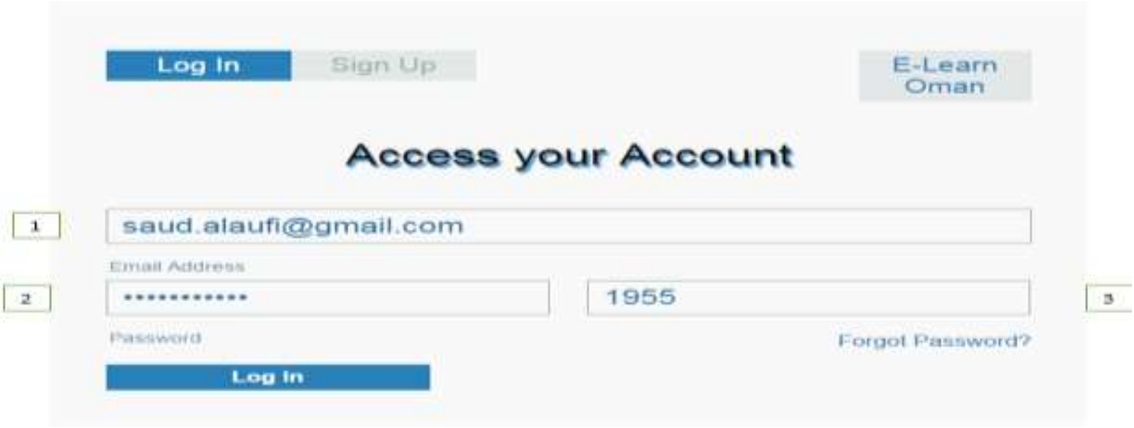
••••••••••••
Passwords matching
Confirm Password

12345678
Ok
Passcode PIN

123
Not matching!

<u>Characteristic of login page</u>

1) When we add email the label title will going down
2) Also the same when entering password the title will going down
3) Here will appear the number which is the speed average of writing password



Access your Account

1

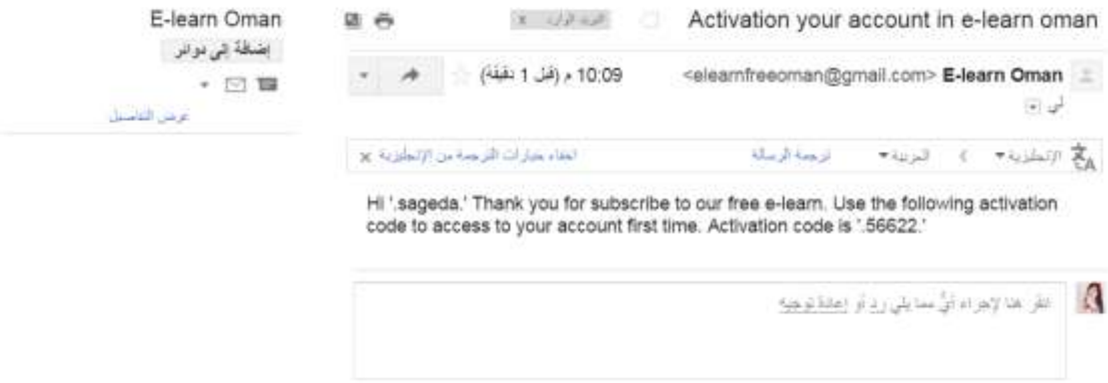
saud.alaufi@gmail.com
Email Address

2

••••••••••••
Password

1955

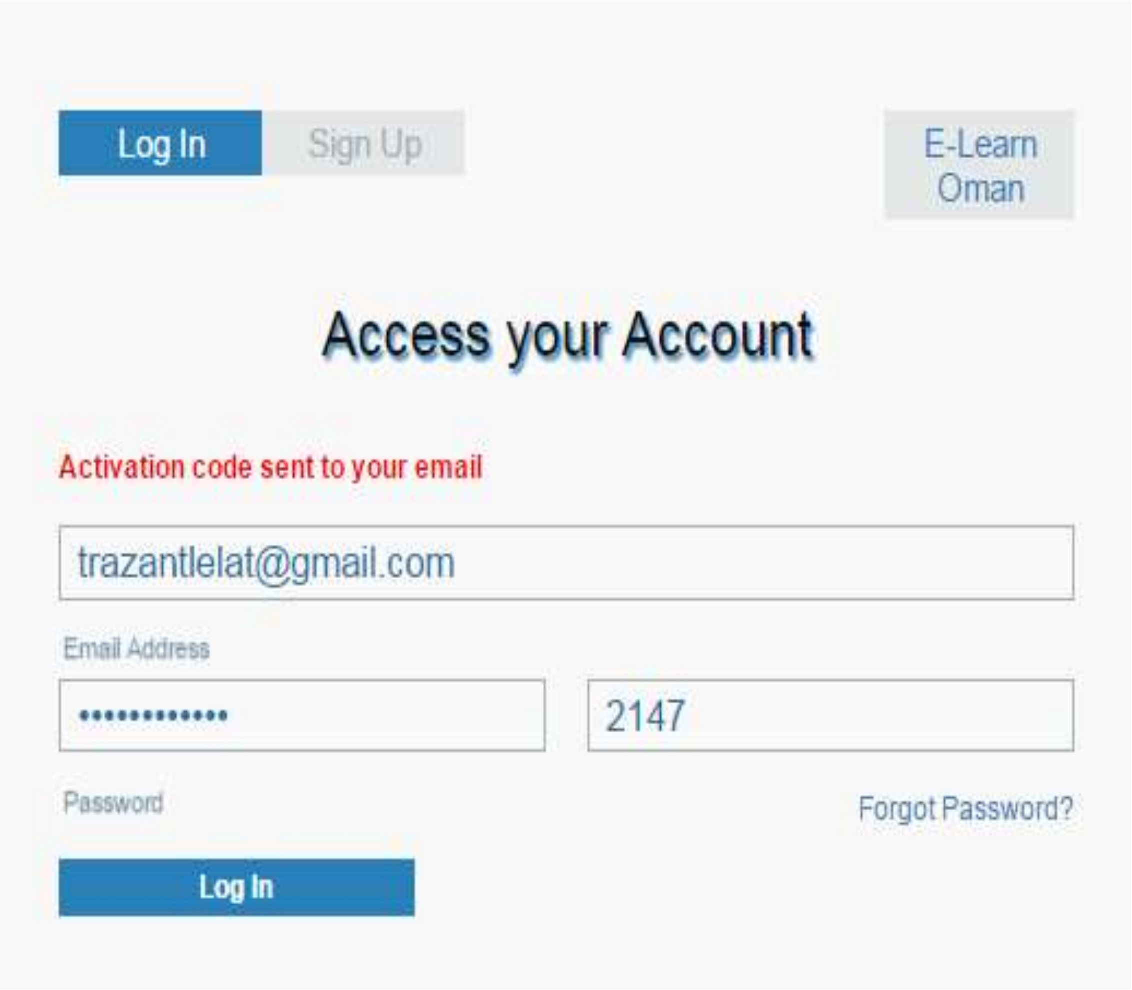
3



Activation your account in e-learn oman

E-learn Oman <elearnfreeoman@gmail.com> 10:09 م (قبل 1 دقيقة)

Hi '.sageda.' Thank you for subscribe to our free e-learn. Use the following activation code to access to your account first time. Activation code is '.56622.'



Access your Account

Activation code sent to your email

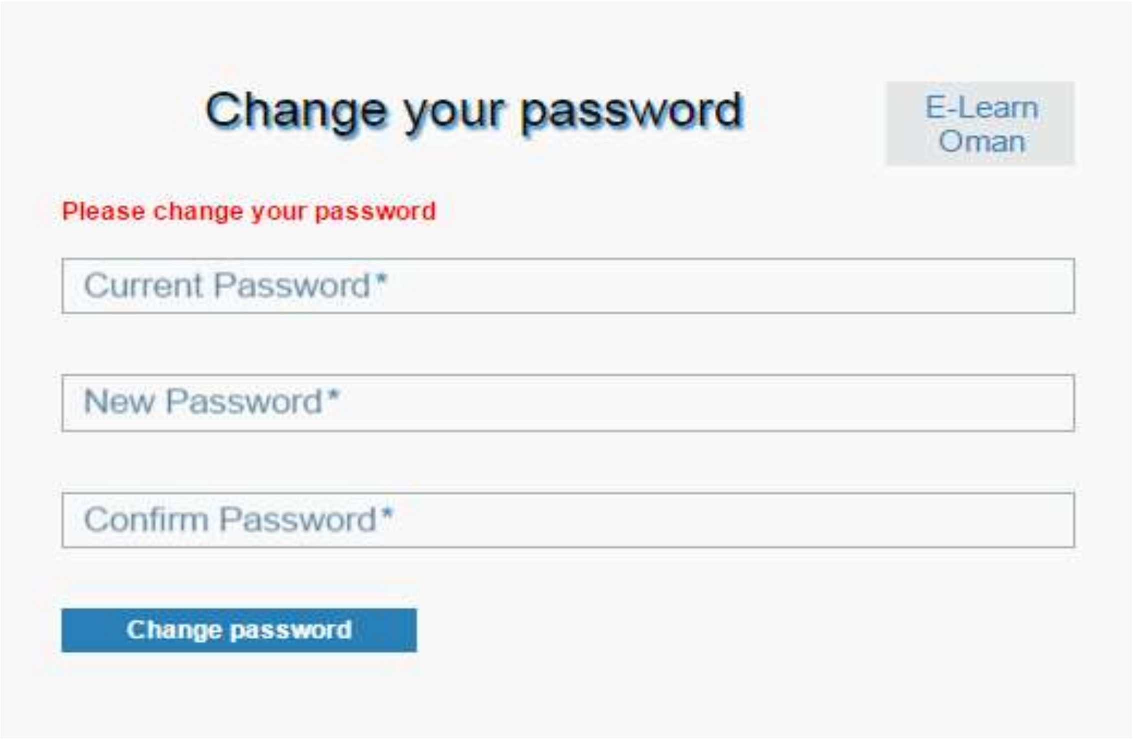
trazantlelat@gmail.com

Email Address

•••••••••••••

2147

Password



Change your password

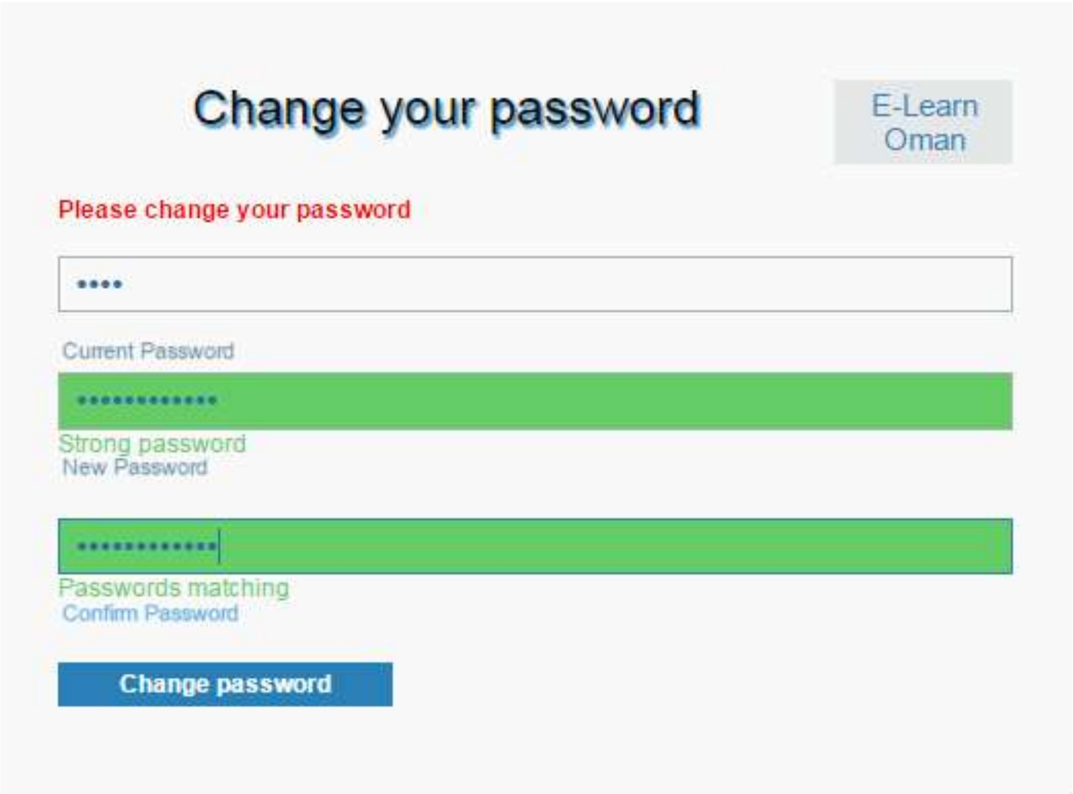
E-Learn Oman

Please change your password

Current Password*

New Password*

Confirm Password*



Change your password

E-Learn Oman

Please change your password

••••

Current Password

•••••••••••••

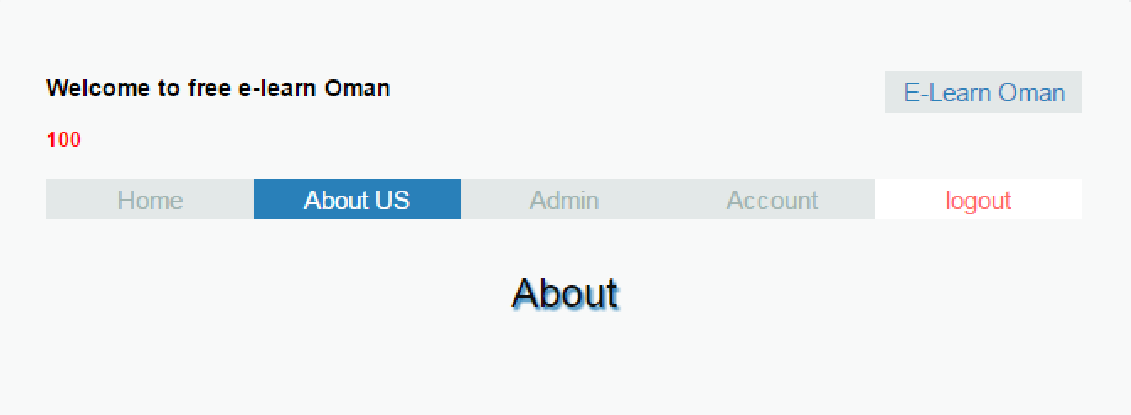
Strong password

New Password

•••••••••••••

Passwords matching

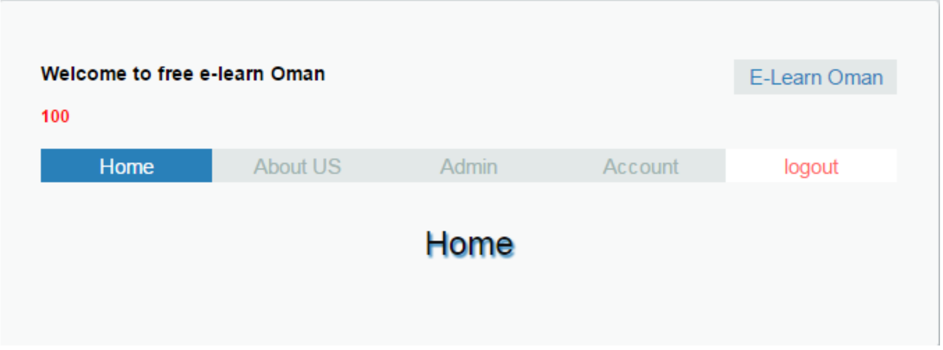
Confirm Password



Welcome to free e-learn Oman

100

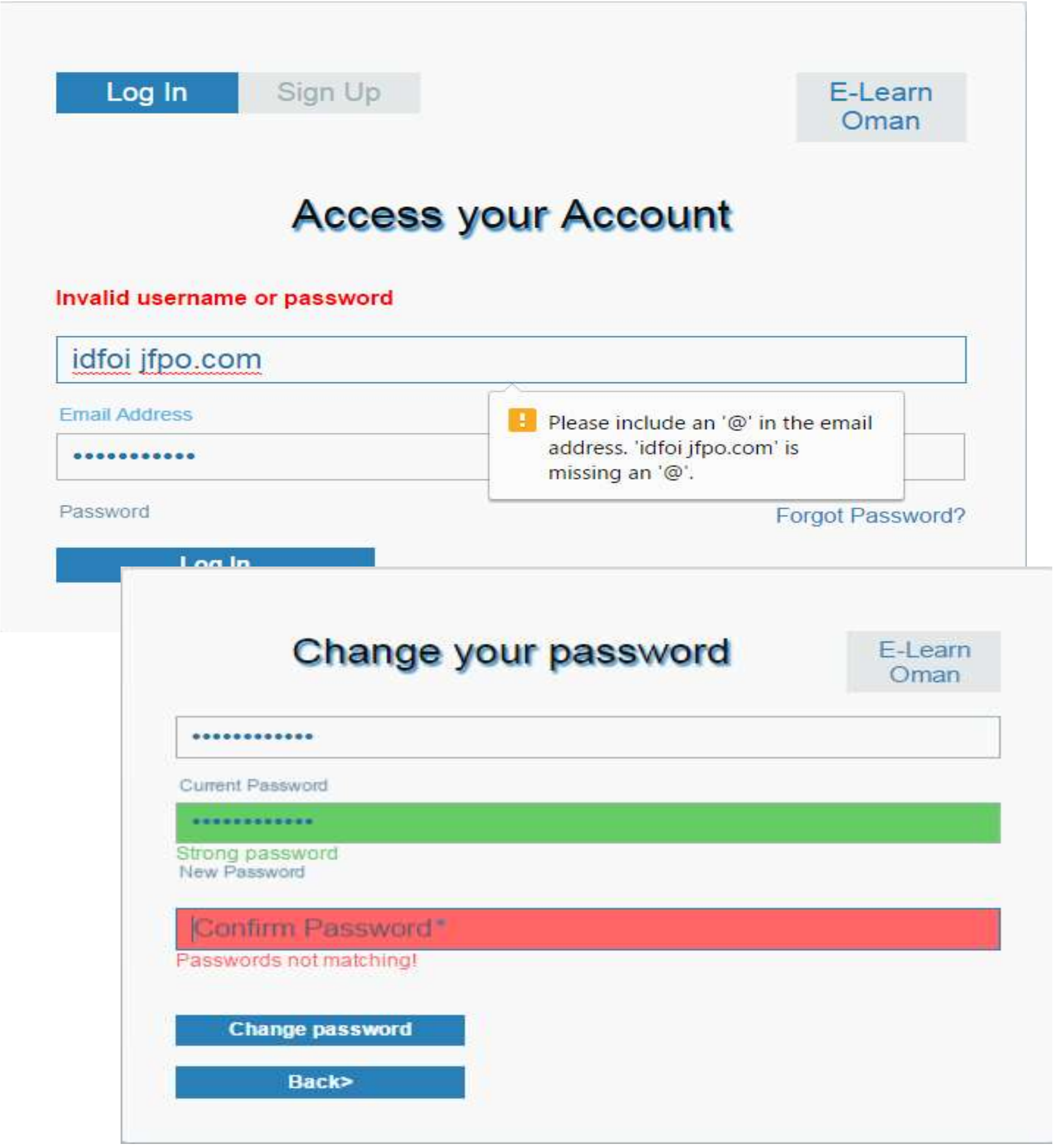
About



Welcome to free e-learn Oman

100

Home



Access your Account

Invalid username or password

Email Address: idfoi jfpo.com

Please include an '@' in the email address. 'idfoi jfpo.com' is missing an '@'.

Password: ●●●●●●●●●●●

Change your password

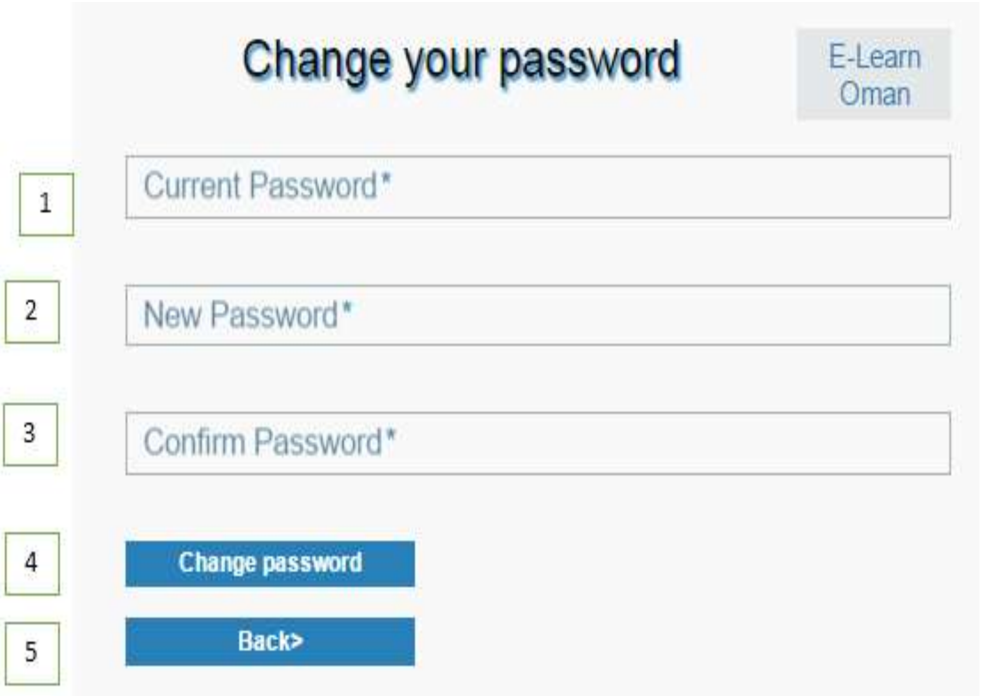
Current Password: ●●●●●●●●●●●●●

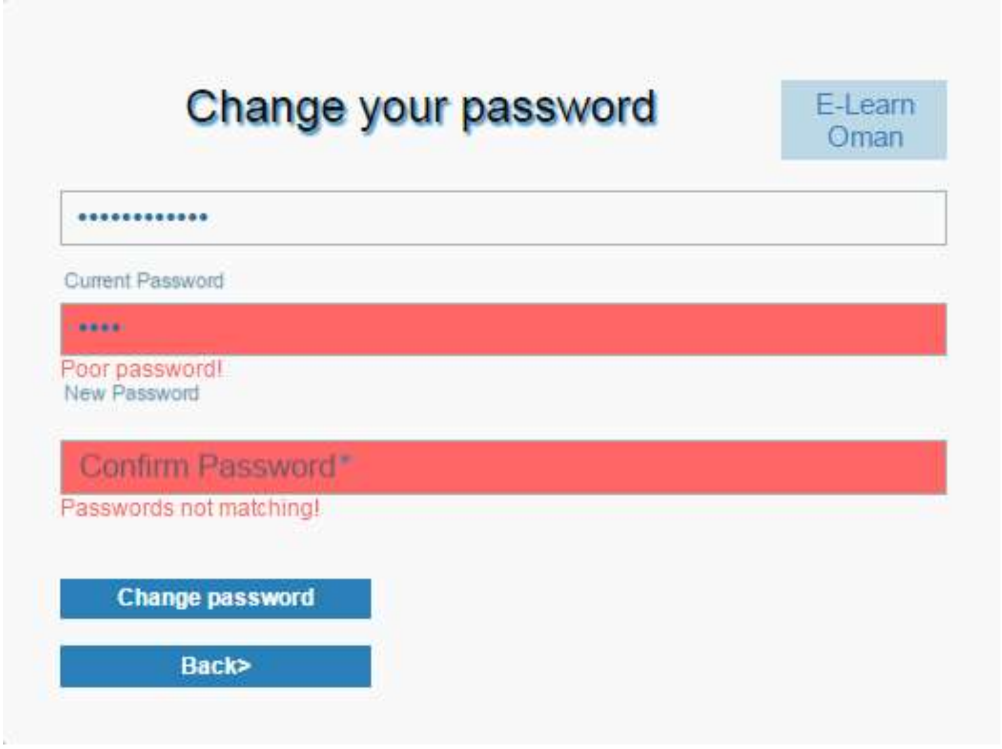
New Password: ●●●●●●●●●●●●●

Strong password

Confirm Password*

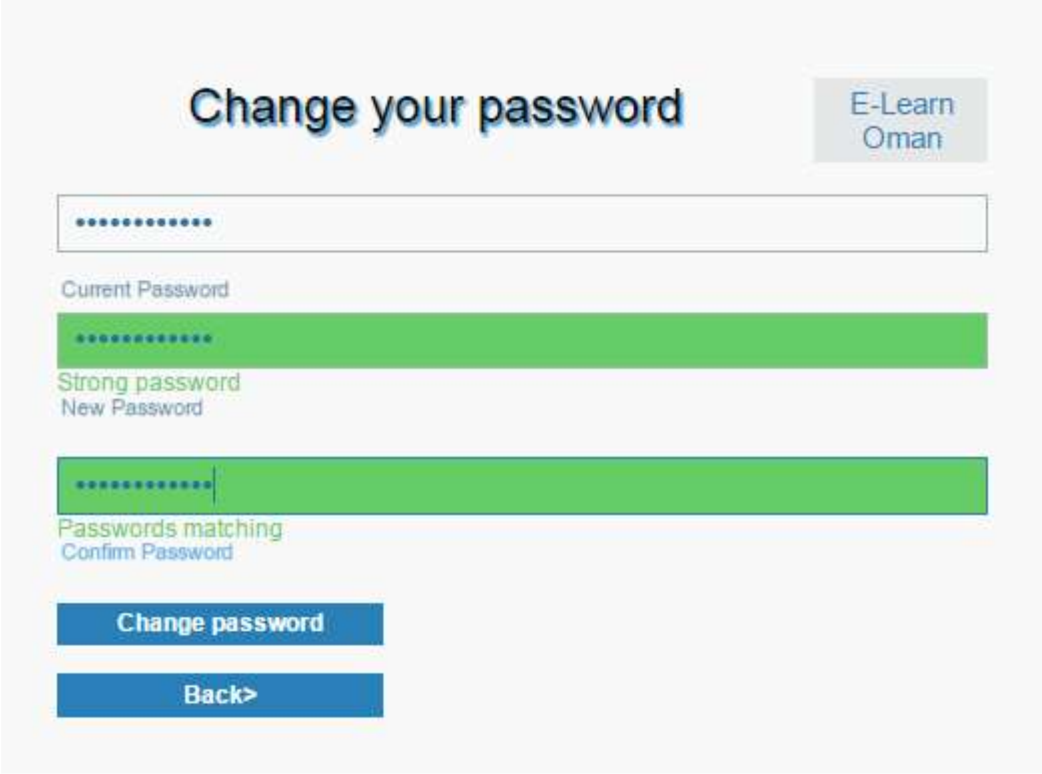
Passwords not matching!





Poor password!

Passwords not matching!



Change your password

E-Learn Oman

•••••••••••••

Current Password

•••••••••••••

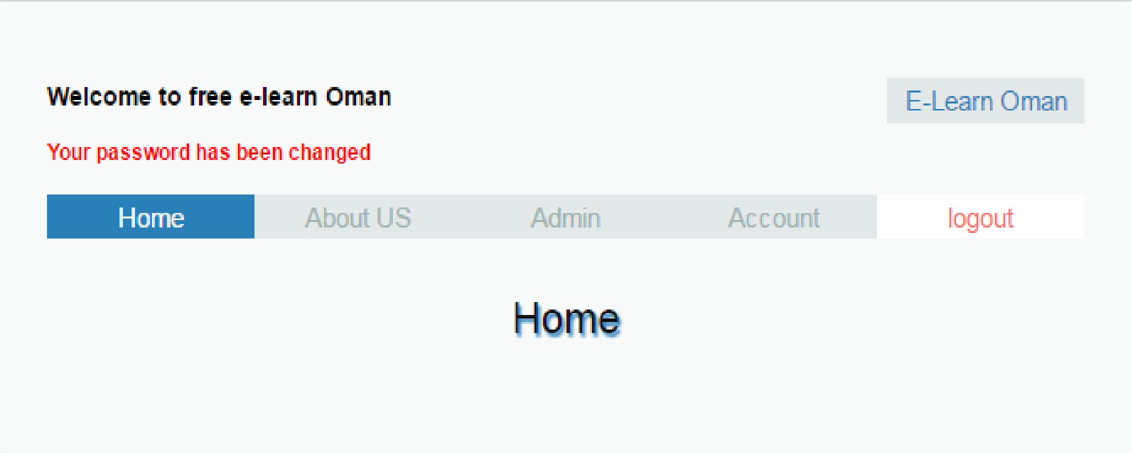
Strong password

New Password

•••••••••••••

Passwords matching

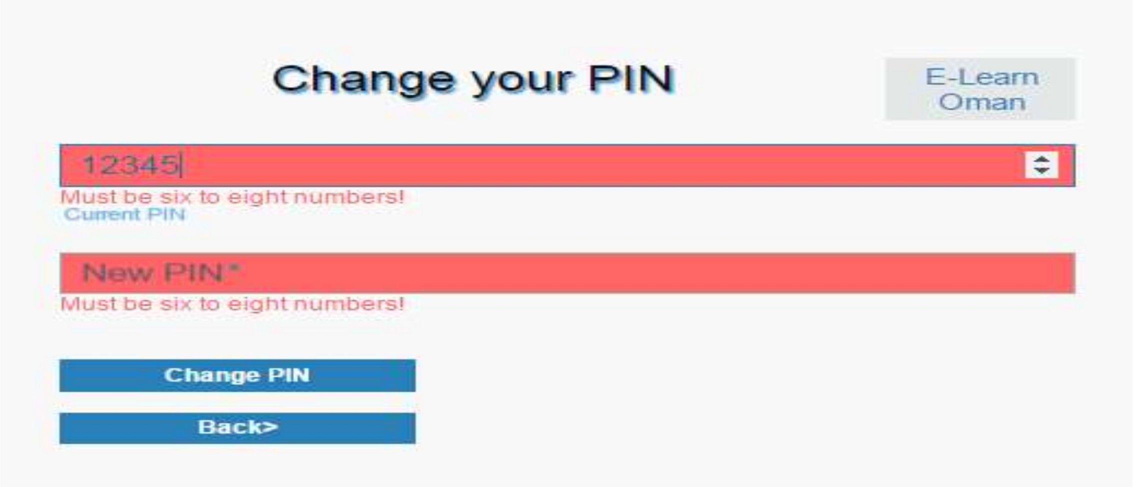
Confirm Password



Welcome to free e-learn Oman

Your password has been changed

Home



Change your PIN

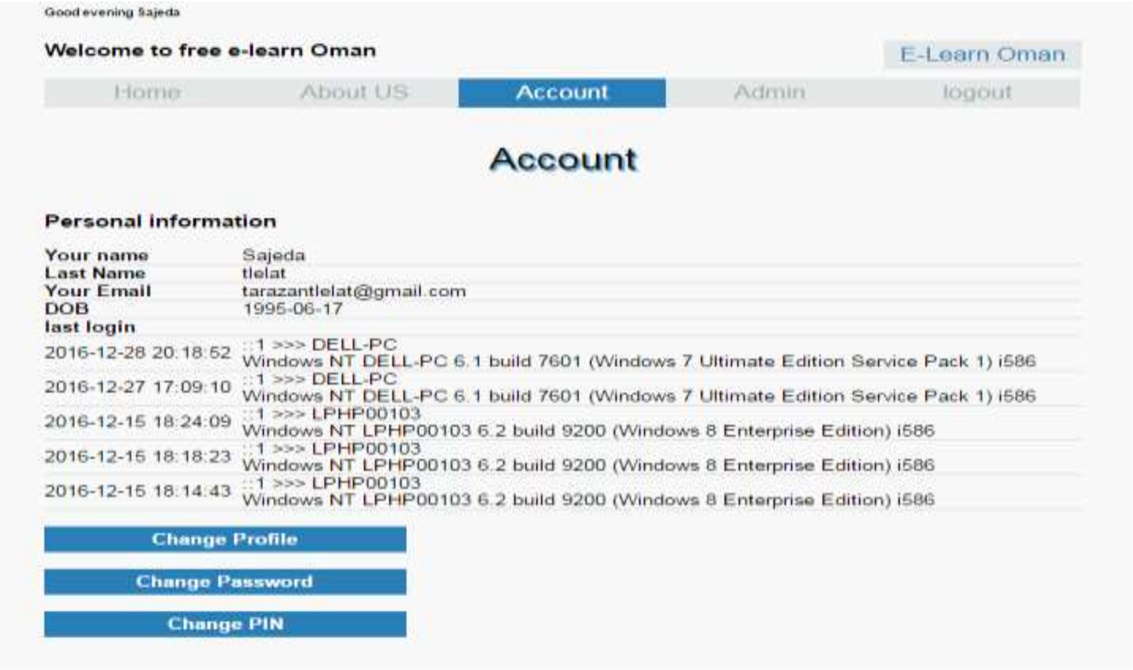
12345

Must be six to eight numbers!

Current PIN

New PIN *

Must be six to eight numbers!



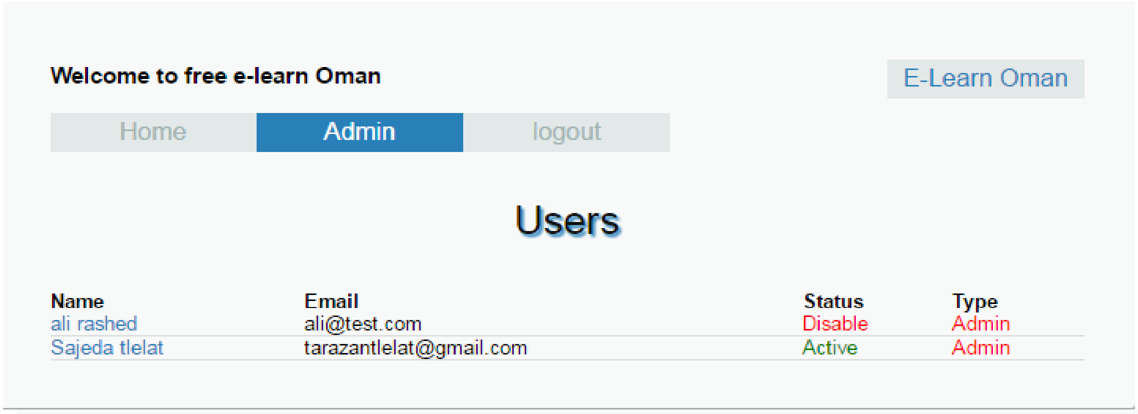
Good evening Sajeda

Welcome to free e-learn Oman

Account

Personal information

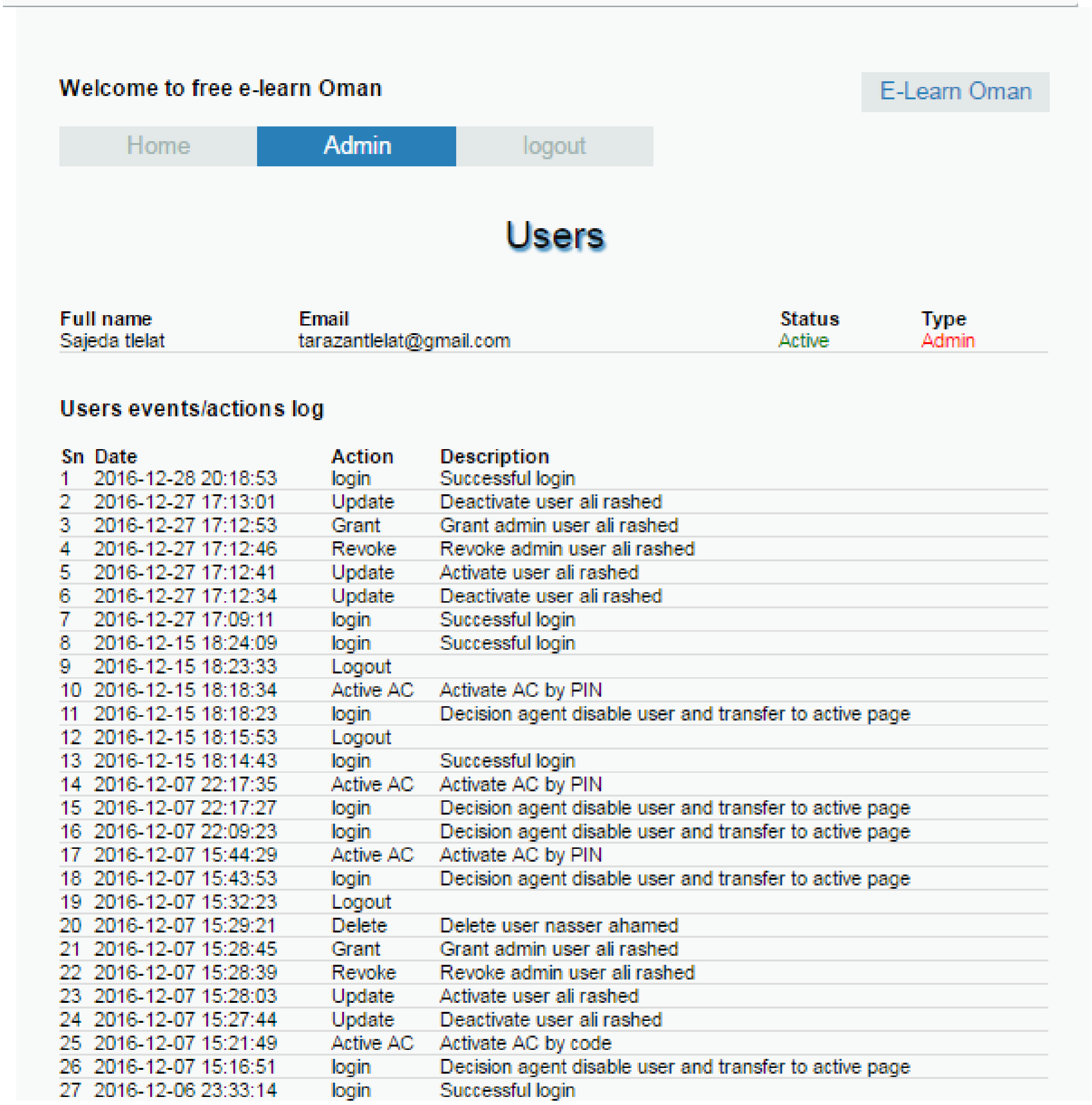
Your name	Sajeda
Last Name	tlelat
Your Email	tarazantlelat@gmail.com
DOB	1995-06-17
last login	
2016-12-28 20:18:52	::1 >>> DELL-PC Windows NT DELL-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586
2016-12-27 17:09:10	::1 >>> DELL-PC Windows NT DELL-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586
2016-12-15 18:24:09	::1 >>> LPHP00103 Windows NT LPHP00103 6.2 build 9200 (Windows 8 Enterprise Edition) i586
2016-12-15 18:18:23	::1 >>> LPHP00103 Windows NT LPHP00103 6.2 build 9200 (Windows 8 Enterprise Edition) i586
2016-12-15 18:14:43	::1 >>> LPHP00103 Windows NT LPHP00103 6.2 build 9200 (Windows 8 Enterprise Edition) i586



Welcome to free e-learn Oman

Users

Name	Email	Status	Type
ali rashed	ali@test.com	Disable	Admin
Sajeda tlelat	tarazantlelat@gmail.com	Active	Admin



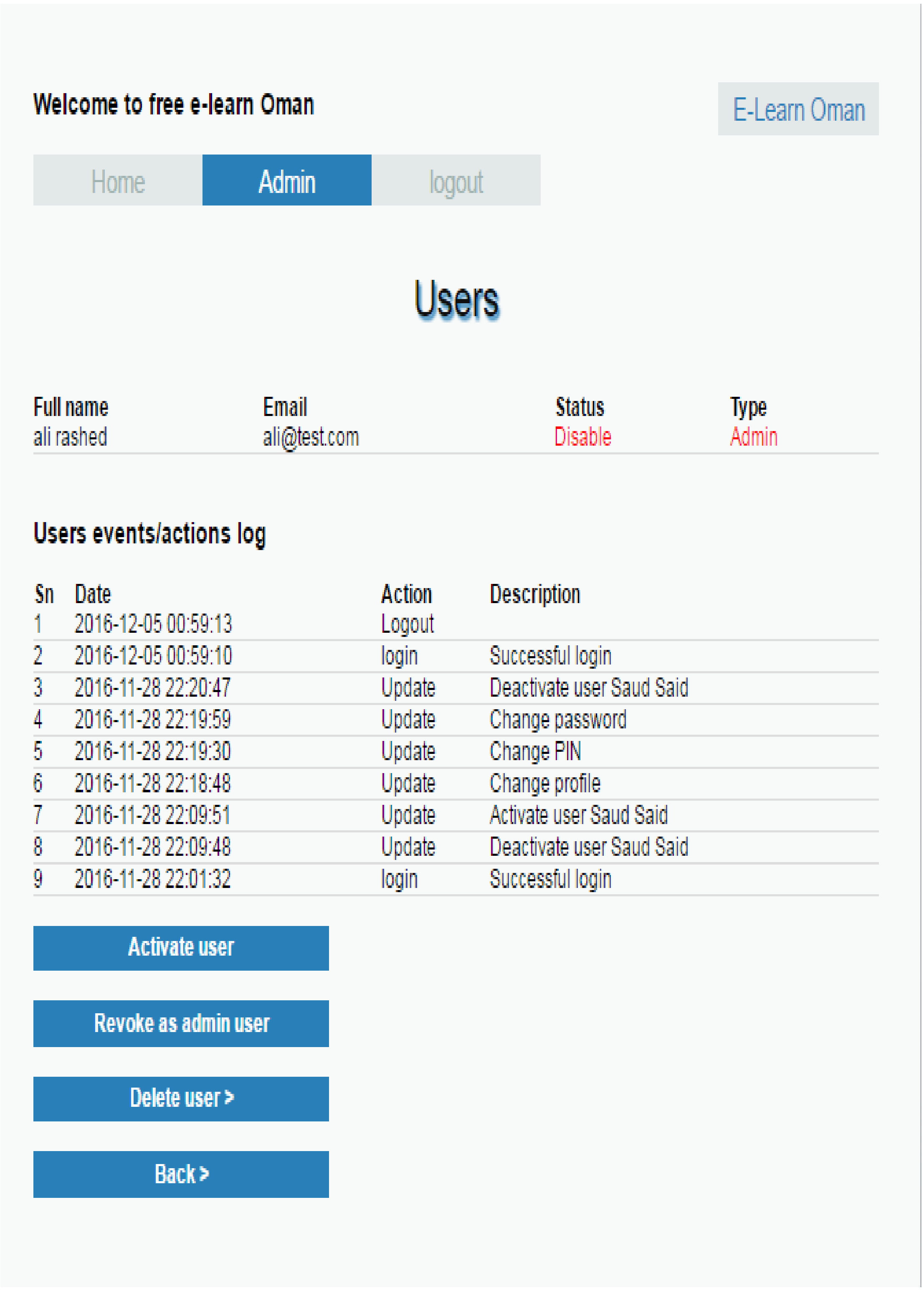
Welcome to free e-learn Oman

Users

Full name	Email	Status	Type
Sajeda tlelat	tarazantlelat@gmail.com	Active	Admin

Users events/actions log

Sn	Date	Action	Description
1	2016-12-28 20:18:53	login	Successful login
2	2016-12-27 17:13:01	Update	Deactivate user ali rashed
3	2016-12-27 17:12:53	Grant	Grant admin user ali rashed
4	2016-12-27 17:12:46	Revoke	Revoke admin user ali rashed
5	2016-12-27 17:12:41	Update	Activate user ali rashed
6	2016-12-27 17:12:34	Update	Deactivate user ali rashed
7	2016-12-27 17:09:11	login	Successful login
8	2016-12-15 18:24:09	login	Successful login
9	2016-12-15 18:23:33	Logout	
10	2016-12-15 18:18:34	Active AC	Activate AC by PIN
11	2016-12-15 18:18:23	login	Decision agent disable user and transfer to active page
12	2016-12-15 18:15:53	Logout	
13	2016-12-15 18:14:43	login	Successful login
14	2016-12-07 22:17:35	Active AC	Activate AC by PIN
15	2016-12-07 22:17:27	login	Decision agent disable user and transfer to active page
16	2016-12-07 22:09:23	login	Decision agent disable user and transfer to active page
17	2016-12-07 15:44:29	Active AC	Activate AC by PIN
18	2016-12-07 15:43:53	login	Decision agent disable user and transfer to active page
19	2016-12-07 15:32:23	Logout	
20	2016-12-07 15:29:21	Delete	Delete user nasser ahamed
21	2016-12-07 15:28:45	Grant	Grant admin user ali rashed
22	2016-12-07 15:28:39	Revoke	Revoke admin user ali rashed
23	2016-12-07 15:28:03	Update	Activate user ali rashed
24	2016-12-07 15:27:44	Update	Deactivate user ali rashed
25	2016-12-07 15:21:49	Active AC	Activate AC by code
26	2016-12-07 15:16:51	login	Decision agent disable user and transfer to active page
27	2016-12-06 23:33:14	login	Successful login

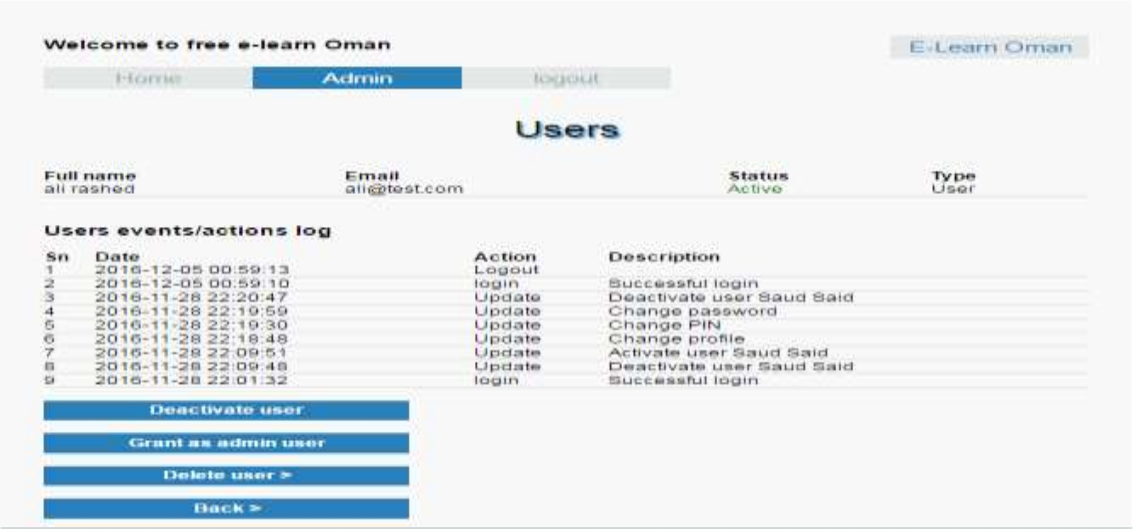


Users

Full name	Email	Status	Type
ali rashed	ali@test.com	Disable	Admin

Users events/actions log

Sn	Date	Action	Description
1	2016-12-05 00:59:13	Logout	
2	2016-12-05 00:59:10	login	Successful login
3	2016-11-28 22:20:47	Update	Deactivate user Saud Said
4	2016-11-28 22:19:59	Update	Change password
5	2016-11-28 22:19:30	Update	Change PIN
6	2016-11-28 22:18:48	Update	Change profile
7	2016-11-28 22:09:51	Update	Activate user Saud Said
8	2016-11-28 22:09:48	Update	Deactivate user Saud Said
9	2016-11-28 22:01:32	login	Successful login

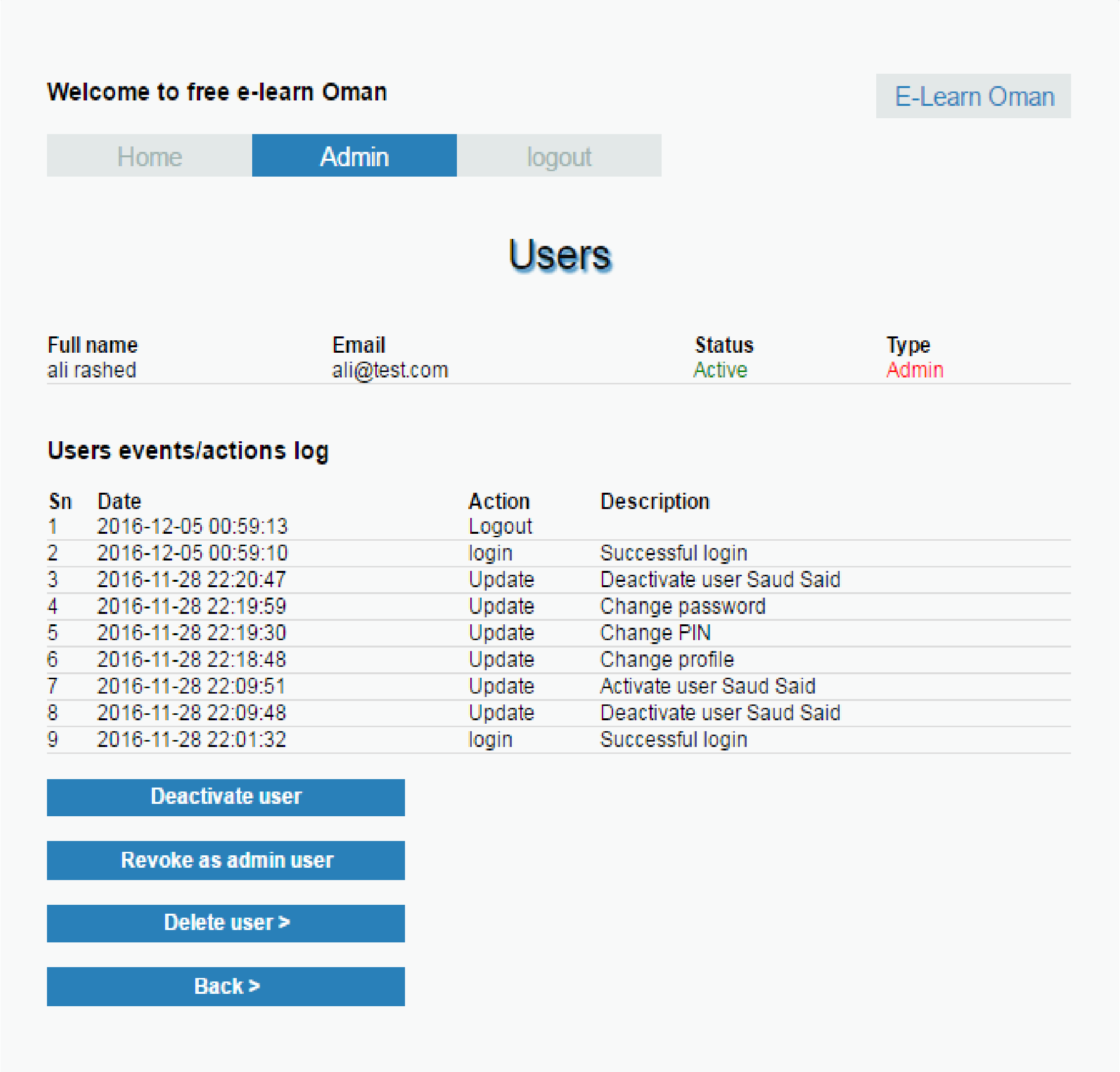


Users

Full name	Email	Status	Type
ali rashed	ali@test.com	Active	User

Users events/actions log

Sn	Date	Action	Description
1	2016-12-05 00:59:13	Logout	
2	2016-12-05 00:59:10	login	Successful login
3	2016-11-28 22:20:47	Update	Deactivate user Saud Said
4	2016-11-28 22:19:59	Update	Change password
5	2016-11-28 22:19:30	Update	Change PIN
6	2016-11-28 22:18:48	Update	Change profile
7	2016-11-28 22:09:51	Update	Activate user Saud Said
8	2016-11-28 22:09:48	Update	Deactivate user Saud Said
9	2016-11-28 22:01:32	login	Successful login

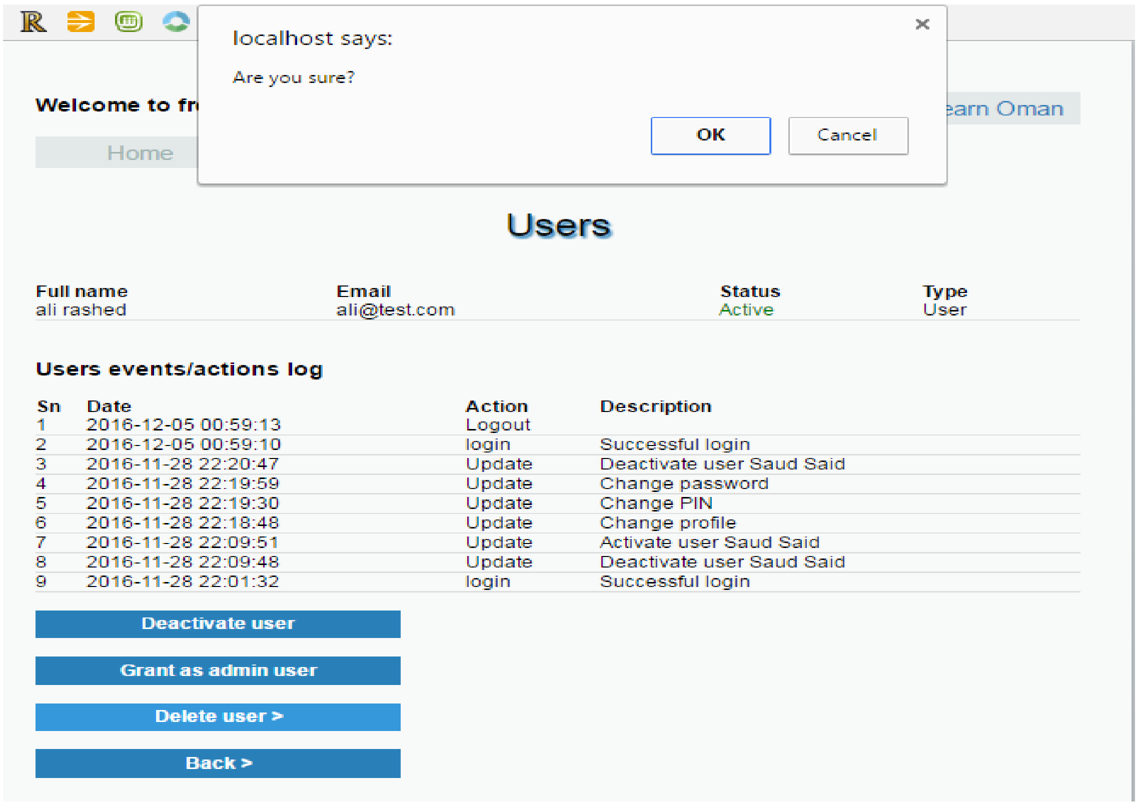


Users

Full name	Email	Status	Type
ali rashed	ali@test.com	Active	Admin

Users events/actions log

Sn	Date	Action	Description
1	2016-12-05 00:59:13	Logout	
2	2016-12-05 00:59:10	login	Successful login
3	2016-11-28 22:20:47	Update	Deactivate user Saud Said
4	2016-11-28 22:19:59	Update	Change password
5	2016-11-28 22:19:30	Update	Change PIN
6	2016-11-28 22:18:48	Update	Change profile
7	2016-11-28 22:09:51	Update	Activate user Saud Said
8	2016-11-28 22:09:48	Update	Deactivate user Saud Said
9	2016-11-28 22:01:32	login	Successful login



localhost says:

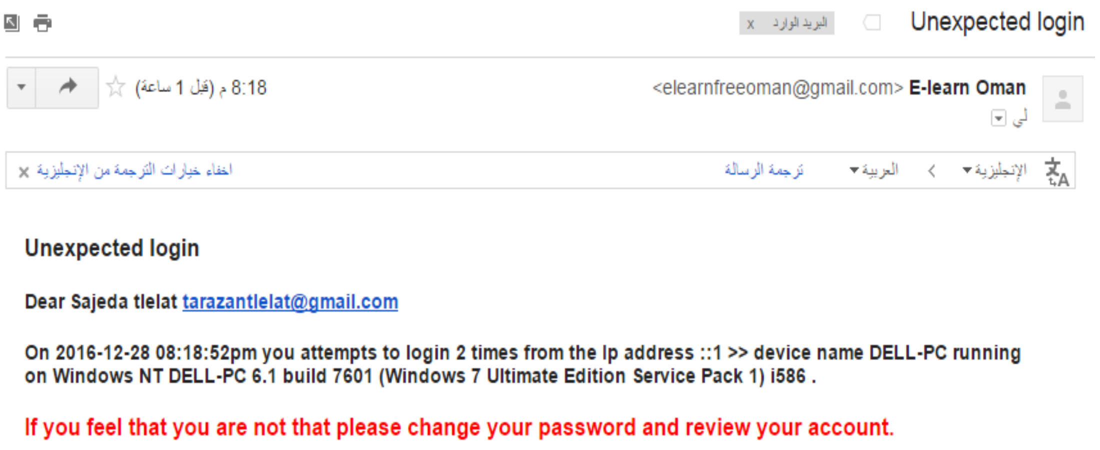
Are you sure?

Users

Full name	Email	Status	Type
ali rashed	ali@test.com	Active	User

Users events/actions log

Sn	Date	Action	Description
1	2016-12-05 00:59:13	Logout	
2	2016-12-05 00:59:10	login	Successful login
3	2016-11-28 22:20:47	Update	Deactivate user Saud Said
4	2016-11-28 22:19:59	Update	Change password
5	2016-11-28 22:19:30	Update	Change PIN
6	2016-11-28 22:18:48	Update	Change profile
7	2016-11-28 22:09:51	Update	Activate user Saud Said
8	2016-11-28 22:09:48	Update	Deactivate user Saud Said
9	2016-11-28 22:01:32	login	Successful login



Unexpected login

E-learn Oman <elearnfreeoman@gmail.com>

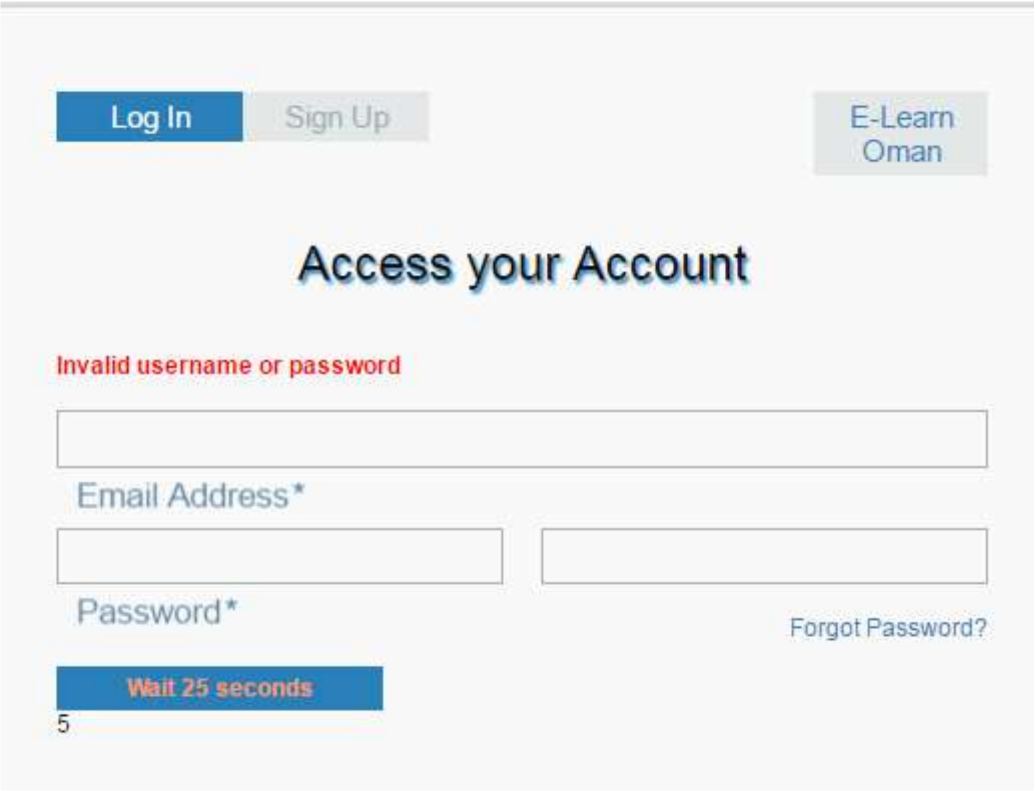
8:18 م (قبل 1 ساعة)

Unexpected login

Dear Sajeda tlelat tarazantlelat@gmail.com

On 2016-12-28 08:18:52pm you attempts to login 2 times from the Ip address ::1 >> device name DELL-PC running on Windows NT DELL-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586 .

If you feel that you are not that please change your password and review your account.



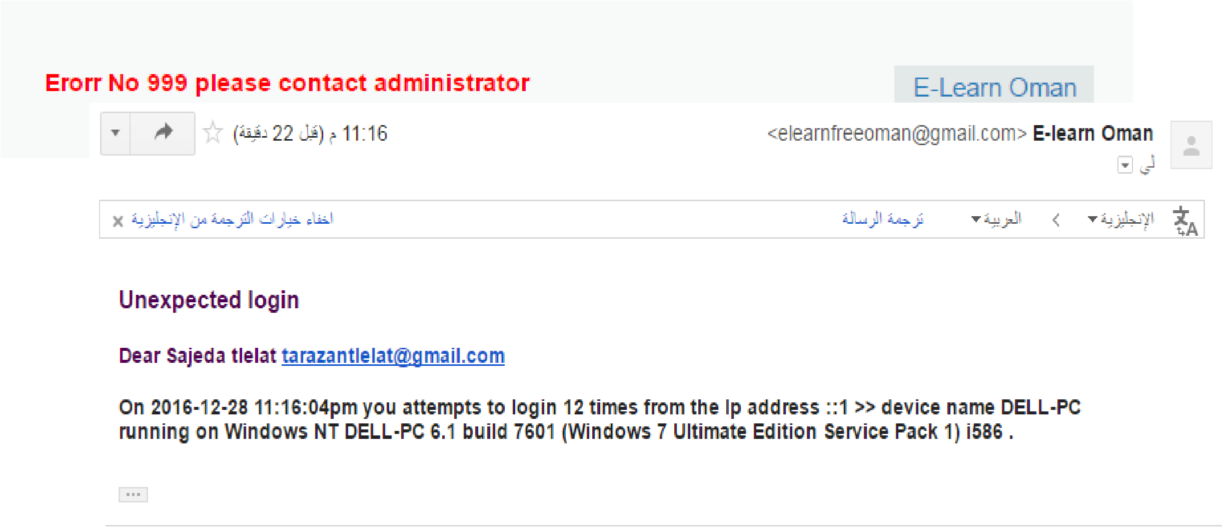
Access your Account

Invalid username or password

Email Address*

Password*

5



Erorr No 999 please contact administrator

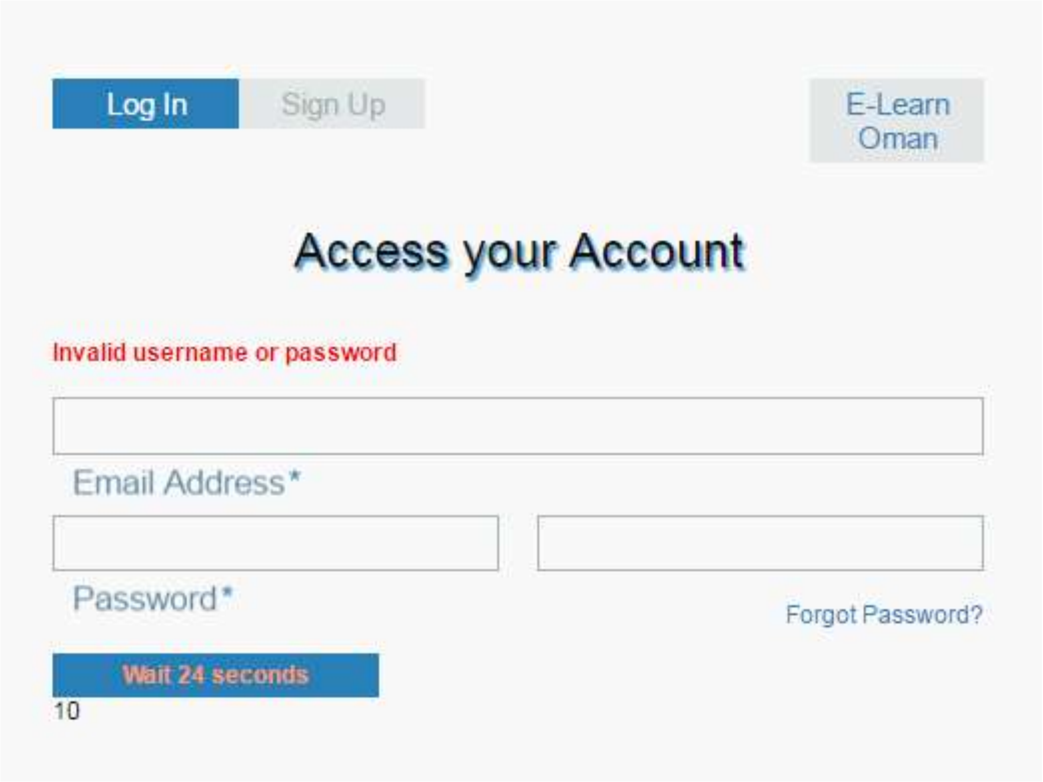
E-learn Oman <elearnfreeoman@gmail.com>

11:16 م (قبل 22 دقيقة)

Unexpected login

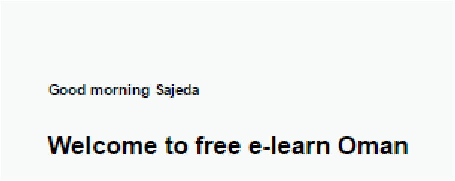
Dear Sajeda tlelat tarazantlelat@gmail.com

On 2016-12-28 11:16:04pm you attempts to login 12 times from the Ip address ::1 >> device name DELL-PC running on Windows NT DELL-PC 6.1 build 7601 (Windows 7 Ultimate Edition Service Pack 1) i586 .



Access your Account

Invalid username or password



Good morning Sajeda

Welcome to free e-learn Oman

Appendix D

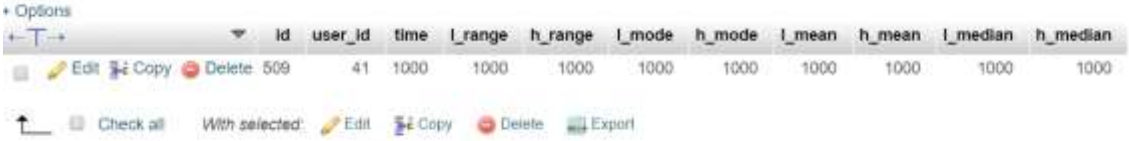
Results of test

Tests on real user login

Test 1

- Data on database table

Table 5.1



←T→	▼	id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□	Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000

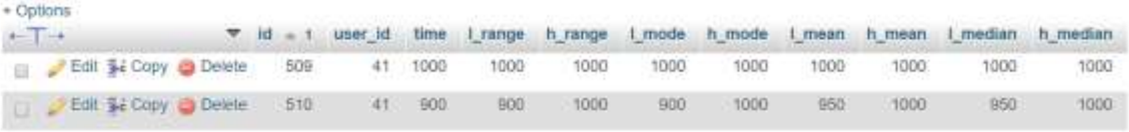
- Data from generated report

This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1083 millisecond
Time floor to 100 >>1000

Test 2

- Data on database table

Table 5.2



←T→	▼	id ▲ 1	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□	Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□	Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000

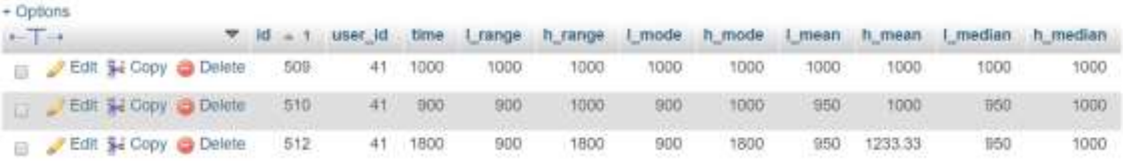
- Data from generated report

This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>999 millisecond
Time floor to 100 >>900
|||||| CR time and integration
Range Low range / High range
low range time 900   High range time 1000
Mean Low mean / High mean
Total time 1900
Number of records 2
Mean time 950
low mean time 950   High mean time 1000
Median Low median / High median
Time records after sorting
1 Time 900
2 Time 1000
Median time 950
low median time 950   High median time 1000
Mode 1000
low mode time 900   High mode time 1000

Test 3

- Data on database table

Table 5.3



+ Options

←T→	▼	id ▲ 1	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□	Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□	Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□	Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000

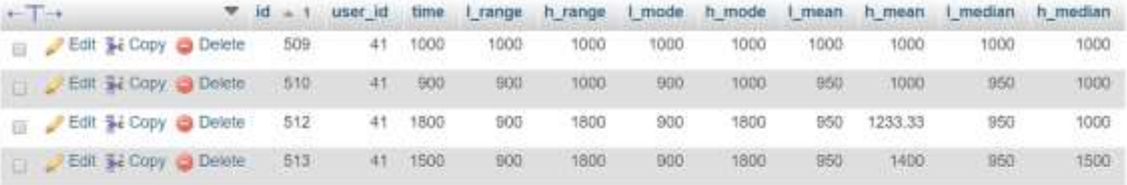
- ➢ Data from generated report

```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1837 millisecond
Time floor to 100 >>1800
  ||||| CR time and integration
  Range Low range / High range
   low range time 900           High range time 1800
  Mean Low mean / High mean
  Total time 3700
  Number of records 3
  Mean time 1233.3333333333
  low mean time 950             High mean time 1233.3333333333
   Median Low median / High median
  Time records after sorting
1  Time 900
2  Time 1000
3  Time 1800
  Median time 1000
  low median time 950           High median time 1000
  Mode 1800
  low mode time 900             High mode time 1800
```

Test 4

- ➢ Data on database table

Table 5.4



←T→	▼	id ▲ 1	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□	Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□	Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□	Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□	Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500

- ➢ Data from generated report

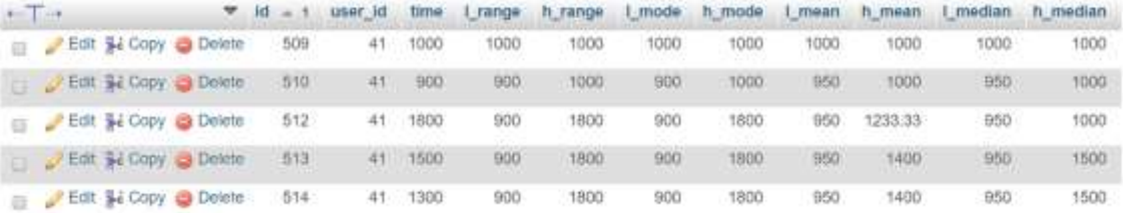
```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1537 millisecond
Time floor to 100 >>1500
  |||||  Z Scores |||||
  Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
 Total time are 3700
Number of records are 3
>>Mean Time> 1233.3333333333
  Finding the variance all X power(X-mean)^2 div by all n-1
  1 power(1000-1233.3333333333)^2=54444.444444444
  2 power(900-1233.3333333333)^2=111111.11111111
  3 power(1800-1233.3333333333)^2=321111.11111111
```

```
>>
 toltal all X power(X-mean)^2 >486666.66666667
>>
 n-1 >2
>>
 Variance time>243333.33333333
  Calculating the standard deviation sqrt(variance)
>>standard deviation of time>493.28828623162
  Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.47301616487964
>>Z Scores of >900 = -0.67573737839949
>>Z Scores of >1800 = 1.1487535432791
>>
 Z Scores of input time  >1500 = 0.54058990271959 within the level
  |||||| CR time and integration
  Range Low range / High range
   low range time 900          High range time 1800
  Mean Low mean / High mean
  Total time 4200
  Number of records 3
  Mean time 1400
  low mean time 950            High mean time 1400
  Median Low median / High median
  Time records after sorting
1  Time 900
2  Time 1500
3  Time 1800
  Median time 1500
  low median time 950          High median time 1500
  Mode 1800
  low mode time 900            High mode time 1800
```

Test 5

➢ Data on database table

Table 5.5



	id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500

➢ Data from generated report

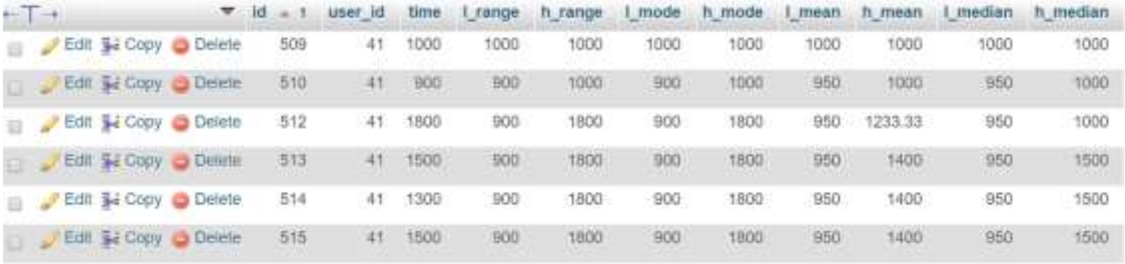
```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1376 millisecond
Time floor to 100 >>1300
  |||||  Z Scores |||||
  Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
 Total time are 5200
Number of records are 4
>>Mean Time> 1300
```

```
  Finding the variance all X power(X-mean)^2 div by all n-1
  1 power(1000-1300)^2=90000
  2 power(900-1300)^2=160000
  3 power(1800-1300)^2=250000
  4 power(1500-1300)^2=40000
>>
 toltal all X power(X-mean)^2 >540000
>>
 n-1 >3
>>
 Variance time>180000
  Calculating the standard deviation sqrt(variance)
>>standard deviation of time>424.26406871193
  Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.70710678118655
>>Z Scores of >900 = -0.94280904158206
>>Z Scores of >1800 = 1.1785113019776
>>Z Scores of >1500 = 0.47140452079103
>>
 Z Scores of input time  >1300 = 0 within the level
  |||||| CR time and integration
  Range Low range / High range
   low range time 900          High range time 1800
  Mean Low mean / High mean
  Total time 5500
  Number of records 4
  Mean time 1375
  low mean time 950            High mean time 1400
   Median Low median / High median
  Time records after sorting
1  Time 900
2  Time 1300
3  Time 1500
4  Time 1800
  Median time 1400
  low median time 950          High median time 1500
  Mode 1800
  low mode time 900            High mode time 1800
```

Test 6

- Data on database table

Table 5.6



	id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500

- Data from generated report

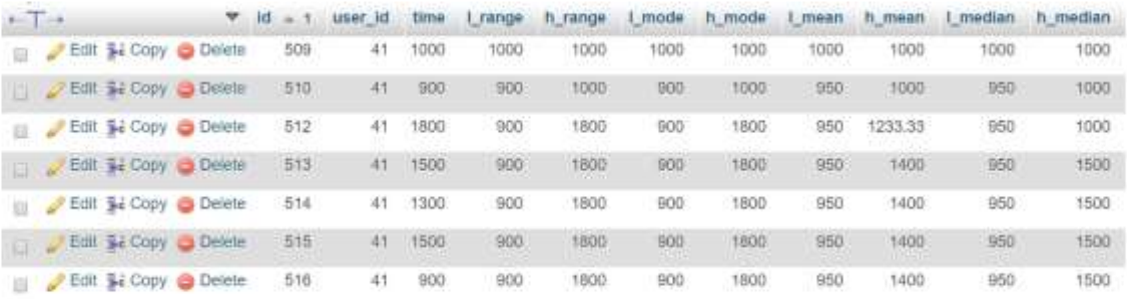
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om

```
User name >>Saud
Input Time >>1519 millisecond
Time floor to 100 >>1500
  ||||||  Z Scores ||||||
  Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
id>514   >>Time>1300
 Total time are 6500
Number of records are 5
>>Mean Time> 1300
  Finding the variance all X power(X-mean)^2 div by all n-1
  1 power(1000-1300)^2=90000
  2 power(900-1300)^2=160000
  3 power(1800-1300)^2=250000
  4 power(1500-1300)^2=40000
  5 power(1300-1300)^2=0
>>
 toltal all X power(X-mean)^2 >540000
>>
 n-1 >4
>>
 Variance time>135000
  Calculating the standard deviation sqrt(variance)
>>standard deviation of time>367.42346141748
  Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.81649658092773
>>Z Scores of >900 = -1.0886621079036
>>Z Scores of >1800 = 1.3608276348795
>>Z Scores of >1500 = 0.54433105395182
>>Z Scores of >1300 = 0
>>
 Z Scores of input time  >1500 = 0.54433105395182 within the level
  |||||| CR time and integration
  Range Low range / High range

  low range time 900            High range time 1800
  Mean Low mean / High mean
  Total time 7000
  Number of records 5
  Mean time 1400
  low mean time 950             High mean time 1400
   Median Low median / High median
  Time records after sorting
1  Time 900
2  Time 1300
3  Time 1500
4  Time 1500
5  Time 1800
  Median time 1500
  low median time 950           High median time 1500
  Mode 1500
  low mode time 900             High mode time 1800
```

Test 7

- Data on database table

Table 5.7



←T→	▼	id ▲ 1	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□	Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□	Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□	Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□	Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□	Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□	Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500
□	Edit Copy Delete	516	41	900	900	1800	900	1800	950	1400	950	1500

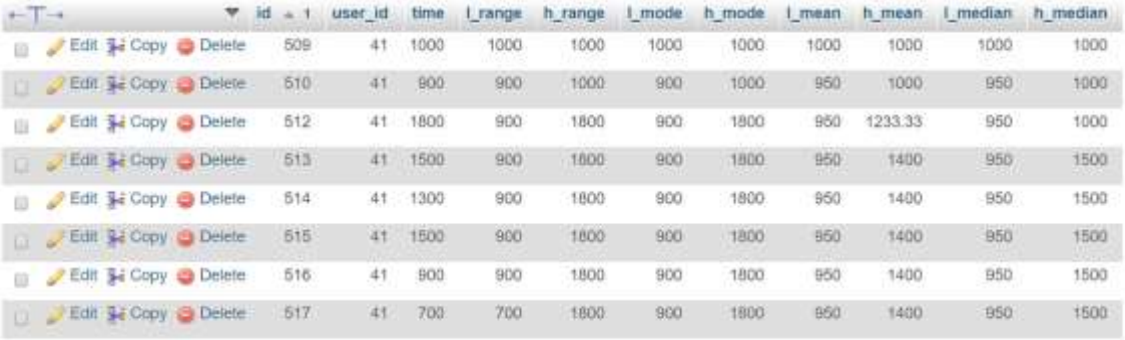
- ➢ Data from generated report

```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>912 millisecond
Time floor to 100 >>900
  ||||||  Z Scores ||||||
  Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
id>514   >>Time>1300
id>515   >>Time>1500
 Total time are 8000
Number of records are 6
>>Mean Time> 1333.3333333333
  Finding the variance all X power(X-mean)^2 div by all n-1
  1 power(1000-1333.3333333333)^2=111111.11111111
  2 power(900-1333.3333333333)^2=187777.77777778
  3 power(1800-1333.3333333333)^2=217777.77777778
  4 power(1500-1333.3333333333)^2=27777.777777778

 5 power(1300-1333.3333333333)^2=1111.1111111111
  6 power(1500-1333.3333333333)^2=27777.777777778
>>
 toltal all X power(X-mean)^2 >573333.33333333
>>
 n-1 >5
>>
 Variance time>114666.66666667
  Calculating the standard deviation sqrt(variance)
>>standard deviation of time>338.62466931201
  Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.9843740386977
>>Z Scores of >900 = -1.279686250307
>>Z Scores of >1800 = 1.3781236541768
>>Z Scores of >1500 = 0.49218701934885
>>Z Scores of >1300 = -0.098437403869769
>>Z Scores of >1500 = 0.49218701934885
>>
 Z Scores of input time  >900 = -1.279686250307 within the level
  |||||| CR time and integration
  Range Low range / High range
   low range time 900           High range time 1800
  Mean Low mean / High mean
  Total time 7900
 Number of records 6
 Mean time 1316.6666666667
 low mean time 950          High mean time 1400
  Median Low median / High median
 Time records after sorting
1  Time 900
2  Time 900
3  Time 1300
4  Time 1500
5  Time 1500
6  Time 1800
 Median time 1400
 low median time 950        High median time 1500
 Mode 1500
 low mode time 900          High mode time 1800
```

Test 8

- Data on database table

Table 5.8



id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
510	41	900	900	1000	900	1000	950	1000	950	1000
512	41	1800	900	1800	900	1800	950	1233.33	950	1000
513	41	1500	900	1800	900	1800	950	1400	950	1500
514	41	1300	900	1800	900	1800	950	1400	950	1500
515	41	1500	900	1800	900	1800	950	1400	950	1500
516	41	900	900	1800	900	1800	950	1400	950	1500
517	41	700	700	1800	900	1800	950	1400	950	1500

- Data from generated report

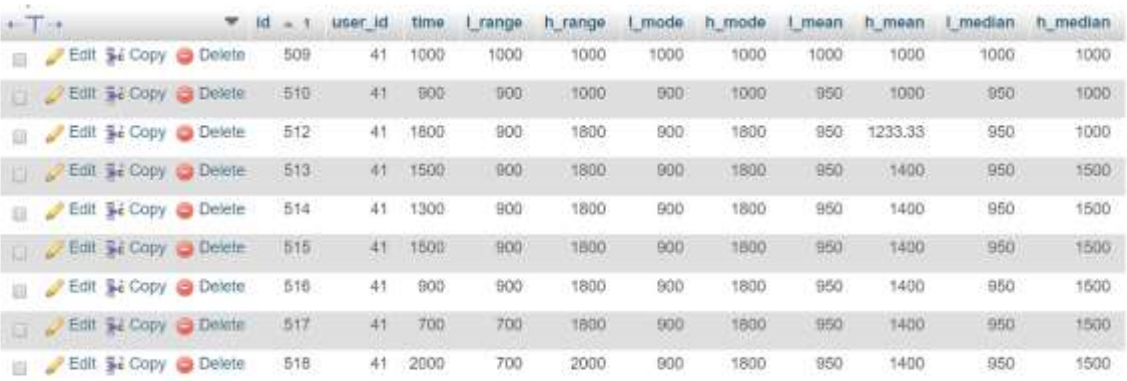
```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>799 millisecond
Time floor to 100 >>700
 |||||  Z Scores |||||
 Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
id>514   >>Time>1300
id>515   >>Time>1500
id>516   >>Time>900
 Total time are 8900
Number of records are 7
>>Mean Time> 1271.4285714286
 Finding the variance all X power(X-mean)^2 div by all n-1
  1 power(1000-1271.4285714286)^2=73673.469387755
  2 power(900-1271.4285714286)^2=137959.18367347
  3 power(1800-1271.4285714286)^2=279387.75510204
  4 power(1500-1271.4285714286)^2=52244.897959184
  5 power(1300-1271.4285714286)^2=816.32653061225
  6 power(1500-1271.4285714286)^2=52244.897959184
  7 power(900-1271.4285714286)^2=137959.18367347
>>
 toltal all X power(X-mean)^2 >734285.71428571
>>
```

```
 n-1 >6
>>
 Variance time>122380.95238095
  Calculating the standard deviation sqrt(variance)
>>standard deviation of time>349.82989063394
  Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.77588730607527
>>Z Scores of >900 = -1.061740524103
>>Z Scores of >1800 = 1.5109384381466
>>Z Scores of >1500 = 0.65337878406338
>>Z Scores of >1300 = 0.081672348007923
>>Z Scores of >1500 = 0.65337878406338
>>Z Scores of >900 = -1.061740524103
>>
 Z Scores of input time  >700 = -1.6334469601585 within the level
  |||||| CR time and integration
  Range Low range / High range
   low range time 700          High range time 1800
  Mean Low mean / High mean
  Total time 8600
  Number of records 7
  Mean time 1228.5714285714
  low mean time 950            High mean time 1400

  Median Low median / High median
  Time records after sorting
1  Time 700
2  Time 900
3  Time 900
4  Time 1300
5  Time 1500
6  Time 1500
7  Time 1800
  Median time 1300
  low median time 950          High median time 1500
  Mode 1500
  low mode time 900            High mode time 1800
```

Test 9

- Data on database table

Table 5.9



	id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	516	41	900	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	517	41	700	700	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	518	41	2000	700	2000	900	1800	950	1400	950	1500

- Data from generated report

```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>2043 millisecond
Time floor to 100 >>2000
  ||||||  Z Scores ||||||
  Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
id>514   >>Time>1300
id>515   >>Time>1500
id>516   >>Time>900
id>517   >>Time>700
 Total time are 9600
Number of records are 8
>>Mean Time> 1200
  Finding the variance all X power(X-mean)^2 div by all n-1
  1 power(1000-1200)^2=40000
  2 power(900-1200)^2=90000
  3 power(1800-1200)^2=360000

 4 power(1500-1200)^2=90000

 5 power(1300-1200)^2=10000

 6 power(1500-1200)^2=90000

 7 power(900-1200)^2=90000

 8 power(700-1200)^2=250000
>>
 toltal all X power(X-mean)^2 >1020000
>>
 n-1 >7
>>
 Variance time>145714.28571429

 Calculating the standard deviation sqrt(variance)
>>standard deviation of time>381.72540616821

 Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.52393683199558
>>Z Scores of >900 = -0.78590524799338
>>Z Scores of >1800 = 1.5718104959868
>>Z Scores of >1500 = 0.78590524799338
>>Z Scores of >1300 = 0.26196841599779
>>Z Scores of >1500 = 0.78590524799338
>>Z Scores of >900 = -0.78590524799338
>>Z Scores of >700 = -1.309842079989
>>
 Z Scores of input time  >2000 = 2.0957473279823 within the level

 |||||| CR time and integration
  Range Low range / High range

  low range time 700            High range time 2000
  Mean Low mean / High mean
  Total time 10600
```

Number of records 8
Mean time 1325
low mean time 950 High mean time 1400

Median Low median / High median
Time records after sorting
1 Time 700
2 Time 900
3 Time 900
4 Time 1300
5 Time 1500
6 Time 1500
7 Time 1800
8 Time 2000

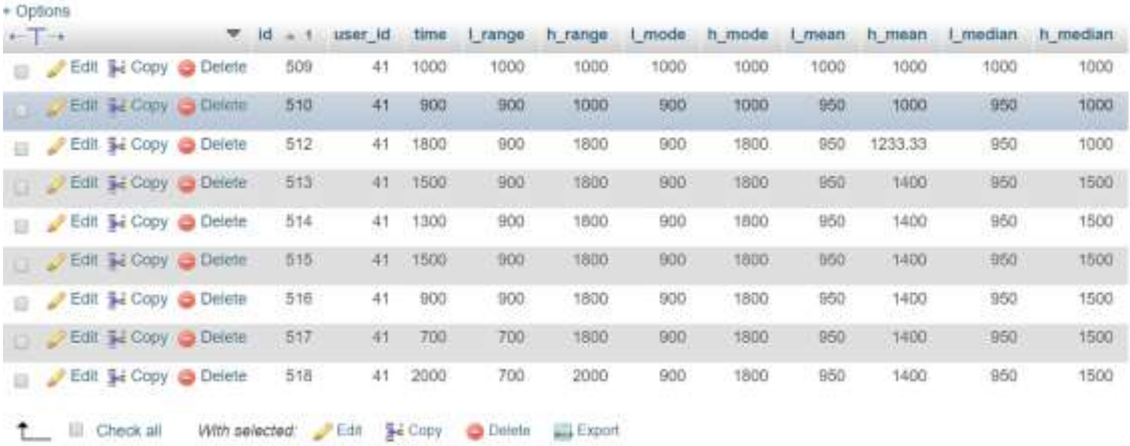
Median time 1400
low median time 950 High median time 1500

Mode 1500
low mode time 900 High mode time 1800

Test 10

- Data on database table

Table 5.10



	id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	516	41	900	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	517	41	700	700	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	518	41	2000	700	2000	900	1800	950	1400	950	1500

- Data from generated report

This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>6000 millisecond
Time floor to 100 >>6000

||||| Z Scores |||||

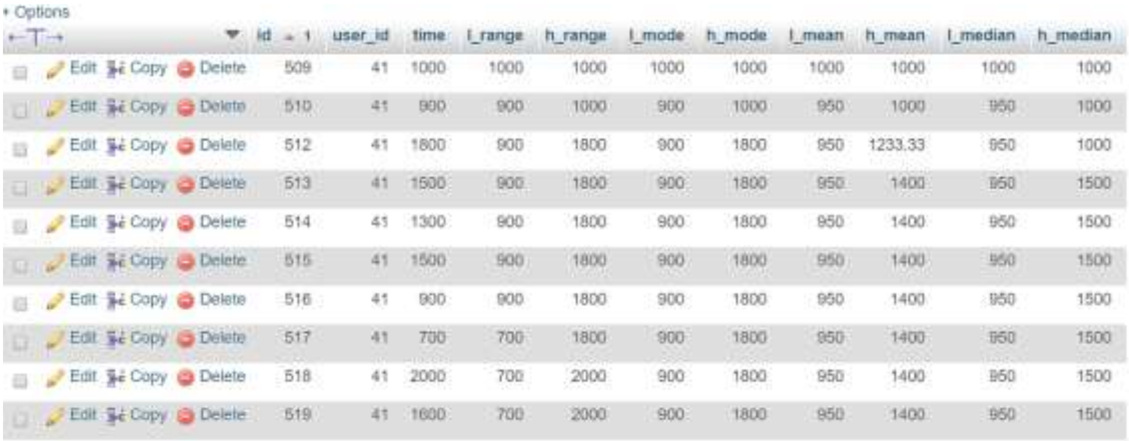
Records
id>509 >>Time>1000
id>510 >>Time>900
id>512 >>Time>1800
id>513 >>Time>1500
id>514 >>Time>1300
id>515 >>Time>1500
id>516 >>Time>900
id>517 >>Time>700
id>518 >>Time>2000

```
 Total time are 11600
Number of records are 9
>>Mean Time> 1288.8888888889

 Finding the variance all X power(X-mean)^2 div by all n-1

 1 power(1000-1288.8888888889)^2=83456.790123457

 2 power(900-1288.8888888889)^2=151234.56790123

 3 power(1800-1288.8888888889)^2=261234.56790123

 4 power(1500-1288.8888888889)^2=44567.901234568

 5 power(1300-1288.8888888889)^2=123.45679012346

 6 power(1500-1288.8888888889)^2=44567.901234568

 7 power(900-1288.8888888889)^2=151234.56790123

 8 power(700-1288.8888888889)^2=346790.12345679

 9 power(2000-1288.8888888889)^2=505679.01234568
>>
 toltal all X power(X-mean)^2 >1588888.8888889
>>
 n-1 >8
>>
 Variance time>198611.11111111

 Calculating the standard deviation sqrt(variance)
>>standard deviation of time>445.65806523736

 Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.64822991307253
>>Z Scores of >900 = -0.87261719067456
>>Z Scores of >1800 = 1.1468683077437
>>Z Scores of >1500 = 0.47370647493762
>>Z Scores of >1300 = 0.024931919733559
>>Z Scores of >1500 = 0.47370647493762
>>Z Scores of >900 = -0.87261719067456
>>Z Scores of >700 = -1.3213917458786
>>Z Scores of >2000 = 1.5956428629478
>>
 Z Scores of input time  >6000 = 10.571133967029 out of level
No record insert to database
```

Test 11

- Data on database table

Table 5.11



	id	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	516	41	900	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	517	41	700	700	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	518	41	2000	700	2000	900	1800	950	1400	950	1500
□ Edit Copy Delete	519	41	1600	700	2000	900	1800	950	1400	950	1500

- Data from generated report

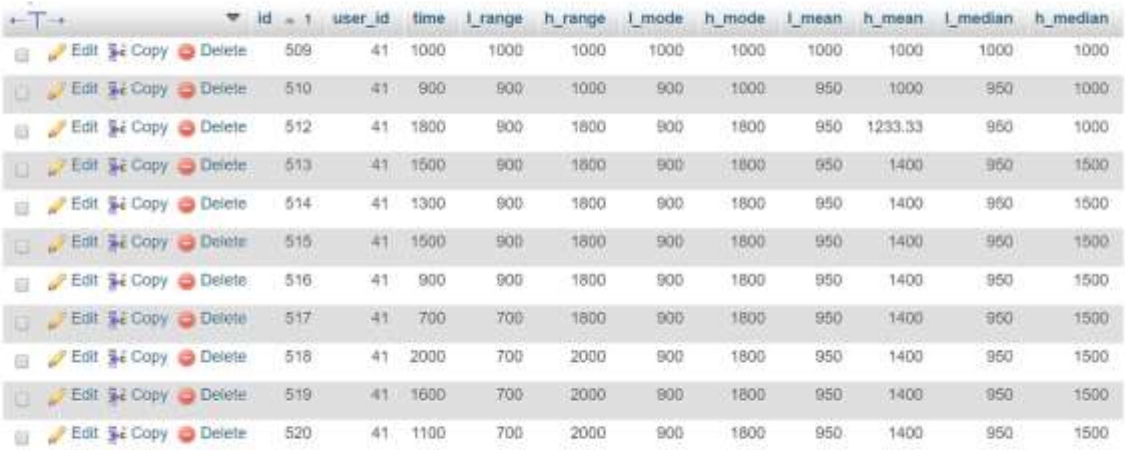
```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1600 millisecond
Time floor to 100 >>1600

 |||||  Z Scores |||||

 Records
id>509   >>Time>1000
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
id>514   >>Time>1300
id>515   >>Time>1500
id>516   >>Time>900
id>517   >>Time>700
id>518   >>Time>2000

 Total time are 11600
Number of records are 9
>>Mean Time> 1288.8888888889

 Finding the variance all X power(X-mean)^2 div by all n-1

 1 power(1000-1288.8888888889)^2=83456.790123457

 2 power(900-1288.8888888889)^2=151234.56790123

 3 power(1800-1288.8888888889)^2=261234.56790123

 4 power(1500-1288.8888888889)^2=44567.901234568

 5 power(1300-1288.8888888889)^2=123.45679012346

 6 power(1500-1288.8888888889)^2=44567.901234568

 7 power(900-1288.8888888889)^2=151234.56790123

 8 power(700-1288.8888888889)^2=346790.12345679

 9 power(2000-1288.8888888889)^2=505679.01234568
>>
```

```
 toltal all X power(X-mean)^2 >1588888.8888889
>>
 n-1 >8
>>
 Variance time>198611.11111111

 Calculating the standard deviation sqrt(variance)
>>standard deviation of time>445.65806523736

 Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.64822991307253
>>Z Scores of >900 = -0.87261719067456
>>Z Scores of >1800 = 1.1468683077437
>>Z Scores of >1500 = 0.47370647493762
>>Z Scores of >1300 = 0.024931919733559
>>Z Scores of >1500 = 0.47370647493762
>>Z Scores of >900 = -0.87261719067456
>>Z Scores of >700 = -1.3213917458786
>>Z Scores of >2000 = 1.5956428629478
>>
 Z Scores of input time  >1600 = 0.69809375253965 within the level

 |||||| CR time and integration
  Range Low range / High range

  low range time 700          High range time 2000
  Mean Low mean / High mean
  Total time 12200
  Number of records 9
  Mean time 1355.5555555556
  low mean time 950           High mean time 1400

  Median Low median / High median
  Time records after sorting
1  Time 700
2  Time 900
3  Time 900
4  Time 1300
5  Time 1500
6  Time 1500
7  Time 1600
8  Time 1800
9  Time 2000

  Median time 1500
  low median time 950         High median time 1500

  Mode 1500
  low mode time 900           High mode time 1800
```

Test 12

- Data on database table

Table 5.12



←T→ ▼	id ▲ 1	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	509	41	1000	1000	1000	1000	1000	1000	1000	1000	1000
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	516	41	900	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	517	41	700	700	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	518	41	2000	700	2000	900	1800	950	1400	950	1500
□ Edit Copy Delete	519	41	1600	700	2000	900	1800	950	1400	950	1500
□ Edit Copy Delete	520	41	1100	700	2000	900	1800	950	1400	950	1500

- Data from generated report

This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1198 millisecond
Time floor to 100 >>1100

||||| Z Scores |||||

Records
id>509 >>Time>1000
id>510 >>Time>900
id>512 >>Time>1800
id>513 >>Time>1500
id>514 >>Time>1300
id>515 >>Time>1500
id>516 >>Time>900
id>517 >>Time>700
id>518 >>Time>2000
id>519 >>Time>1600

Total time are 13200
Number of records are 10
>>Mean Time> 1320

Finding the variance all X power(X-mean)^2 div by all n-1

1 power(1000-1320)^2=102400

2 power(900-1320)^2=176400

3 power(1800-1320)^2=230400

4 power(1500-1320)^2=32400

5 power(1300-1320)^2=400

6 power(1500-1320)^2=32400

7 power(900-1320)^2=176400

8 power(700-1320)^2=384400

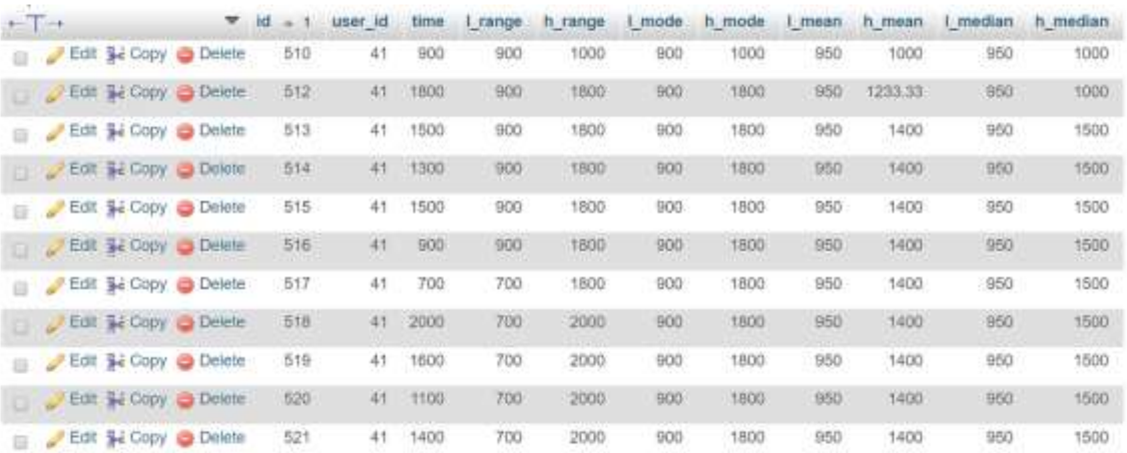
9 power(2000-1320)^2=462400

```
 10 power(1600-1320)^2=78400
>>
 toltal all X power(X-mean)^2 >1676000
>>
 n-1 >9
>>
 Variance time>186222.22222222

 Calculating the standard deviation sqrt(variance)
>>standard deviation of time>431.53472887153

 Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >1000 = -0.74153939090095
>>Z Scores of >900 = -0.9732704505575
>>Z Scores of >1800 = 1.1123090863514
>>Z Scores of >1500 = 0.41711590738179
>>Z Scores of >1300 = -0.04634621193131
>>Z Scores of >1500 = 0.41711590738179
>>Z Scores of >900 = -0.9732704505575
>>Z Scores of >700 = -1.4367325698706
>>Z Scores of >2000 = 1.5757712056645
>>Z Scores of >1600 = 0.64884696703833
>>
 Z Scores of input time  >1100 = -0.50980833124441 within the level

 |||||| CR time and integration
  Range Low range / High range

  low range time 700            High range time 2000
  Mean Low mean / High mean
  Total time 13300
  Number of records 10
  Mean time 1330
  low mean time 950             High mean time 1400

  Median Low median / High median
  Time records after sorting
1  Time 700
2  Time 900
3  Time 900
4  Time 1100
5  Time 1300
6  Time 1500
7  Time 1500
8  Time 1600
9  Time 1800
10  Time 2000

  Median time 1400
  low median time 950          High median time 1500

  Mode 1500
  low mode time 900             High mode time 1800
```

Test 13

- Data on database table

Table 5.13



←T→ ▼	id ▲ 1	user_id	time	l_range	h_range	l_mode	h_mode	l_mean	h_mean	l_median	h_median
□ Edit Copy Delete	510	41	900	900	1000	900	1000	950	1000	950	1000
□ Edit Copy Delete	512	41	1800	900	1800	900	1800	950	1233.33	950	1000
□ Edit Copy Delete	513	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	514	41	1300	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	515	41	1500	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	516	41	900	900	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	517	41	700	700	1800	900	1800	950	1400	950	1500
□ Edit Copy Delete	518	41	2000	700	2000	900	1800	950	1400	950	1500
□ Edit Copy Delete	519	41	1600	700	2000	900	1800	950	1400	950	1500
□ Edit Copy Delete	520	41	1100	700	2000	900	1800	950	1400	950	1500
□ Edit Copy Delete	521	41	1400	700	2000	900	1800	950	1400	950	1500

➢ Data from generated report

```
This file generated automatically to verify the calculation
User ID >>41
User email >>m120130303019@buc.edu.om
User name >>Saud
Input Time >>1493 millisecond
Time floor to 100 >>1400
  |||||  Z Scores |||||
 Records
id>510   >>Time>900
id>512   >>Time>1800
id>513   >>Time>1500
id>514   >>Time>1300
id>515   >>Time>1500
id>516   >>Time>900
id>517   >>Time>700
id>518   >>Time>2000
id>519   >>Time>1600
id>520   >>Time>1100
 Total time are 13300
Number of records are 10
>>Mean Time> 1330
  Finding the variance all X power(X-mean)^2 div by all n-1
 1 power(900-1330)^2=184900
 2 power(1800-1330)^2=220900
 3 power(1500-1330)^2=28900
 4 power(1300-1330)^2=900
 5 power(1500-1330)^2=28900
 6 power(900-1330)^2=184900
 7 power(700-1330)^2=396900
 8 power(2000-1330)^2=448900
 9 power(1600-1330)^2=72900
 10 power(1100-1330)^2=52900
>>
 toltal all X power(X-mean)^2 >1621000
>>
 n-1 >9
>>
 Variance time>180111.11111111
 Calculating the standard deviation sqrt(variance)
>>standard deviation of time>424.39499421071
  Calculating the Z Scores
 Max level of Z Score 3
 Min level of Z Score -3
>>Z Scores of >900 = -1.0132070497196
```

```
>>Z Scores of >1800 = 1.1074588682982
>>Z Scores of >1500 = 0.40057022895891
>>Z Scores of >1300 = -0.070688863933925
>>Z Scores of >1500 = 0.40057022895891
>>Z Scores of >900 = -1.0132070497196
>>Z Scores of >700 = -1.4844661426124
>>Z Scores of >2000 = 1.578717961191
>>Z Scores of >1600 = 0.63619977540533
>>Z Scores of >1100 = -0.54194795682676
Z Scores of input time  >1400 = 0.16494068251249 within the level
  |||||| CR time and integration
  Range Low range / High range
   low range time 700           High range time 2000
  Mean Low mean / High mean
  Total time 13800
  Number of records 10
  Mean time 1380
  low mean time 950             High mean time 1400
   Median Low median / High median
  Time records after sorting
1  Time 700
2  Time 900
3  Time 1100
4  Time 1300
5  Time 1400
6  Time 1500
7  Time 1500
8  Time 1600
9  Time 1800
10  Time 2000
  Median time 1450
  low median time 950           High median time 1500
  Mode 1500
  low mode time 900             High mode time 1800
The oldest record of id 509 has been deleted
```

Appendix E

Oraganization Policices, Role and responsibility , Planning

a. Policies

This section describes the main policies outlined, such as standards for business and stakeholders. Policies are different from country to country, and from layer to layer, and throughout the whole framework. The structure of the policies is built depending on many factors, such as country laws, size of the organization, and level of awareness.

i. Standards

a. Business

1) Classify all data depending on the nature of the data;
2) Prevent data that has been classified as high level and semi-sensitive from suspicious users;
3) Prevent whole data from unauthorized users;
4) Monitor whole system accounts;

b. User

1) Classify all users into three main types: legal, illegal, and suspicious;
2) Classify all authorize users into multi-security levels;
3) Monitor legitimate user behavior; and
4) Availability of data depends on the user authority level.

b. **Roles and Responsibilities**

This section describes the roles and responsibilities outlined in the security framework. The main outline can be divided into three topics: 1) standards, 2) critical security procedure, and 3) monitoring. The purpose of this topic e is to determine the whole mechanism, including encryption, uploading, level of authority and data, and critical procedures.

i. Standards

a. Business

1) The mechanism for uploading data on the public cloud;
2) The mechanism for activating any penetration of accounts;
3) Classify all data into three main types, which are high level, semi-sensitive, and normal (see Figure 4.5):

A. High level (00) data has a very high-security level and can tremendously affect the main pillars of the organization.

B. Semi sensitive (10) data has a certain level of importance and can influence the organization aspects.

C. Normal data is data that the organization wishes to announce to everyone.

b. User

1) Mechanism of data availability for legal, illegal, and suspicious users.
2) Classify all legal users into five types: user 00, user 01, user 10, user 11, and Normal, based on organization policies, as shown below:

A. Full Authority User (00): has full authority to edit, add, read, write, copy, and modify all data in the organization from the level of data 00 through 11.

B. Higher Authority User (01): has the authority to edit, add, read, write, copy, and modify all data in the organization from the level of data 01 through 11.

C. Authority User (11): has the authority to edit, add, read, write, and modify all data in the organization from the level of data 11 only.

c. Accountable

An organization must have regulations included for whole-organization activities, including who is responsible for any activity that is relevant to data and the users. Besides, all layers have their roles and responsibilities to achieve the targets of the security framework.

c. Planning

This section presents the structure of the process that is associated with authentication. We select three mains process, which are monitor, evaluate, and direct, as shown below[191]:

a) Monitor

Monitoring represents the sequence of processes that are associated with the security framework in three aspects. First, the authentication layer receives the results of the EPSB generated from the confidence range algorithm and checks the authority of the users. Second, in the classification layers, it receives the results of the data security classification and determines the length of the key encryption according to the data security level.

b) Evaluate

This entity can compare between current users and the previous history of that authorized user. The purpose of this process is to examine the rate of compatibility between them to diagnose if the user is authorized, unauthorized, and a suspicious user, which can save the data security level.

1) **Authorized User**
   The user who has the authority to login into data based on the organization policies on the distribution of the authority level of the user.
2) **Suspicious User**
   The user who has the specifications of both authorized and unauthorized.

3) **Unauthorized user**
   The entity logging into the data illegally.

c) Direct Activity

This section presents the processes that will be applied based on the results of the evaluation sector. This is also considered as the execution sector. It works to synchronize all layers in a security framework. The outline of procedures is as shown below:

1. Availability of all data for users based on authorized users.
2. Active critical security procedure.

The system will follow a set of activities and procedures in case it detects any suspicious use by examining the user's behavior. Decision agents have the power to activate these procedures. The main purpose behind these procedures is the security protection for protecting the data and the system from any suspicious access. These procedures are as follows:

1. Blocking the high-level secured data.

2. Sending an e-mail to the main/in charge user's account and:
    - 2.1 Sending the first activation e-mail that will be valid for 3 minutes.
    - 2.2 If the user confirms the received e-mail, the block will be removed from the data, and the system will work smoothly.
    - 2.3 If the user does not confirm the received e-mail, the first email will expire, and another email will be sent, and similarly, it will be activated for another 3 minutes.
    - 2.4 In case of no confirmation, the following procedures will be taken:
        - 2.4.1 Blocking the user's account.
        - 2.4.2 An e-mail is sent to the main user and the admin for the re-activation process.
        - 2.4.3 The main user should first activate the account, and the admin should confirm that process.

Biodata

Mohanaad Shakir is a Senior Lecturer at Alburaimi University College, information technology department, Oman. He. Holds a BSc Degree in Computer Science from the University of Almamoon, Baghdad, Iraq; Post Graduate Diploma in Computer Security from University of Technology, Iraq and M.Sc. in Information Technology (MIT) from the University of Tenaga National(UNITEN), Putrajaya, Malaysia. He is currently a PhD candidate in Information Communication Technology at the University of Tenaga National (UNITEN), Putrajaya, Malaysia. His research interests include Cipher Algorithm, Authentication Model, Security, Aided Learning and Cloud Computing Security. He can be contacte at mohanaad@buc.edu.om, mohanaadshakir@gmail.com