Journal of Theoretical and Applied Information Technology
31st December 2016. Vol.94. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# APPLICATION OF CONFIDENCE RANGE ALGORITHM IN RECOGNIZING USER BEHAVIOR THROUGH EPSB IN CLOUD COMPUTING

[1,2] MOHANAAD SHAKIR, [3] ASMIDAR BIT ABUBAKAR, [3]YOUNUS YOUSOFF, [4] MOSTAFA AL-EMRAN , [1,5]MAYTHAM HAMMOOD

[1] Senior Lecturer, IT Department, Alburaimi University Collage(BUC), Oman
[2] Ph.D. Candidate in ICT, COIT, University Tenaga National(UNITEN), Malaysia
[3] Senior Lecturer, COIT, University Tenaga National(UNITEN), Malaysia
[4]Ph.D. Candidate in FSKKP, University Malaysia Pahang(UMP), Malaysia
[5] Senior Lecturer, Computer Science Dept., Tikrit University, Iraq

E-mail: [1]mohanaad@buc.edu.om , [3]asmidar@uniten.edu.my,[3]Yunusy@uniten.edu.my, [4]malemran@buc.edu.om , [5]mmhammood@ualr.edu

**ABSTRACT**

Within the security scope, Authentication is considered as a core model to control accessing any system. Password is one of the most significant mechanisms which diagnose the authorized user from others. However, it is facing many problems such as spoofing and man in the middle attack(MitMA). When unauthorized user has got the correct password. Then, this user would be able to access into the data and change previous password which causes significant loss in efforts and cost. Similarly, the hacker "who don't have a password" is also trying to penetrate the system through predicted a set of words. In fact, both of authorized and hacker users work to input a wrong password, but authorized user may have only one or two wrong characters while the hacker inputs a whole wrong password. The aim of this paper, established an algorithm under the name of "Confidence Range ". The main tasks of this algorithm are monitoring all the activities which associated with the password on time, error, and style to the authorized user to recognize any suspicious activity. For that reason, a unique **EPSB**," Electronic Personal Synthesis Behavior", has been generated to the authorized user by the application of confidence range algorithm.

**Keywords:** *Information system security, Data Security, Hybrid Cloud computing, Confidence Range(CR), Data classification. Electronic Personal Synthesis Behavior(EPSB)*

## 1. INTRODUCTION

Authentication model is a model that allow just authority users to access. There are many authentication models built by using various mechanism. Cloud computing is 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. Cloud computing need to develop authentication model for improve the level of security for users. Authentication model insure individual identity, reduce the risk of penetration and the need for maintenance, and Provide access to all systems in a safe manner. There are many mechanism doing to ensure authentication access such as public key, key management, Symmetric key encryption, digital certificate …etc. whole this mechanism work for avoid not authorized access. Cloud computing is a new technology that be using form many type of organization for ensure to access into pool of data from anywhere at any time. According to the Institute of NIST [16,17], any security plan in cloud computing must be included:

a) Policies, or a series of decisions that made the administration to defend the organization against perceived threats, which can be expressed through standards and guidelines, Or procedures.

b) Roles and responsibilities, which had to be who is responsible for the tasks that need to be done for implement security policy.

c)Planning, or the means that will be implemented security during each stage of the system lifecycle. In the case of cloud storage, this may relate primarily to the data life cycle, which imposes a set of more stringent standards, especially about privacy.

d)Ensure, or determine the extent to which the cloud is secure work in environment.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

d)Accreditation, the system matching all most of the required specifications. Generally, organizations or institutions are very concerned in improving the security of cloud computing through the application of the authority model and dynamic classification of data model based on the multi-level security [14]. The motivation of this study, each human has unique features which prevent any spoofing, or Impersonation such as handwriting, fingerprint, voice, face recognize, and life behavior. In the other hand, password in any authentication model is very weak with a spoofing, and man in the middle attack (MitMA). Wherefore, the main objective of this study is to simulate the human features " behavior" on authentication model to improve a performance of password, by improving predictive model based on Multi-Agent principals and statistical analysis with authentication model for determining level of confidence range through generate **EPSB** ,"Electronic Personal Synthesis Behavior : It stands the electronic diagnostic process to agave out the manner of the authorized user", for all users depends on analysis of previous data such as choose style of a password, time of write password, and the most frequent error in password location by using statistical tools, as shown as figure 1 EPSB below.


*Figure 1 EPSB*

## 2. RELATED WORK

In [1], the authors mention their proposed PKI research to find an appropriate resolution to the situation in Bangladesh. More specifically, they introduce the concepts of E-Finance and E-Government – a solution which can be implemented in two stages, the first being the use of PKI domains, and the second – certificate authority and certificate hierarchy layers. The proposition is believed to be the most suitable one for Bangladesh's current situation. Furthermore, in [2, 3], a model is introduced as a reliable approach towards increasing the reliability, privacy, and safety of the cloud computing which can be use. In [4], the notion of SLA (Service Level Agreement) is pointed as a possible answer to the cloud computing dependability dilemma. The model comprises cloud consumer module, cloud services directory, and SLA agents. In [5], the current firewall software and trust models are evaluated and a collaborative trust model is presented based on practical algorithms regarding trust appraisal and cloud theory. In [6], a cloud security trust model is suggested and certain social security problems have been pinpointed. These problems have been further sub-classified into three core groups – multiple stakeholders, open space, and handling of critical information issues. In addition to that, the authors note that once the cloud service provider authenticates the data and place it in the cloud, it becomes available for third parties, which may not always have a good interest in heart. In [7], a trust model is introduced. It aims at enhancing the standard security model through a supplementary security framework, and suggests relevant solutions to already existing issues concerning both cloud providers and users. In [8], several SaaS concerns are pinpointed, starting with the fact that cloud data can be accessed via any installed software. This can be settled through a mechanism separating the software from the data provided by the coordinator, software or data provider, and users. In [9], the research presents a safe communication architecture where B2B is involved through a CaaS model (inter- and intra-cloud communication).

In [10], inter-cloud specifications are explained, along with trending frameworks and mechanism for an applicable architecture. The authors further propose a coRBAC cloud authentication model, which supplies the user with three authentication levels upon login [11]. The first level requires a legitimate certificate issued by the organization where the cloud service is purchased or which has made the cloud service available for its employees. The second and third steps involve certificate validity checks and appointing the user to a specific server, which they are authorized to use.

Victor Chang at al. proposed a security framework for business cloud computing under named cloud computing adoption framework (CCAF), this framework includes three layers. Firstly, tasks for layer 1 are password protection, network, and IP-based firewall and access control. Secondly, tasks for layer 2 are out-of-band authentication and

Journal of Theoretical and Applied Information Technology
31st December 2016. Vol.94. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

openID serving for identity management. Finally, tasks for layer 3 encryption and decryption for authentication file [12]. The authentication model was proposed in CCAF do not include model it has the potential of predictive a behaviour print for a user. In this paper, author is suggested a confidence range algorithm for recognizing user behavior through EPSB in cloud computing. The benefits of behaviour print add new security level to avoid any unauthorized password change and avoid stop temporary login based on previous error and time of write. Report Identification (RID) service Model, it's adopted for censorship on all user activates (time, Password, error) as shows as in figure 2 Adapted Authentication model below.

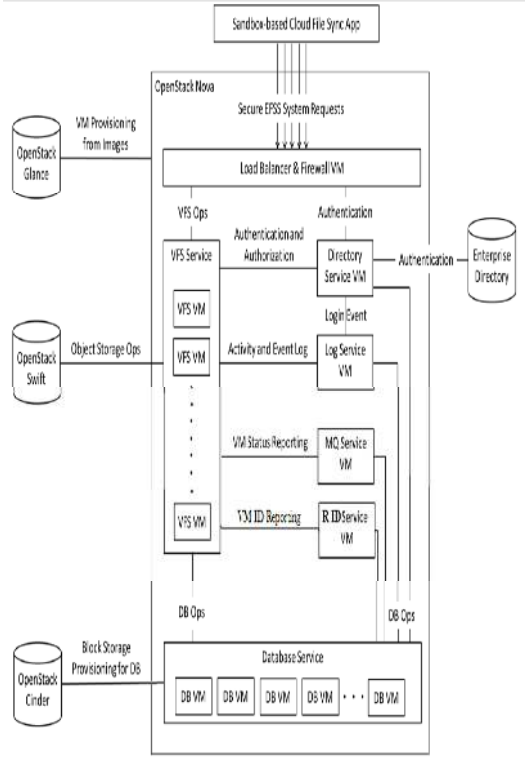



*Figure 2 Adapted Authentication model*

## 3. CONFIDENCE RANGE "CR":

The algorithm determines the lowest and highest confidence range values that relate to each user's account. Accordingly, it analyses the entered values for each of the (time, password and error) using statistical analysis methods as shown in figure 3 R ID Service model.

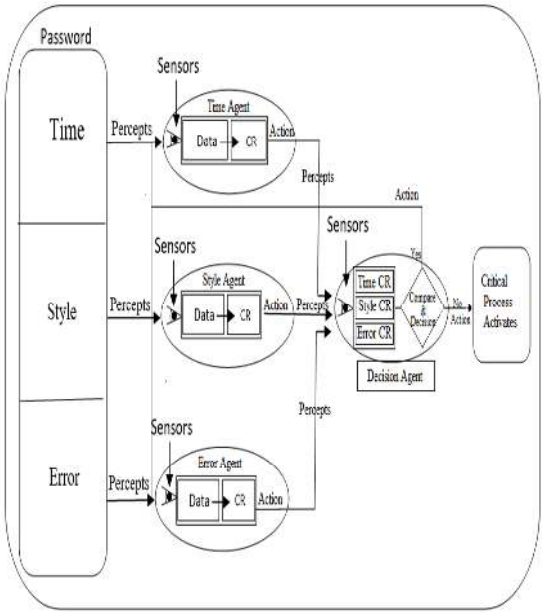



*Figure 3 R ID Service Model.*

User's EPSB, his or her unique attribution, is generated based on the graphical analysis of the statistical analysis for the confidence range below which works according to the application of the following statistical formula.

Confidence Range(CR)=$l + h\left({}^{fm-f1}/_{2fm-f1-f2}\right), \sum_i \frac{xi}{n}, l + \frac{h1}{f}$((n/2)-C)

Where
l=lower boundary modal class
h=size of mode class
fm=frequency corresponding to modal class
f1=frequency preceding to modal class
f2= frequency proceeding to modal class
x= Data value
n= Number of items
h1=size of median class interval
f= frequency corresponding of median class
C= Cumulative frequency preceding median class

**<<CONFIDENCE RANGE ALGORITHEM(CR)>>**

Initialize N(time, password style , error, Decision agents)
Function CR
Define N;M
Input: N agent:
For M till $M_n$
N agent = Data [M…..$M_n$);
Calculate N [MODE, MEAN, MEDIAN]
Output:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Confidence range N [min Mode, max Mode], [min Mean, max mean], [min median, max median];
Generate EPSB,
End Function CR
N= time, or password style, or Error;
$M_1$=Data [time], $M_{2=}$ Data [upper case], $M_{3=}$Data [lower case], $M_4$= Data [Especial symbol], $M_5$=Data[Number], $M_6$= Data[Number letter], $M_{7=}$Data[Length of password], $M_8$=Data[Length of error password], $M_{9=}$Data[Upper case error pw],$M_{10=}$ Data[Lower case error pw], $M_{11}$= Data[Especial symbol error pw], $M_{12=}$Data[Number error pw], $M_{13=}$Data[No. letter error];
If N [M….$M_n$] agent
Active Function CR;
If decision 1
Input = output of N[M] agents;
Rate of compare:
If rate >= 60
Integrate EPSB
Update current EPSB
Else
Active critical security procedure
Block on Data high level security
For I = 2
If confirm
Unlock Data
Integrate EPSB
Update current EPSB
Else
Deactivate account
Send active code into Authentication user
Send active code into Administration

## 4. Architecture and Design Predictive behavior model

In this section, we Predictive user behaviour in a password(EPSB) by apply statistical analysis. User behaviour in password has many futures such as time, password, and error. Therefore, the use of a password in organizations or institutions may pose many of security problems in availability, such as unauthorized password change, and stop temporary login. To avoid these problems, we firstly proposed four-time agent, password agent, error agent, and Decision agent. Each agent is responsible for following up, registering and analysing the intended data via following up the legitimate user's behaviour in terms of different factors. First, the time when the legitimate user needs to enter a password. Second, the user's behaviour in selecting and formulating his / her password. Third, the previous errors that the legitimate user makes when he tries to login the system. The related data to the legitimate user will be approved based on user successful access with error rate (less than 5 mistakes) followed by a successful login. Otherwise, the data will be ignored as it doesn't relate to the legitimate user behaviour. Decision agent works on receiving the results from other agents and determines the rate or relationship between the current process behaviour (for current user) and the approved confidence range for legitimate user. If the entire identical rate is (>= 60 %), then it is within the authentic range. Otherwise, a confirmation e-mail will be sent to the legitimate user for confirmation. If the legitimate user will confirm the e-mail, the login will be considered as a legitimate access. In case the user will not confirm the e-mail within 3 minutes, the link will be deactivated and another link will be sent to the same e-mail. In case of not confirming the new link, the account will be deactivated permanently and an e-mail will be sent for both (the legitimate user and the admin) for re-registration along with the details showing the (time and IP address) for the person who tries to login. The mechanism that showing how the confidence range works to generate EPSB), as shows in figure 4 :

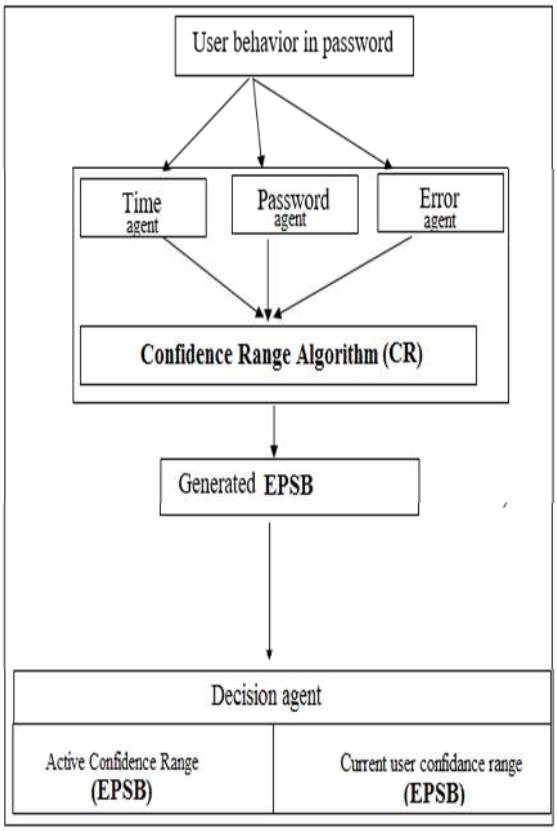



*Figure 4 Architecture Predictive Behaviour Model*

Journal of Theoretical and Applied Information Technology
31st December 2016. Vol.94. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

## 5. TIME AGENT

This section describes the time agent, main tasks to create a EPSB based on confidence range for any user, depends on a speed of click on keyboard from start to input password till press on login. The authors focus on time for diagnosis unauthorized user according to time confidence range.

The EPSB generated based on results of apply confidence range algorithm on outputs of time agent. Normally, the speed of using keyboard has been differing from user to others according to a location of keys, using two or one hands, time of using PC, using keyboard directly and spontaneity, and familiar keyboard. Agent. In addition, time of activation in system concern in an actual time of input password. The purpose of this agent is to monitor the timely behaviour of the user by recording the required time for password entrance for all successful logins. Later, these logins will be saved in a separated table and a set of statistical analysis processes will be performed for generating an approved confidence range based on the user's timely behavior. This agent aims at finding a relationship between the time and the password for detecting any suspicious login even if the intrusive person has the real password as shows in table 2 time agent, and table 1 list of abbreviation below:

*Table 1a List Of Abbreviation*

| | |
|---|---|
| M1 | Mode |
| M2 | Mean |
| M3 | Median |
| Min | Minimum |
| Max | Maximum |
| TCR | Total Confidence range |

*Table 2 Time Agents*

| ID | | MOHANAAD ALNASEERI | | | | | |
|---|---|---|---|---|---|---|---|
| Attempt | Time | Min M1 | Max M1 | Min M2 | Max M2 | Min M3 | Max M3 |
| TCR | | | | | | | |
| | | | CR 1 | | CR 2 | | CR 3 |

## 6. PASSWORD STYLE AGENT

In this section, the author tries to determine a EPSB for the user behavior in creating the style of password for preventing any suspicious password changes. This agent works on monitoring the user's behavior in selecting the password through the analysis of historical previous passwords and tries to find the confidence range for that user based on the following:

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

Then the agent stores all these data and performs the statistical analysis processes in order to generate the confidence range through the use of confidence range algorithm, as shows in table 3 password style agent.

*Table 3 Password Style Agent*

| Attempt | T.CR | Upper case | Min M1 | Max M1 | Min M2 | Max M2 | Min M3 | Maxi M3 |
|---|---|---|---|---|---|---|---|---|
| | | L. case | CR4 | | CR 5 | | CR 6 | |
| | | Number | CR7 | | CR 8 | | CR 9 | |
| | | Length | CR 10 | | CR 11 | | CR 12 | |
| | | Symbols | CR13 | | CR14 | | CR 15 | |
| | | T. Letter | CR 16 | | CR17 | | CR 18 | |
| | | | CR 19 | | CR 20 | | CR21 | |

## 7. DESCRIPTION ERROR AGENT

In this section, the agent tries to determine a EPSB from the errors and categorize them whether they are authenticated or not based on monitoring the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

user behavior while entering the password. In most cases, there are many of repetitive errors for the legitimate user such as: using an old password, repeating a character, using another account's password, not paying attention to the enabled language, or writing the capital letters as small letters and vise-versa. In such cases, most systems deactivate the account for temporal period and then the account will be re-activated after a period. While this agent records and analyzes all the authenticated errors for the legitimate user (authenticated errors is the process of entering wrong password / failure login followed by a successful login given that. Number of wrong attempts will not exceed five attempts). The agent monitors and analyzes the following stored points:

1. Recording the entire wrong password.
2. The number of capital letters in the wrong password.
3. The number of small letters in the wrong password.
4. The overall letters.
5. The number of numeric values in the wrong password.
6. The number of special characters in the wrong password.
7. The length of the password (the number of the overall characters).
8. The number of unsuccessful attempts
9. followed by a successful attempt.

Then the agent records all these errors and analyzes them by applying the confidence range algorithm for all the recorded data, as shows as in table 4 description error agent below.

*Table 4 Description Error Agent*

| Attempt | T.CR | Upper case(Error) | Min M1 | Max M1 | Min M2 | Max M2 | Min M3 | Max M3 |
|---|---|---|---|---|---|---|---|---|
| | | L. case(Error) | CR22 | | CR 23 | | CR24 | |
| | | Number(Error) | CR25 | | CR 26 | | CR 27 | |
| | | Length (Error) | CR 28 | | CR29 | | CR 30 | |
| | | Symbols(Error) | CR31 | | CR32 | | CR 33 | |
| | | T. Letter (Error) | CR 34 | | CR35 | | CR 36 | |
| | | | CR 37 | | CR 38 | | CR39 | |

## 8. DECISION AGENT

This agent monitors and follows up the new user behavior for determining whether she is the legitimate user or not. The agent records and stores the data for the current user and tries to compare it with the activated a EPSB through monitoring the (time, error and password) for the current user and analyze them by applying the confidence range algorithm for generated a EPSB as shows in figure 5 below.


*Figure 5 active EPSB*

Then it extracts the confidence range for the current user and compares it with the approved confidence range in all related issues. In case that the rate is (< = 60 %), then it will send the data as it will be considered as an approved data to 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.

## 9. Critical Security Procedure

Set of activities and procedures that the system will follow in case of detecting any suspicious case 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 [18]. These procedures are as follows:

1. Blocking the high level secured data.
2. Sending an e-mail to the main / in charged user's account and as follows:
   - 2.1 Sending the first activation e-mail and that would be valid for 3 minutes.
   - 2.2 If the user confirms the received e-mail, the block will be removed from

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the data and the system will work smoothly.

2.3 If the user will not confirm the received e-mail, the first email will be expired and another email will be sent and similarly it will be activated for another 3 minutes.

2.4 In case of un confirmation, the following procedures will be taken:

2.4.1 Blocking the user's account.

2.4.2 Sending an e-mail to both (main user and admin) for the re-activation process.

2.4.3 To activate the account, the main user should first activate the account and the admin should confirm that process.

## 10. EVENTS ACTIVE AGENT

The model is facing various events while it is being performed. Usually, each agent's work relates to the events, as he /she records the activities at the beginning of the event until it finishes. The model considers the following three main events as shows as below: -

- Time agent starts when the user enters the password and presses enter.
- Password Style Agent works when the user changes the password.
- Error works when the user enters a wrong password.

## 11. MANUFACTURE, IMPLEMENT & TEST

The model is improved by using PHP, Java Script, these languages are selected for inclusion and checking in a web domain. The model's main components work together to get the required and necessary data for generating the confidence range, see the confidence output diagram. The model is working in coincidence with data classification model to know the data security level. The model controls the user's behavior, recording all the activities done by the user, analyzing them statically and sending the results periodically to decision agent for comparing the new entry with the previous confidence range results to determine the identification percentage and whether the data could benefit the model's data integration. "see figure 6 agents" activities".

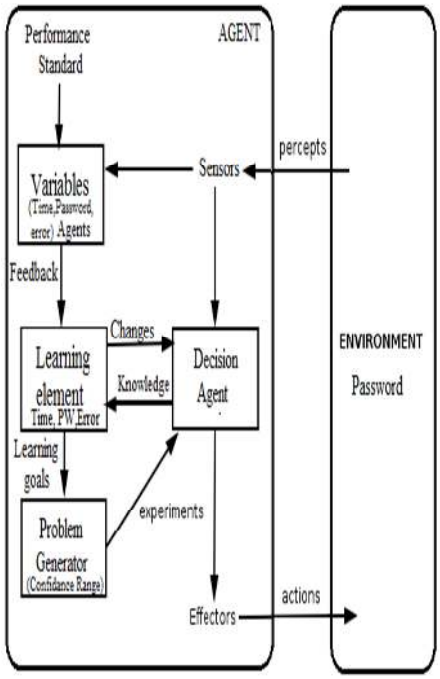



*Figure 6 Agents Activities*

Accordingly, this module works based on the mechanism below: If the user enters correctly form the first attempt to the system, the agent that is monitoring the user would be the time agent only. Yet, other agents will be inactive because users' operation will be out of the agent scope of interest as there are no wrong entries and changes for the passwords. In such a way, the time agent will generate new EPSB as shows as in table 5 figure 7 and below:

*Table 5 current EPSB*

| Max | Min | Current CR(Time) |
|---|---|---|
| 3.3 | 3.3 | **Mode** |
| 3.2 | 3.2 | **Mean** |
| 3.5 | 3.5 | **Median** |

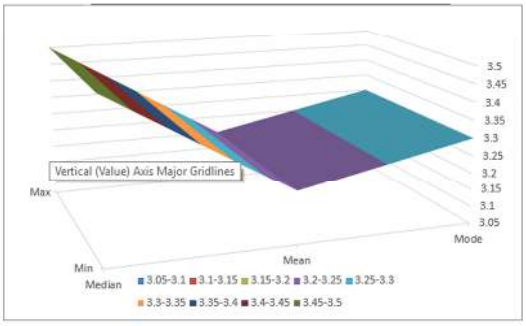



*Figure 7current EPSB*

Journal of Theoretical and Applied Information Technology
31st December 2016. Vol.94. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

for the current user and compare it with the previous dependent one to determine to what extent the old and new EPSBs are the same as shows as in table 6 and figure 8 below.

*Table 6 Previous EPSB*

| ID | Mohanaad Alnaseeri | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Attempt | Time | | Min M1 | Max M1 | Min M2 | Max M2 | Min M3 | Max M3 |
| 1 | 3.4 | TCR | 3.4 | 3.4 | 3.4 | 3.4 | 3.4 | 3.4 |
| 2 | 3.4 | TCR | 3.4 | 3.4 | 3.4 | 3.4 | 3.4 | 3.4 |
| 3 | 3.6 | TCR | 3.4 | 3.6 | 3.4 | 3.5 | 3.4 | 3.4 |
| 4 | 3.8 | TCR | 3.4 | 3.8 | 3.4 | 3.65 | 3.4 | 3.5 |
| 5 | 3.4 | TCR | 3.4 | 3.8 | 3.4 | 3.65/3.525 | 3.4 | 3.4 |
| 6 | 3.9 | TCR | 3.4 | 3.9 | 3.4 | 3.775 | 3.4 | 3.5 |
| 7 | 3.9 | TCR | 3.4 | 3.9 | 3.4 | 3.837 | 3.4 | 3.6 |
| 8 | 3.9 | TCR | 3.4 | 3.9 | 3.4 | 3.868 | 3.4 | 3.7 |
| 9 | 4.2 | TCR | 3.4 | 4.2 | 3.4 | 4.034 | 3.4 | 3.8 |
| 10 | 3.2 | TCR | 3.2 | 4.2 | 3.4 | 4.034 | 3.4 | 3.8/ |
| | | | | CR 1 | | CR2 | | CR3 |

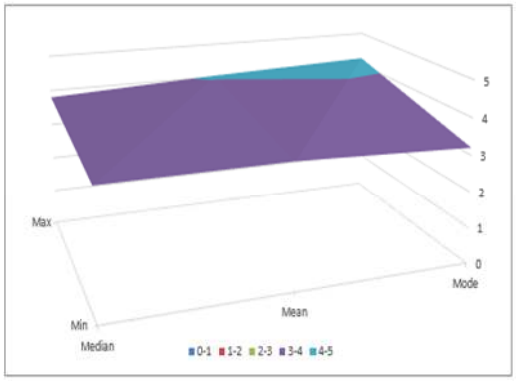



*Figure 8 Previous EPSB*

The decision agent will accept and integrate the EPSB if the similarity is more than 60% or activate Critical Security Procedure if the similarity is less than 60%. The time agent will start consider the time operation from the second character of the password to obtain the closest estimated corrected range when it generates the EPSB. The time agent and the error password agent will monitor and track the user if she fails to inter the password from one to five times. Hence, these agents will generate a new EPSB based on time, length of password, number of letters, number of upper cases, number of lower cases, number of special characters, and how many numbers have been included. All these characters inside the error password will be examined and then generated new EPSB according to these characters as shows in table 7 and figure 9 below.

*Table 7 Current EPSB Error*

| MAX M3 | MIN M3 | MAX M2 | MIN M2 | MAX M1 | MIN M1 | |
|---|---|---|---|---|---|---|
| 3.3 | 3.3 | 3.3 | 3.3 | 3.3 | 3.3 | Time |
| 2 | 2 | 2 | 2 | 2 | 2 | Error PW (Upper case) |
| 0 | 0 | 0 | 0 | 0 | 0 | Error PW (L. case) |
| 7 | 7 | 7 | 7 | 7 | 7 | Error PW(No.) |
| 14 | 14 | 14 | 14 | 14 | 14 | Error PW(Length) |
| 5 | 5 | 5 | 5 | 5 | 5 | Error PW(Symbols) |
| 1 | 1 | 1 | 1 | 1 | 1 | Error PW (Total. L) |

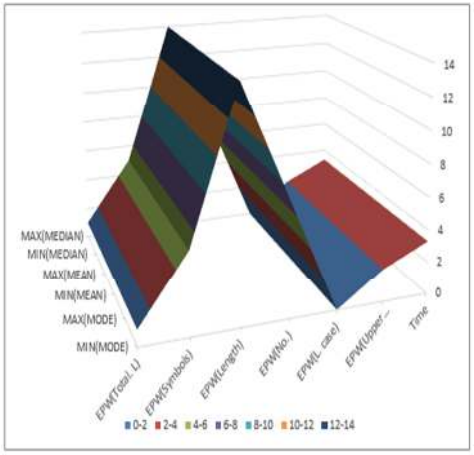



*Figure 9 Current EPSB Error*

This generated EPSB will be compared with previous dependent one as shows as figure 10 and table 8 and below:

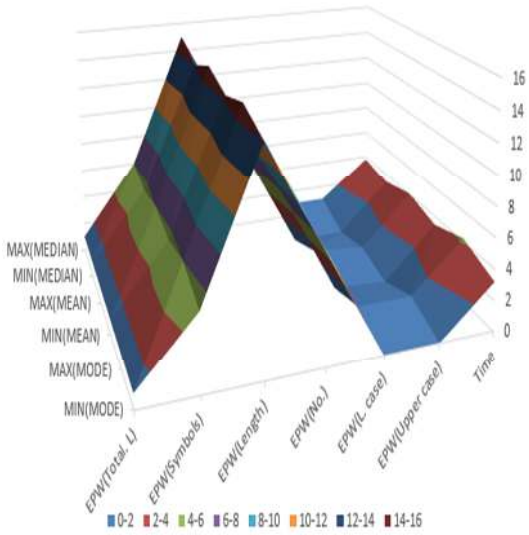



*Figure 10 Previous Error*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Table 8 Previous EPSB Error*

| 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 | | | **0** | **1** | **0** | **0.6** | **0** | **1** |
| If max Rounded into max values | | | | | | | | |
| | | **L. case** | **CR22** | | **CR23** | | **CR24** | |
| @@@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** | **CR25** | | **CR26** | | **CR27** | |
| @@@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 | | | **7** | **8** | **7.5** | **8** | **7** | **8** |
| If max Rounded into max values | | | | | | | | |
| | | **Length** | **CR28** | | **CR29** | | **CR30** | |
| @@@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** | **CR31** | | **CR32** | | **CR 33** | |
| @@@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** | **CR34** | | **CR35** | | **CR36** | |
| @@@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 |
| | | | **1** | **1** | **1** | **1** | **1** | **1** |
| | | | **CR37** | | **CR38** | | **CR39** | |

This operation will also work within the frame of similarity ration under decision agent control. Consequently, the last ten error attempts followed by correct try will be accepted and then integrated with the previous dependent EPSB.

The password agent is activated only when the user changes the password. This agent will generate EPSB for the current user based on the length of password, number of letters, number of upper cases, number of lower cases, number of special characters, and how many numbers have been included as shown in table 9 and figure 11 below:

*Table 9current EPSB PW*

| MAX M3 | MIN M3 | MAX M2 | MIN M2 | MAX M1 | MIN M1 | |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | PW (Upper case) |
| 2 | 2 | 2 | 2 | 2 | 2 | PW (L. case) |
| 4 | 4 | 4 | 4 | 4 | 4 | PW(No.) |
| 13 | 13 | 13 | 13 | 13 | 13 | PW(Length) |
| 5 | 5 | 5 | 5 | 5 | 5 | PW(Symbols) |
| 2 | 2 | 2 | 2 | 2 | 2 | PW (Total. L) |

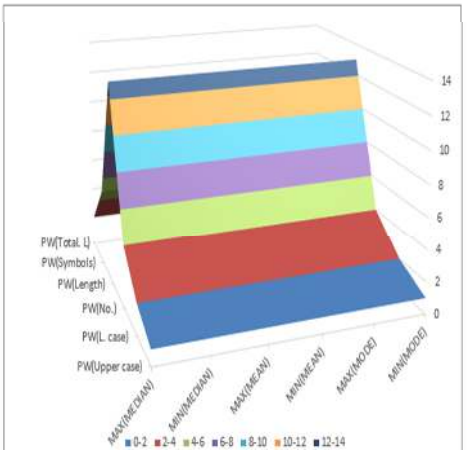
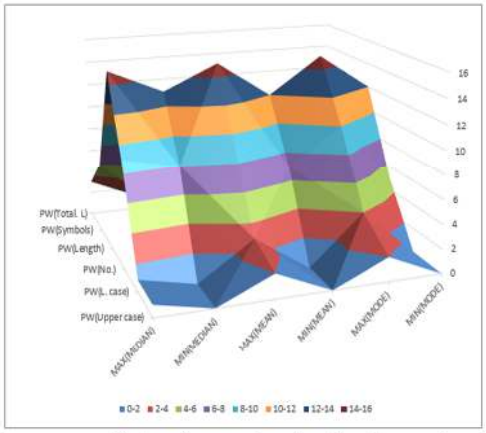



*Figure 11 Current EPSB PW*

Then it sends current EPSB to the decision agent to compare it with previous dependent EPSB according the similarity rule as shows as in table 10 and figure 12 below.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

*Table 10 Previous EPSB PW*
*Figure 12 Previous EPSB PW*




| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Max |
| M1976@1976moh | TCR | 3 | 0 | 3 | 0 | 1.875 | 0 | 1 |
| Lkikh1##1976 | TCR | 4 | 0 | 4 | 0 | 3/2.94 | 0 | 1 |
| If min Rounded into min values<br>If max Rounded into max values | | | 0 | 4 | 0 | 3 | 0 | 1 |
| | | Number | CR7 | | CR 8 | | CR 9 | |
| @@@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/ 8.5 | 8 | 9 |
| Lkikh1##1976 | TCR | 5 | 5 | 10 | 7 | 9 | 8 | 9 |
| If min Rounded into min values<br>If max Rounded into max values | | | 5 | 10 | 7 | 9 | 8 | 9 |
| | | Length | CR 10 | | CR 11 | | CR 12 | |
| @@@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 | CR13 | | CR14 | | CR 15 | |
| @@@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 16 | | CR17 | | CR 18 | |
| @@@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 19 | | CR 20 | | CR21 | |

| M3 |
|---|
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 1 |
| 6 |
| 0 |
| 0.5 |
| 1 |

The model is implemented on 12 students from IT department in Al-Buraimi University College(BUC), Oman by using hybrid cloud computing for 10 days. Students have selected their own passwords, signed in and out and used the system. The model recorded and analyzed all the activities of each user. Generally, the model produces three EPSB based on confidence ranges for each part used in the analysis, as shows as in figure 12 snapshot from password agent:

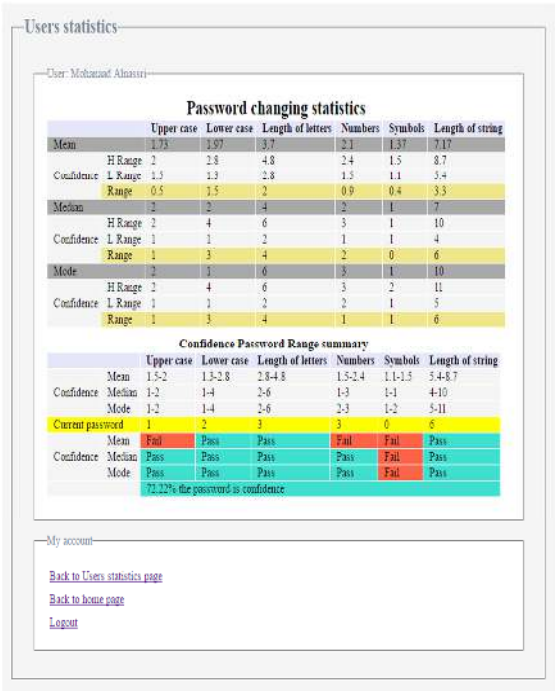



*Figure 12 Snapshot From System*

During the last day, users have been substituted, as each user has used another user's password to check the system's ability in diagnosing the right user. The results were as the following:

- The model could diagnose 8 users out of 12 password entries.
- The model could diagnose 9 users out of 12 password change.
- The model could diagnose 10 users out of 12 as wrong users.
- The model could diagnose all entry trials of wrong users.

## 12. CONTRIBUTION OF STUDY

The contributions of this study will enhance the level of data confidentiality within the cloud computing through:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. proposing a new algorithm (confidence range) which works on monitoring the behavior of each user and generating EPSB for each. It connects with the user account to achieve the following points:
a. To be able to diagnoses the unauthorized user when s/he logs in form the first attempt directly;
b. to be able to diagnoses the errors of authorized user to avoid temporary pending;
c. To be able to diagnoses the unauthorized change for the password.

## 13. CONCLUSION

According to the above test results, implementing the above model in any organization strengthens the users' confidence through the wrong user diagnosis possibility even if their password is correct and they used the in charge user's laptop based on the time taken while password entry; consequently, this will add a new security level to the user. It will also strengthen the wrong user's password change diagnosis based on the Password Style Agent, so you can determine the closest reliable range while choosing the password; if the change is not included in this range, it will not be changed until following all critical security procedures. Additionally, the model also could diagnose ultimate amount of reliable errors made by the in charge user, depending on saving the in charge user's previous errors and differentiation them from the wrong user's entries; consequently, the system prevents the temporary blockings and strengthens availability. Applying critical security procedures while diagnosing any suspicious activity of the user results in reducing possible impact and damage of the data that are with high security level and have a major impact on the system to strengthen confidence range and data availability.

## REFERENCE

[1] A. Parvez, "Design and Implementation of Public Key Infrastructure: a Proposed Solution for Bangladesh", MSc Thesis, Independent University, Bangladesh, May 2006.

[2] Z. Shen, Li Li, Fei Yan, and Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform," in International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 1, Changsha, China, 2010, pp. 942 – 945.

[3] Z. Shen and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," in 2nd International Conference on Signal Processing Systems (ICSPS), vol. 2, Dalian, China, 2010, pp. 11-15.

[4] M. Ashamed, T. Dillon and E. Chang, "SLA-based Trust Model for Cloud Computing," in 13th International Conference on Network-Based Information Systems, Takayama, Japan, 2010, pp. 321 – 324.

[5] Z. Yang, L. Qiao, C. Liu, C. Yang, and G. Wan, "A Collaborative Trust Model of Firewall-through based on Cloud Computing," in 14th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Shanghai, China, 2010, pp. 329 – 334.

[6] H. Sato, A. Kanai, and S. Tanimoto, "A Cloud Trust Model in a Security Aware Cloud," in 10th IEEE/IPSJ International Symposium on Applications and the Internet (SAINT), Seoul, South Korea, 2010, pp. 121 – 124.

[7] W. Li, L. Ping, and X. Pan, "Use trust management module to achieve effective security mechanisms in cloud environment," in International Conference on Electronics and Information Engineering (ICEIE), vol. 1, Kyoto, Japan, 2010, pp. 14-19.

[8] Z. Song, J. Molina and C. Strong, "Trusted Anonymous Execution: A Model to RaiseTrust in Cloud," in 9th International Conference on Grid and Cooperative Computing (GCC), Nanjing, China, 2010, pp. 6 – 138.

[9] S. Chen, S. Nepal, and R. Ping Liu, "Secure Connectivity for Intra-cloud and Inter-cloud Communication", ICPP Workshops, 2011, pp. 154-159.

[10] N. Grozev and R. Buyya, "Inter-Cloud Architectures and Application Brokering: Taxonomy and Survey" Cloud Computing and Distributed Systems (CLOUDS) Laboratory, Department of Computing and Information Systems, The University of Melbourne, VIC 3010, Australia, 2012.

[11] Zhu Tianyi, Liu Weidong, and Song Jiaxing," An efficient Role Based Access Control System for Cloud Computing", 11th IEEE International Conference on Computer and Information Technology,2011.

[12] Victor Chang, Yen-Hung Kuo, Muthu Ramachandran, Cloud computing adoption

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

framework: A security framework for business clouds, Future Generation Computer Systems 57 (2016) 24–41

[13] M. Shakir, A. Abubakar, Y. Yousoff, M. Wassem, M. Hammood," cloud computing (security and privacy): A review", Journal of Theoretical and Applied Information Technology, 2016

[14] M. Shakir, A. Abubakar, Y. Yousoff,A. Sagher, H. Alkayali ,"Diagnosis security problems in cloud computing for business cloud", Journal of Theoretical and Applied Information Technology, 31st August 2016. Vol.90. No.2.

[15] M. Shakir, S. Ajaj ," The Application of the Enterprise Systems through the Cloud Computing in Company: A Review and Suggestions", Journal of Al-TURATH University college, (ISSN 2074-5621), Apr.2015.

[**16**] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Technical Report, Version 1.0, February, 2014

[17] NIST, An introduction to computer security. Publication 800-12, 1996, downloaded from http://csrc.nist.gov/publications/ nistpubs/800-12/handbook.pdf.

[18] M. Shakir , A. Abubakar,Y. Yousof, M. Waseem , M. Al-emran," Model of security level classification for data in hybrid cloud computing",Journal of Theoretical and Applied Information Technology, 31st December 2015. Vol. 94 No 2