Measuring the Efficiency and Usability of Session Password based Authentication Systems

Annum Tasneem, Huma Tauseef, Saima Farhan, Muhammad Abuzar Fahiem

Department of Computer Science

Lahore College for Women University, Lahore, Pakistan

***Abstract*— Key factor that can determine the success and failure of a software system is known as the usability attribute. The aim of this research is to highlight the factors that can help in understanding usability for such authentication systems where privacy and security play an important role. For that purpose a comprehensive literature survey has been conducted to evaluate the usability factors included in various well-known usability models. After analyzing the results 10 factors were chosen to form the proposed usability model UMA14 (Usability Model of Authentication 2014).The novelty of the proposed model lies in the fact that it contains the usability criteria for measuring usability factors. Defining the usability criteria helps one understand the usability factors in detail so that there is no ambiguity while comprehending them. Two authentication schemes based on session passwords are developed and the proposed usability model is testing using GNU PSPP.**

***Keywords*— Authentication Systems, Usability Factors, Usability Models, Session Passwords.**

I. INTRODUCTION

User authentication has become the key feature for accessing various network facilities and computing services nowadays. Nearly everything is password protected and requires some form of validation. Hence, in order to reach a particular destination, one has to go through the process of authentication. In such scenarios, both usability and security play an important part.

However, security and usability do not merge well together because they both have interest conflicts when it comes to the system users and owners [1]. But according to [2] usability aims at making actions desirable for system users whereas security aims at making actions undesirable for system users. So it can be possible that improving one can improve the other.

Usability plays a major role in covering up the inconsistencies and any other faltering blocks in the system of user and product interaction. For better product quality it is necessary to measure usability at every stage of the process. This is done by applying the methods of usability testing and by Analysis of the defects.

Usability consists of product attributes like important system properties, functionality, efficiency, style of the interface, reliability and structure. The successful designing of product attributes is very important because the entire usability measurement process relies upon them. Determining the correct usability factors for a given scenario is a challenging task and often requires a lot of focus and understanding of the target domain. Once identified, the next step is to organize them in the form of a model or framework so that it can be used as a standard tool. Such a model or framework is called a Usability Model.

Authentication is the process that allows a remote access client to connect with a remote access server. This is usually done using specially designed authentication protocols. There are in general 3 factors of user authentication factors. They are passwords, tokens and biometrics. The most common and simple form of an authentication model in terms of implementation a Password. However, when it comes to reliability, passwords turn out to be very weak because they can be easily guessed or hacked. A Token is any device or object that can be used for authenticating a user. Common examples of tokens are credit cards, ATM cards and physical keys. Since tokens are simple and quite cheap, they become easy to forge and hence can be reproduced. To secure tokens, they are normally implemented with PIN codes [3]. The third factor of authentication is known as Biometrics. Biometric Systems are measured using a physical characteristic which is found to be unique to a particular individual. Common Biometric systems include Voice recognition, Retina scan, Fingerprint scan, Facial recognition [3].

There are 3 common methods of authentication; digital signature, public key cryptography and one time password. A digital signature is calculated from a signed document. It is verified by the client who, decrypts it with the server's public key and then compares it with the value calculated from the message received. The Public key cryptography makes use of two keys (one private and one public). Both keys are linked together using a mathematical equation. The public key is used for both encryption and verification. There are two types of One-time Password, challenge response password and password list. They both help avoid problems associated with password reuse. In the challenge response password after the user is identified a challenge value is issued in response. On the other hand a password list is used to make a list of all the passwords that are used by a person while accessing the

system in sequential order.

II. LITERATURE REVIEW

The term usability cannot be described using a standard definition because it is impossible to express it in a single objective measure. Bevan described his definition of usability in terms of three factors; Efficiency, Effectiveness and Satisfaction [4]. Nielsen on the other hand described his usability factors to be Efficiency, Learnability, Memorability and Satisfaction [5]. Shneiderman defined five measurable human factors (Speed of performance, Subjective satisfaction, Retention over time, Time to learn and rate of error by users) that can be further used for the evaluation of human factor goals [6]. Dix et.al defined three main headings of usability factors such as learnability, robustness and flexibility and then further divided those factors into sub factors [7]. According to Scholtz, usability mainly has 5 attributes (Learnability, Efficiency, Memorability, Errors and user satisfaction) and its significance varies from application to application [8]. Authors like [9] believed that usability comprised of three factors; such as efficiency, effectiveness and satisfaction. According to [10] the usability measures used in around 180 studies and research include Effectiveness, Accuracy, Recall, Completeness, Quality of outcome and Experts' assessment. A comparative analysis of usability factors and their preference by different authors is given in table 1.

Determining the correct usability factors for a given scenario is a challenging task and often requires a lot of focus and understanding of the target domain. Once identified, the next step is to organize them in the form of a model or framework so that it can be used as a standard tool. Such a model or framework is called a Usability Model.

According to [11] there are 3 ways of measuring the usability of a product. Usability can be measured from: 1) the products view, by using the attributes of a product. 2) The users view, by understanding the users' attitude and effort. 3) The examination of product and user interaction.

There are some well-known metric models. General electric models/ factors, criteria, metrics model (FCM) is a hierarchal quality model proposed by [12]. It consists of 11 quality factors, about 25 supporting quality criteria and 41 quality metrics. In this model the usability criteria is divided into 3 parts; Operability, Training and Effectiveness.

Boehm's quality model defines the quality of a software qualitatively, using a set of attributes and metrics. Boehm's model is structured around three types of characteristics, which are high-level, intermediate and primitive. The high-level characteristics answer three important software questions that buyers usually have, like Portability, Maintainability and Utility. The Intermediate-level characteristics represent 7 quality factors (Portability, Reliability, Efficiency, Usability, Testability, Understandability and Flexibility) that are expected in every software system [13].

The MUSic Model, also known as The Metrics for Usability Standards in Computing [14] was introduced to define such measures which could help in determining software usability. An example of one such usability metric would be the user performance measures. Quality in Use Integrated Model (QUIM) [15] is a hierarchal usability measurement model that decomposes usability into 3 parts. They are factors, criteria and metrics. QUIM serves as a consolidated model, which means that other models can be derived from it. Eason Model [16] is a usability model that is divided into 3 independent variables (User characteristics, System Functions and Task characteristics) and one dependent variable (User reaction). In this model usability is envisioned as a relationship. By varying the independent variables the outcome of usability can be changed.

ISO 9126 (ISO, 1991) model defined the sub attributes of usability such as Understandability, Operability, Learnability, Compliance etc.

The usability models proposed so far are very effective. They can be used to target a number of software products. However, if one was to design a usability model for a more specific field of interest like authentication systems, the approach used would be quite different from the rest.

Authentication systems do not compromise over safety at all. Therefore, while designing a usability model for an authentication system one should include such usability factors that relate with authentication. From Table 1, a graph has been constructed and presented in Figure 1. It illustrates the significance and usage of usability factors in ascending order.

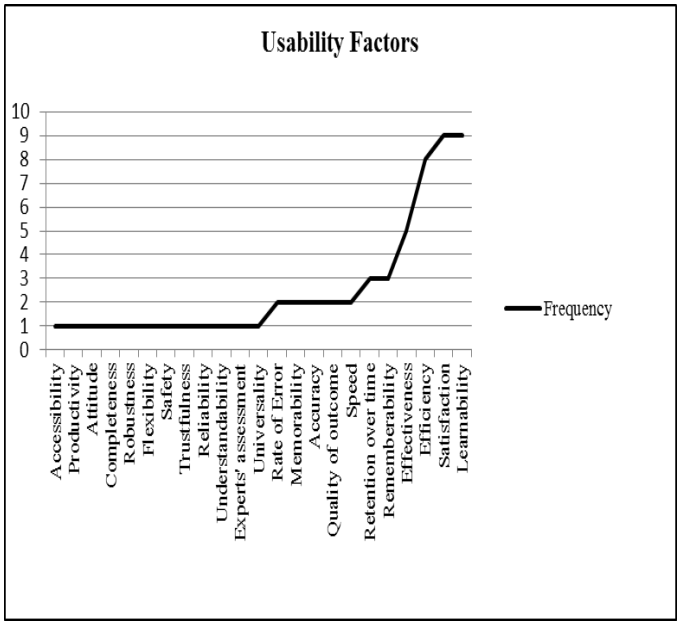

Fig.1: Different Usability Factors Used in Literature

TABLE 1
COMPARISON OF REQUIREMENT VALIDATION TECHNIQUES PROPOSED BY VARIOUS AUTHORS

Usability Factors	Nielson, 1994 [5]	Bevan, 1994 [4]	Dix, 1998 [7]	Ben, 1998 [6]	Lauesen, 1998 [17]	Ferre, 2001 [18]	Scholtz, 2004 [8]	Frokjaer, 2000 [9]	Hornbaek, 2006 [10]	Constantine, 1999 [19]	Shackel, 1991 [20]	Seffah, 2006 [15]
Efficiency	✓	✓	×	×	✓	✓	✓	✓	×	✓	×	✓
Effectiveness	×	✓	×	×	×	×	×	✓	✓	×	✓	✓
Satisfaction	✓	✓	×	✓	✓	✓	✓	✓	×	✓	×	✓
Learnability	✓	×	✓	✓	✓	✓	✓	×	×	✓	✓	✓
Retention over time	×	×	×	✓	×	✓	×	×	×	×	✓	×
Rememberability	×	×	×	×	✓	×	×	×	✓	✓	×	×
Memorability	✓	×	×	×	×	×	✓	×	×	×	×	×
Rate of Error/Reliability	×	×	×	×	×	✓	✓	×	×	✓	×	×
Flexibility	×	×	✓	×	×	×	×	×	×	×	×	×
Robustness	×	×	✓	×	×	×	×	×	×	×	×	×
Completeness	×	×	×	×	×	×	×	×	✓	×	×	×
Productivity	×	×	×	×	×	×	×	×	×	×	×	✓
Accuracy	×	×	×	×	×	×	×	×	✓	×	×	✓
Universality	×	×	×	×	×	×	×	×	×	×	×	✓
Quality of outcome	×	×	×	×	×	×	×	×	✓	×	×	✓
Safety	×	×	×	×	×	×	×	×	×	×	×	✓
Trustfulness	×	×	×	×	×	×	×	×	×	×	×	✓
Accessibility	×	×	×	×	×	×	×	×	×	×	×	✓
Attitude	×	×	×	×	×	×	×	×	×	×	✓	×
Understandability	×	×	×	×	✓	×	×	×	×	×	×	×
Experts' assessment	×	×	×	×	×	×	×	×	✓	×	×	×
Speed	×	×	×	✓	×	×	×	×	×	×	✓	×

I. METHODOLOGY

A comprehensive literature survey is conducted to evaluate the usability factors included in various well-known usability models. By reviewing these different usability models a new framework by the name of UMA14 (Usability Model of Authentication 2014) has been proposed. It includes various usability factors from the ones mentioned in Table 1. The novelty of the proposed model lies in the fact that it contains the usability criteria for measuring usability factors. Defining the usability criteria helps one understand the usability factors in detail so that there is no ambiguity while comprehending them.

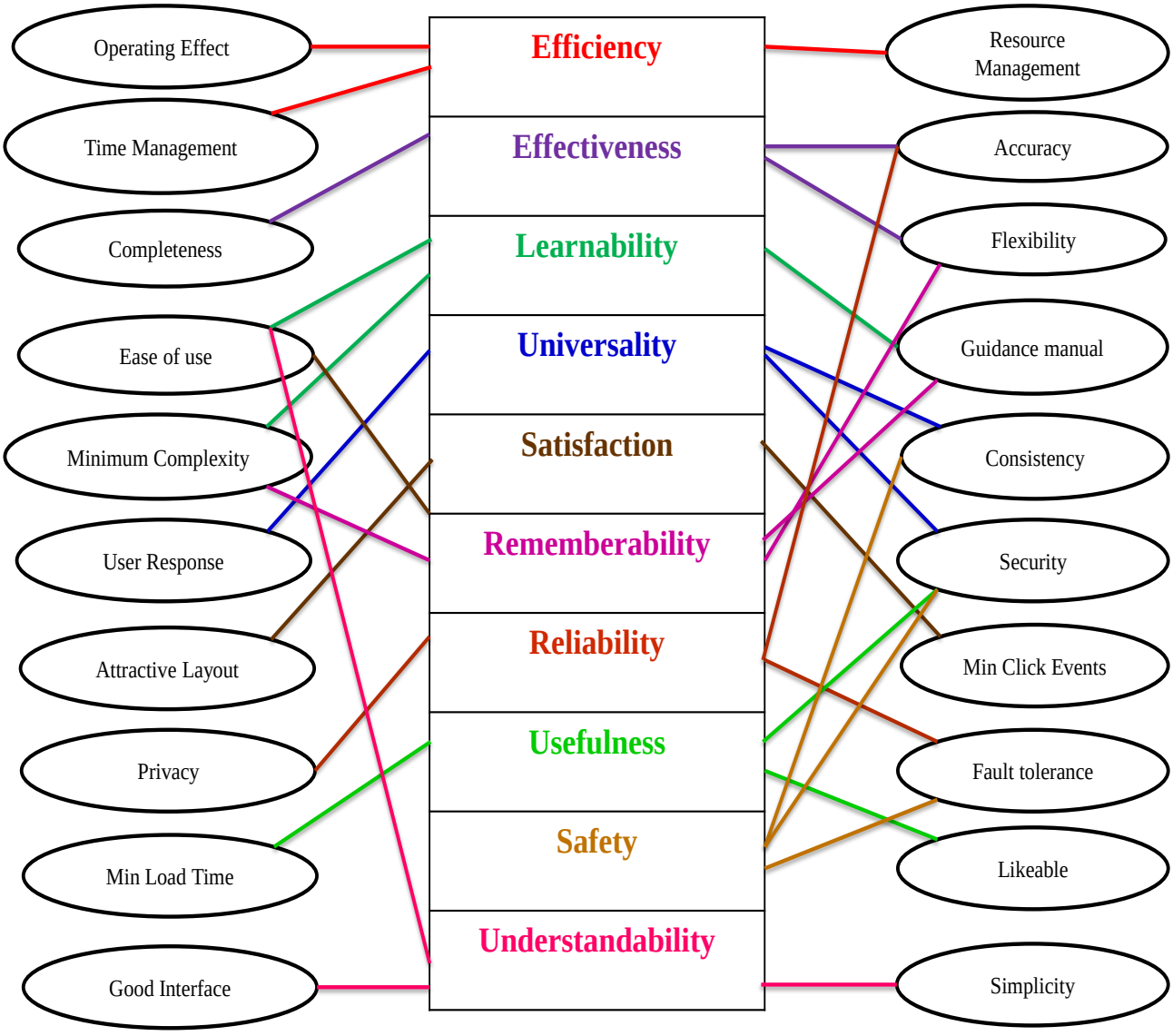

Fig.2: Proposed UMA14Model

To validate the proposed usability model, two authentication schemes were designed based on session passwords given below:

- Hybrid-Textual Authentication Scheme

The user registers by first entering a user name, email address and then assigning priority from 1-8 to the colours displayed on screen as shown in Figure 3. Same priority can also be assigned to different colours.

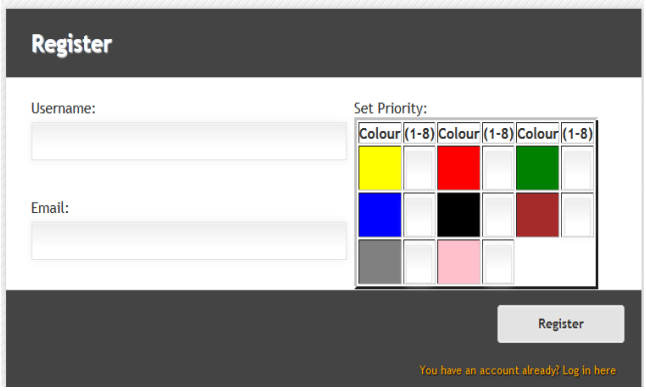

Fig.3: Registration Module For Hybrid-Textual Authentication Scheme

After successfully registering, user logins to his/her account as shown in Figure 4.

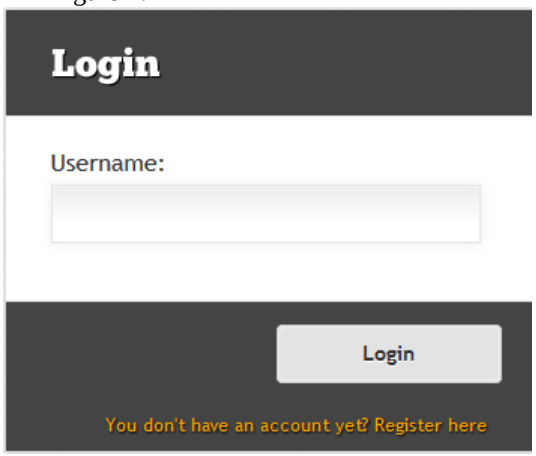

Fig 4: Login Interface For Hybrid Textual Authentication Scheme

The user must enter his/her login name before clicking on the login button. The new interface displayed will consist of an 8x8 grid filled with random numbers and a colour strip of 8 colours randomly paired into groups of 2. Each pair will act as the row and column of the grid [21]. The number obtained by the intersection of the row and column will provide the session password. However, the user must remember the digits that he/she entered at the time of registration and the corresponding colours. The login procedure through session passwords is explained and shown below in Figure 5, 6 and 7 with an example.

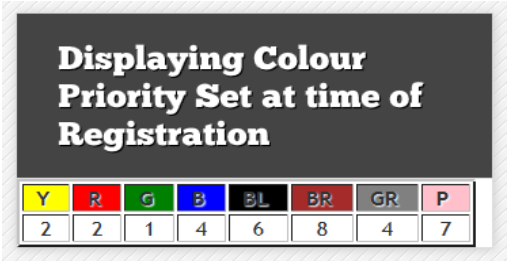

Fig 5: Setting Priority Of Colours

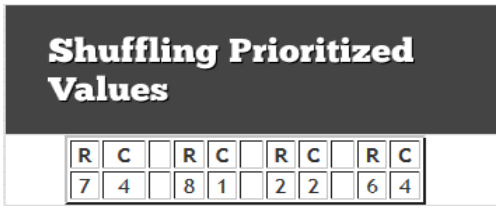

Fig 6: Shuffling Priority Values And Pairing Them In Groups Of 2

The values shown in Figure 6 will become the row and column of the 8x8 grid shown in Figure 7. Hence a session password of 4 digits will be acquired.

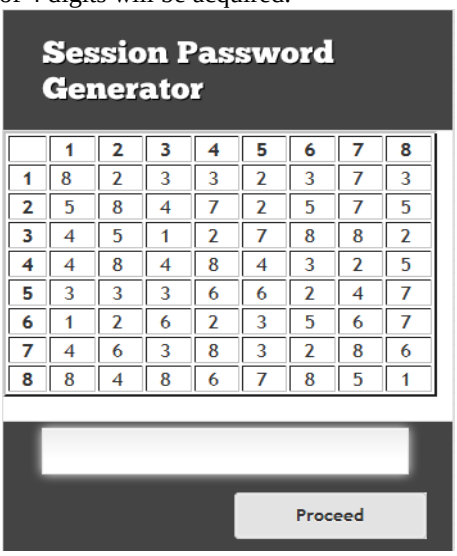

FIG 7: Grid.

- Pair-based Authentication Scheme

The user registers by entering a user name and an alphanumeric password of length 8.

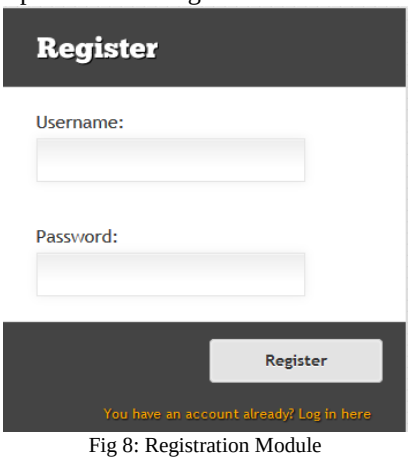

Fig 8: Registration Module

The password is known as a secret pass and it is used to generate the session password. During the login phase, the user must enter his/her login name as shown in Figure 9.

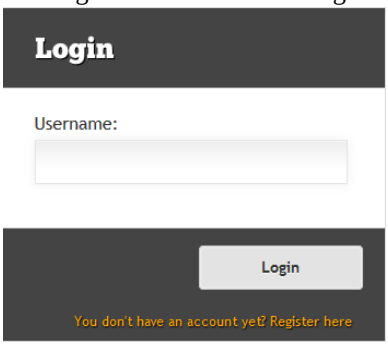

Fig 9: Login Module

After clicking on the login button, a new interface will open. It will consist of a 6x6 grid filled with random alphanumeric characters. The user must enter the password according to his/her secret pass. The secret pass has to be considered in terms of pairs such that each pair becomes a row and a column of the grid [22]. Figure 10 and 11 given below will help understand the working of pair based authentication scheme better.

Fig 10: Pairing Of Secret Pass

Figure 10 shows the secret pass entered by the user. The 8 character password is divided into 4 pairs. Each pair will act as the row and column of the grid shown in Figure 11.

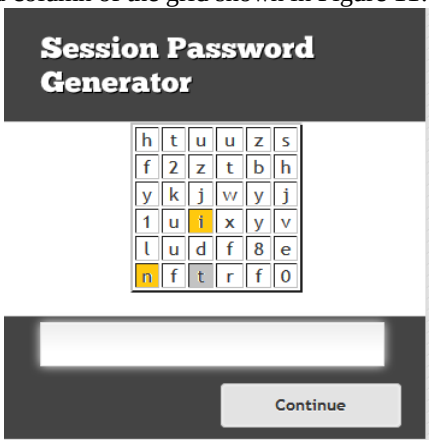

fig 11: 6x6 Grid.

From figure 10, we can see that “n” is the first row and “i” is the first column, so we trace them on the grid of Figure 11 and get “t”. This will act as the first character of the session password. The rest of the session password can be traced in the same manner.

After the validation of the proposed model a refined model is proposed. The refined model is given in figure 12.

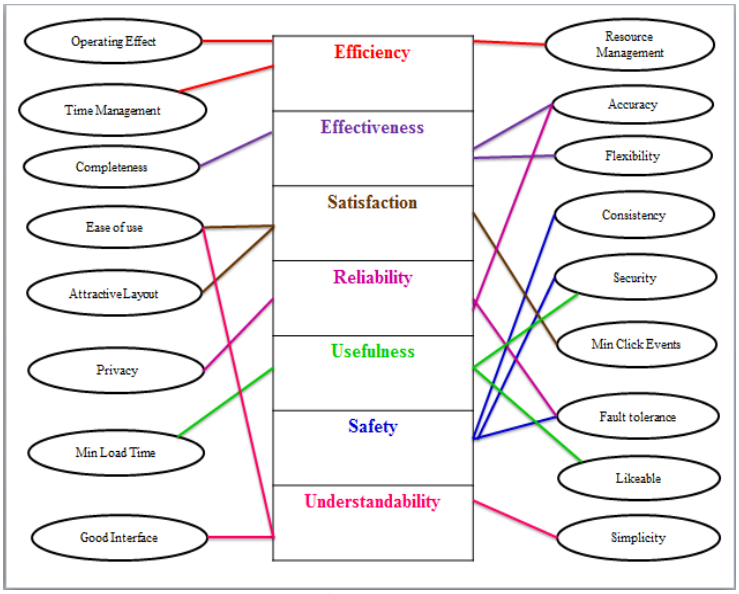

Fig 12: Refined UMA14

I. RESULTS AND DISCUSSION

For the justification of the proposed usability model, a survey was conducted. A total of 30 respondents affiliated with the field of computer science were asked to take the survey. Respondents included students, professionals and both. Results pertaining to the usability factors included in the proposed usability model are illustrated in figures 13 to 22.

According to the results of the second survey it can be inferred that people find session passwords to be a better choice than ordinary textual or graphical passwords since they ensure more safety and security from attacks like dictionary and brute force. And that the usability of authentication systems based on session passwords can be measured using the

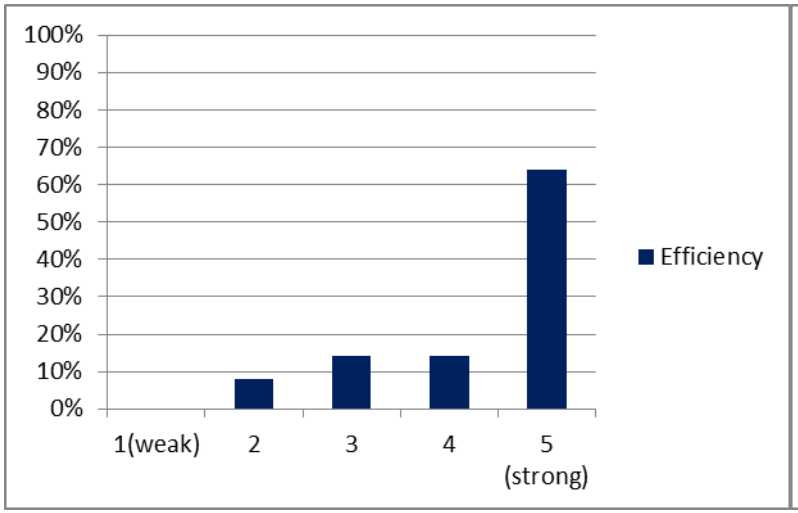

Fig 12: Efficiency Graph

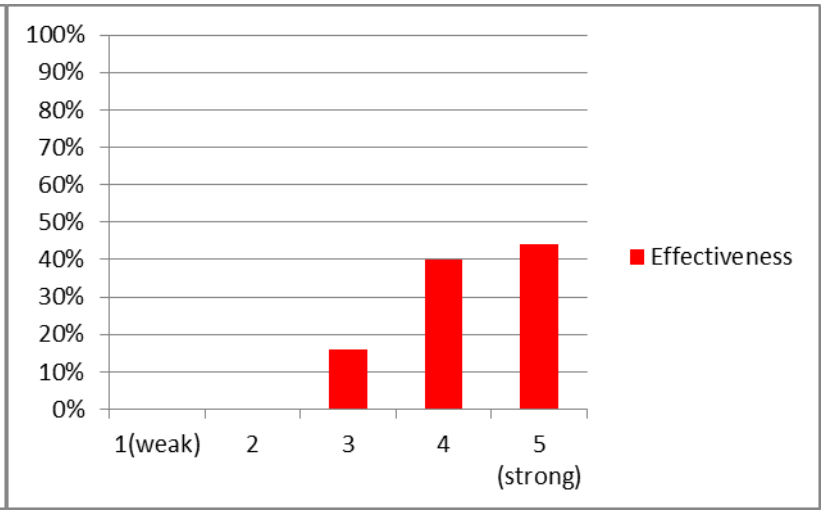

Fig 13: Effectiveness Graph

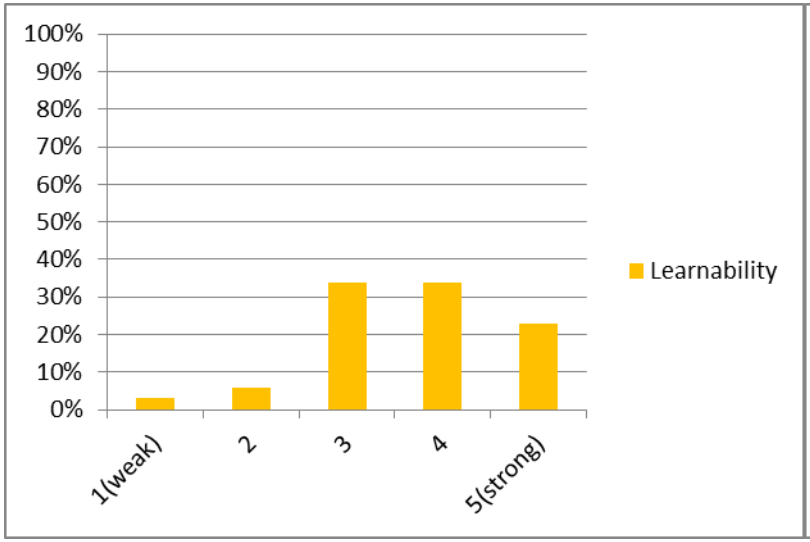

Fig 14: Learnability Graph

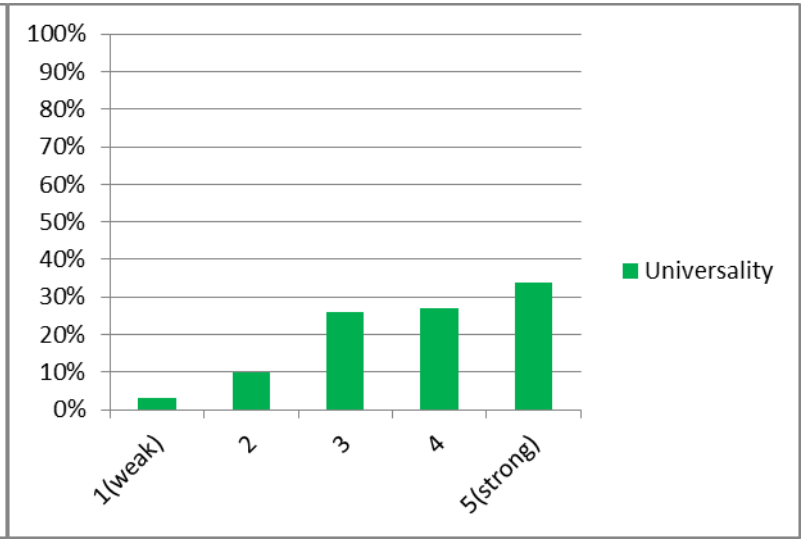

Fig 15: Universality Graph

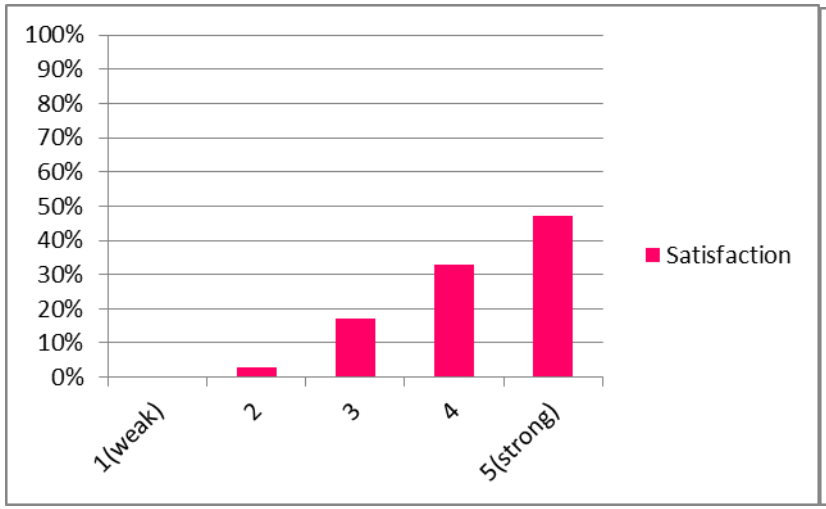

Fig 16: Satisfaction Graph

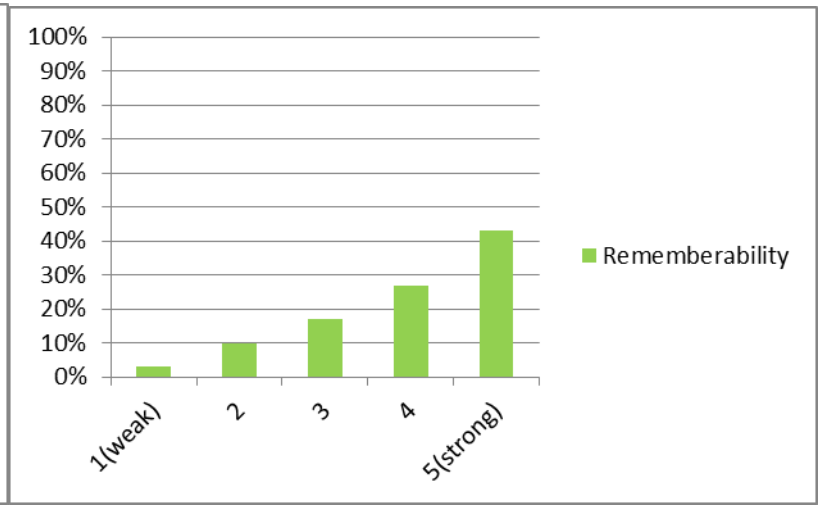

Fig 17: Rememberability Graph

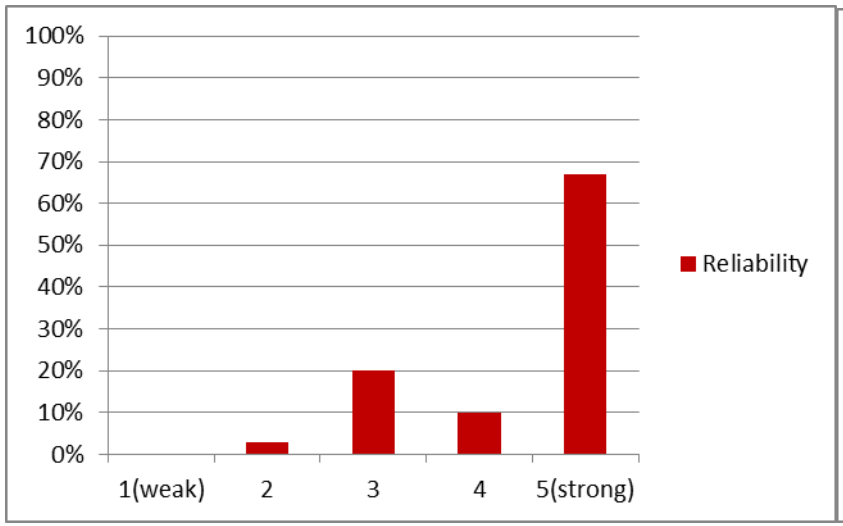

Fig 18: Reliability Graph

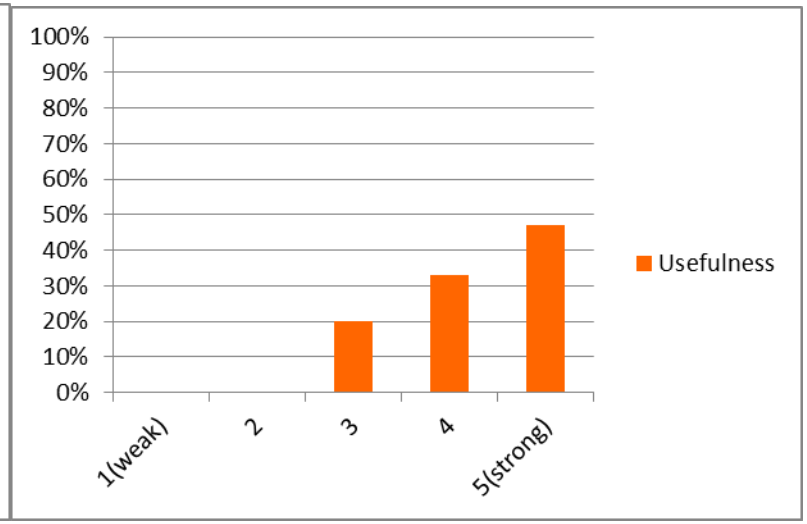

Fig 9: Usefulness Graph

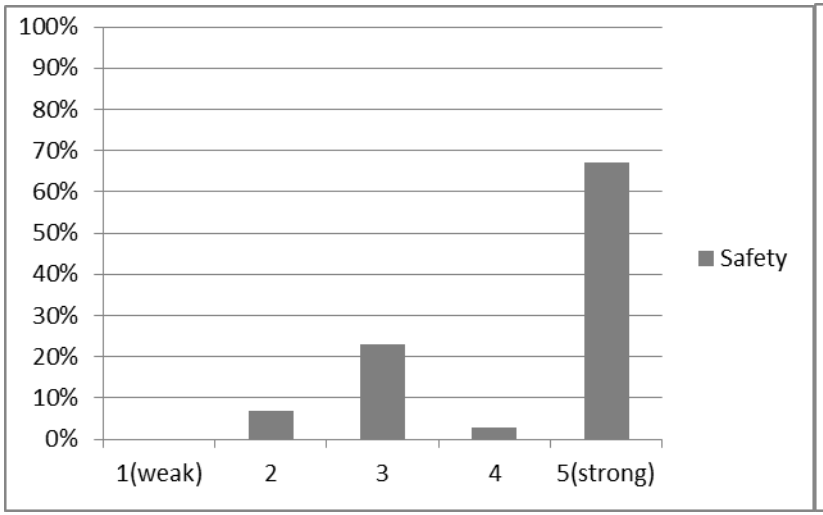

Fig 10: Safety Graph

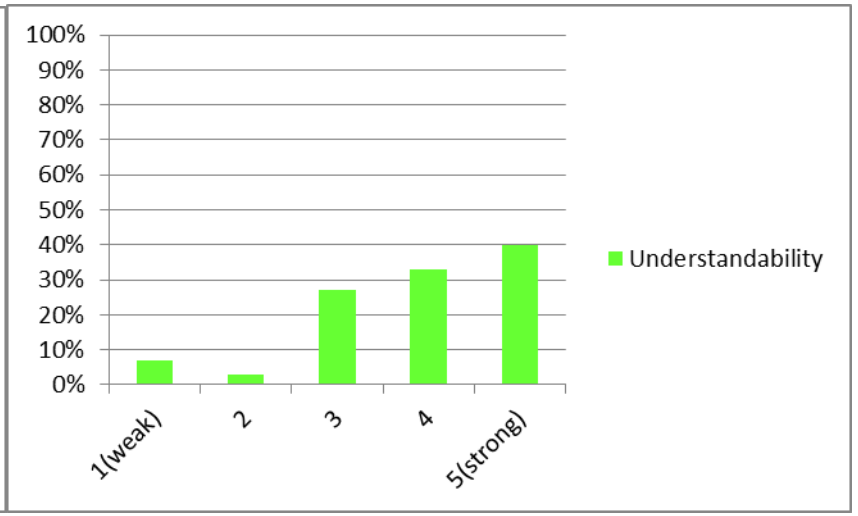

Fig 11: Understandability Graph

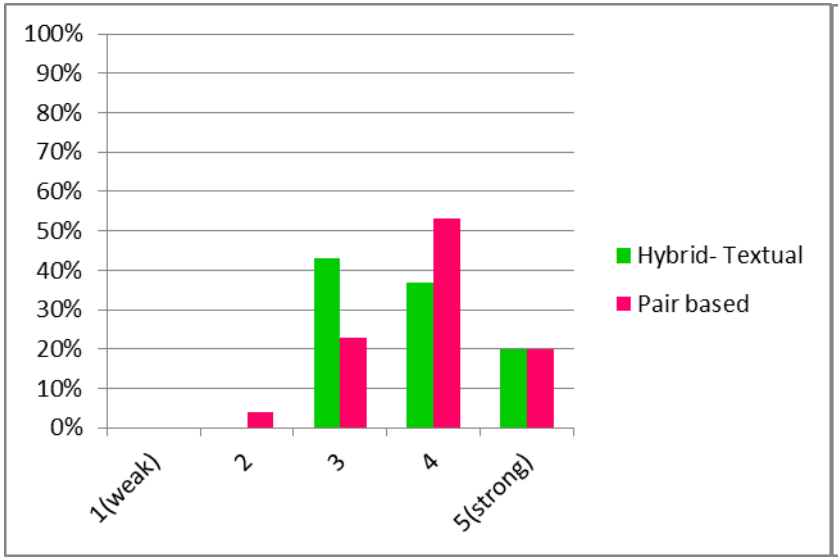

Fig 12: Usability Ratings Of Hybrid-Textural And Pair Based Authentication Schemes.

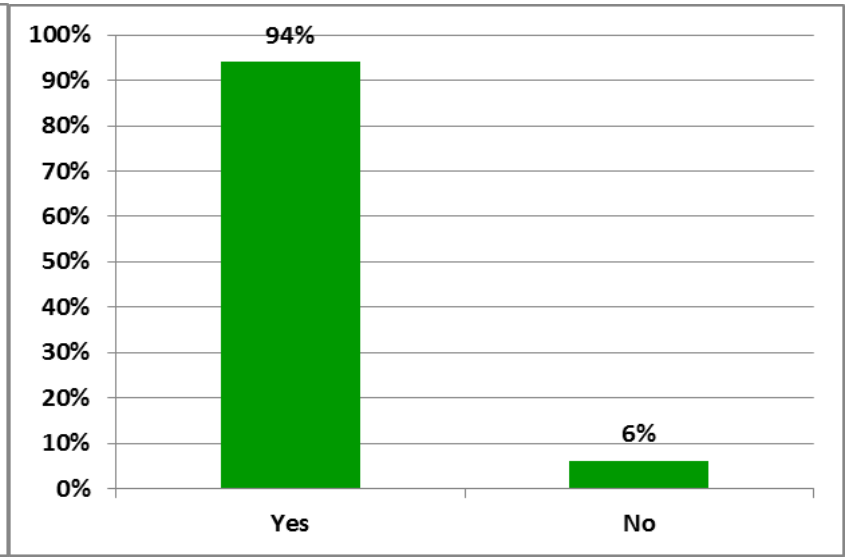

Fig 13: Satisfaction Ratings Of Hybrid-Textural And Pair Based Authentication Schemes

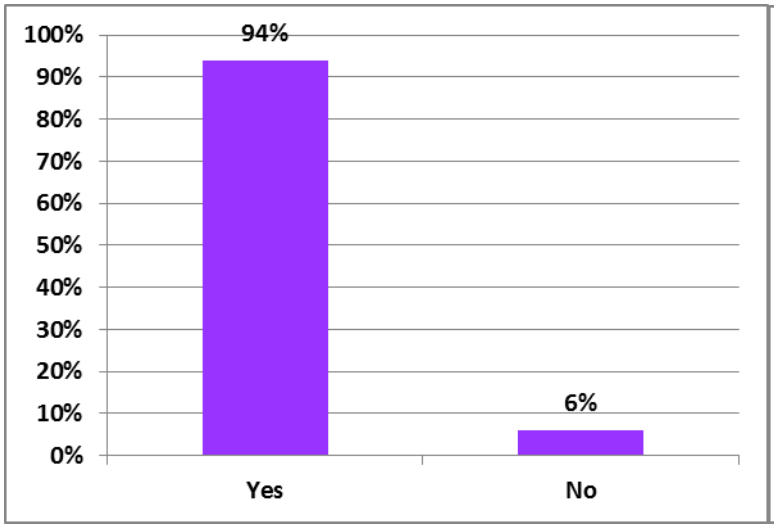

Fig 14: Safety And Reliability Ratings Of Hybrid-Textural And Pair Based Authentication Schemes

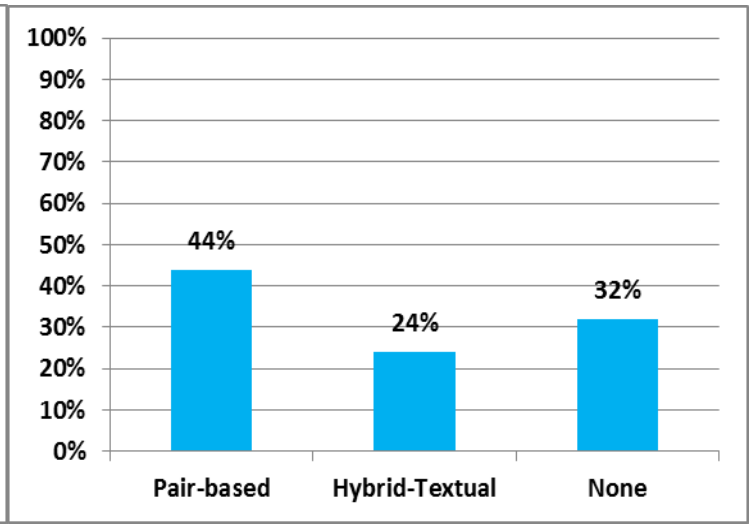

Fig 15: Understandability Ratings Of Hybrid-Textural And Pair Based Authentication Schemes

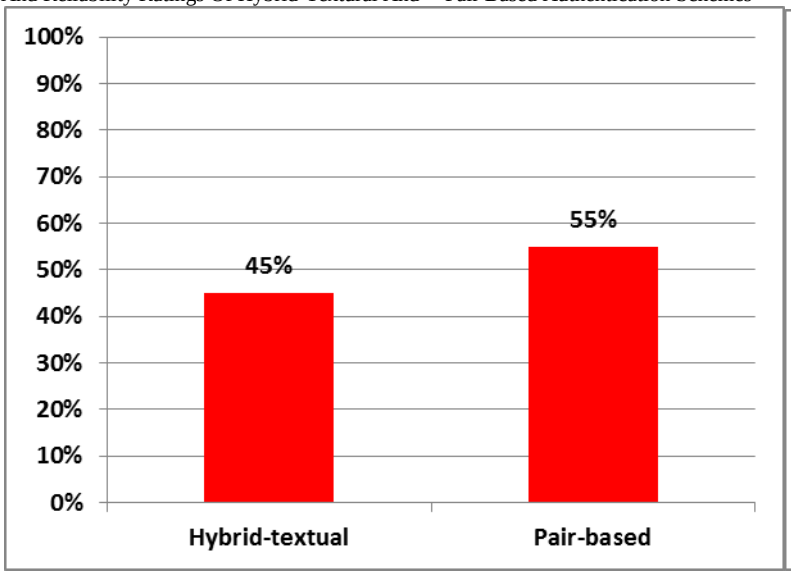

Fig 16: Efficiency Ratings Of Hybrid-Textural And Pair Based Authentication Schemes

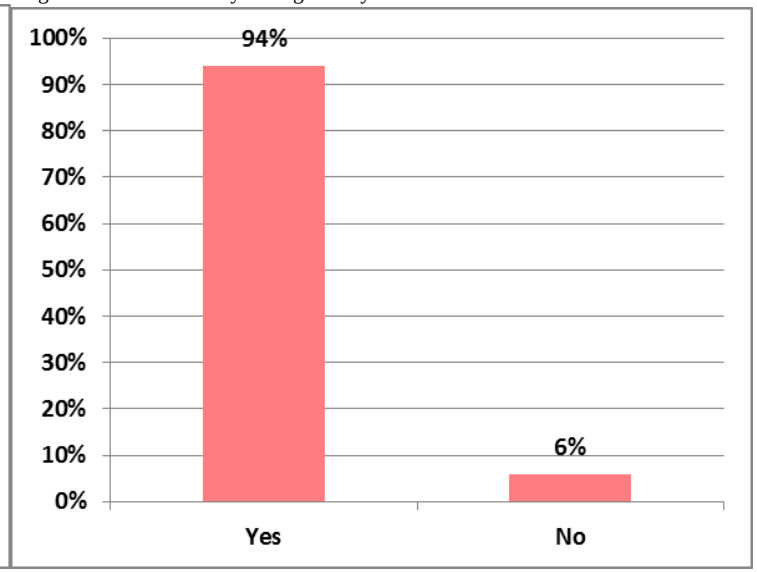

Fig 17: Effectiveness Ratings Of Hybrid-Textural And Pair Based Authentication Schemes

7 factors (Efficiency, Understandability, Safety, Reliability, Satisfaction, Effectiveness and Usefulness) of the Refined Usability Model.

The Software used for judging results is GNU PSPP Statistical Analysis Software.

Efficiency can be evaluated [23] by using the following measures:

- The Time required to perform a particular task.
- The Time required to execute a specific set of instructions.
- Number of clicks or keys pressed to achieve a task.
- Number of back buttons used.
- Number of screens visited to complete a specific task.

The Efficiency of Hybrid Textual and Pair-based authentication schemes will be measured by calculating the time required to Register and Login to the stated authentication schemes.

Two tasks are performed for calculating the Efficiency of Hybrid Textual Scheme.

- Time Required to Register
- Time Required to Login

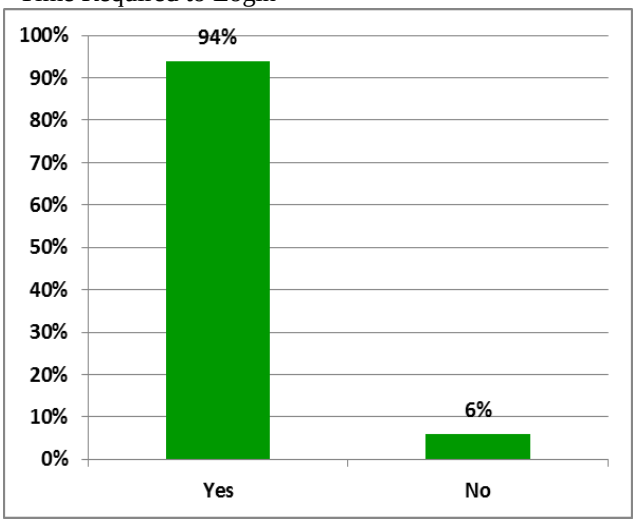

Fig 18: Usefulness Ratings Of Hybrid-Textural And Pair Based Authentication Schemes

TABLE 2
REGISTRATION TIME RECORDS OF HYBRID TEXTUAL AUTHENTICATION SCHEME

Hybrid_Reg

Value Label	Value	Frequency	Percent	Valid Percent	Cum Percent
	18.00	2	6.67	6.67	6.67
	19.00	2	6.67	6.67	13.33
	20.00	1	3.33	3.33	16.67
	21.00	4	13.33	13.33	30.00
	22.00	4	13.33	13.33	43.33
	23.00	4	13.33	13.33	56.67
	25.00	2	6.67	6.67	63.33
	27.00	3	10.00	10.00	73.33
	28.00	4	13.33	13.33	86.67
	30.00	2	6.67	6.67	93.33
	31.00	1	3.33	3.33	96.67
	43.00	1	3.33	3.33	100.00
	Total	30	100.0	100.0	

TABLE 3
COMPUTED RESULTS OF REGISTRATION MODULE.

Hybrid_Reg

N	Valid	30
	Missing	0
Mean		24.50
Std Dev		5.12
Minimum		18.00
Maximum		43.00

The average time required to register to a Hybrid Textual Authentication scheme based on the data collected by the respondents selected for performing usability testing is 24.50 seconds. And the Standard Deviation calculated is 5.12.

TABLE 4.
LOGIN TIME RECORDS OF HYBRID AUTHENTICATION SCHEME

Hybrid_login1

Value Label	Value	Frequency	Percent	Valid Percent	Cum Percent
	11.00	1	3.45	3.45	3.45
	12.00	6	20.69	20.69	24.14
	13.00	4	13.79	13.79	37.93
	14.00	4	13.79	13.79	51.72
	15.00	4	13.79	13.79	65.52
	17.00	4	13.79	13.79	79.31
	18.00	3	10.34	10.34	89.66
	19.00	3	10.34	10.34	100.00
	Total	29	100.0	100.0	

TABLE 5
COMPUTED RESULTS OF LOGIN MODULE.

Hybrid_login1

N	Valid	29
	Missing	0
Mean		14.83
Std Dev		2.54
Minimum		11.00
Maximum		19.00

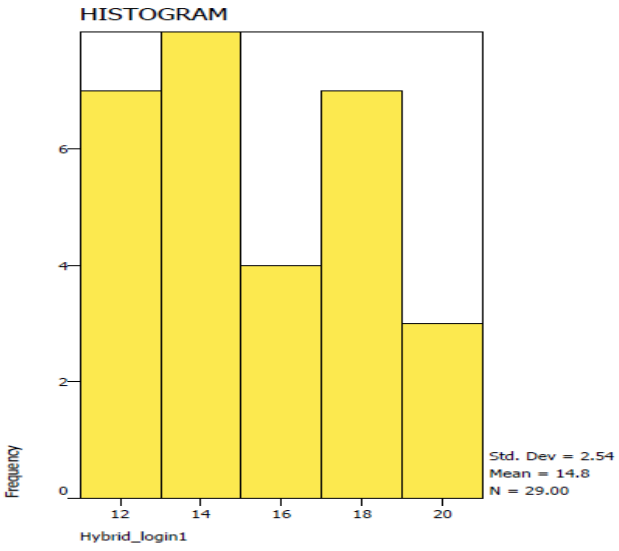

Fig 30: Login Module Histogram Of Hybrid Authentication Scheme

The average time required to Login to a Hybrid Textual

Authentication scheme based on the data collected by the respondents selected for performing usability testing is 14.83 seconds. And the Standard Deviation calculated is 2.54. The Histogram obtained is a random distribution.

Two tasks are performed for calculating the Efficiency of Pair-based Authentication Scheme.

- Time Required to Register
- Time Required to Login

TABLE 6
REGISTRATION RECORDS OF PAIR-BASED AUTHENTICATION SCHEME

Pair_Reg

Value Label	Value	Frequency	Percent	Valid Percent	Cum Percent
	6.00	1	3.33	3.33	3.33
	8.00	1	3.33	3.33	6.67
	10.00	2	6.67	6.67	13.33
	11.00	2	6.67	6.67	20.00
	12.00	3	10.00	10.00	30.00
	14.00	3	10.00	10.00	40.00
	15.00	2	6.67	6.67	46.67
	16.00	3	10.00	10.00	56.67
	19.00	3	10.00	10.00	66.67
	20.00	4	13.33	13.33	80.00
	21.00	4	13.33	13.33	93.33
	31.00	2	6.67	6.67	100.00
	Total	30	100.0	100.0	

Pair_Reg

N	Valid	30
	Missing	0
Mean		16.50
Std Dev		5.82
Minimum		6.00
Maximum		31.00

Table 7. Computed results of Registration Module.

The average time required to register to a Pair-based Authentication scheme based on the data collected by the respondents selected for performing usability testing is 16.50 seconds. And the Standard Deviation calculated is 5.82.

Table 8
Login Time records of Pair-based Authentication Scheme

Pair_login1

Value Label	Value	Frequency	Percent	Valid Percent	Cum Percent
	11.00	4	13.33	13.33	13.33
	12.00	3	10.00	10.00	23.33
	13.00	4	13.33	13.33	36.67
	14.00	4	13.33	13.33	50.00
	15.00	3	10.00	10.00	60.00
	16.00	3	10.00	10.00	70.00
	17.00	2	6.67	6.67	76.67
	18.00	3	10.00	10.00	86.67
	19.00	2	6.67	6.67	93.33
	23.00	1	3.33	3.33	96.67
	24.00	1	3.33	3.33	100.00
	Total	30	100.0	100.0	

Table 9
Computed results of Login Module.

Pair_login1

N	Valid	30
	Missing	0
Mean		15.13
Std Dev		3.35
Minimum		11.00
Maximum		24.00

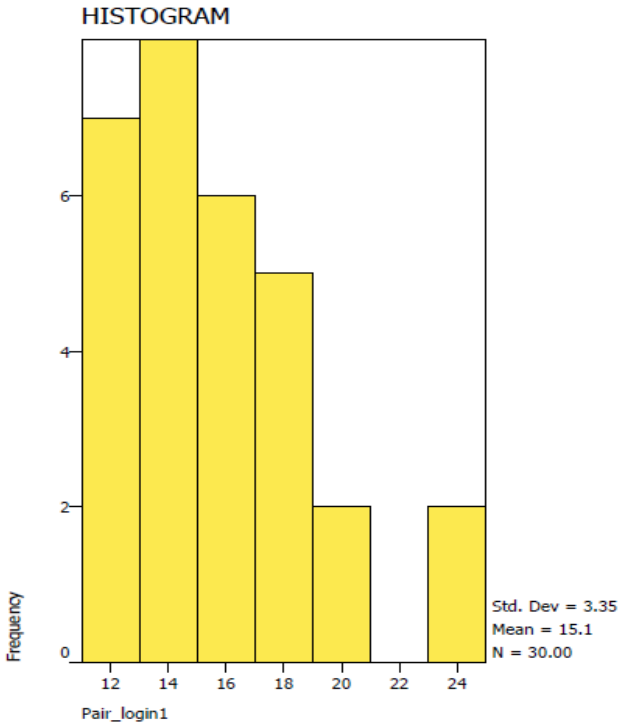

Fig 31: Login Module Histogram of Pair-based Authentication Scheme

The average time required to Login to a Pair-based Authentication scheme based on the data collected by the respondents selected for performing usability testing is 15.13 seconds. And the Standard Deviation calculated is 3.35. The Histogram obtained is a Right Skewed distribution.

From the above outcomes, it is remarked that the median time required to register to a Hybrid & Pair-based Authentication Scheme is 24.5 and 16.5 minutes respectively. The average time required to login to a Hybrid & Pair-based Authentication scheme is 14.83 and 15.13 seconds respectively. So it can be concluded that in terms of the Registration Module, Pair-based Scheme is more efficient whereas for the Login Module Hybrid Textual Scheme wins the title.

In order to test an instrument's reliability, several tests of internal consistency and replication can be used. To test the consistency and reliability of the Hybrid Textual and Pair-based schemes the methods used are:

- Test-Retest.
- Cronbach's alpha.

The Test-Retest method requires administrations of an

instrument to the same respondents so that the instruments consistency and reliability can be accessed. To compute the Test-Retest Reliability, a correlation coefficient needs to be computed. This can be done by choosing the bivariate correlation. The Bivariate correlation measures the relationship between two variables. The range can start from an absolute value of 1 and go to 0. If the value determined is closer to 1, then it means that the relationship is strong. The relationship between the two variables can either be positive or negative.

The Cronbach's alpha was provided so that the internal consistency of a test or scale could be assessed. It is expressed between two numbers (0 and 1). Internal consistency can be used to describe to what extent all the items present in a test measure the same concept [24].

TABLE 10
TEST-RETEST RELIABILITY OF HYBRID SCHEME

Correlations

		Hybrid_login1	Hybrid_login2
Hybrid_login1	Pearson Correlation	1.00	.90
	Sig. (2-tailed)		.000
	N	15	15
Hybrid_login2	Pearson Correlation	.90	1.00
	Sig. (2-tailed)	.000	
	N	15	15

TABLE 11. CRONBACH'S ALPHA

Case Processing Summary

		N	%
Cases	Valid	15	100.00
	Excluded	0	.00
	Total	15	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.92	2

From the above results, it can be seen that the correlation factor achieved is 0.90 and Cronbach's alpha coefficient is 0.92. Both results indicate that the instrument is very reliable and consistent.

TABLE 12
TEST-RETEST RELIABILITY FOR PAIR-BASED SCHEME

Correlations

		Pair_login1	Pair_login2
Pair_login1	Pearson Correlation	1.00	.98
	Sig. (2-tailed)		.000
	N	15	15
Pair_login2	Pearson Correlation	.98	1.00
	Sig. (2-tailed)	.000	
	N	15	15

TABLE 13
CRONBACH'S ALPHA

Case Processing Summary

		N	%
Cases	Valid	15	100.00
	Excluded	0	.00
	Total	15	100.00

Reliability Statistics

Cronbach's Alpha	N of Items
.91	2

From the above results, it can be seen that the correlation factor achieved is 0.98 and Cronbach's alpha coefficient is 0.91. Both results indicate that the instrument is very reliable and consistent. Effectiveness can be defined as the accuracy and completeness with which a user can reach his/her goal. Common measures [23] that can be included are:

- Rate of Error.
- Request for help.
- Path taken to complete a task.
- Severity of errors.

For both Hybrid Textual and Pair-based Authentication schemes, it was observed that all participants were successful in creating their accounts and then connecting with them. No technical problems were encountered. However, human error was observed in 2/30 respondents.

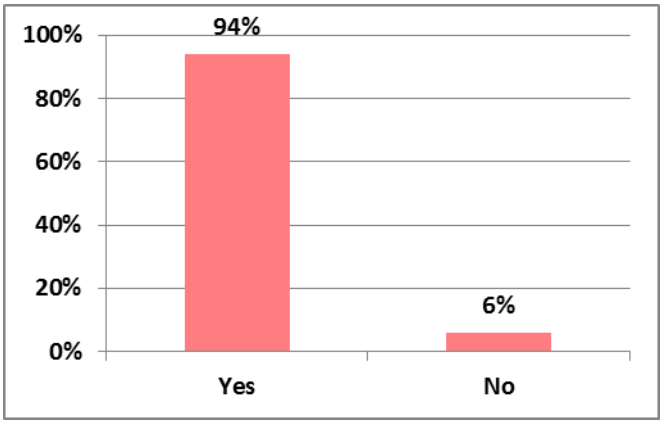

Fig 32: Effectiveness Ratings

About 94% of the Respondents that participated in the Testing of Hybrid and Pair-based Authentication schemes stated that they found the schemes to be satisfactory and useful at the same time as they are a better choice than simple text and graphical passwords.

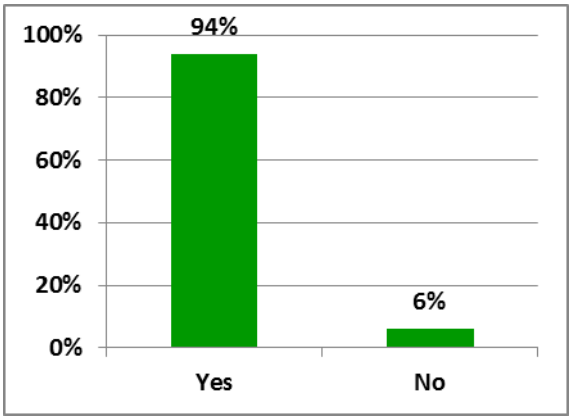

Fig 33: Satisfaction Ratings

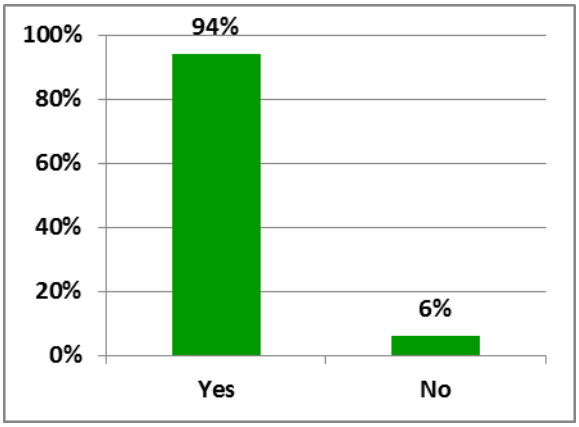

Fig 34: Usefulness Ratings

About 44% of the Respondents stated that they experienced difficulty in understanding Pair-based Authentication scheme. About 24% respondents stated that they had trouble in understanding Hybrid Textual Authentication scheme and 32% respondents stated that they had no trouble at all in understanding both Pair-based and Hybrid Textual schemes.

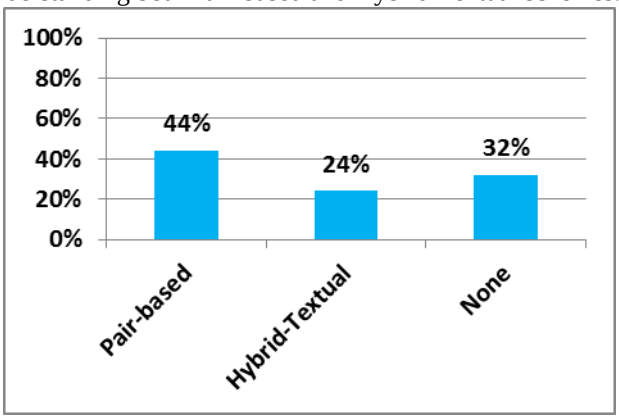

Fig 35: Understandability Ratings

Hybrid Textual and Pair-based authentication schemes were found to be more secure than simple Textual and Graphical passwords as they could not be hacked using brute force and other dictionary attacks.

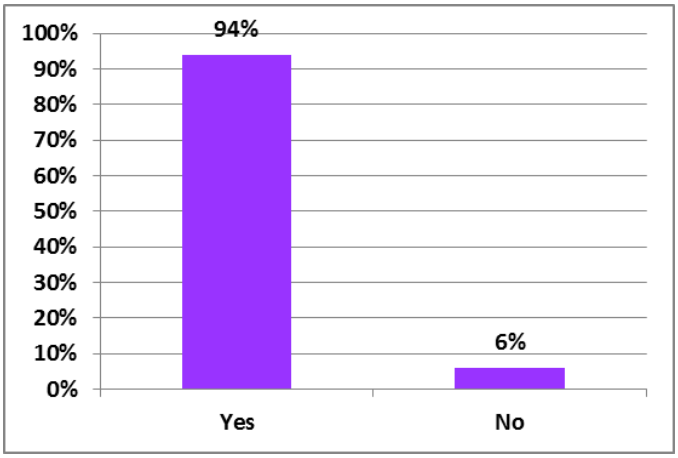

Fig 36: Safety Ratings

I. CONCLUSION

Usability plays an important role in the success and failure of a software system. In the field of computer science, many researchers have presented their theories on the different ways of measuring usability. These noticeable models are no doubt good but they do not emphasize on the complexities that one has to face when dealing with an authentication system. Because of this ambiguity a new model has been proposed in this research that deals with the usability of authentication systems. The usability factors proposed in this model have been identified by keeping in mind the necessary attributes that one finds necessary in every authentication system. Furthermore, the usability factors are subdivided into groups of three to help them understand better. A survey consisting of 30 respondents has been conducted to test the usability model. After analyzing the results, the usability model has been refined by reducing the usability factors from 10 to 7. Two authentication schemes based on session passwords by the name of Hybrid-Textual and Pair-based have been developed to test the usability model. Results show that the usability model maps well with the authentication schemes.

REFERENCES

[1] 1 Yee, K.-P.: 'Aligning security and usability', IEEE Security & Privacy, 2004, (5), pp. 48-55
[2] 2 Fléchais, I.: 'Designing secure and usable systems', University College London, 2005
[3] 3 Mallow, C.: 'Authentication Methods and Techniques', SANS®+ S™ Training Program for the CISSP® Certification Exam, 2007
[4] 4 Bevan, N.: 'Ergonomic Requirements for Office Work With VDT's', in Editor (Ed.)^(Eds.): 'Book Ergonomic Requirements for Office Work With VDT's' (Technical Report 9241-11, ISO, 1994, edn.), pp.
[5] 5 Nielsen, J.: 'Usability engineering' (Elsevier, 1994. 1994)
[6] 6 Ben, S., and Catherine, P.: 'Designing the user interface', in Editor (Ed.)^(Eds.): 'Book Designing the user interface' (Reading, Mass.: Addison Wesley Longman, 1998, edn.), pp.
[7] 7 Dix, A., Finlay, J., and Abowd, G.: 'R. Beale (1998): Human Computer Interaction', in Editor (Ed.)^(Eds.): 'Book R. Beale (1998): Human Computer Interaction' (Prentice Hall Europe, 1998, edn.), pp.
[8] 8 Scholtz, J.: 'Usability evaluation', National Institute of Standards and Technology, 2004

[9] 9 Frøkjær, E., Hertzum, M., and Hornbæk, K.: 'Measuring usability: are effectiveness, efficiency, and satisfaction really correlated?', in Editor (Ed.)^(Eds.): 'Book Measuring usability: are effectiveness, efficiency, and satisfaction really correlated?' (ACM, 2000, edn.), pp. 345-352

[10] 10 Hornbæk, K.: 'Current practice in measuring usability: Challenges to usability studies and research', International journal of human-computer studies, 2006, 64, (2), pp. 79-102

[11] 11 Bevan, N.: 'Kirakowski and J., Maissel, J. 1991. What is usability', in Editor (Ed.)^(Eds.): 'Book Kirakowski and J., Maissel, J. 1991. What is usability' (1991, edn.), pp.

[12] 12 Company, G.E., McCall, J.A., Richards, P.K., and Walters, G.F.: 'Factors in Software Quality: Final Report' (Information Systems Programs, General Electric Company, 1977. 1977)

[13] 13 Berander, P., Damm, L.-O., Eriksson, J., Gorschek, T., Henningsson, K., Jönsson, P., Kågström, S., Milicic, D., Mårtensson, F., and Rönkkö, K.: 'Software quality attributes and trade-offs', Blekinge Institute of Technology, 2005

[14] 14 Macleod, M., Bowden, R., Bevan, N., and Curson, I.: 'The MUSiC performance measurement method', Behaviour & Information Technology, 1997, 16, (4-5), pp. 279-293

[15] 15 Seffah, A., Donyaee, M., Kline, R.B., and Padda, H.K.: 'Usability measurement and metrics: A consolidated model', Software Quality Journal, 2006, 14, (2), pp. 159-178

[16] 16 Eason, K.D.: 'Towards the experimental study of usability', Behaviour & Information Technology, 1984, 3, (2), pp. 133-143

[17] 17 Lauesen, S., and Younessi, H.: 'Six Styles for Usability Requirements', in Editor (Ed.)^(Eds.): 'Book Six Styles for Usability Requirements' (1998, edn.), pp. 155-166

[18] 18 Ferré, X., Juristo, N., Windl, H., and Constantine, L.: 'Usability basics for software developers', IEEE software, 2001, (1), pp. 22-29

[19] 19 Constantine, L.L., and Lockwood, L.A.: 'Software for use: a practical guide to the models and methods of usage-centered design' (Pearson Education, 1999. 1999)

[20] 20 Shackel, B.: 'Usability-context, framework, definition, design and evaluation', Human factors for informatics usability, 1991, pp. 21-37

[21] 21 PANCHAL, V., and PATIL, C.P.: 'Authentication schemes for session password', International Journal of Scientific Engineering Research, 4

[22] 22 Tapkir, R., Khalate, S., Sarade, P., Bukan, S., and Patil, S.: 'Two Level Authentication Schema', in Editor (Ed.)^(Eds.): 'Book Two Level Authentication Schema' (ESRSA Publications, 2013, edn.), pp.

[23] 23 HIMSS, E.: 'Usability Task Force', Defining and testing EMR usability: Principles and proposed methods of EMR usability evaluation and rating, 2009, 2013

[24] 24 Tavakol, M., and Dennick, R.: 'Making sense of Cronbach's alpha', International journal of medical education, 2011, 2, pp. 53