Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 5 – No.8, August 2016 – www.caeaccess.org

Enhancing Authentication Schemes for Multi-Level Graphical Password in Cloud Environment

Ramandeep Kaur
Research Scholar
Department of
Information Technology,
CEC Landran, Mohali, India

Amanpreet Kaur
Assistant Professor
Department of
Information Technology,
CEC Landran, Mohali, India

ABSTRACT

The graphical password patterns are in the rising trend in world with the abundance of the touch screen devices. A variety of touch screen devices are present for the users such as mobile phones, tables, touch-enabled laptops, touch-enabled notebooks, etc. The graphical password has evolved with the invention of the touch-screen devices. The popular graphical schemes known as Pass-Go Pattern, Pass-point pattern and other similar schemes has been studied for the development of the new graphical password scheme. The existing models based upon pass-go and pass-point model stays as the basic model for our research for the development of the effective and secure graphical password scheme. It becomes difficult to input the alphanumeric passwords on the touch screens. The alphanumeric input lacks the high order accuracy as well as requires more focus to input the password. Most of the popular schemes have used the 3x3, 3x4 or 4x3 point-grid method for prompting the patterns to the users. The clue-point method is another popular method to display the graphical grid for the password input. In the proposed graphical model, graphical authentication model based upon the images has been aimed at to resolve the issues persisting in the existing models. In this model, the shuffling pattern based method has been used for the mitigation of the shoulder surfing attacks. The shuffling pattern scheme changes the primary display for password input every-time, which also restructure the input grid to overcome the threat caused by the shoulder surfing attacks.The proposed model has been designed to offer the robust graphical password scheme with the face images randomly collected by the users. The random point module for the visualization of the password input module plays the key role in the proposed graphical password scheme. The proposed model is a circular point model where the points are placed on the circle and the images are drawn on the given points. The user has to input the graphical pattern by joining the images with each other in the certain sequence. The proposed model requires less focus and highly accurate and easy to use. The experimental results have been evaluated in the factors associated with the study of the usability, memorabiltiy and difficulty in password creation. The proposed model has been compared against the existing models on the basis of the latter factors, where the proposed model has outperformed the existing models.

Keywords

Graphical Authentication, Cue-points, pattern lock, pattern password, cloud authentication, mobile authentication.

1. INTRODUCTION

Mobile devices are becoming an integral part of our everyday life. Nowadays mobile devices are being built with advanced computing capability, high resolution touch screens and better connectivity. Mobile devices have become ubiquitous, as it is used to check email, surf the web, e-commerce and variety of other tasks. Users store their private as well as sensitive information in these devices. In their paper, Dinesha, H. A.et. al. [2] has developed the multi-level authentication technique for accessing cloud services for the protection of the data of cloud users. The authors have developed multi-level authentication scheme to generate passwords in multiple levels for user authentication purposes. The use of proposed scheme has been suggested as a middleware authentication scheme. This technique helps in generating the password in many levels of organization so that the strict authentication and authorization is possible. This information must be protected from unauthorized accesses. For this, various authentication methods are available. An interesting observation is that most of the smartphone owners are unwilling to use authentication methods that are too complex, while simpler one compromises security.

ShraddhaM.Guravet. al. [8] has proposed the graphical password authentication. The authors have tried to create a user friendly scheme to ease out the users of the application equipped with the proposed scheme. The capability of human mind to remember images more than the text data is being explored in the proposed scheme. The proposed scheme is the combination of username and image based password. The proposed scheme is based on the images of alphabets which generate a number series at the backend used for the matching and authorizing purposes. Maninder Singh and Sarbjeet Singh, et al. [9] have designed and Implemented of Multi-tier Authentication Scheme in Cloud. The proposed authentication scheme belongs to the multi-tier authentication paradigm. The proposed scheme focuses on the secure use of third party cloud servers. The proposed scheme consists of two authentication levels to protect against the malicious third party cloud servers. The first level authentication includes the text based username and password. The second level password includes the combination of pre-determined steps. The decision logic is returned in the form of success (S) and failure (F). Neha Singh, et al [10] has worked on usability and security goal in authentication systems which help user's select better passwords and thus increase the effective password space. This can be due to lack of awareness about the risks associated with sensitive information. The most commonly used method of authentication is text based. In text based, user is supposed to choose alphanumeric password. User touches the screen and makes input by using virtual keyboard. Since there is less display space available for full virtual keyboard in mobile device, numeric keypad is preferred. For text based passwords, user chooses 4 digit number (referred to as Personnel Identification Number (PIN)) that user memorizes and uses it to unlock the locked mobile device. A study has revealed that text based passwords are more prone to shoulder surfing attacks. Shoulder surfing is the technique to get information by looking over someone's shoulder. Graphical passwords are used as an alternative to text based password and biometric authentication. Graphical passwords are easier to remember than alphanumerical passwords. A study has revealed that the likeability of graphical passwords is more than text based passwords. Widely used method of graphical authentication is Android Pattern Lock. Although this method is quite fast and popular, yet it is found to be insecure as it is prone to shoulder surfing attack and smudge attack. So the current study aims to design robust graphical user authentication scheme.

Tanvi Naiket. al. [12] has worked on Multi-Dimensional and Multi-Level Authentication Techniques. A novel multi-level and multi-dimensional method of authentication has been developed in this research using the combination of text, biometric and graphical password scheme. The graphical methods in the earlier told technologies are developed to protect against the dictionary based brute force attacks. All of the methods are prominently focusing upon the use of non-dictionary based passwords, which are also easy to remember. The non-dictionary passwords are difficult to crack and cannot be cracked using the traditional dictionary based hybrid or brute force attacks. The techniques include many options for multi-level authentication, like Change position of object, Textual password, Graphical password, Biometric password, and Play audio. The user is free to choose between the combinations for his customized multi-level authentication scheme.

2. MATERIALS AND METHODS

For the implementation of the proposed method of graphic authentication, Matlab tool has been used. The set-up of the simulated environment and real device are presented in the following subsection. The proposed work has been done in two levels as shown in Fig 1.. First level is already explained in previous paper. Now continue with second level.

As the trend of mobile devices is on the rise, every kind of internet application is being easily accessible locally using mobile apps. The proposed technique will be using one-level double-trap image based authentication for the login protection in cloud platforms on mobile devices. The one-level authentication scheme consists of various small images, which are made of single numerical or alphabetical characters each, in 3x3 point grid formation. The grid points (or grid images technically) will be displayed in the point shuffling based grid formation. The first stage will consist of a sequence to differentiate between the user and the auto bots or the botnets (automatic hacking tools created by the hackers). In this stage, the user will be shown with the same image grid as the first stage, but will need to enter the image in the sequence given in a verify code windows. The verify code window will contain the images in a particular sequence. At this stage, an auto bots or botnets can be easily trapped and filtered out, and only human users can lead through.

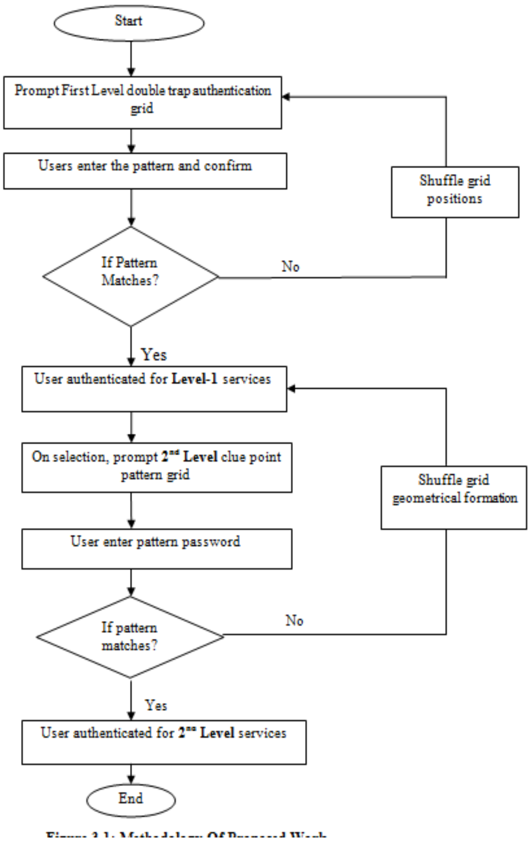
Start
Prompt First Level double trap authentication grid
Users enter the pattern and confirm
Shuffle grid positions
If Pattern Matches?
No
Yes
User authenticated for Level-1 services
On selection, prompt 2nd Level clue point pattern grid
Shuffle grid geometrical formation
User enter pattern password
If pattern matches?
No
Yes
User authenticated for 2nd Level services
End

Fig.1: Methodology Of Proposed Work

On the second stage, the user will need to provide input by selecting the images in the order elected during signup for the first stage of one-level authentication. The secure code on the back end will be hashed and matched with the secure code hash stored in the server and the decision logic would be returned. The second level password is a 9 clue-points grid based password scheme for pattern passwords. The pattern password is a scheme where the patterns are drawn by combining the points in order to draw the password pattern for the purpose of authentication. The pattern password input grid is in the static arrangement and does not change at any point of time. The traditional 9 clue-point scheme will additionally allow the overlapping patterns, hence they are prone to the shoulder surfing attacks, whereas the proposed scheme is based on shuffling geometrical shape and the overlapping password pattern to mitigate the threat of shoulder surfing attacks. The shoulder surfing attacks are the attacks where the attacker copies the users by watching their input.

3. RESULTS

The system has been tested with the 25 random persons of 16 years to 42 years of age. Most of the people become available for the test lies between the 23 and 33. The age variation has been counted as the factor towards testing the ease of access to the proposed graphical password scheme. The graphical password success rate, probability of failed login attempts, choice of features, etc.

Table 1: Average login time obtained after testing with people from different age groups

Sr. No.	Age Group	Total Persons in the Age Group	Total Attempts	Successful Attempts	Success Rate
1	<20	5	102	100	98.03%
2	<30	13	280	267	95.35%
3	<40	6	115	111	96.52%
4	<42	1	16	14	87.50%

For the login option, the results have been observed for the all 25 people. The quickest login times has been achieved by the youngsters under age of 20 years. But there is no significant difference found between the people in their 30s and 40s, where the people below 30 have taken significantly lower time than the people in 30s and 40s. The average login time describes the quickness of the person to understand and respond to the login screen. For the login option with biometric, again the quickest login times has been achieved by the youngsters under age of 20 years. But there is no visible difference found between the people in their 20s and 30s, where the person above 40 has taken significantly higher time. The average login time describes the quickness of the person to understand and respond to the login screen.

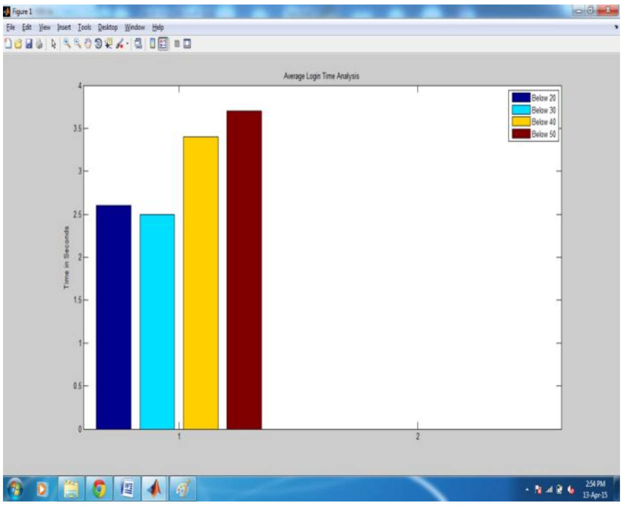

Fig.2: The graphical representation of the average login time of various groups of users

Figure 2 describes the results obtained for the average login time in the proposed model for the different age groups. All of the people in the age groups below 40 have performed significantly well, whereas the people near 42 years of age have been found with difficulties in using the proposed graphical password scheme as per shows in the following table 1. The table 5 shows the consistent accuracy rate for the people below 40, which has been observed higher than the range of 95% for all of the age groups.

Table 2: The successful attempts and success rate by the testing user set

Sr. No.	Age Group	Total Persons in the Age Group	Average Login Time (in seconds)
1	<20	5	2-3
2	<30	13	2-3
3	<40	6	3-4
4	<42	1	3-4

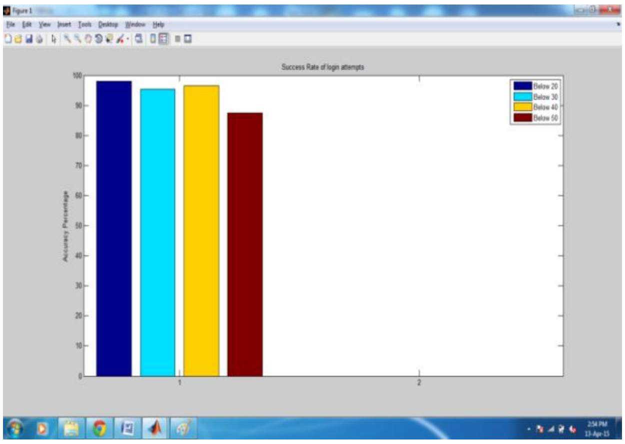

Fig.3: The login accuracy by the testing users of various age groups

In the figure 3, the testing users have been measured in the terms of accuracy, which represents the probability of remembrance of the graphical password patterns. The accuracy has been measured higher in terms of number of successful attempts and success rate in percentage. Results of the proposed method of graphic authentication have been obtained by taking feedback from user. A questionnaire was given to users after they become familiar with application. Questionnaire was based on 5 point Likert Scale. A total of 60 participants were called in an informal way and only 48 responded. Participants has been divided into three groups i.e. government employees, private employees and students. Of 48 participants, there were 10 government employees, 14 private employees and 24 students as shown in Figure. From figure it is very clear that 50% of the participants were students, 30% were private employees and 20% government employees.

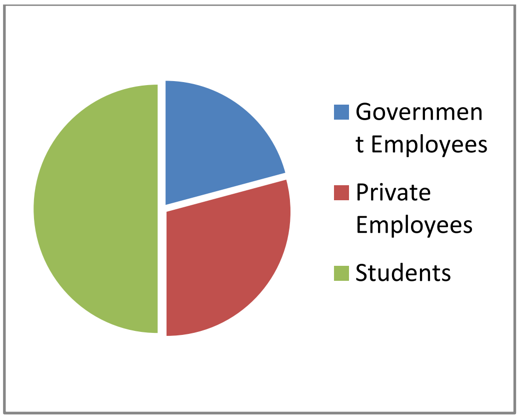

Fig.4: Showing Distributions of Participants

Students belonged to age group 18-28 where as government employees belonged to age group 22-53 and private employees belonged to age group 23-31. The average age of students was 23 years whereas average age of government employee was 30 years and average age of private employee was 26 years. All the participants had good knowledge of authentication schemes. Majority of the participants used mobile device for at least 1hour/day. On analyzing data it has been found that 70% of the government employees use their mobile phone for at least 4 hours/day, 10% of the government employees have low familiarity with Android, 60% have medium and 30% have high familiarity with android OS.

Feedback of the private employees to the questionnaire has been obtained by assisting them in filling up the quesssionarie. From table it has been found that 36% of the private employees use their mobile phone for at least 2 hours/day, 64% of private employees have familiarity with Android OS and 36% of the private employees have good familiarity with Android OS. 29% of private employees have good knowledge of Android Pattern Lock. There were 24 students which participated in the survey. On analyzing their results it has been found that 8% of the students use their mobile for less than 1 hour/day, 17% of the students use their mobile phone for at least 1 hour/day and 4% of the students use their mobile device for more than 8 hours/day. 46% of students which participated in survey have high knowledge of Android Pattern Lock, 37.5 % of the students have deep knowledge of Text passwords and PIN.

4. DISCUSSIONS

The usability of the system is the term to measure the ease of using the system for the users, login time, signup time, accuracy of the system and reliability. The usability of the system has been studied against the Singh 2015[10] with improved authentication scheme using password enabled persuasive cued click points. The usability has been tested over the 20 persons of different ages. The following table has been collected for the result evaluation of the proposed model:

Table 3: Performance evaluation of the proposed model in multiple performance factors

Successful Password Creation	20/20	100%
Password Memorability	18/20	90%
Successful Login	19/20	95%

The table 3 depicts the performance of the proposed model in the form of various performance parameters such as successful password creation, password memorability and the successful login attempts using the proposed model. The proposed model has been obtained as the excellent performed in the terms of such parameters. All of the parameter values has been obtained higher or equal to 90%, which shows the significant strength of the proposed model.

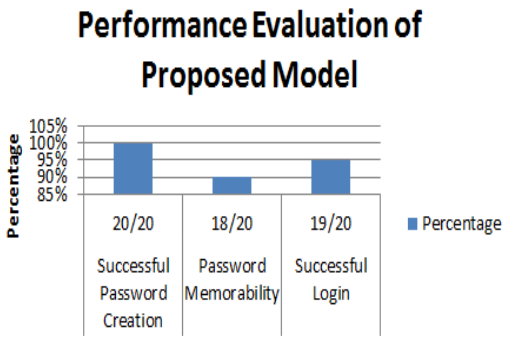

Fig.5: Graphical Representation of the proposed model performance

The figure 5 shows the results obtained in the table 3 in the graphical form which clearly indicates the robustness of the proposed model based upon the graphical passwords. The user memorabiltiy, successful password attempts and successful password creation has been well tested under this experimental section. The comparative analysis has been produced against the existing scheme of the Singh 2015. [10] The proposed model has been found quite efficient in the terms of successful login attempts, password memorability and successful signup. The following table has been produced for the comparison study of the proposed model against the existing model:

Table 4: The evaluation of the proposed model against the existing model on the basis of people density

	Successful Password Creation	Password Memorability	Successful Login
Singh 2015	18/20	15/20	16/20
Proposed Model	20/20	18/20	19/20

Table 4 shows the comparative analysis of the proposed model against the scheme proposed in Singh 2015. The proposed model has posted the successful attempt accuracy at 19/20 against the 18/20 in the existing model. The password memorability cases have been increased from the 15/20 to 18/20 in comparison with the existing model.

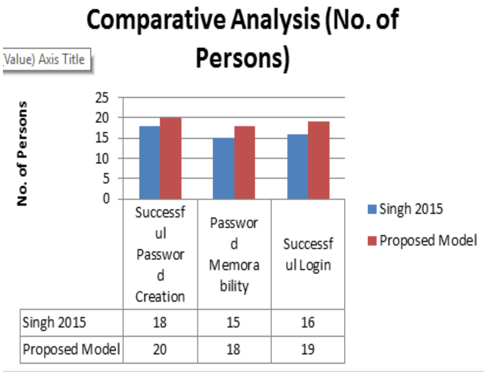

Fig 6: The comparative analysis on the basis of number of persons

Figure 6 signifies the overall results obtained from the proposed model, where it can be clearly observed that the proposed model is the clear winner in all of the resulting domains analyzed under this section. The successful password creation has hit the top mark with 20/20 against the 18/20, which shows the ease of access in the proposed model in comparison with the existing model.

Table 5: The evaluation of the proposed model against the existing model on the basis of percentage

	Successful Password Creation	Password Memorability	Successful Login
Singh 2015	90%	75%	80%
Proposed Model	100%	90%	95%

Table 5 shows the results of the table 2 in the form of percentage of accuracy on the basis of the various domains. The accuracy of the proposed model has been tested in the terms of password memorability, successful logins and the successful attempts made for creation of the graphical password.

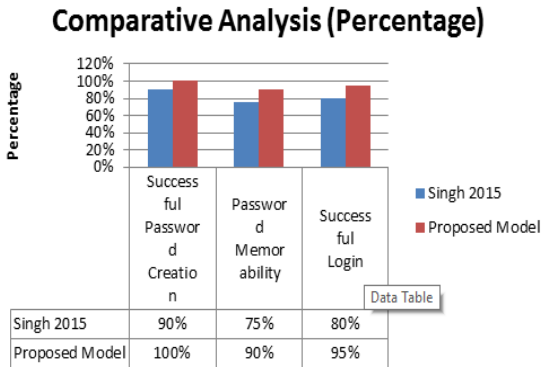

Fig.7: The comparative analysis on the basis of percentage

Figure 7 describes the overall accuracy of the proposed model against the Singh 2015 scheme [10]. The figure 7 clearly shows the results obtained for the accuracy of successful password creation attempts, memorabiltiy and the successful login attempts made towards the similar direction. The proposed model has outperformed the existing model on the basis of all of the parameters.

S. Wiedenbeck 2005 [14] have proposed the method based upon the pass points, which inherits the application design from the image based passwords. Our proposed model has been compared against the S. Wiedenbeck 2005 model. The proposed model has clearly outperformed the existing model in the terms of learning complexity and time complexity. Also the measure of accuracy has been defined in the form of the standard deviation computed over the statistics collected from the repetitive analysis of the proposed model.

Table 6: Mean (Standard deviation) evaluated from the questions about the password creation phase

Questions		Existing Mean (SD)	Proposed Mean (SD)
Number of Incorrect submissions	Alphanumeric	0.40 (0.68)	0.65 (0.80)
	Graphical	4.80 (7.16)	5.15 (7.40)
Total practice time (seconds)	Alphanumeric	66.08 (4.92)	20.00 (3.00)
	Graphical	171.89 (24.46)	55.21 (9.71)

Table 7: Means (calculated in the form of standard deviation) of the incorrect submissions and the overall time in learning phase

Question	Mode	Existing Mean (SD)	Proposed Mean (SD)
I did not have much trouble thinking up a password	Alphanumeric	3.30 (1.59)	3.30 (1.59)
	Graphical	2.35 (1.57)	2.65 (1.85)
It did not take me long to think up a password	Alphanumeric	3.15 (1.63)	3.15 (1.63)
	Graphical	2.60 (1.42)	3.05 (1.73)

The following table clearly elaborates the comparison between the proposed and existing model. The total number of input iterations (N) for the alphanumeric and graphical passwords has been kept on the 20 each in both of the following scenarios.

Chiang, Hsin-Yi 2013 [15] have proposed the scheme known as Touch-screen Multi-layered Drawing (TMD) scheme. The proposed model has been evaluated against the proposed model on the basis of usability under the session 2 login. Our proposed model has two phases, first phase and second phase of authentication. The proposed model has been evaluated on the basis of second phase due to its similar functionality with the Chiang, Hsin-Yi 2013 scheme. The following table shows the comparative analysis between the existing and proposed model.

Table 8: Session 2 Login Time based analysis of proposed model and existing model

TMD	Phone	25 sec
	Tablet	28 sec
DAS	Phone	19 sec
	Tablet	18 sec
Proposed	Phone	30 sec
	Tablet	32 sec

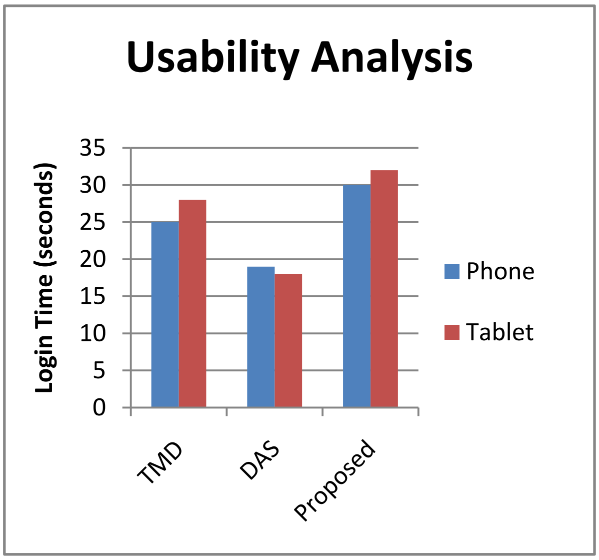

Fig.8: Graphical representation session 2 Login Time based analysis of proposed model and existing model

5. CONCLUSION

Graphical authentication scheme works by using pictures or by drawing something on the mobile device. Graphical authentication systems are widely used. Android Pattern Lock is the most popular method of graphic authentication. Other schemes used for authentication are Text Passwords and PIN. The major challenge faced in case of graphical authentication schemes is that most of the schemes are vulnerable to shoulder surfing and smudge attack. The literature review reveals various methods of graphic authentication and vulnerabilities in these methods.

For the current study, secured method of graphic authentication is developed. This method is implemented by making application of it for mobile devices running on Android OS.. Its novelty is that, images are always shown randomly and user has to select images according to the order of images and shift function. This increased the shoulder surfing and smudge resistance. It has been confirmed by feedback from user. A total of 20 participants were called in an informal way for survey. Feedback from users is based on two parameters i.e. usability and likeability. The prototype of the application was installed in Motorola Moto E mobile device and was used by participants, after that their feedback was taken. A questionnaire was designed based on 5 point Likert Scale, to take feedback from participants. The result of the feedback from all the participants was tabulated and then analyzed. The result shows that the proposed method of graphic authentication outperformed the already existing methods.

6. FUTURE WORK

Future work may be done in order to find the usability and likeability of proposed method of graphic authentication in other systems which are vulnerable to shoulder surfing attacks like in ATM's. In the current study the proposed technique is implemented only in smartphone running on Android OS. Future work may be done to implement the proposed technique in other operating systems and devices.

7. ACKNOWLEDGMENT

This research work was supported by Ms.Amanpreet Kaur, Assistant Professor, Department of Information Technology, Chandigarh Engineering College, Landran (Mohali), Punjab, India.

8. REFERENCES

[1] Bashier, H. K., Hoe, L. S., & Han, P. Y. "Graphical Password: Pass-Images Edge Detection", In Signal Processing and it's Applications (CSPA), IEEE 9th International Colloquium , Pp. 111-116 , 2013.

[2] Dinesha, H. A., And V. K. Agrawal. "Multi-Level Authentication Technique For Accessing Cloud Services." Computing, Communication And Applications (ICCCA), 2012 International Conference On.IEEE, Pp 1-4, 2012.

[3] Hussain, Abdulameer. "Enhanced Authentication Mechanism Using Multilevel Security Model." Int. Arab J. E-Technol. V.1.2 , Pp 49-57,2009.

[4] Ku, Wei-Chi, Dum-Min Liao, Chia-Ju Chang, And Pei-Jia Qiu. "An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme." In Communications In China (ICCC), IEEE/CIC International Conference On, Pp. 204-208, 2014.

[5] Kaur, R., & Kaur, A. (2015). Multi-Factor Graphical Password for Cloud Interface Authentication Security. International Journal of Computer Applications, 125(7).

[6] Renaud, K., Mayer, P., Volkamer, M., & Maguire, J. "Are Graphical Authentication Mechanisms As Strong As Passwords" In Computer Science And Information Systems (Fedcsis), Federated Conference On Pp. 837-844, 2013.

[7] Revar, A. G., & Bhavsar, M. D. "Securing User Authentication Using Single Sign-On In Cloud Computing" In Engineering (Nuicone), Nirma University International Conference On Pp. 1-4, 2011.

[8] Shraddham. Gurav, "Graphical Password Authentication", ICESSPCT, Vol. 1, Pp. 479483,2014.

[9] Singh, M., & Singh, S. "Design And Implementation Of Multi-Tier Authentication Scheme In Cloud" IJCSI International Journal Of Computer Science Issues, 9(5), Pp. 87-90.

[10] Singh, N., & Bomanwar, N. (2015, October). Improved Authentication scheme using password enabled Persuasive Cued Click Points. In Green Computing and

Internet of Things (ICGCIoT), 2015 International Conference on (pp. 1394-1398). IEEE.

[11] Tao, Hai, And Carlisle Adams. "Pass-Go: A Proposal To Improve The Usability Of Graphical Passwords." IJ Network Security 7, Pp.273-292.2 ,2008.

[12] Tanvi Naik, Sheetal Koul, “Multi-Dimensional And Multi-Level Authentication Techniques”, IJCA ,Vol. 75, Issue 12, Pp.17-22, 2013.

[13] Yi-Lun Chen, Wei-Chi Ku, Yu-Chang Yeh, Dun-Min Liao, “A Simple Text-Based Shoulder Surfing Resistant Graphical Password”, ISNE, Vol. 1, Pp. 161-164,2013.

[14] Wiedenbeck, Susan, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. "PassPoints: Design and longitudinal evaluation of a graphical password system." International Journal of Human-Computer Studies 63, no. 1 (2005): 102-127.

[15] Chiang, Hsin-Yi, and Sonia Chiasson. "Improving user authentication on mobile devices: A touchscreen graphical password." In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services, pp. 251-260. ACM, 2013.