Secure User Authentication Using Graphical Passwords

Fariya Ghori
MS Computing,
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology
90 and 100 Clifton
Karachi -75600

Kashif Abbasi
Department of Computing,
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology
90 and 100 Clifton
Karachi -75600

Abstract— **The paper discusses secure user authentication mechanisms using graphical passwords. Graphical Password is an alternative to a textual password, which uses images, designs patterns etc. as a password instead of alphanumeric password. Graphical passwords provide better security and usability over textual password, but along with so many advantages of graphical password, they have a major issue of Shoulder Surfing Attack. In this report different techniques of graphical passwords are discussed.**

To combat shoulder surfing attack, two different techniques of graphical password based authentication are implemented as part of this project. Different user based surveys are conducted. Based on results of user surveys, a comparative analysis is carried out between two prototypes developed in this project. In the end, conclusion is written in terms of application's security, reliability, user convenience and security against the shoulder surfing attack.

Keywords-Graphical Passwords; authentication; security; recall based systems; recognition based systems*;*

I. Introduction

Generally, textual passwords or the alpha numeric usernames and passwords are used for the user authentication [1][2]. This method is being used since decades and is quite adoptable in sense of usability, but it has many security threats and one the major security threat is that it can be steal easily, because users keep easy passwords so that they can remember it [1].

Graphical password is an alternative authentication method of textual passwords which uses pictures or graphics or patterns as passwords [1][3]. Graphical Passwords can be divided into two main categories, which are recognition based authentication system and recall based authentication system [1]. In recognition based authentication system user are provided with many images and he/she has to recognize all those images which he has selected during registration process [1][3]. While in recall based authentication system user needs to create the similar design as he drawn during registration process to authenticate him or herself [1][3].

Graphical Password provides better defense against dictionary attacks [1][4]. It could be because of that it takes input from mouse instead of keyboard and also because there are no pre-existing dictionaries for graphical information [1]. In spite of having advantages of using Graphical Passwords that it is easier to remember or recall and have maximum defense against dictionary attacks it has a shoulder surfing threat [2]. Shoulder surfing attack is a technique used to steal passwords by observing the users passwords while the user is entering the password [5]. There is a high probability that if shoulder surfer observes the few login sessions of the user, the shoulder surfer may figure out the users password.

In this research two anti-shoulder surfing techniques had been implemented and there security and usability had been analyzed.

II. Problem Background

Alphanumeric usernames and passwords is the most common and widely used authentication technique. It is being used for many years even though it has much vulnerability. Textual passwords are difficult to remember that is why most of the people keep easier passwords, could be their family name or some dictionary word [1][2][6][7]. And there are several hacking softwares which can easily hack the textual passwords. A weak password or poor management of passwords could cause great losses in businesses [1]. There are many ways to break the passwords for example, brute force attack and spying the key strokes. In brute force attack, attacker tries every possible guess or combination, and continues trying it until he cracked the users' password. In spying or recording key strokes, different key logging softwares are used to record the key strokes of the user while typing passwords. These vulnerabilities can lead loss to the companies.

To overcome these vulnerabilities researches have come up with an alternative authentication technique, which is authentication using Graphical Password. In Graphical Password user is not required to use keyboard or the input, input can easily be provided using mouse or stylus for the touch screens [1]. The major problem which graphical passwords face is that it is more vulnerable to shoulder surfing attack [2]. Any person can stand behind the user entering the password can observe the password and remember it. And later can try to login by clicking those observed points where user had clicked and can get access to the application.

Thus, this research has been conducted to analyze currently available anti-shoulder surfing techniques of graphical password. Two mechanisms had been implemented and analyzed in order to get a best mechanism between two, in terms of usability and security towards shoulder surfing.

III. Literature Review

These days many of the individuals and the organizations use PC, laptops, PDA's etc. for their personal and business purposes. They store huge amount of digital data over there, either the data is stored on local hard drives, or on a cloud over an internet, user may require some privacy so that no one else can have access to his/her confidential data. Hence mechanism of user authentication is used to authenticate and authorize the user, so that he/she can access data.

User authentication is the process of authorizing the user and his/her credentials, and then allowing the user to access the application or user data.

A. Classification of Authentication Methods

There are different kinds of authentication methods:

1) *Token based:* Token based authentication methods use smart cards and bank cards along with pic number. For example ATM cards are used with a pin number [1][8][9].

2) *Biometrics based*: Biometrics based authentication system identifies the humans by their traits and characteristics, for example finger prints, and authenticate user based on those characteristics [1][8][9]. Biometrics based authentication system is further divided into two types, contact biometric technology in which user has to maintain physical contact or touch the biometric device to authenticate himself for example, finger print, while the other type is contactless biometric technology in which user does not need to touch the biometric device, for example eye retina scanning [1][8][9]. Biometric authentication methods are not used much, because they are very expensive, though they offer higher security level.

3) *Knowledge based:* Knowledge based authentication system is a technique in which user has to answer at least one question correctly. Hence users need to have some secret knowledge or need to remember something to authenticate himself [1][8][9]. Knowledge based authentication methods are the most widely used authentication methods. The very common form of knowledge based authentication system is textual passwords. Graphical Passwords are also lie under the category of knowledge based authentication methods

B. Graphical Passwords

Graphical Passwords are an alternative to textual password, in which instead of alphanumeric passwords pictures based passwords or handmade drawing/designs are used as passwords [6][7]. According to the many psychological studies, it has concluded that human's ability to remember pictures and images is more than remembering texts [6][7]. As textual passwords are seems to be difficult to remember, people set an easy passwords and uses same passwords for different application authentication, which results in security threats over weak passwords [10]. Hence this becomes the motivation behind the idea of Graphical Passwords, as they are easy to remember.

Graphical Passwords uses images and pictures instead of the alphanumeric passwords, in spite of having many advantages over textual passwords, it do have some security threats for example shoulder surfing attack. Graphical Passwords are further divided into four categories [8].

1) *Recognition Based Systems:* In recognition based systems users need to select images, graphics, icons from the large random collection of pictures and graphics, which they had chosen or selected while registering to the application [8]. Once they have chosen the correct images/icons etc. they can get access of that application.

2) *Recall Based Systems:* In recall based authentication techniques, users are required to reproduce something that he/she had created or chosen before during the process of registration [8].

3) *Cued Recall Based Systems:* In cued recall based systems, users are also required to recall there passwords, but as the name reflects, few of the hints are provided to the user so that a user can recall the password easily and authenticate oneself [8].

4) *Hybrid Systems:* Hybrid systems are the combination of any two techniques or schemes [8]. For example combination of recall based systems and recognition based systems, or the combination of recognition based systems with textual passwords

IV .Implementation

Prototype Model has been chosen for the development of graphical passwords application, because prototype model has greater user involvement. Users can respond and interact with the prototype. By prototyping model we can get greater and better feedback from the users, and prototype helps to give a basic idea of what the application is all about, which was very helpful for the research work.

Prototypes which were developed are:

A. Draw-a-Secret with Line Snaking Mechanism

Draw-A-Secret (DAS) is considered to be the first recall-based graphical password technique [5]. DAS consist of a 2D grid and users need to draw their password on a 2D grid using mouse or stylus [5]. Drawing can be consists of multiple pen stroke or the continuous stroke.

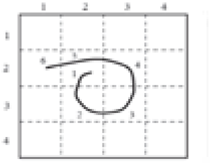


Fig 1 Draw-a-Secret Scheme

While logging in user needs to draw the same strokes, passing through the same grids, which user had drawn during registration process. The user drawn password is encoded by the system in form of the sequence of coordinates of the grid cells from which the drawing passed through for example the password of Figure 3.1 would be (2,2)(2,3)(3,3)(3,2)(2,2)(1,2). The length of the password is equal to the pair of cell coordinates across all strokes. Figure 3.1 is taken from [5].

In Draw a secret technique of recall based systems, all the strokes are visible to user during login process, and hence anyone can see the strokes and memorize it, which leads to the security risk. Hence to reduce the risk of shoulder surfing attack, different techniques have been proposed by different researchers, among them one is line snaking mechanism in line snaking [5].

The line snaking techniques was proposed to gain defense against shoulder surfing attack, especially for passwords having long strokes [5]. In this technique, the stroke information starts disappearing after few seconds, like a snake, while the stroke is being drawn [5] as shown in Figure 3.3.

The speed of the snaking of the strokes would depend on the speed of the users drawing, if the user is drawing quickly then the strokes will also disappear quickly and if the strokes are being drawn slowly it will disappear slowly from the canvas or screen. This was thought by keeping in mind the usability of the solution, else either the strokes will be removed too slow or too fast [5]. This is controlled by the timer function in implementation, that as the stroke is being penned down or the user starts drawing, the timer starts which controls the disappearing of the strokes. Below are the two figures, one shows the DAS technique without defense shoulder surfing mechanism and other with Defensive technique using line snaking mechanism Figure 3.2 and Figure 3.3 are both taken from [5].

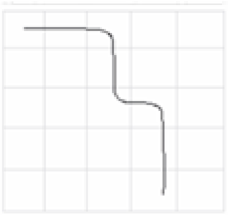


Fig 2. DAS without Line Snaking Defense

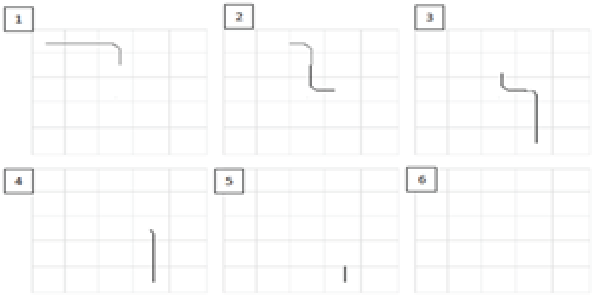


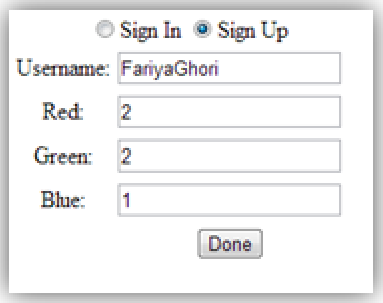
Fig 3. DAS with Line Snaking Defense (left to right proceeds with time)

5) *Colored Grid (Anti-Shoulder Surfing Mechanism)*

Colored Grid method is a new authentication method based on the combination of recognition based system and textual password, that is a hybrid system based solution. It consists of a Colored Grid Pattern. Every user has to select specific color palettes to set a password. This type of Graphical Password Method is a unique method which has been used here.

In this mechanism, user has to choose a combination of colors among three colors red, green and blue, so that the sum is 5. For example, 2 red, 2 green and 1 blue as shown in the Figure 3.5, during registration process. This combination should be memorized by the user. While logging in, a user has to type that which/how many rows have all the same combinations which he has entered during registration (2R, 2G, 1B).

Hybrid password schemes can reduce the security threats specially shoulder surfing attack, because user will be seeing the pictures/grid on screen and at same time type password on keyboard. So for shoulder surfer it will be difficult to observe both things at same time quickly. This will increase complexity for shoulder surfer, and thus enhance security of authentication method.



○ Sign In ● Sign Up

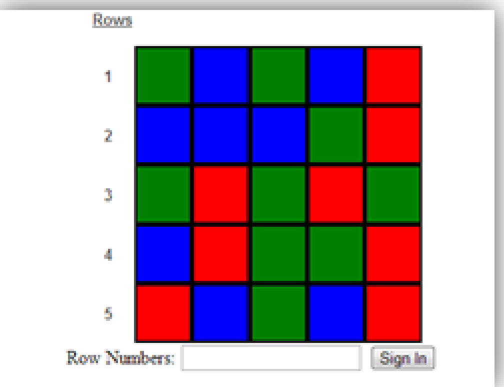
Username: FariyaGhori

Red: 2

Green: 2

Blue: 1

Fig 4> Registration User Interface of Colored Grid Prototype



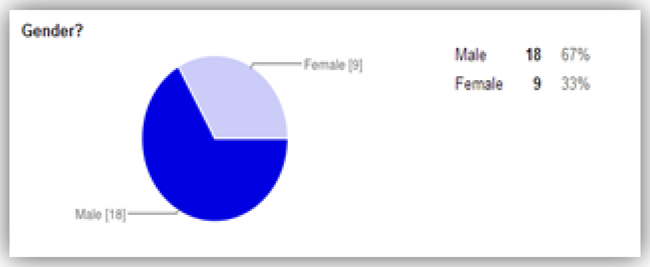
1	🟩	🟦	🟩	🟦	🟥
2	🟦	🟦	🟦	🟩	🟥
3	🟩	🟥	🟩	🟥	🟩
4	🟦	🟥	🟩	🟩	🟥
5	🟥	🟦	🟩	🟦	🟥

Fig 5 Login Grid View of Colored Grid Prototype

V. Survey

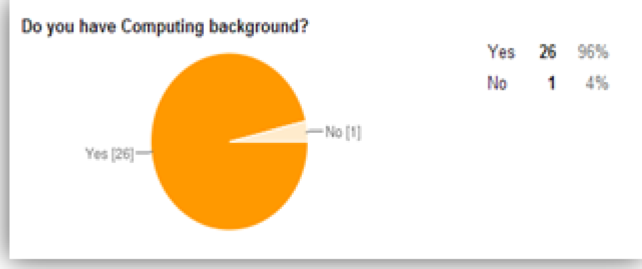
A survey has been conducted, to know whether the proposed solutions has reasonable shoulder surfing defense or not. Following figures shows the survey results.

A. *General Questions*


Gender?

Male	18	67%
Female	9	33%

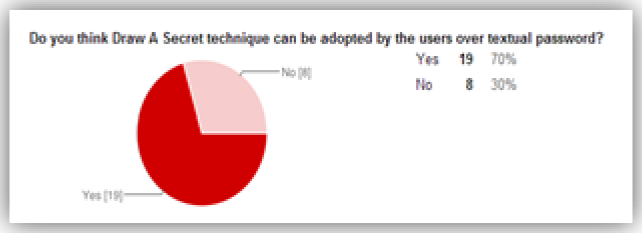
Fig 6 Distribution of Gender for survey users


Do you have Computing background?

Yes	26	96%
No	1	4%

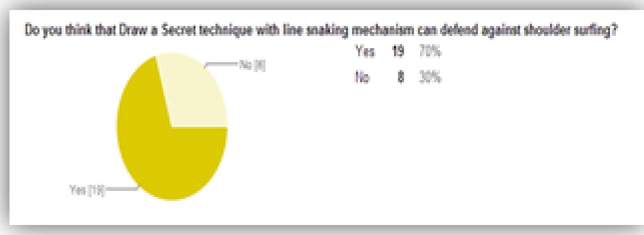
Fig 7 Distribution of Computing background for survey users

B. *Results of Line Snaking Questions*


Do you think Draw A Secret technique can be adopted by the users over textual password?

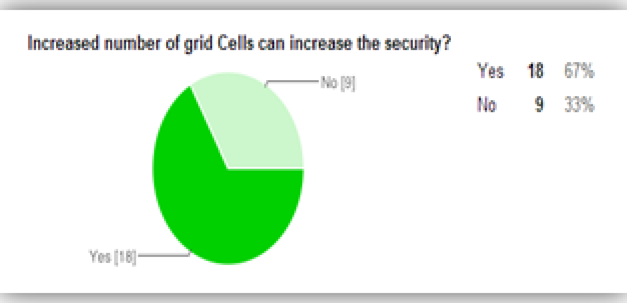
Yes	19	70%
No	8	30%

Fig 8 Distribution of Adoption of DAS over textual passwords


Do you think that Draw a Secret technique with line snaking mechanism can defend against shoulder surfing?

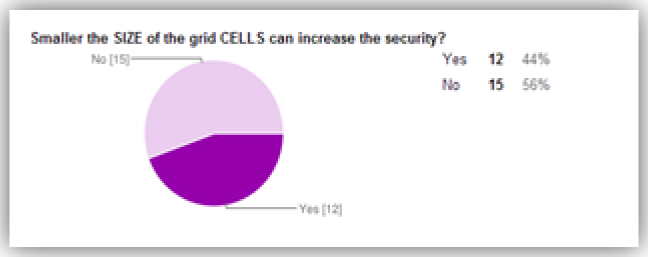
Yes	19	70%
No	8	30%

Fig 9 Shoulder Surfing Defense using Line Snaking Mechanism


Increased number of grid Cells can increase the security?

Yes	18	67%
No	9	33%

Fig 10 Effect of number of Grid Cells on DAS


Smaller the SIZE of the grid CELLS can increase the security?

Yes	12	44%
No	15	56%

Effect of Size of Grid Cells on security of DAS mechanism

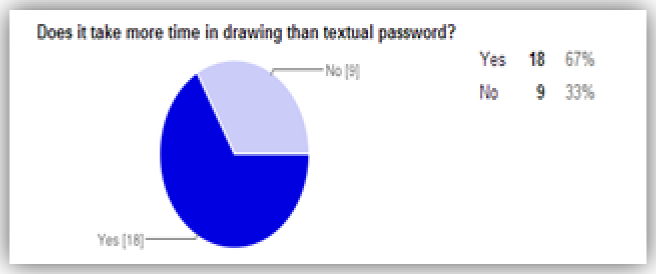


Fig 11 Time utilization for drawing Password in DAS against Textual Passwords

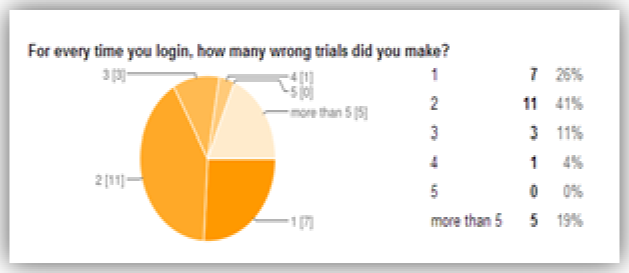


Fig 12 Distribution of Error rate in DAS Mechanism

C. *Results of Colored Grid Mechanism*

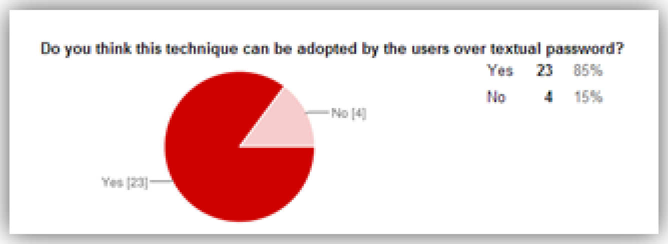


Fig 13 Distribution of Adoption of Colored Grid Mechanism over textual passwords

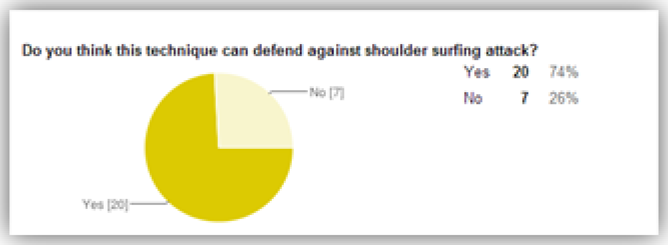


Fig 14 Shoulder Surfing defense using Colored Grid Mechanism

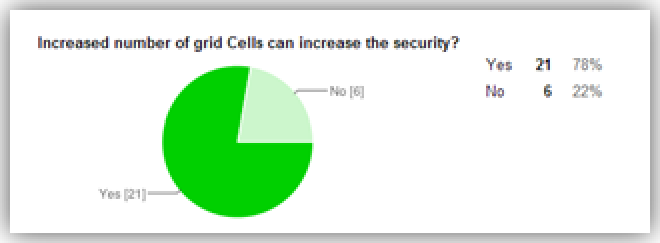


Fig 15 Effect of Number of Grid Cells on security of Colored Grid

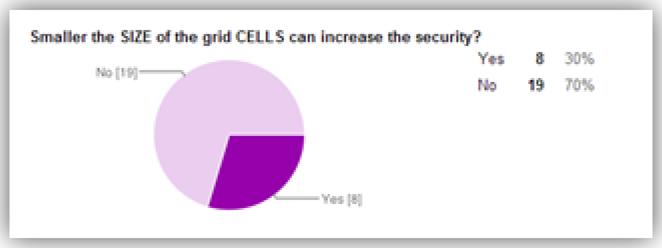


Fig 16 Effect of Size of Grid Cells on security ofColored Grid Mechanism

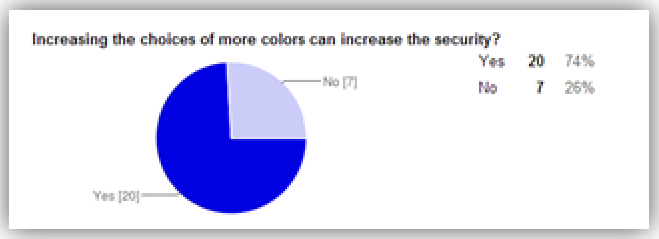


Fig 17 Effect of Increased Number of color choices on security of Colored Grid Mechanism

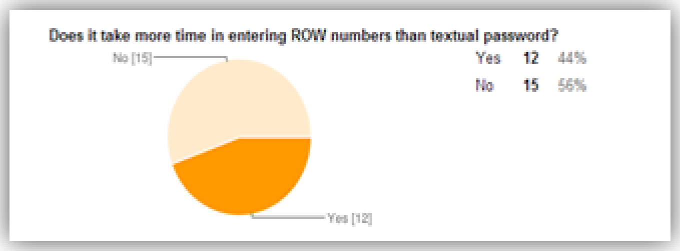


Fig 18 Time Utilization of Authentication using Colored Grid Mechanism

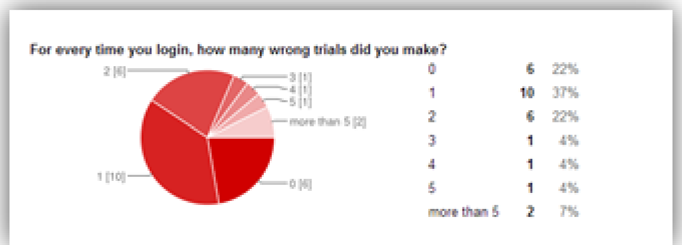


Fig 19 Distribution of Error Rate in Colored Grid Mechanism

D. *Comparative Results*

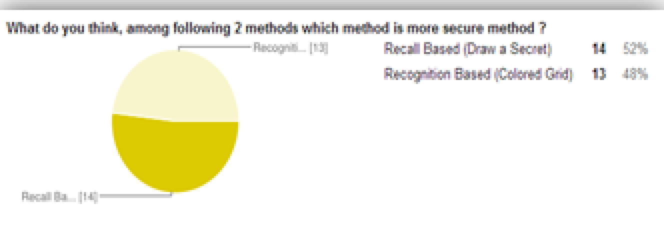


Fig 20 Security of DAS Mechanism over Colored Grid Mechanism

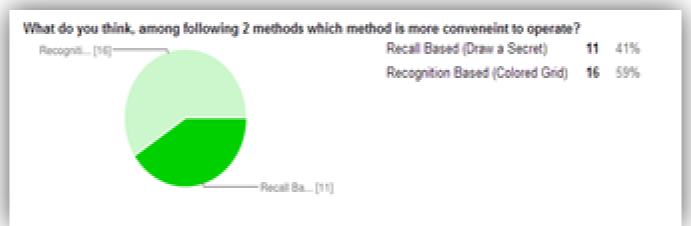


Fig 21 Convenience of Colored Grid Mechanism over DAS Mechanism

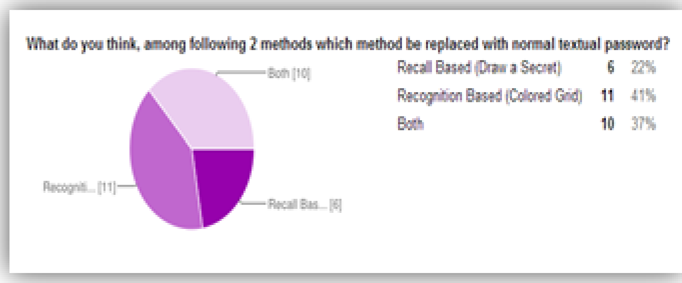


Fig 22 Adaption of DAS Mechanism and Colored Grid Mechanism over Textual Passwords

V. CONCLUSION

This research was done on anti-shoulder surfing techniques of Graphical passwords. Two anti-shoulder surfing techniques were implemented, Line Snaking on DAS and Colored Grid on Recognition System. Both the techniques were analyzed on the scale of usability and security. By analyzing the overall results of survey, it can be concluded that almost both the methods are at equal place, just Colored grid mechanism has bit more positive results. The practice sessions of Graphical Passwords can help the users to adopt them, and by then error rate can also be minimized.

The Colored Grid method implemented here is a new idea proposed by my supervisor, Kashif Abbasi, and it is based on hybrid authentication method. As per survey, 41% of users have preferred the Colored Grid method as compared to 22% of users who have accepted other method. In terms of convenience and security, users have shown their satisfaction for Colored Grid Method.

VI. FUTURE WORK

Due to the time constraint, less number of surveys were conducted during the research and also users were given enough time to practice first on the prototypes developed, hence in future there could be some practice session before the users' feedback is taken. Automatic time calculations methods could be implemented to calculate the time taken by the users during registration and sign in processes. Different surveys could be conducted by changing the number and size of the grid cells of the applications and increasing the number of color choices in colored grid mechanism, and then results could be compared for more accurate and comprehended results.

Acknowledgment

The Author thanks Almighty Allah by the grace of Whom she was abled complete her research. She also liked to thank her supervisor, Kashif Abbasi. He helped her a lot and was always there to help her and guide her to achieve her goal. Without the help of Sir Kashif, she would not have been able to complete her research within the time limit.

References

[1] Victor Plaintiram, Alex Jacob, "Anti-Shoulder Surfing Mechanism Comparison For Graphical Password". Thesis 2009, Universiti Teknologi Malaysia. [Online] Available: http://ir.fsksm.utm.my/343/

[2] Arash Habibi Lashkari, Dr. Omar Bin Zakaria, Samaneh Farmand, Dr. Rosli Saleh, "Shoulder Surfing attack in graphical password authentication". Published in *International Journal of Computer Science and Information Security*, Vol. 6, No. 2, 2009. [Online] Available: http://arxiv.org/ftp/arxiv/papers/0912/0912.0951.pdf

[3] Partha Pratim Ray, "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices". *Published in Journal of Information Engineering and Applications*, ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.2, 2012. [Online] Available: http://www.iiste.org/Journals/index.php/JIEA/article/view/1207/1128

[4] Rosanne English, Ron Poet, "Towards a Metric for Recognition-Based Graphical Password Security". Published in *Network and System Security (NSS), 2011 5th International Conference* on 6-8 Sept. 2011, Pages 239 – 243. [Online] Available:

[5] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6060007&contentType=Conference+Publications

[6] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, Jeff Yan, "Shoulder Surfing Defence for Recall-based Graphical Passwords". [Online] Available:

[7] http://cups.cs.cmu.edu/soups/2011/proceedings/a6_Zakaria.pdf

[8] M. Joshuva, T. Sudha Rani, M. Samuel John, "Implementing CHC to Counter Shoulder Surfing Attack in PassPoint – Style Graphical Passwords". Published in *International Journal of Advanced Networking and Applications 906 Volume: 02, Issue: 06, Pages: 906-910 (2011).* [Online] Available: http://www.ijana.in/papers/v2i6-4.pdf

[9] Ali Mohamed Eljetlawi, Norafida Ithnin, "Graphical Password: Comprehensive study of the usability features of the Recognition Base Graphical Password methods". Published in *Third 2008 International Conference on Convergence and Hybrid Information Technology*. [Online] Available: http://dl.acm.org/citation.cfm?id=1472003

[10] Partha Pratim Ray, "Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices". Published in *Journal of Information Engineering and Applications*, ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.2, 2012. [Online] Available: http://www.iiste.org/Journals/index.php/JIEA/article/view/1207

[11] Wazir Zada Khan, Mohammed Y Aalsalem,Yang Xiang, "A Graphical Password Based System for Small Mobile Devices". Published in *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 5, No 2, September 2011. [Online] Available:

[12] http://arxiv.org/ftp/arxiv/papers/1110/1110.3844.pdf

[13] L. Y. Por, X. T. Lim, M.T. Su, F. Kianoush, "The Design and Implementation of Background Pass-Go Scheme Towards Security Threats". Published in *Journal WSEAS Transactions On Information Science & Applications Volume 5 Issue 6, June 2008 Pages 943-952*. [Online] Available: http://dl.acm.org/citation.cfm?id=1467059