ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

Enhancement of the Security of Pass-Go Pattern Password Using Shuffling Grid-Shapes

Deepika jyoti, Dr.Amandeep Verma

M.tech student, Dept. of CSE., Punjabi University, Regional Center for IT and Management, Mohali, India

Assistant Professor, , Dept. of CSE., Punjabi University, Regional Center for IT and Management, Mohali, India

ABSTRACT: The trend of the graphical passwords is rising and every year a number of new password scheme are being launched by researchers from the various parts of the world.Password patterns, as used on current Android phones, and other shape-based authentication schemes are highly usable and memorable. In terms of security, they are rather weak since the shapes are easy to steal and reproduce. In this work, we introduce an implicit authentication approach that enhances password patterns with an additional security layer, transparent to the user. In short, users are not only authenticated by the shape they input, but also by the way they perform the input. The smart phones which use number based authentication scheme or a fixed point based android like pattern scheme are prone to the shoulder surfing attacks, which is a type of password guessing using social engineering as a hacking tool. We have proposed security critical authentication model for the smart phones, which is purely based on the uniqueness of the password combinations and ease of access. We have proposed and implemented a critical improvement in the existing pass-go pattern password based scheme. The improved scheme is using shuffling points and shuffling shapes based pattern password scheme is designed to mitigate the threat of the password guessing attacks (graphical) as well as encouraging developers to adopt much secure password schemes.

KEYWORDS: Graphical Pattern Password; Shuffling point pattern password techniques; Circular shape, Rectangular shape, shape and Polygonshape, Implicit Authentication

I. INTRODUCTION

For the purpose of authenticating a user is the central task for almost every application running on any computer based devices. Text-based username password scheme is an the most used technique for user authentication, but it is well-known and proved by various researchers (see for example [2]) that users typically choose weak passwords, and have problems to remember the stronger ones. As an alternative to these techniques, a unique password pattern based authentication [4] has been proposed in this research. These schemes are motivated by psychology research results suggesting that the human brain is particularly well-suited to remember graphical information [2].Although providing the highest level of security, biometrics still cannot be used widespread because of its high costs. This bleeding edge technology involves device cost, deployment cost and the support cost. All of these costs cut companies back the usage of biometrics as well as some environmental issues. For example, it is not reliable to use a sound recognition based technique in a noisy environment. Token-based authentication is a two-step authentication technique. It needs to be combined with knowledge based methods in order to achieve a greater level of security. Users should have an external device like ATM cards or smartcards which should be used together with a password or a PIN code. They are used to prove one's identity electronically. The token is used in place of a password or more generally with a password in order to prove that the customers are who they claim to be.

Knowledge based systems can be classified in two categories: text based and picture based. Text based authentication requires the use of alpha numerical methods and distinctly have a wider use. However textual passwords have important drawbacks due to the important amount of human involvement in them.

In this research, we are addressing the knowledge based passwords security issues and proposing a technique which is stronger than the existing knowledge based password techniques. Text based knowledge based passwords are prone to a number of hacking attacks, includes dictionary attack, brute force attacks, etc. Human factors are often considered the weakest link in a computer security system using knowledge based passwords. There are three major areas where

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

human computer interaction is important: authentication, security operations, and developing secure systems. Here we focus on the authentication problem. The most common computer authentication method is for a user to submit a user name and a text password. The vulnerabilities of this method have been well known. One of the main problems is the difficulty of remembering passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can also be easily guessed or broken.

The pass-go graphical password used on Android devices is prone to the guessing attacks. In case, somebody once see a user entering the pattern password can easily remember or guess the pattern and can take access to the device. Our major goal is to overcome this security issue. To overcome this security issue, we are making modifications in the existing pattern password scheme. Existing password pattern are shown in a 3 x3 grid option, and its point positions remains fixed at all of the times. When user enters the password pattern, it graphically looks similar every time.

We have proposed a major modification in graphical pattern passwords by using the new 9 clue-points grid every time in different geometrical shapeswill be called GRID-SHAPES.GRID-SHAPESwill be randomly selected and printed every time the user will lock-unlock the smart phone. The clue-points in the grid will be in a number sequence. A user when signup will create a pattern by joining the number points with each other to create a pattern. To gain the access to the device, the user has to remember that number sequence and need to enter the same sequence every time by drawing a pattern. Every time when user enters a password, the graphical shape of the pattern will be different, it enhances the security of the existing pass-go pattern password.

II. LITERATURE REVIEW

S.Balaji*et al*. has worked on authentication techniques for engendering session passwords with colors and text [7]. In this paper, authors have proposed two authentication schemes for generating the session passwords which is identified as the primary level of authentication. Once the user has cleared the primary level, he is then allowed to deal with the secondary level of authentication involving a graphical password scheme. This method is most apposite to the PDAs besides other computing devices, as it is resistant to shoulder surfing.

S. Wiedenbeck *et al.* Have worked on authentication using graphical passwords: effects of tolerance and image choice [20]. In this study authors have explained and expanded the human factors testing by studying the effect of tolerance, or margin of error, in clicking on the password point and the effect of the image used in the password system. In our tolerance study, results show that accurate memory for the password is strongly reduced when using a small tolerance (10 x 10 pixels) around the user's password points. This may occur because users fail to encode the password points in memory in the precise manner that is necessary to remember the password over a lapse of time. In this image study authors have compared user performance on four everyday images. The results indicate that there were few significant differences in performance of the images. This preliminary result suggests that many images may support memorability in graphical password systems.

A. Luca *et al*. have proposed Hussmann Touch me once and I know it's you! Implicit Authentication based on Touch Screen Patterns [5]. In this paper, authors have presented an implicit approach to improve authentication on current mobile devices. The basic idea was to exploit touch screen data of common smartphones (with-out adding additional hardware) to identify users based on the way they perform an action. For this, they have chosen to evaluate unlock screens as well as password patterns that come with Android phones. The basic assumption was that password patterns are convenient and usable but at the same time highly insecure. By adding implicit authentication, an invisible layer of security is added to the input, which makes the system resilient to attacks under the worst circumstances (stolen mobile phone and password pattern).

J. Bonneau. et al. has working on guessing Human-chosen Secrets. The goals of this dissertation were to introduce a sound framework for analyzing guessing attacks and apply it to large real-world data sets to accurately estimate guessing difficulty [6]. To the first goal, our partial guessing metrics are a significant improvement over Shannon entropy or guesswork, both of which are difficult to estimate from a sample and don't provide meaningful information for practical distributions. It is also easy to find examples where entropy estimation formulas misinterpret password semantics and produce misleading results.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

T.Hai has developed a Pass-Go, a New Graphical Password Scheme [13]. In this paper, authors are inspired by an old Chinese game, Go and they have designed a new graphical password scheme, Pass-Go, in which a user selects intersections on a grid as a way to input a password. The new scheme supports most application environments and input devices, rather than being limited to small mobile devices (PDAs), and can be used to derive cryptographic keys. The study the memorable password space and show the potential power of this scheme by exploring further improvements and variation mechanisms. In this paper learnt that Pass-Go could be a solid platform for future research and study.

III. DESIGN

This chapter provides an overview to the design of the android application and algorithm. An enhanced graphical pattern is developed for authentication process to prevent shoulder surfing and smudge attack. This pattern uses different shapes which are used to prevent shoulder surfing attack. Different shapes are used to change the password pattern of user at runtime according to the arrangement of dots shown to the user. It is described later in this section. In the method of proposed graphic authentication, different graphical shapes which are used in Android pattern lock. In the proposed method of graphic authentication different pattern are developed circle, rectangle, triangle, and polygon.

A. *REGISTRATION*:

When user starts application, then graphical shape is displayed selected by the user. When user select random number sequence as pass code .The pattern is displayed on the device and then unlocks the device. The graphical shapes are randomly select by the device.

B. *AUTHENTICATION:*

When user starts application, then graphical shape are shown randomly which was same as selected by user during registration process. During authentication user selects random number sequence. When user enters the number sequence as password the pattern was displayed on the device. If the sequence which the user selects is matched with the set of system generated passcode then the user is authenticated otherwise user have to choose sequence again for authentication.

C. *GRAPHICAL PATTERN PASSWORD*:

Once user unlocks the phone, the pattern password application starts its operations. The first step leads the application towards the selection of the random shape selection, which is printed on screen where the user enters the pattern password. If the entered pattern password matches the pattern password created at the time of registration, the user gets authenticated and the lock opens. Whereas, if the entered pattern password does not match the stored pattern, the user is returned to the re-enter state with different shape which is again randomly selected and the whole procedure is again performed to obtain the access of the smart phone interface.

D. *SOURCE FILES:*

The development of the proposed system has been done using Text Editor and the realization and testing of the proposed model has been done using the Chrome web browser. The front end proposed model has been written in HTML language. The front end entity design has been created using cascade style sheet (CSS). The event handling and event response have been managed using JavaScript.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

a. Circle.html

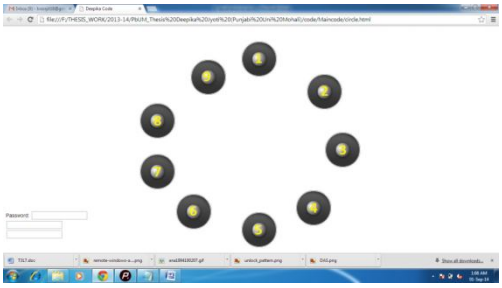

Figure 4.3: The circular design of proposed model

This is the file handling the front end of circular shape of the pattern password. The circular shape has been created as one of the four proposed shapes for shuffling shapes based proposed model of pattern passwords. The circle has been draw mathematically with invisible boundaries. The position of the grid points on the circle circumference have been evaluated using the mathematical formula of circle circumference and distance calculation. The grid points have been defined with the images.

b.Trinangle.html

This is the file used to handle the triangular shape, which is one of the proposed model shapes. The grid points have been evaluated manually using the mathematical formula and then the grid points (or grid images) have been positioned on such specific position in the triangular design. The position of the grid points has been carefully evaluated before positioning them to ensure their perfect alignment.

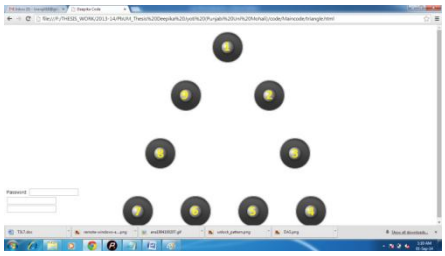

Figure 4.4: The triangular design of proposed model

The triangle shape has also been defined or programmed using the combination of HTML, JavaScript and CSS.

c. Polygon.html

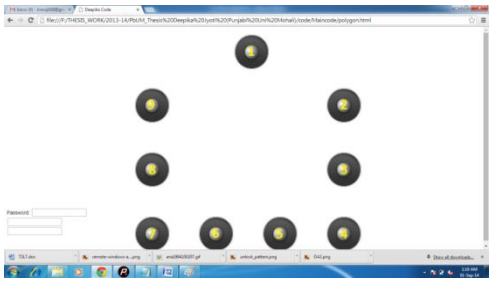

Figure 4.5: The polygon design of proposed model

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

The polygonal shape has been defined using the html file polygon.html. The front end code of HTML has been written in this file. The polygonal shape has been defined manually using the point position evaluation from mathematical formula for polygonal boundary points. The distance formula has been used to compute the distance between the points. The polygonal shape can be considered as a balanced shape as it allows users to draw a higher number of combinations.

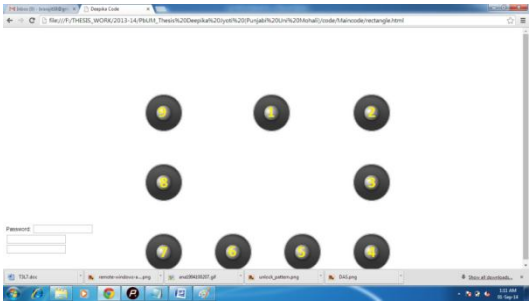

Figure 4.6: The rectangular design of proposed model

a. Rectangle.html

This is the file used to handle the rectangular shape, which is one of the proposed model shapes. The grid points have been evaluated manually using the mathematical formula and then the grid points (or grid images) have been positioned on such specific position in the square pattern password design. The position of the grid points has been carefully evaluated before positioning them to ensure their perfect alignment. Similar to the above defined shapes, the rectangular shape has also been defined or programmed using the combination of HTML, JavaScript and CSS.

b. jquery-1.9.1.min.js

This file is contains the code of jquery (or java query language), which is used as a fundamental programming to create the program which draw the lines between the points on the basis of moving cursor. Jquery or Java query is a new programming paradigm for the front end effects. The javascript is the language used for front end effects. The 1.9.1 version of jquery has been used under this development. The jquery file contains many pre-written front-end effects. We have enhanced the pre-embedded front end effects according to our need. The functions coded using jquery are written to draw lines or pattern, get the number associated with the grid point, etc.

c. patternlock.js

The patternlock.js is the program which computes many mathematical formulas to position the grid points in specific positions. Various geometric or trigonometric mathematical formulas have been used to defined and executed from the patternlock.js file.

d. Css.css

The Css.css file is used to define the cascade style sheet entities, like the style definitions under class, id or tag. This file is responsible for the front end looks of the project shapes. All of the shapes are using the various types of style definitions from CSS.

IV. RESULT ANALYSIS

The implemented work includes the new shuffling points based pattern password scheme which is designed to prevent the security risks of the currently popular pass-go pattern scheme. In this research work, HTML with JavaScript has been used for the purpose of implementation of the proposed pattern password scheme. This scheme is designed using the HTML and CSS (Cascade Style Sheets) combination, because they are simple and used to create attractive & flexible designs. Also this pattern scheme is developed in the duo, because these two are widely used for the iPhone and Android application development purposes. For the backend programming, i.e. the result retrieval, javaScript is used. Javascript is used to create the number sequence which acts as a numerical representation of the front end pattern password and saved in the database. When a user enters the pattern passwords, a numerical code for the pattern

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

password is generated on the basis of the grid point indexing numbers. JavaScript code is divided into the various functions to perform the various types of functions.

Additionally, proposed pattern password scheme is designed in way to make use capable of drawing an overlapping pattern, i.e. user can draw can cross-line pattern, which adds more probability of pattern designs. In this way, more secure passwords can be generated, and also it may help one to generate a more visually complex patter password, which will be definitely difficult to guess and will be less or not prone to the shoulder surfing attacks.

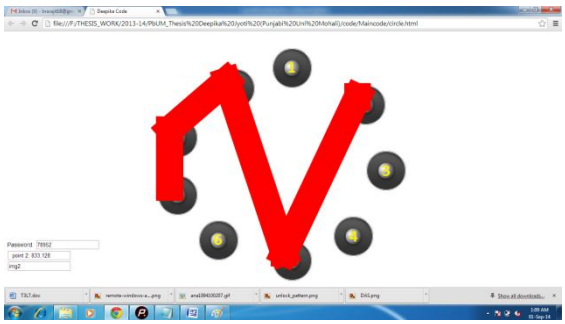

Figure 5.1: The circular shape with pattern drawn

The proposed scheme has been developed with four major trigonometric shapes: circle, rectangle, polygon and triangle. The circular coordinates has been calculated using the circular formula to draw the invisible circle and to position the nodes on the boundary of the circle.

In the above figure (5.1), the circular shape has been represented with the pattern drawn on it. Either circular shape may carry some of the pattern limitations of visible clarity of the pattern drawn in the shape like in the case of 1-2-3-1 password.

The proposed scheme has also been developed in the polygonal shape for the shuffling shape and pattern based graphical password. The rectangular shape carries some of the critical shape drawbacks. Even after the lack in the clear visibility of the password pattern scheme in the polygonal shape it is capable of drawing the password like in the case of 2-5-4-2.

In figure 5.2, the password pattern scheme snapshot has been shown for the rectangular shape. The rectangular shape has been designed by matching the all nine points in the rectangular shape by positioning the sequence number images on the edge of the rectangle on certain edge points. The rectangular shape is having total nine points drawn of the edge of the invisible rectangular shape. The rectangular shape also carries some of the drawbacks similar to the polygon, which can be removed in the future research works for the enhancement of the proposed shuffling points pattern password scheme. The proposed scheme is using the point to point line drawing for the front-end, whereas in the backend the specific number is returned to the backend memory for the user authentication purpose.

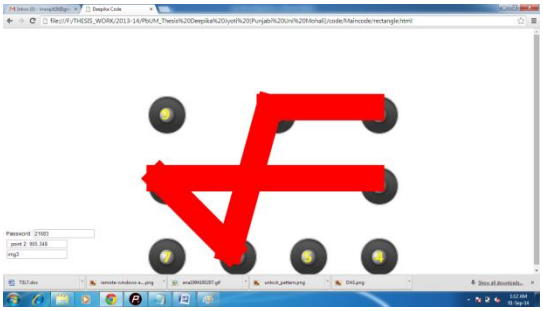

Figure 5.2: The rectangular shaped password for proposed scheme

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

In figure 5.3, the password pattern scheme snapshot is showing the triangular trigonometric pattern password shape. The triangular shape has been designed by matching the all nine points in the triangular shape by positioning the sequence number images on the edge of the triangle on certain edge points. The triangular shape is having total nine points drawn of the edge of the invisible rectangular shape. The triangular shape also carries some of the drawbacks similar to the polygon, which can be removed in the future research works for the enhancement of the proposed shuffling point's pattern password scheme. The proposed scheme is using the point to point line drawing for the front-end, whereas in the backend the specific number is returned to the backend memory for the user authentication purpose.

The triangular and circular shapes in the proposed scheme can be considered as the most balanced schemes out of all four shapes developed under the password pattern scheme. The shapes in the proposed scheme have been evaluated for the various password pattern schemes. The most balanced password scheme is circular scheme, where all of the matching points and the lines or connections drawn between those points are clearly visible in any possible shape. The square shape was considered least compatible and most confusing shape; hence it was dropped from the possible graphical pattern password schemes.

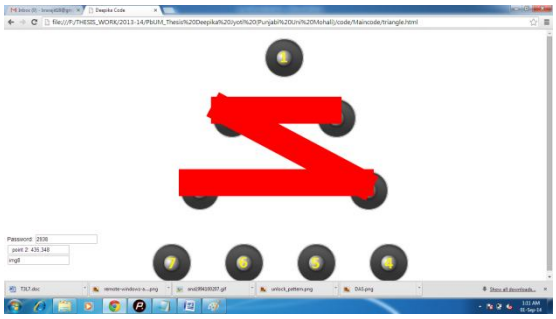

Figure 5.3: The triangular shaped password for proposed scheme

V. CONCLUSION

The pass-go graphical password used on Android devices is prone to the guessing attacks. Existing password pattern are shown in a 3 x3 grid option, and its point positions remains fixed at all of the time. Existing graphical password based approaches offer a user to create a memorable pattern password by combining the clue-points in the grid, that are easy for attackers to copy by watching the input because the points are stationary and password patterns looks exactly same every times when the user enters it. So it can be said that graphical pattern passwords are prone to shoulder surfing attacks.

In case, somebody once see a user entering the pattern password can easily remember or guess the pattern and can take access to the device. Our major goal is to overcome this security issue. To overcome this security issue, we are making modifications in the existing pattern password scheme. When user enters the password pattern, it graphically looks similar every time. We have proposed a major modification in graphical pattern passwords by using the new 8 clue-points grid every time in different geometrical shapes called GRID-SHAPES. The GRID-SHAPES are randomly selected and printed every time the user locks and re-opens the smart phone. The clue-points in the grid are in a random number sequence. A user when signup creates and stores a pattern by joining the number points with each other to create a pattern. To gain the access to the device, the user has to remember that number sequence and need to enter the same sequence every time by drawing a pattern. Every time when user enters a password, the graphical shape of the pattern is displayed differently, i.e. in different geometrical shapes, which enhances the security level of the existing pass-go pattern password schemes.

The proposed scheme has been evaluated as effective, robust, ease of access and wide adaptability of the scheme for the various smart phone platforms. The proposed scheme has been evaluated under various situations. All of the password pattern based graphical shapes has been evaluated individually with various pattern shapes (number sequence combinations). The triangular and circular shapes in the proposed scheme can be considered as the most balanced

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

schemes out of all four shapes developed under the password pattern scheme. The shapes in the proposed scheme have been evaluated for the various password pattern schemes. The most balanced password scheme is circular scheme, where all of the matching points and the lines or connections drawn between those points are clearly visible in any possible shape. The square shape was considered least compatible and most confusing shape; hence it was dropped from the possible graphical pattern password schemes.

VI. FUTURE WORK

The drawbacks or limitations concerned with the different geometrical shapes can be mitigated in the future researches, which can be considered as the critical enhancement or improvement in the proposed system. A new scheme can be developed following the design and pattern schemes of the proposed scheme.

REFERENCES

[1] K.Renaud, P. Mayer, M. Volkamer and J.Maguire, "Are Graphical Authentication Mechanisms As Strong As Passwords?", *In proceeding of Federated Conference onComputer Science and Information System (FedCSIS)* , vol. 1, pp. 837-844, 2013.
[2] H.K Bashier, H. Lau Siong and H. Pang Ying , "Graphical Password: Pass-Image Edge Detection",*In Proceeding of IEEEInternational Colloquium on Signal Processing and its Application (CSPA),* vol.no, pp. 111-116,March 2013.
[3] C.Yi-Lun, K.Wei-Chi, Y. Yu-Chang and L.Dun-Min , "A Simple Text-Based Shoulder Surfing Resistant Graphical Password", *InProceedings of 2013 IEEE International Symposium onNext-Generation Electronics (ISNE),* ,vol. 1, pp. 161-164, Feb. 2013.
[4] U.Sebastian , D. Markus , W.Christopher and H.Thorsten ,"Quantifying The Security Of Graphical Passwords:The Case Of Android Unlock Patterns", *In Proceedings of the ACM SIGSAC conference on Computer & communications security*,vol.no, pp. 161-162,2013.
[5] L.AlexanderDe ,H.Alina ,B. Frederik ,L. Christian and H. Heinrich "Touch Me Once And I Know It's You! Implicit Authentication Based On Touch Screen Patterns", *CHI'12 Proceeding of the SIGCHI Conference on Human Factor in Computing Systems on,* vol. 1, pp. 987-996, CHI, 2012.
[6] J. Bonneau, "Guessing Human-Chosen Secrets" Ph.D Dissertation, University Of Cambridge, May 2012.
[7] S.Balaji, A.Lakshmi, V.Revanth, M.Saragini and V.Venkateswara"Authentication Techniques For Engendering Session Passwords With Colors And Text", *AITM*, vol. 1,No. 2,pp. 71-78, 2012.
[8]S.K Gajbhiye and P. Ulhe "Authentication Schemes For Session Passwords Using Color And Gray-Scale Images", *Journal of Systems and Software* 73.3*JSIP*, pp. 405-414, 2012.
[9] M.Ordean and K.Renaud , "Catch Me If You Can: Using Self-Camouflaging Images To Strengthen Graphical Passwords",*In proceeding of IEEE International Conference on Intelligent Computer Communication and processing (ICCP)* , vol. 1, pp. 309-315,Sep 2012.
[10] G. Ming-Huang, L. Horng-Twu , H. Li-Lin , H. Chih-Yuah and Y. Chih-Ya , "Authentication Using Graphical Password In Cloud", *In Proceeding of 15th International Symposium on Wireless Personal Multimedia Communication (WPMC)*, vol. 1, pp. 177-181,2012.
[11] M.Yuxin , "Designing Click-Draw Based Graphical Password Scheme For Better Authentication", *In Proceeding of 7th IEEE International Conference on Networking, Architecture and Storage(NAS)*, vol. 1, pp. 39-48, June 2012.
[12] S.Farmand and O.BinZakaria ., "Improving Graphical Password Resistant To Shoulder-Surfing Using 4-Way Recognition-Based Sequence Reproduction (RBSR4)", *In Proceeding of2nd IEEE International Conference onInformation management and Engineering (ICIME),* vol. 1, pp. 644-650, 2010.
[13] T. Hai, "Pass-Go, A New Graphical Password Scheme Resistant to Shoulder Surfing", Thesis, University Of Ottawa, June, 2006.
[14] Passfaces. "The Science Behind Passfacestm For Windows" *People and Computers XIV—Usability or Else!*.Springer London, pp. 405-424, 2005.
[15] S.Xiaoyuan, "A Design And Analysis Of Graphical Password" Thesis, Georgia State University, 2006.
[16] O.Van , P. C and J.Thorpe ,"On The Security Of Graphical Password Schemes",*SSYM In Proceeding of the 13th conference on USENIX Security Symposium*,vol. 13, pp .11-11 ,2005.
[17] F. Monrose and M.K Reiter, "Graphical Passwords Security and Usability",*ACSAC '10 In Proceeding of Conferenceon the 26th Annual Computer security applications*, vol .1, pp. 79-88, 2005.
[18] X.Suo, Y.Zhu, and G.S Owen,"Graphical Passwords: A Survey" *In Proceeding of 21st Conference on Annual Computer Security Applications (Acsac)* ,vol.1, pp.5-9,2005.
[19] S.Wiedenbeck,J. Waters, J.Birget, A.Brodskiy, and N. Memon, "Passpoints: Design And Longitudinal Evaluation Of A Graphical Password System"*International J. of Human-Computer Studies (Special Issue On Hci Research In Privacy And Security)* 63, pp.102–127, 2005.
[20] W.Susan , B. Jean-Camille and B.Alex "Authentication Using Graphical Passwords: Effects Of Tolerance And Image Choice", *InProceeding of the Symposium on Usable Privacy and security(*ACM*)* ,pp, 1-12,2005.

BIOGRAPHY

Deepika Jyoti is a Research Assistant in the Computer Science Department, from Punjabi University Regional Campus for Information and Management technology, Mohali. She received Bachelor of technology (B.tech) degree in 2012 from BCET, Gurdaspur (Punjab) India and defended her dissertation of M.tech in 2014 .Her research interests are Digital Image Processing.