Increasing Security in Click Based Graphical Password with Kerberos

Prof. Leena H. Patil, Prof. Uma Patel, Ms. Preeti Ramtekkar

Abstract- **Graphical user authentication system is an alternate solution to a textual password system. Textual based password are versatile and easy to implement but the drawback with this technique is that in case of short length password it can be easily guessed by an attacker so the alternate solution is graphical user authentication system. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information. If the credentials match, the process is completed and the user is granted authorization for access. Here the PCCP (persuasive cued click point) is used as an authentication technique and with addition of BDAS (Background Draw A Secret) algorithm. On the other hand the PCCP technique is implemented on the 10 images. So combinely this technique called as modified PCCP technique. This can increases the security of overall system. This authentication system is a standalone application.**

The two main disadvantage of graphical user authentication system: hotspot problem and shoulder surfing problem can be overcome by using modified PCCP. Hotspot problem can be overcome by using the concept of viewport and shoulder surfing problem can be remove by using the concept that out of 10 images randomly 5 images are visible during login time. The result show that time taken for password creation by modified PCCP is more or near about same to PCCP but it is more secure than existing PCCP. Second level of security can be provided by Kerberos a network authentication protocol which can granted authorization for access.

Index term- **hotspot , Kerberos, PCCP, shoulder surfing, viewport.**

Preeti Ramtekkar (MTech. student)
CSE Department, PIET
Nagpur, Maharashtra, India

Prof. Leena H. Patil (Lecturer)
CSE Department, PIET
Nagpur, Maharashtra, India

Prof. Uma Patel (Lecturer)
CSE Department, PIET
Nagpur, Maharashtra, India

I. INTRODUCTION

In early days, text based passwords are used for authentication. Text based passwords are contain string of characters. In textual passwords, peoples always creates password which is easy to remember but these passwords are easy for attackers to break. For more security, users use strong system assigned passwords which will be difficult for users to remember. Biometric and tokens are used as an alternative to text based passwords but has its own drawbacks such as it requires extra hardware which were expensive so these methods are costly. As an alternative to all these methods, graphical passwords are used because psychology studied says that human brain can recognize

images better than the text . Graphical passwords are of three types: Click based graphical password scheme, choice based graphical password scheme and draw based graphical password scheme.

Pass-Points: Pass-Point technique comes under click based graphical password scheme. In Pass-Points password consists of sequence of 5 different click points on a single image. The main disadvantage of this scheme is HOTSPOTS and pattern formation attacks [2].

Cued Click Points: Cued Click Points comes under click-choice based graphical password scheme. Cued Click Points [2] was designed to reduce patterns and to reduce the usefulness of hotspots for attackers. Instead of five click-points on one image, CCP uses one click-point on five different images. The next image displayed is based on the location of the previously entered click-point. One best feature of Cued Click Point is that the message of Authentication failure is displayed after the final click-point, to protect against incremental guessing attacks. But this technique has several disadvantages like false accept (the incorrect click point can be accepted by the system) and false reject (the click-point which is to be correct can be reject by the system).In this system pattern formation attack is reduced but HOTSPOT remains since users are selecting their own click-point.

Persuasive Cued Click Points: Persuasive Cued Click Points technique comes under click-choice based graphical password scheme. By adding a persuasive feature to CCP, PCCP encourages users to select less predictable passwords, For password creation PCCP uses terms like viewport & shuffle. To avoid known hotspots the viewport is positioned randomly rather than specifically. The most useful advantage of PCCP is attackers have to improve their guesses.

In this paper we proposed a system in which we use the features of PCCP technique and combine with BDAS (Background Draw A Secret) algorithm. During registration time user is asked to select a click point on 10 different images and save this in the database , next time when user login only 5 random images is appear from that 10 images .Every time when user login random 5 images from that 10 images is visible user has to select their click points on images . System will be proceeding if and only if all the click points are correctly selected.

Additional security in our proposed system is provided by Kerberos protocol [2] which is a computer network authentication protocol which works on the basis of "tickets" to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its aimed is to provide authentication. Kerberos protocol messages are protected against eavesdropping and replay attacks.

II. LITERATURE SURVEY

In [4] a Sound Signature Integrated Graphical Password Authentication Mechanism has been presented. This system presents an innovative idea that integrates graphical passwords with sound signature. The system encourages the user to select click points from images as their passwords rather than textual words. According to human psychology, one can memorize the click points easily when compared to the textual passwords. The number of click points and the number of images included in the password creation depend upon the user's choice. Apart from the click points, the system provides sound files that can be integrated to the user's password. While logging in, the system verifies the click points as well as the sound file. Hence the system provides an efficient method to create more secured passwords which are easier to manage. This System is the integration of sound signature into graphical password scheme. The Graphical password scheme is very secure and difficult to hack and it is quite easy to remember. In our new system, an extra feature is added to this

technology, i.e. Sound Signature. The user is given the privilege to select a sound file as well as tolerance level while he is creating the new login account. When then user logs in, if the click points are correct, the selected sound file will be played. Otherwise the sound file will not be played.

In [5] new click based graphical password scheme can be introduced. In graphical user authentication system image can be used as password .Image can be suffer with number of drawbacks like hotspot problem and shoulder surfing problem. So hotspot problem can be removed completely with persuasive cued click point method. To deal with shoulder surfing problem another method has been introduced called improved persuasive cued click point. This method is similar to the persuasive cued click point but there is some change in the login phase of the method and also the concept of single and double click has been used. During single click empty value has been accept and during the double click actual click point value has been accepted .So using this two types of click an attacker which is peeping over the shoulder of an authenticated user can get be confused and not get the exact click point values and in this way the shoulder surfing problem can be removed.

In [6] security is the high priority issue. When security is high priority issue textual based password is not enough there is a need for something more secure so the solution is an integration of cued click point technique in Kerberos authentication protocol is a solution. Kerberos credential will give the proper login to the system as well as their application. When the user want to login in the system user has to click on points system will be proceed if and only if all the click points are correctly selected and this process will be protected in the backend by the Kerberos protocol which will generated a ticket to authenticate the user.

In [7] image based authentication can be used for folder that contain the confidential information or more secure information. In this two technique has been used PCCP i.e. persuasive cued click point and SHA1 i.e. secure hash algorithm .PCCP can be used to provide the better and strong password and SHA1 can be used to provide a security to a folder. PCCP and SHA1 can provide an environment in which a folder will be in the safe condition .In this a software model has been design which provide the image based authentication as well as encrypting folder using the secure hash algorithm. Before encrypting folder will be converted into zip file which does not allow to entering any viruses to the file make damage in the file.

III. PROPOSED SYSTEM

Our proposed system is also a graphical user authentication system in which image can be used as a password. For authentication PCCP (persuasive cued click point) technique is used in between that BDAS (Background Draw A Secret) algorithm is implemented which increases the security of overall system. Second level of security is provided with the Kerberos which is a network authentication protocol. After the successfully login Kerberos can granted a ticket to the user which the user can further used for access the services of the network. The techniques and algorithm used in our proposed system is discussed here.

Centered Discretization algorithm

Centered Discretization algorithm improves the usability and security of our system. It offers centered-tolerance, which increases security because the size of grid squares can be reduced (to 2rx2r instead of 6rx6r), thereby increasing the password search space without negatively impacting usability since the same minimum tolerance r is guaranteed. It further increases usability by behaving in accordance with users'likely mental models and eliminating false rejects and false accepts.

Background DAS (BDAS)

This method was proposed in 2007. In this method both the background image and the drawing grid can be used to for drawng. User must have a secret in mind, and then draw it using the point from a given backgroundimage. The user's choice of secret is affected by various characteristic of the image.

Persuasive cued click point technique (PCCP)

This is the graphical user authentication technique in which concept of viewport is introduced to avoid the known hotspot attack. User is allow to click inside the viewport only to choose the password. Persuasive Technology was first introduced by Fogg [13] as technology to motivate and convinced the people to behave in a desired manner. An authentication system which applies Persuasive Technology should guide and encourage users to select stronger passwords, but not impose system-generated passwords.

Kerberoes

Kerberos gets its name from Greek mythology. Cerberus, also known as Kerberos, was a three headed beast that guarded the Underworld and kept the living from entering the world of the dead Kerberos protocol design began in the late 1980s at the Massachusetts Institute of Technology (MIT), as part of project Athena. It is a secure authentication mechanism designed for systems, which assumes the network is unsafe. It enables a client and a server to mutually authenticate before establishing a connection.

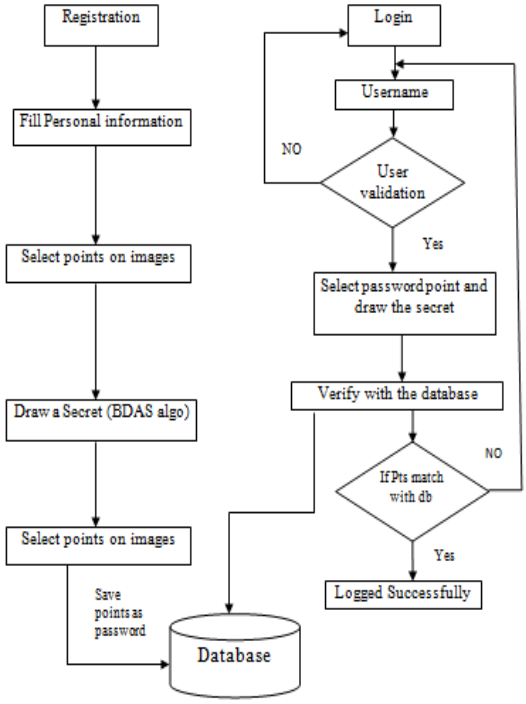

Figure 1: Proposed research methodology

EXPERIMENTAL RESULTS

Registration page

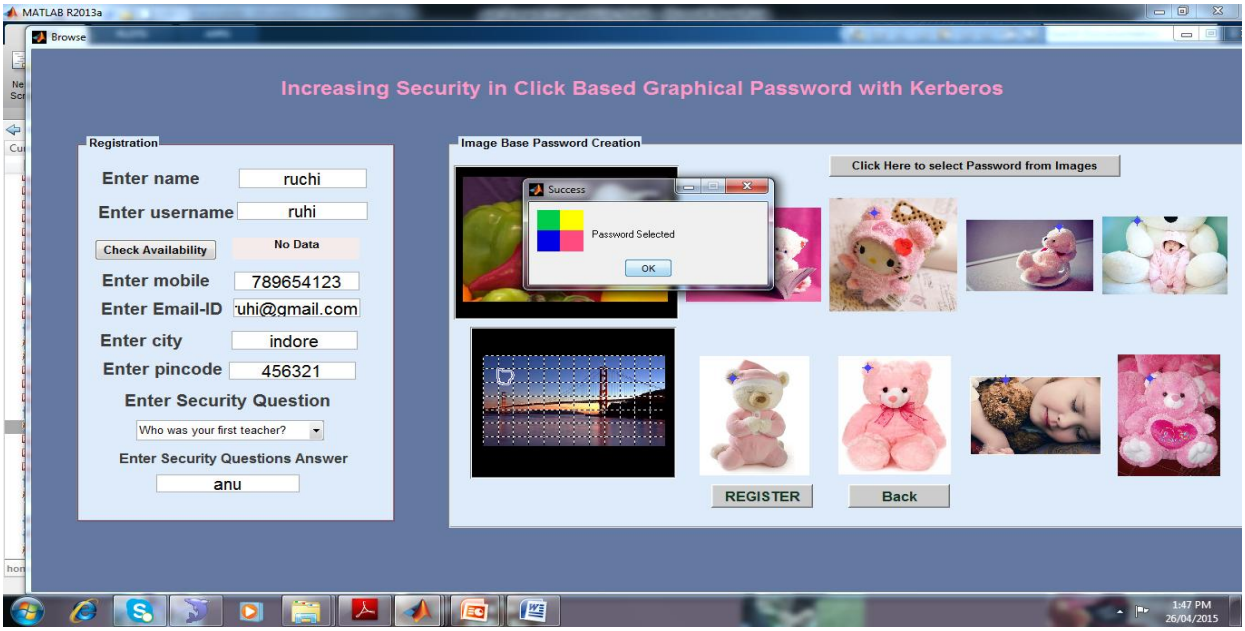

Figure 2: After selecting a point on each image register. This points is saved in database for login purpose

Login page

Figure 3: Enter a user name and then select the points on images(which is your password points) and draw a secret figure

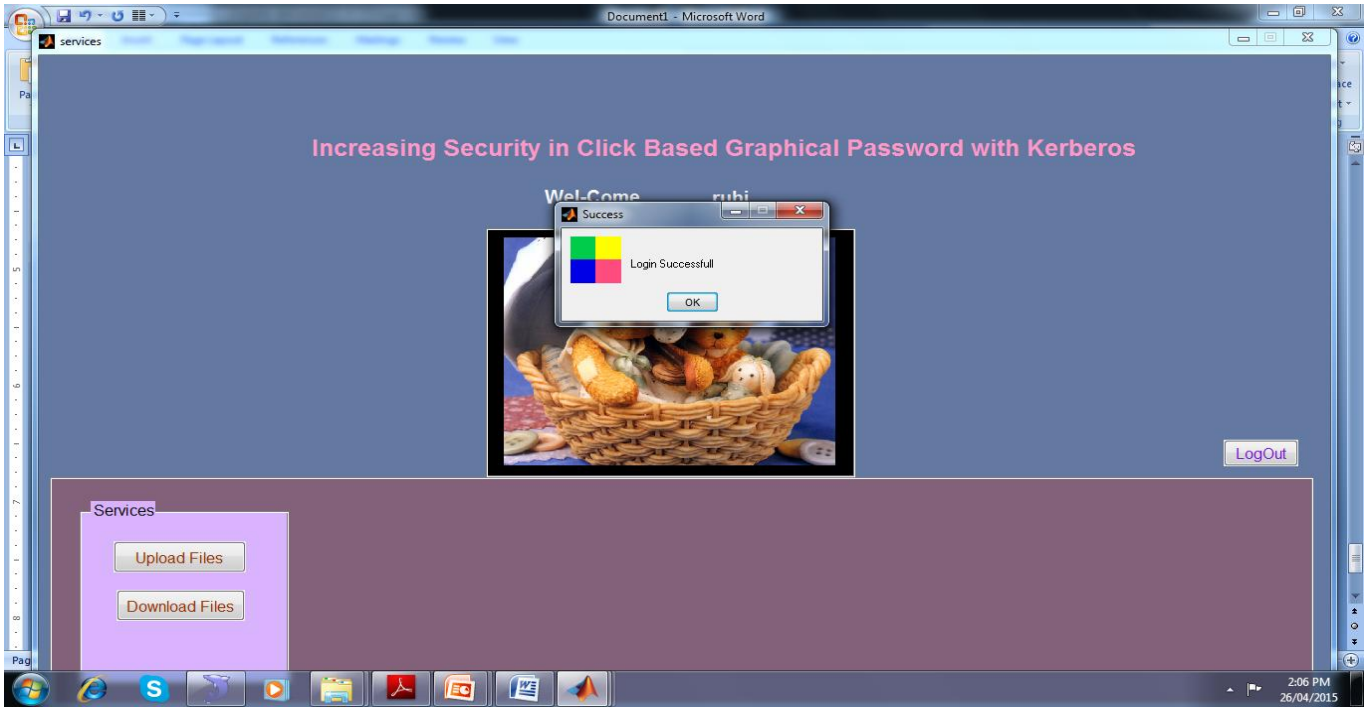

Figure 4: login successfully

Figure 5: Ticket has been granted to the authenticated user

IV. CONCLUSION

Now a day's data security is very important issue. Alphanumerical password has been used but it's not providing the efficient security in case when we chose the small password because it can be easily guessed or hacked by an attacker. Alternate solution is using a graphical user authentication system in which image can be used as a password. Our proposed graphical user password system can provide high security and usability. Also if user is an authenticated then ticket can be granted to the user. This ticket can identified the user or proof that user is an authenticated not the fake user. It can overcome with the hotspot and shoulder surfing problem. Graphical passwords have been introduced as an alternative to the traditional authentication process. Though the graphical password schemes provide a way of making more user friendly passwords, while increasing the level of security. Therefore, we have not only created a strong image based authentication system but also strengthen it with Kerberos authentication protocol.

V. ACKNOWLEDGMENT

Professor Leena H. Patil and Professor Uma Patel has guided me along the way for the completion of this paper and the project. With their support and expert advice on the subject matter I was able to complete this paper successfully. I thank them for their valuable input and time.

VI. FUTURE SCOPE

This system can be further enhance by providing the number of services to the user after the ticket can be granted. This system is quit complex from the point of view of remembering the password click points on ten images. But this system can provide high security which can be most important in most area like military or other information which is highly secure .So the complexity can be degraded but not in expense of security.

REFERENCES

[1] Susan Wiedenbeck, Jim Watersa, Jean- Camille Birget, Alex Brodskiy, Nasir Memon," PassPoints: Design and Longitudinal evaluation of a graphical password system" Int. J. Human Computer Studies 63 (2005) 102–127.

[2] Sonia Chiasson1,2, P.C. van Oorschot1, and Robert Biddle , "Graphical Password Authentication Using Cued Click Points", April 10, 2007.

[3] Sonia Caisson, Elizabeth Stobert, Alai Forget,Robert Biddle, and Paul C. van Oorschot "Persuasive Cued Click Points: Design, Implementation, and Evaluation of a Knowledge- Based Authentication Mechanism" Ieee Transactions On Dependable And Secure Computing, Vol. 9 No. 2, March/April 2012.

[4] Sarisha Satheesan, A. Ilayarajaa " A Sound Signature Integrated Graphical Password Authentication Mechanism" International Journal Of Innovative Technology Exploring Engineering (IJITEE)ISSN: 2278-3075Volume-2, Issue-4, March 2013.

[5] Suresh Pagidala, C. Shoba Bindu " Improved Persuasive Cued Click Points for knowledge based Authentication" International Journal of Computer Science and Information Technologies,Vol. 4 (6) , 2013, 1000-1003

[6] Pathan Mohd. Shafi1, Dr Syed Abdul sattar2, Dr. P. Chenna Reddy "Cued Click-Points image based Kerberos authentication protocol" Volume 4, Issue 3, May-June 2013, pp.

[7] S.Hande, N.Dighade , R.Bhusari, M. Shende, " Image Based Authentication for Folder Security using Persuasive Cued Click-Points and SHA" Journal of Computer Engineering Volume 16, Issue 2, Ver.IX Mar-Apr. 2014, PP 124-128.

[8] El-Emam, E. Koutb, M. Kelash, H. Allah , "An optimized Kerberos authentication protocol "Authority for Remote Sensing & Space Sci.,Cairo, Egypt, pp no. 508-513 Dec 2009.

[9] F. Towhidi "A Survey on Recognition-Based Graphical User Authentication Algorithms" International Journal of Computer Science and Information Security Vol. 6, No. 2, 2009

[10] Uma D. yadav,Prakash S.Mohod "Adding Persuasive features in Graphical Password to increase the capacity of KBAM" Volume 4, Issue 3, May-June 2013, pp. 560-569

[11] Nelson, D.L., U.S. Reed, and J.R. Walling. "Picture Superiority Effect" Journal of Experimental Psychology Human Learning and Memory 3, 485-497, 1977.

[12] Uma D.Yadav,. P. S. Mohod,"Enhancement of Knowledge Based Authentication Mechanism using Graphical Password via Persuasion" Journal Of Computer Science And Engineering, Volume 17,Issue 2, February 2013

[13] B. Fogg," Persuasive Technologies: Using Computers to Change What We Think And Do" Morgan Kaufmann Publishers, 2003.

