© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Review of Multimedia Graphical Grid Based Text Password Authentication for Advanced User

Tasnim Kausar[1], Prof. Naziya Pathan[2], Prof. Shyam Dubey[3]
[1]M. Tech, Research Scholar NCEOT, Nagpur, Maharashtra, India
[2]Asst. Professor NCEOT, Nagpur, Maharashtra, India
[3]Asst. Professor & HOD NCEOT, Nagpur, Maharashtra, India

ABSTRACT

Proposed work is used to solve the problem of text based password system. It deals with geographical password structure. It is used to increase the reliability of password for advanced users by modifying a combination of text and graphical passwords. It will ensure more secure way to users for granting access to an authenticated system. Proposed work uses color code authentication which provides two step authentication to the user. Each time user logged in with generated one time password.

This scheme is tested with different kinds of security attacks. User has to memorize only the sequence of three colors and three shades selected at the time of registration. This scheme is useful for secure authentication method for data protection on cloud and also in banking system.

Keywords: Advance user, security, password, access control,color code authentication,geographic authentication, CSR, MySql, JDBC, Tomcat Server, Bootstrap Template, Eclipse, JDK, Servlet.

I. INTRODUCTION

Authentication system plays an important role in every application. It allows an application to authenticate user and provide him access control for the application. A weak authentication system leads to various vulnerable attacks. When it comes to user authentication, the first Scheme comes in minds is text based authentication. In cloud computing to access data one has to authenticate the system. The common authentication method used to access data on cloud is password. The major drawbacks of text based passwords are weak password, forgot password, stealing of password etc. So it requires strong and secure authentication method for the protection of data on cloud.

The strength of authentication system lies in the password. Passwords are simple alpha-numeric strings shared between server and the user. Important factor to note here is that alphanumeric passwords are not stored ―as it is‖ on the server but rather are saved in encrypted form after hashing. Passwords are most simple means of user authentication as no extra hardware (bio metric device) is needed, but have the disadvantage that strong passwords are difficult to remember. User tends to keep shorter passwords which are weak and could be easily broken by dictionary attack and brute force attack.

Graphical passwords systems are the most promising alternative to conventional text based passwords but prone to shoulder surfing. In this scheme, a new authentication system which combines the advantages of both graphical password authentication system and one time session key is proposed. The system uses user defined images as image passwords and system defined pictures are used as dummy images.

Today, authentication is achieved through the use of password technique. To prove and maintain the identity. Every user uses a password authentication. The traditional method of password is a textual (alphanumeric) password. It is the combination of alphabets, digits and special symbols.

A. Categorization of Graphical password authentication techniques:

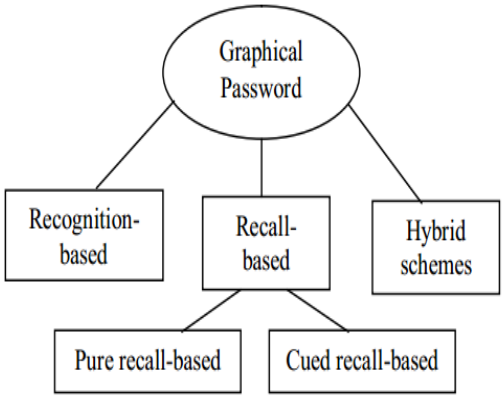

Figure 1

Recognition-Based Technique:

In this category, users will select images, icons or symbols from a collection of images. At the time of authentication, the users need to recognize their images, symbols or icons which are selected at the time of registration among a set of images.

Pure Recall-Based Technique:

In this category, users have to reproduce their passwords without being given any type of hints or reminder. Although this category is very easy and convenient, but it seems that users can hardly remember their passwords. Still it is more secure than the recognition based technique.

Cued Recall-Based Technique:

In this category, users are provided with the reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to the recall based schemes but it is recall with cueing.

Hybrid Schemes:

In this category, the authentication will be typically the combination of two or more schemes. These schemes are used to overcome the drawbacks of a single scheme, such as spyware, shoulder surfing and so on.

II. LITERATURE SURVEY

R. Dhamija, and A. Perrig in their work "Déjà Vu: A User Study Using Images for Authentication" presented the security of the systems relies on recognition-based, rather than recall-based authentication. They examine the requirements of a recognition-based authentication system and propose Deja Vu, which authenticates a user through her ability to recognize previously seen images. Deja Vu is more reliable and easier to use than traditional recall-based schemes, which require the user to precisely recall passwords or PINs. Furthermore, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others. They develop a prototype of Deja Vu and conduct a user study that compares it to traditional password and PIN authentication. Our user study shows that 90% of all part[1].

The paper "A New Approach For Instigating Security Using single Zoom Mouse Click Graphical Password" presented by MerinSebastiian, Biju Abraham Narayamparambil proposed a graphical password scheme which is more secured than other method. This method also depends not only on image but also number of mouse click on the image. This method reduces the huge image database, as well as images being too simple to cause collisions on points selected for different users[2.]

The paper "Authenticating Mobile Device User through Image Selection" presented by W. Jansen,, describes a general-purpose mechanism for authenticating users through image selection. The

underlying rationale is that image recall is an easy and natural way for users to authenticate, removing a serious barrier to users compliance with corporate policy. The approach described distinguishes itself from other attempts in this area in several ways, including style dependent image selection, password reuse, and embedded salting, which collectively overcome a number of problems in employing knowledge-based authentication on mobile devices[3].

In the paper of Xiyang Liu, JinhuaQiu, Licheng Ma, HaichangGao, and Zhongjie Ren "A Novel Cued-recall Graphical Password Scheme" they purposed a novel cued-recall graphical password scheme CBFG (Click Buttons according to Figures in Grids).Inheriting the way of setting password intraditional cued-recall scheme, this scheme is also added the ideology of image identification. CBFGhelps users tend to set their passwords more complex.Simultaneously, it has the capability against shoulder surfing attack and intersection analysis attack. Experiments illustrat**A.** that CBFG has better performance in usability**B.** especially in security[4].

In the paper of S.Man, D. Hong, and M.Mathews "A shouldersurfing resistant graphical password scheme" they propose and evaluate a new shoulder-surfing resistant ssscheme which has a desirable usability for PDAs. Their inspiration comes from the drawing input method in DAS and the association mnemonics in Story for sequence retrieval. This scheme requires users to draw a curve across their password images orderly rather than click directly on them. The drawing input trick along with the complementary measures, such as erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images provide a good resistance to shouldersurfing. A preliminary user study showed that users were able to enter their passwords accurately and to remember them over time[5].

Mohammad Sarosh Umar and Mohammad QasimRafiq presented "A Novel Recognition-based Graphical User Authentication Scheme".In that they propose a novel recognition-based image authentication system called "Select-to-Spawn" which is secure, robust and convenient to use. The scheme can be easily implemented on computers, hand held devices, mobile phones and ATMs[6].

The paper "Proposal for novel 3D password for providing authentication in critical web applications" represented by A.S. Yeole. This paper presents and evaluate on the 3-D password. The 3-D password is a multifactor authentication scheme. Instead of depending on one factor add more security component which will make hackers and crackers job more difficult. In this paper we tried to enhance the password security by adding two more components to a password one is Challenge response protocol and second is USB Token[10].

Limitation of Existing System

The existing system is a text based password authentication Scheme. It's a combination of Text & OTP (one time password) based approach.

The user authentication is done in two phase Registration and Login phase. A user creates his/her profile by providing personal details & username, password. The system sends verification email or OTP on his/her email or phone number. Then user provides the details given. After verification is done user registration is done.

Disadvantages:

- It is easy to hack or guess.
- It is found that users are not selecting and handling
  text based passwords in insecure manner
- Humans can only memorize very few passwords due to this fact Users are writing down, share or Use the same passwords for many accounts.

- To remember easily, here the passwords are kept short and simple like personal names, family member names, birth dates, pet names, phone numbers etc. and so vulnerable to various types of attacks like easy to guess, brute force, dictionary attack, shoulder surfing, hidden camera, social engineering and malicious software's like key logger, spyware etc.

1. Proposed Scheme

The proposed system will use the pictographic and geographical based password authentication scheme which will overcome the problems of text based password. In order to provide a robust and secure mechanism proposed work will allow user to select a color and geo location for login and registration and also validate user using OTP (one time password). The main objective of this purposed scheme is to form a nine digit one time password with latitude and longitude location.

Proposed work is an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than typing alphanumeric words. Graphical passwords are more memorable compared to the alphanumeric passwords because it is easier to remember an image of flower than a set of alphabets and numbers. It will develop a secure and robust mechanism for authentication using pictograph and geographical password. In it Java J2EE will be use for developing the system. It will design a banking web application with the purposed authentication scheme to demonstrate the usability of system.

Text based password are susceptible to dictionary attack, shoulder surfing, eavesdropping. To overcome some of these problems pictographic password will be introduced. This paper propose a pictographic based authentication Scheme which includes

1.
2.

- ✓ Color Code Authentication Scheme
- ✓ Geographic Authentication Scheme

In Color Code Authentication Scheme the user requires to choose the color on a color code selection form at the time of registration and enter same color when user will login. Geographic Authentication Scheme in which the user requires to choose a place on a digital map to authentication with (a location password). The proposed scheme will use GeoPass and allow user to annotate that location with some keywords (an annotated location password). In geographic Scheme, users would authenticated by correctly entering both a location and an annotation. Proposed scheme's aims to provide a robust and secure authentication mechanism for

- ✓ Online banking
- ✓ E-Commerce sites
- ✓ Social Networking sites
- ✓ Government organizations

A. Working Mechanism:

The proposed system has two phase registration and login.

The step by step pictorial description of the registration phase is given as:

Figure 1. Signup Page

Signup page of regisration phase has Signup Form, Color Code Selection Form and Geo Authentication Form.During registration the user reqiures to fill his details as Name, Add - ress and Email Address in the Signup Form. Then the user requires to choose any three colors from color code selection form and needs to remember those colors.After Color Code Selection user rquires to enter a place name in the Geo Authentication Form and needs to remember place name. After the completion of filling Signup Page system will generate OTP and send it to user.After OTP verification user details will be store on database and registration will be suceesful. Whole process of registration illustrated in the following pictures:

3.

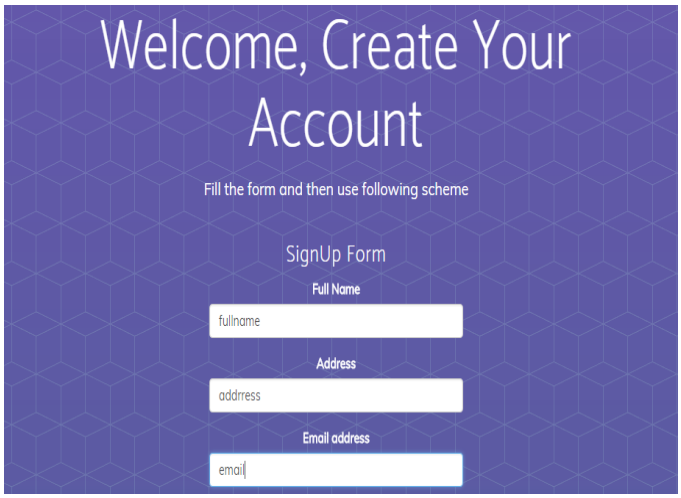

Figure 3. Signup Form

Figure 4. Color Code Selection Form

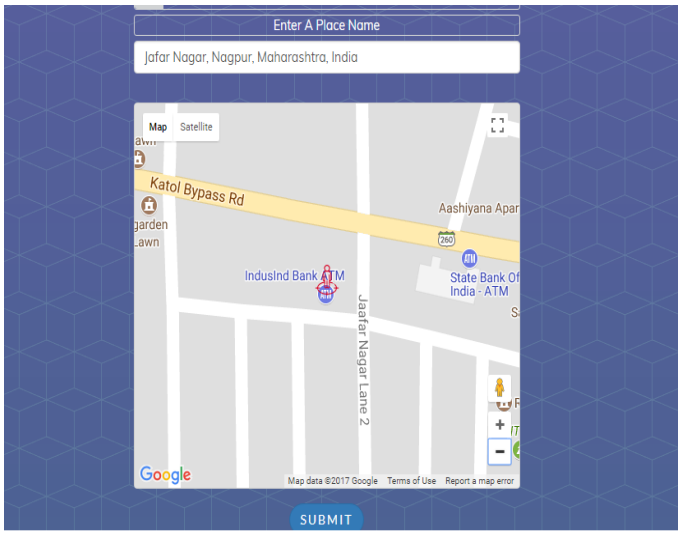

Figure 5. Geo Authentication Form

4. The step by step pictorial description of the Login Phase is given as:

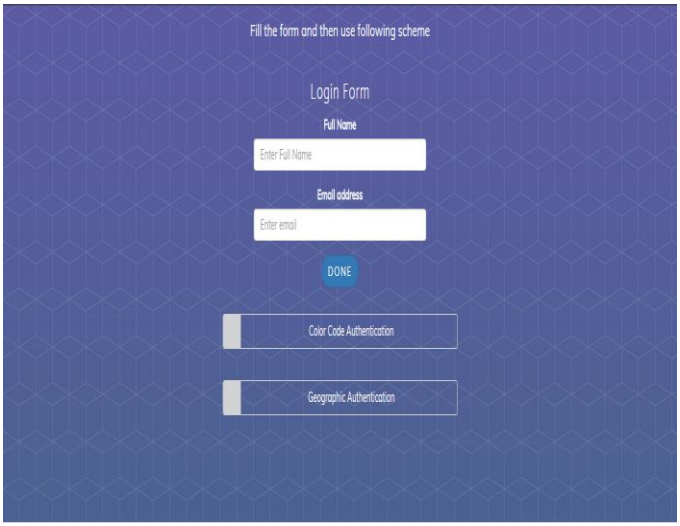

Figure 6. Login Page

During login user needs to enter his name and e-mail address in login form.After entering Name and e-mail system verifies that Name and e-mail is valid or not.If it is valid system proceeds further if not system stops it. In the case of valid Nmme and e-mail user needs to enter Color Code Authentication. When user enter on Color Code Authentication,system will show color grid from which user needes to select those three colors which user has already selected at the time of registration. After color selecion user requires to enter Geographic Authentication, system will show map and user requires to select location which name which he has already entered during registration phase. After the filling of login fom system will check user details from database, if it corrects and match to the database, system will login to the user. In case of incorrect information and information do not match the database system will sotp user login process.It is the overal mechanism of proposed work.

III. CONCLUSION

The proposed work intend to provide a new and more secure graphical password system which will be designed using Java. It intend to combine Color code and geographical based password to provide a robust and more secure graphical password scheme on cloud application. The purposed system will provide a safe guard against Dictionary Attack, Guessing Attack, Shoulder Surfing etc. A banking application will be developed to demonstrate the use of proposed scheme.

IV. FUTURE WORK

As compare to plain text authentication scheme, the proposed scheme is expected to provide more robust and secure mechanism. We will integrate color code and geographical functionality to build this system. This system still needs few updates to provide a complete authentication framework for cloud based application. In future work we can implement fingerprint, face recognition using iris sensor of android smart phone. Currently this scheme is suitable for user authentication only in future we can work in the direction of providing this scheme for payment, ticketing system, and other form of security application where authentication system is needed.

V. REFERENCES

[1]. R. Dhamija, and A. Perrig. -Déjà Vu: A User Study Using Images for Authentication. In 9th USENIX Security Symposium, 2000

[2]. MerinSebastiian, Biju Abraham Narayamparambil, -A New Approach For Instigating Security Using single Zoom Mouse Click Graphical Password International Journal of Communication Network Security ISSN:2231-1882, Volume- 1,Issue-4,2012

[3]. W. Jansen, "Authenticating Mobile Device User through Image Selection," in Data Security, 2004.

[4]. JinhuaQiu, Xiyang Liu, Licheng Ma, Haichang Gao and ZhongjieRen,A Novel Cued-recall Graphical password Scheme, International Conference on Image and Graphics page949-956, Washington,2011

[5]. S.Man, D. Hong, and M.Mathews, "A shouldersurfing resistant graphical password

scheme" in Proceedings of International conference on security and management. LasVergas, NV, 2003 Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, -A New Graphical Password Scheme Resistant to Shoulder-Surfing.

[6]. Mohammad Sarosh Umar, Mohammad QasimRafiq, -A Novel Recognition-based Graphical User Authentication Scheme, International Conference on Signal Processing, Computing and Control (ISPCC), WaknaghatSolan, 2012.

[7]. William Stallings and Lawrie Brown. Computer Security: Principles and Practice. Pearson Education, 2010.

[8]. P. Dunphy, Andreas P. Heiner, and N. Asokan, A Closer Look at Recognition-based Graphical Passwords on Mobile Devices. Symposium on Usable Privacy and Security (SOUPS), Redmond, WA USA, July 14–16, 2010.

[9]. ArashHabibiLashkari, Abdullah Gani, Leila GhasemiSabet and Samaneh Farman, -A new algorithm on Graphical User Authentication (GUA) based on multi-line grids, Scientific Research and Essays Vol. 5 (24), pp. 3865-3875, 18 December, 2010

[10]. A.S. Yeole. -Proposal for novel 3D password for providing authentication in critical web applications, Proceedings of the International Conference & Workshop on Emerging Trends in Technology ICWET '11, ACM New York, NY, USA 2011