"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 , [2, 3]Asst. Professor NCEOT, Nagpur

Abstract: Multimedia Graphical Grid Based Text Password Authentication For Advance User deals with graphical password structure. It is used to increase the reliability of text based 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. This idea can be very useful in banking system.
Keywords: Advance user, security, password, access control, authentication, CSR,JDBC, MySql,, Tomcat Server, Bootstrap Template, Eclipse, JDK, Servlet.

I.   INTRODUCTION

Authentication system play an important role in every application. Its allow 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 serverand 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.

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 illustrate that CBFG has better performance in usability, 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].

III.   LIMITATIONS 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.

A.   Disadvantages
1)   It is easy to hack or guess.
2)   It is found that users are not selecting and handling
        text based passwords in insecure manner
3)   Humans can only memorize very few passwords due to this fact Users are writing down, share or Use the same passwords for many accounts.
4)   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.

IV.   PROPOSED WORK

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

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.

V. SYSTEM CONFIGURATION

A. Hardware Requirement

Minimum hardware requirement of the proposed is a PC with the following specification:

1) Processor   -   Pentium –Dual Core
2) Speed   -   1.1 Ghz
3) RAM   -   1 GB(min)
4) Hard Disk   - 20 GB Free Space
5) Key Board   - Standard Windows Keyboard
6) Mouse   -   Two or Three Button Mouse
7) Monitor   -   12inch lcd Monitor

B. Software Requirement

1) Operating System   : Windows95/98/2000/XP
2) Front End   : Java Swing
3) Backend   : MySQL
4) IDE   : Eclipse Kepler

VI. IMPLEMENTATION

The system will be implemented using J2EE, it will use servlet to handle the client side request. To demonstrate the use of proposed system will implement a banking application which use the proposed authentication system. Overall functionality will be develop using java and jdbcapi for database, in it MySQL database is use. The application will be provide color code and geographical authentication scheme. The UI of application will be developed using bootstrap and jquery. The access control system will be provide a Challenge Response System.

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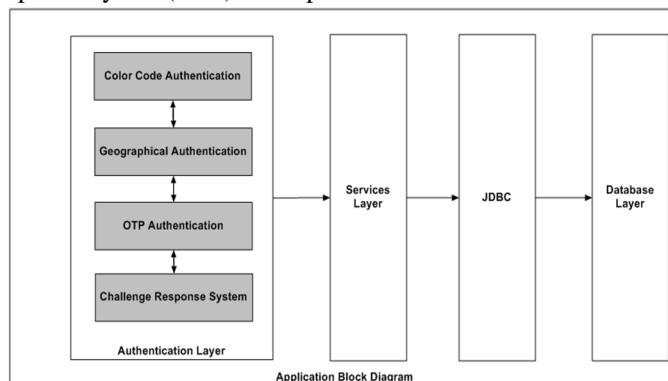
Text based password are susceptible to dictionary attack, shoulder surfing, eavesdropping. To overcome some of these problems pictographic password will be introduced. This paper propose a pictographic based authentication Scheme which includes Color Code Authentication Scheme Geographic Authentication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

A. Modules

In the proposed system following modules will be implemented:

B. Web Application

It's basically a banking ebsite, it consist Color Code Authentication Scheme(CCA) ,Geographic Authentication Scheme ,OTP(One Time Password) and Challenge Response System(CRS) for implementation.

Color Code Authentication:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

1) This will handle the color gird functionality and service.
2) We will implement a service to get & save the gird colors.
3) Here we will implement methods to retrieve colors codes from database at runtime.
4) The CCA provide service end point interface to call from javascript.
5) The CCA get the response of login authentication from CRS module.
6) We use java servlet for creating service.

C. Geographic Authentication
1) This layer will handle the google map functionality and service.
2) In this layer we will provided methods to retrieve latitude and longitude from user pin location.
3) We implement this module using both javascript and java.
4) In javascript we use to display the map and to get the latitude and longitude.
5) On java side we use it service to save this latitude and longitude. At the timeof login & registration.

D. Challenge Response System (CRS)
1) In CRS module layer user has to register the responses with the system and then system will give a challenge to the user for which only user has to answer.
2) This module handle CCA module request and GAS module request for login and registration.
3) The both CCA and GAS module will provide to input to CRS module and CRS give its response to CCA and GAS for login action and registration action.
4) This module will have separate methods for CCA request and GAS module request
5) This module connected with JDBC to access the database.
6) This module act as a middle layer between JDBC and CCA,GAS module.

In this work instead images ,colors elements and geographical map will be provided.

System will show a random grid where user click on the colors shades and there will also show 3 color shades White, Gray and Black.

These random sequence of shades need to be memorized by the user. It is required at the time of login. If User failed to provide correct sequence it will not be authenticated.

VII.   ALGORITHM &FLOWCHARTS

A. The Proposed Work Use Aes Algorithm
The Advanced Encryption Standard, or AES, is a symmetric block cipher chosen by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key   search attack. Triple DES was designed to overcome this drawback but it was found slow.

B. The Features Of Aes Are As Follows
symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, Stronger and faster than Triple-DES, Provide full specification and design details,

Software implementable in C and Java. In the proposed work Application Flowchart consist two flowcharts

One is for user registration and another for user login. Both are shown below, figure 1 and figure 2 consist registration and login flowchart .Registration flowchart describes mechanism of user registration and login flowchart describes whole mechanism of user login.
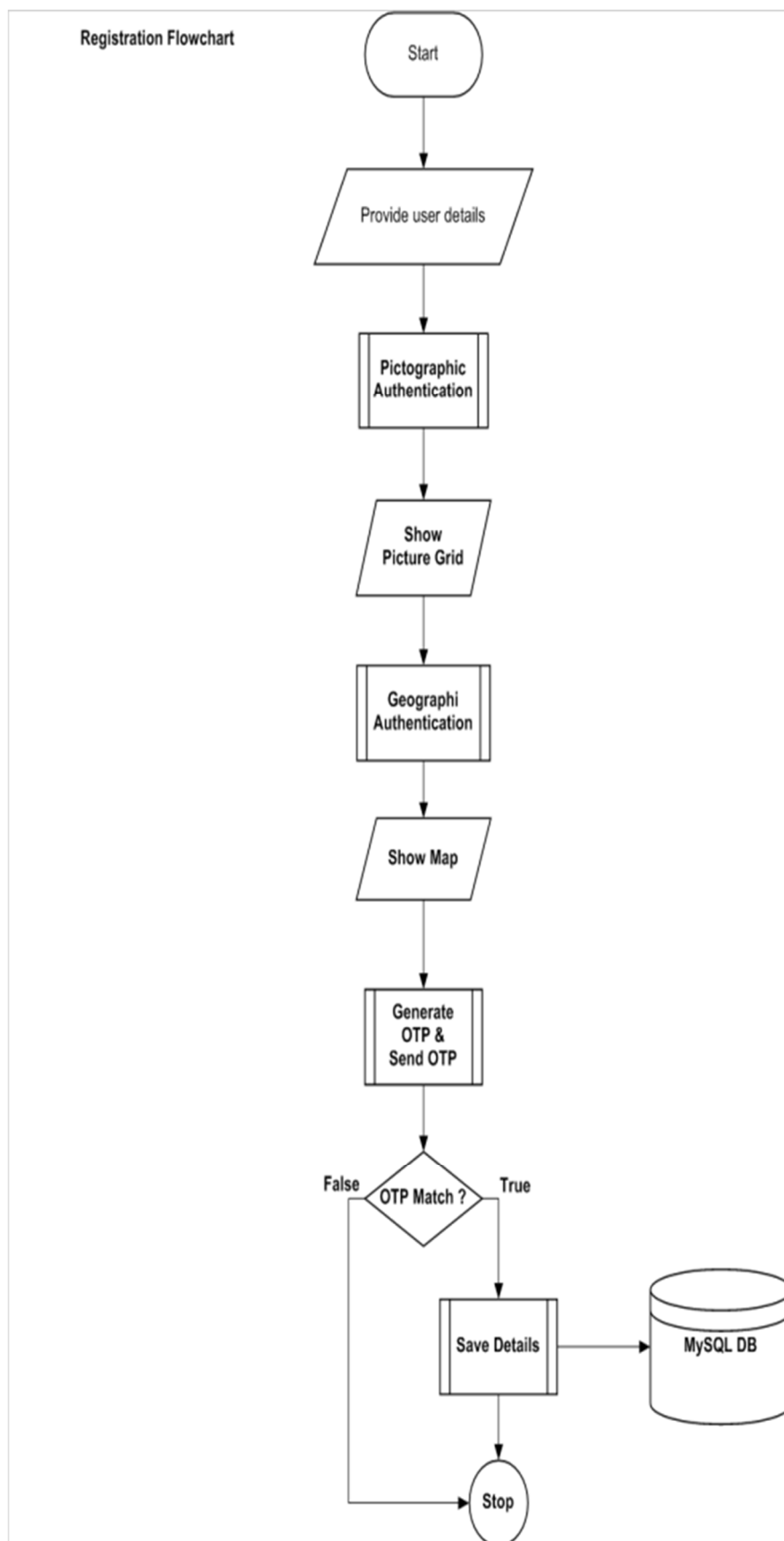
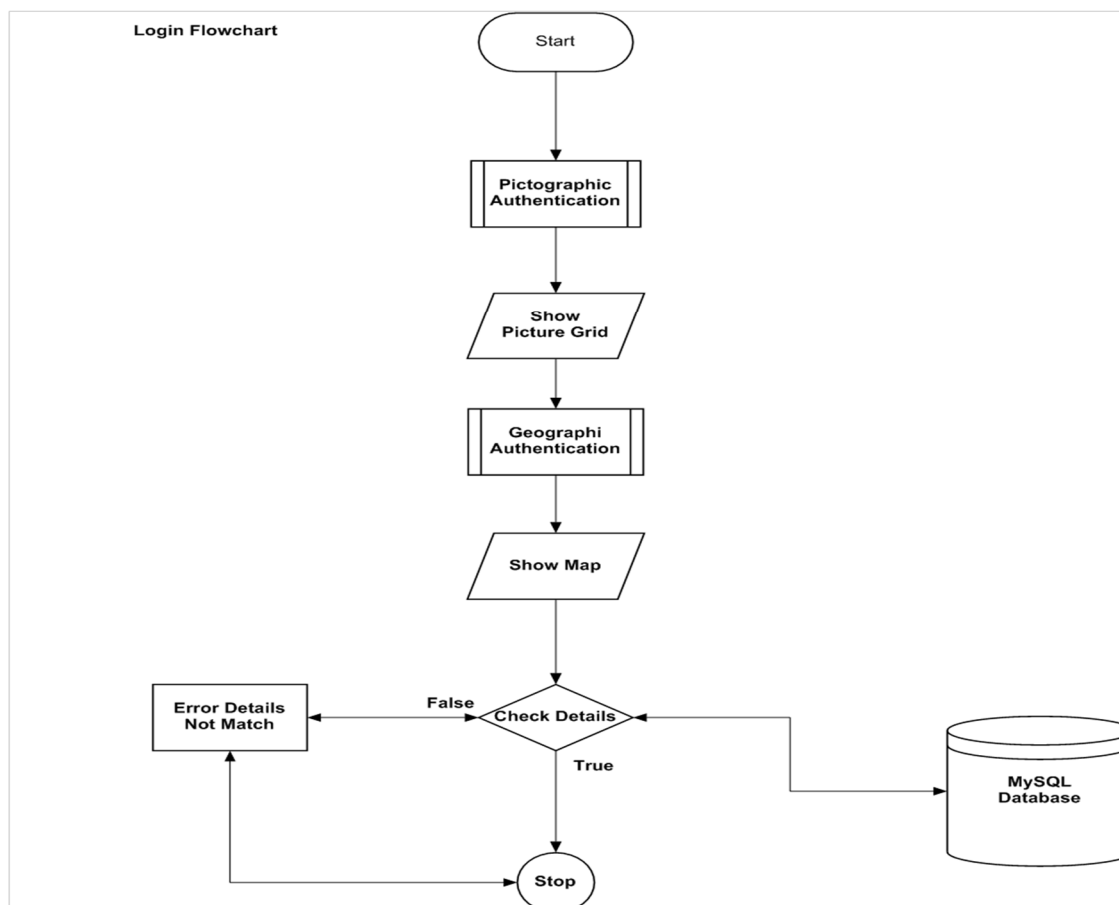Fig1: Registration flowchart

Fig2: Login Flowchart

VIII. 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.

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.

INTERNATIONAL JOURNAL
FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 ⊘ (24*7 Support on Whatsapp)