Image Pin Entry With Shoulder Surfing

[1]Mahesha L S, [2]Zareena Taj, [3]Mahendra R S
[1]Senior Scale Lecturer, [2]Senior Scale Lecturer, [3]Senior Scale Lecturer
[1]Computer Science and Engineering, [2]Computer Science and Engineering, [3]Computer Science and Engineering,
[1]Govt. Polytechnic, Mirle-571603, [2]DACG Govt. Polytechnic, Chikkamagalur-577101, [3]Govt. Polytechnic, Holenarasipura-573211

Abstract : Authentication oriented access to the applications is enormously used for computer privacy and security. Although humans are prone to plump for the fragile password which are easy to remember like date of birth, their phone number dearest person name and many more. instead of using combination of alphabets, Numerals and special characters strings but human tend to use short password which are easy for them to remember. With internet programs and cell apps piling up, human can access these application anytime and anywhere with various devices. The evolution brings outstanding comfort. However additionally will increase the opportunity of revealing passwords to shoulder surfing assaults. Attackers can oversee directly or use extraneous recording gadgets to accumulate customers credentials. To triumph over this problem, we proposed a unique authentication system pass matrix primarily based on graphical passwords to face up to shoulder surfing assaults. With one time legitimate login indicator and circulative horizontal and vertical bars overlaying the whole scope of pass pictures. Even though if the attackers do multiple camera based attacks. Pass matrix does not give a small clue for attackers to estimate and find out the password.

Keywords: Authentication, Graphical Password, Graphical Pin Entry System, Shoulder Surfing Attacks.

I. INTRODUCTION

Graphical password authentication schemes have been advanced to cope with the issues and weaknesses related to textual passwords. Based on a few research humans have great memory for remembering the pictures for long-time period rather than verbal representations. Image oriented passwords have been proved to be simpler to retain in numerous user research. As a result, customers can compose a complicated authentication password and are efficient of recollecting it after a long term although the reminiscence isn't activated periodically. However, maximum of those image-oriented passwords are susceptible to shoulder browsing assaults (SSAs). This form of assault uses direct observation, likely looking over someone's shoulder or applies video taking approaches to get passwords, PINs, or other liable personal credentials. We have also implemented a Pass Matrix prototype on android and accomplished real user experiments to evaluate its memorability and usability. From the experimental results, The proposed system achieves better resistance to shoulder surfing attacks while maintaining usability.

II. LITERATURE SURVEY

Graphical password authentication using colour login technique is proposed to secure every user account from external threats, These traditional passwords are engaged to the most common and easiest attack which is shoulder surfing attack. Thus biometrics & graphical passwords are utilized to defeat these issues related with the traditional authorization technique of alphanumeric password method. this assures safety of users account & data.[6].This technique is proposed in order to make the login system easy and efficient this scheme clears the resistance of the proposed technique to shoulder surfing and accidental login there by examining its security and usability. The main theme or goal of this method is supporting the users in selecting passwords of higher security and this is the main objective of knowledge-based authentication system. It uses interactive GUI to provide secure login to the user so attacker can't hack or collect the information of users.[8].This application provide a personal storage for children to store their notes in soft copy forms. Nowadays using hand written notes is rare almost all users use soft copy notes than printed notes. For those this method is best mainly for children because children are unable to remember the password. This technique helps children to remember the password and it also helps them in future because they would make a sense to protect privacy by setting up passwords[9].This password schema promises the user for better robustness and memorability and also it provides a more effective graphical image pattern password. This method overcomes the concrete analysis against common attacks such as phishing attacks,

SQL Injection etc. These XML schema represent the graphical image. It gives reliability and robustness against various aspects.[10]

III. PROPOSED SYSTEM

In the proposed model to overcome the security weakness of the traditional PIN method, the easiness of obtaining passwords by observers in public, the compatibility issues to devices. We introduced a graphical authentication system called PassMatrix. In PassMatrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images (i.e., n) is user-defined. In PassMatrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the PassPoints scheme.

IV. RESEARCH METHODOLOGY

In the methodology we have mainly two steps, user registration, user login process, Hash code generation and admin.

USER REGISTRATION

In the user registration, the user should go under the registration process by giving some information; three images will be shown to the user, in those images user has to select some given random squares of the images as the graphical password. The details of selected random squares of all images will be stored in the database with respect to the user.

HASH CODE GENERATION

After setting successfully the same images, the given data and details will be stored in the database, we should join all the three images should be same for the generation of the hash code, for that and store in the database with respect to the users.

USER LOGIN PROCESS

Only registered user can able to login by using his/her user id and password; The user id and password will be valid through OTP will be sent to the user's e-mail, the OTP contains the random pair of vertical and horizontal slider same points of all the three images. After successful login, three assigned images will be displayed to the user with horizontal and vertical sliders; user has to set the horizontal and vertical sliders for all the three images, where the OTP coordinate value should be equal to the coordinates chosen by the user at the time of password setting. The hash code will be generated for all OTP coordinates by concatenating. If the hash code is matched with the existing hash code user can successfully enter into the home page, else, the process will ends and login page will be displayed.

ADMIN

Admin has to login to his account by the registered user name and password. Admin can view all the users' details that are successfully registered.

SYSTEM REQUIREMENTS

The hardware and software requirements are very minimal and the software can run on most of the machine even of the past. Here we have used the system of below specification to develop. To be used efficiently, all computer software needs certain hardware components or other software resources to be present on a computer. These prerequisites are known as (computer) system requirements and are often used as a guideline as opposed to an absolute rule. Most software defines two sets of system requirements: minimum and recommended. With increasing demand for higher processing power and resources in newer versions of software, system requirements tend to increase over time.

Hardware Requirements

System : Pentium IV 2.4 GHz.
Hard Disk : 500 GB.
Ram : 4 GB
Any desktop / Laptop system with above configuration or higher level

Software Requirements

Operating system : Windows 10
Coding Language : Java (Jdk 1.7)
Web Technology : Servlet, JSP
Web Server : TomCAT 7.0
IDE : Eclipse Galileo
Database : My-SQL 5.0

UGI for DB : SQLyog
JDBC Connection : Type 4 - Native Drive

V. SYSTEM DESIGN

In the existing system, the user's activities such as typing from their keyboard or clicking on the pass-images or pass-points in public areas can exposes their passwords to people with bad intention. Existing system is not safe for shoulder surfing attacks. We introduced a graphical authentication system called Pass-Matrix. In Pass-Metrics, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images is user-defined. In Pass-Matrix, users choose one square per image for a sequence of n images rather than n squares in one image as that in the Pass-Points scheme. In the system analysis, we have the proposed system and the existing system, in that we have some advantages and the disadvantages. Some applications for this; they are, social media, web applications, Gmail Accounts, job portals, etc...

A. System Architecture

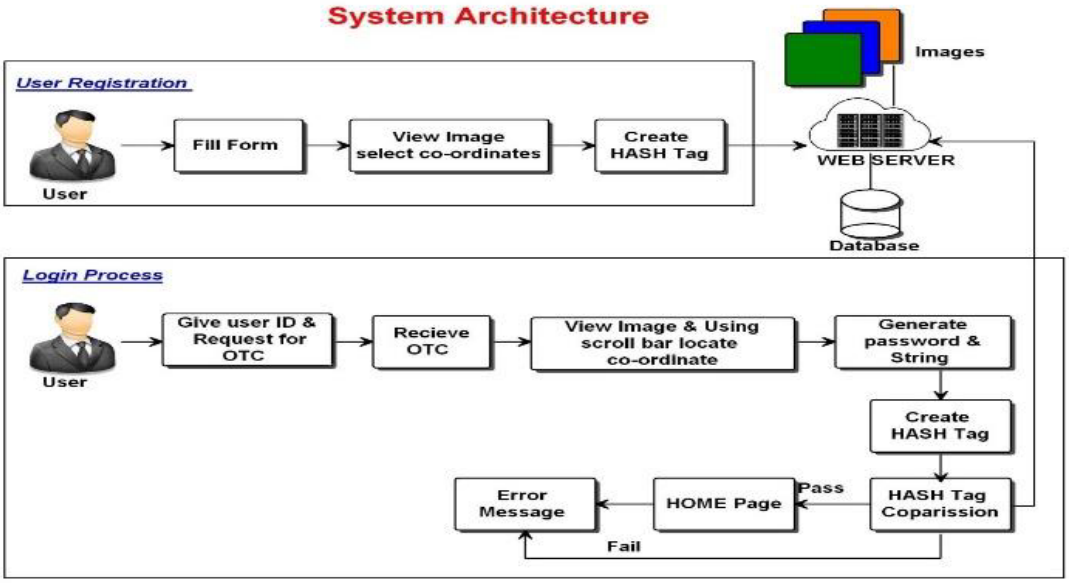

Figure 1: Block Diagram

B. Data flow Diagram

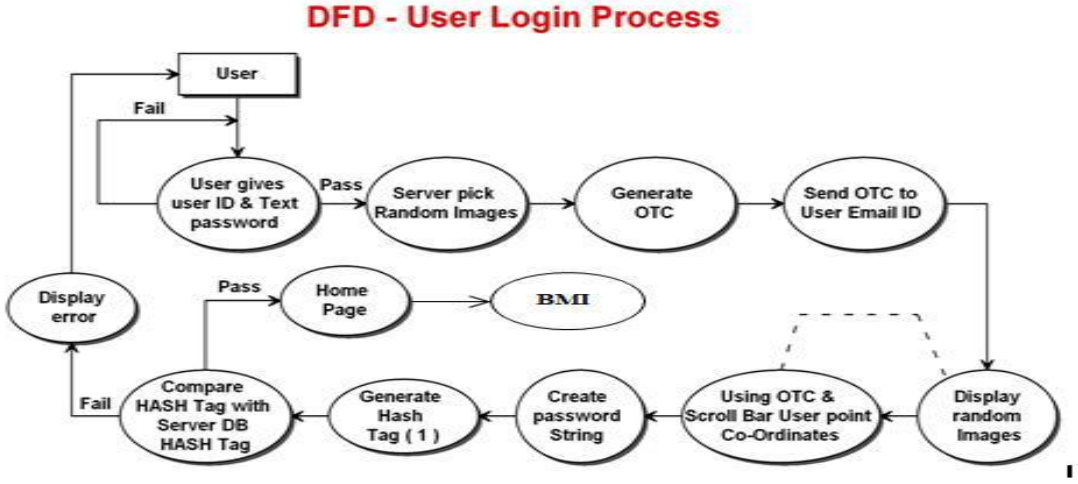

Figure 2: User Login Process

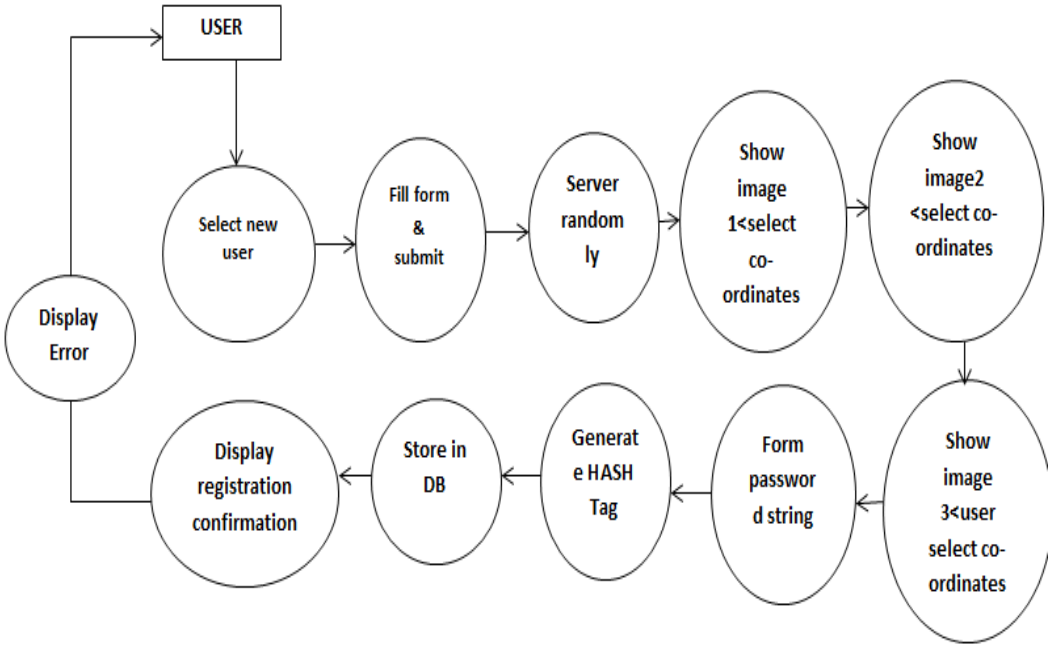

Figure 3: User Registration Process

VI. RESULTS

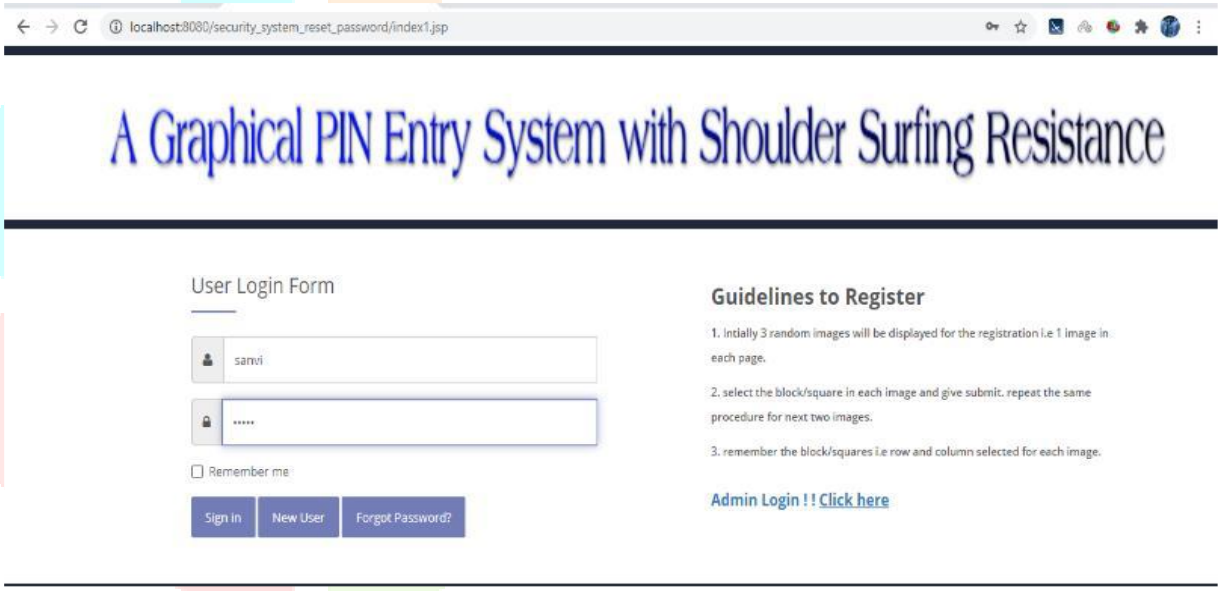

Figure 4: User Login Form

This the user login page, The user is able to login by giving the required information.

Figure 5: Image 1 for selecting the coordinates

This is image 1 for selecting the coordinates, similarly two more images will appear to select the coordinates.

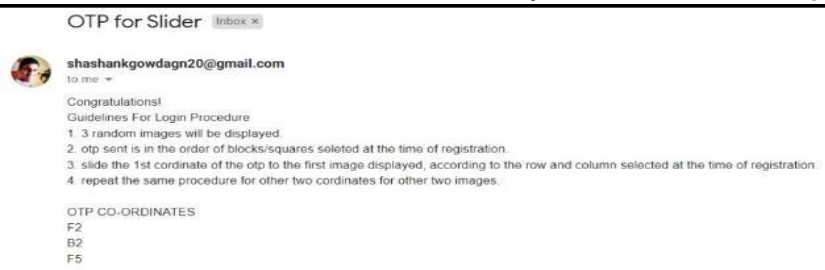

Figure 6: OTP sent to the user

When the user login by giving the information, A mail is sent to the user which contains the OTP.

Figure 7: Image for matching the coordinates

The user after receiving the OTP the user must rearrange the coordinates in order to login.

VII. CONCLUSION

To overcome the security weakness of the traditional PIN method, it is very easy to get the passwords by observers in public areas. We introduced a graphical authentication system called Pass Matrix. In Pass Matrix, a password consists of only one pass-square per pass-image for a sequence of n images. The number of images is user-defined. In Pass Matrix, users should choose one square or one image for a sequence of n images rather than n squares in one image as that in the Pass Points scheme. A novel authentication system Pass Matrix, based on graphical passwords to protect shoulder surfing attacks. In future we can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many authentication system but they have their own advantages and disadvantages.

VIII. REFERENCES

[1] Bhumika Patel, Amaan Sarwar, Prof. Sachin Chavan, “Graphical password authentication using color login technique”, published in the year 2016.

[2] Khaja Mizbahuddin Quadry, “Design, Analysis, and Implementation of a two factor authentication scheme using graphical password”, published in the year 2015.

[3] Neerukonda Jitendra, “Text-Based shoulder surfing and key logger resistant graphical password”, published in the year 2018.

[4] Muhammad Ilyas, “Wheel Authentication based Multi-level Scalable Color-Textual Graphical Password System”, published in the year 2014.

[5] Sarhad Baez Hasan, “Graphical Based Authentication System by Picture Based Password”, published in the year 2016.

[6] Baez Hasan, “Graphical Based Authentication System by Picture Based Password”, published in the year 2010.

[7] Ankitha Vaddet, “Graphical passwords, behind the attainment of goals”, published in the year 2020.

[8] Mrs. Aakansha S. Gokhale, “The shoulder surfing resistant graphical password authentication technique”, published in the year 2012.

[9] Manasi Shah, Radhika Naik, Sheetal Mullakodi, Sangita Choudhari, “Comparitive analysis of different graphical password techniques for security”, published in the year 2018.

[10] Tay Yi Yang, Palaniappan Shamala, Muruga Chinniah, Cik Feresa Mohd Foozy, “Graphical password authentication for child personal storage application”, published in the year 2018.