Graphical Authentication System to Prevent the Shoulder Surfing

In today’s world authentication plays a vital role. The most common approach used for authentication is textual password. There are various limitations for textual passwords, they are exposed to shoulder surfing attack however strong textual passwords are tough to memorize. Shoulder surfing attack is not the common attack used around the world. But it is also one of the dangerous attacks. This attack does not need any technical skill for finding the password of the user. In this, the attacker will see the password while it is entering from the behind. So, we use a new technique for securing the password from the attackers. So as an alternative Graphical Passwords are introduced to resist the Shoulder surfing attack. Looking at the success of this system, using graphical password as input and grid lines for image point verification and enrich it to provide security using normal login and graphical password. This system can be used in the field such as banking application, military application, civilians, forensic labs, etc. This paper gives a new scheme for graphical password that uses images that are unexplainable and have larger password space.

Keywords: Authentication, Graphical Password, Shoulder Surfing Attack.

I. INTRODUCTION:

In current state it is very important to secure system. Where the need of authentication is required for high security, there are various methods to provide authentication like password authentication but this type of authentication cannot provide in the fields like banking application, military, forensic labs, etc. The most widely adopted technique in authentication is Textual passwords are hard to memorize and recollect. Textual passwords are attacked by Masquerading, Eavesdropping, Dictionary attack, Shoulder surfing attack etc...To overcome this drawback graphical passwords were introduced. It is recognized that humans can remember images for long duration than textual representation. Using graphical password user is able to set up a complex authentication password and is able to recollect it, even if the memory is not activated periodically. Authentication is topic of the information security which deals with the protection of the user’s privacy. It is a process which gives permission to allowed the user in particular system. Authentication techniques are categorized as Token based authentication, Biometric based authentication, knowledge based authentication. In the shoulder surfing attack the attacker watches the key strokes of the user while he is entering the password. This is done by the attacker from the behind the shoulder. So, this attack is named as shoulder surfing attack. The human actions such as choosing bad passwords for new accounts and inputting passwords in an insecure way for later logins are observed as the weakest link in the authentication chain. Therefore, an authentication strategy should be perform to overcome these vulnerabilities. To overcome this problem, we proposed an innovative authentication system Pass Matrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time accurate login signal and spread straight and perpendicular bars covering the entire scope of pass-images, Pass Matrix offers no hint for attackers to figure out or narrow down the password even they plan multiple camera-based attacks. But this System does not resist the shoulder surfing attack and also vulnerable to smudge attack. The simple shoulder surfing attack graphics is shown in fig.

Figure 1. Shoulder Surfing Assault

Users may have various login ids that will be hard to remember their password. Users may forget password that do not use frequently. Most users choose easy passwords so they can remember them. Use of easy passwords increases the probability of guessing. Complex passwords will be forgotten easily. Choosing same passwords for different accounts or writing down the passwords endangers the security of passwords. Alphanumeric or text-based passwords are also difficult to remember. One solution is to use graphical passwords that are more secure than alphanumeric password. Graphical passwords are more secure against brute force attacks, dictionary attacks and social engineering attacks. This paper presents a new scheme for graphical password that is resistant to shoulder-surfing attacks.

II. LITERATURE REVIEW:

Due to the rapid development of new technologies, a secured password has become indispensable to secure the information for users. Conventional password scheme is a widely used authentication technique where users log into the computer
system using the usernames and passwords. The system authenticates users via user database and grants access to the system on the basis of authentication. This technique is useful in protecting user data as it allows only an authenticated user to access the system. However, this scheme is vulnerable to various types of attacks including shoulder-surfing attacks, key loggers, brute force attack, dictionary attack, spyware, eves dropping etc. One of the conventional password schemes is a textual password \[1\]. Users usually prefer short and simple passwords that are easy to recall. This makes it more insecure and susceptible to attack. Using a long and random password is secured but it is an unfeasible approach as users need to remember longer and complex password characters. Graphical Password scheme has been proposed to address the problem. Graphical passwords are easy to recall and recognize. Considering the fact that graphics are easy to remember and that humans are the weakest bond in any authentication mechanism this scheme can deliver a decent bargain between usability and security. Nonetheless, shoulder surfing risk is becoming more serious in such graphical passwords because of the visual interface. An intruder can easily capture graphical passwords through direct human observations or video surveillance. Shoulder-surfing is a known risk where an intruder observes or records the authentication session, thereby capturing the password \[2\]. In order to mitigate shoulder-surfing risk found in graphical password scheme, many approaches have been proposed. However, they still hold disadvantages in term of substantial usability, generally in time and effort to log in, making them less suitable for everyday authentication. Also, many of the schemes are traceable and can be exposed on continuous observations. Due to these substantial usability disadvantages, there is a strong need to propose an extended version of the authentication solution which can address the issue for everyday authentication purpose \[3\]. The alternative for the alphanumeric password the best innovation is graphical password in that user given challenge to access them by click on images instead of type alphanumeric password. Alphanumeric password is lengthy password hence hard to memorized instead of graphical password is easy to memorized and easy to use as compare with alphanumeric password. As psychological experimental and evidently proved that human brains are friendlier with easy to remember images or video instead of alphanumeric password in a random fashion. In alphanumeric password need to arrange proper then memorized password which is tedious. In Graphical password using images and pictures is provide more secure constrain to the password as using text and numbers \[4\]. In graphical based password authentication Pass Point, Cued Click Points techniques are used. In Pass Point Graphical password scheme consist of four different click points on given image. To generate password user selects on any pixel in the image. The only limitation is that the user can easily guess the password because pattern formation takes place as a secret code for remembrance so the attacks are easily possible. Cued Click Points uses one click point on three different images in sequence instead of four click points on one image. The next image will be demonstrated on the basis of previously selected point. This method reduces pattern realization attack \[4\].

### III. PROPOSED SYSTEM

There are many attacks taking place regarding the authentication process of the existing system. So we come up with the new authentication system which includes cued click point algorithm to resist shoulder surfing attack based on image password selected by user from image grid and image point is stored in the form of rows and columns as password.

### IV. PASSMATRIX

To conquered the security weakness of the traditional PIN method, the easiness of obtaining passwords by observers in public, and the compatibility issues to devices, we introduced a graphical authentication system called PassMatrix. In PassMatrix, a password rest of only one pass-square per pass-image for a arrangement of n images. The number of images (i.e., n) is user-defined. In Pass Matrix, users choose one pass-image for a arrangement of n images rather than n squares in one image as that in the PassPoints scheme. Based on the user study of Cued Click Points (CCP), the CCP method does a good job in helping users recollect and remember their passwords. If the user clicks on a faulty region within the image, a different image will be shown to give the user a threatening feedback. However, aiming at alleviating shoulder surfing attacks, we do not recommend this approach since the feedback that is given to users might also be obtained by attackers. PassMatrix’s authentication consists of a registration phase and an authentication phase as described below:

#### Registration phase

At this stage, the user creates an account which contains a username and a password. The password consists of only one pass-square per image for a arrangement of n images. The number of images (i.e., n) is resolved by the user after considering the trade-off between security and usability of the system. The only purpose of the username is to give the customer an imagination of having a personal account. The username can be omitted if PassMatrix is applied to authentication systems like screen lock. The user can either adopt images from a provided list or upload images from their device as pass-images. Then the user will pick a pass square for each selected pass-image from the grid, which was divided by the image discretization module. The user repeats this step until the password is set.

#### Authentication phase

At this stage, the user uses his/her username, password and login indicators to log into Pass Matrix. The following describes all the steps in detail:

1) The user inputs his/her username which was generated in the registration phase.
2) A new indicator involves a letter and a number is created by the login indicator generator module. The indicator will be shown when the user uses his/her hand to form a circle and then tap the screen. In this case, the indicator is transmitted to the user by visual feedback. The indicator can also be expressed through a predefined image or by audio feedback.

3) Next, the first pass-image will be shown on the display, with a straight bar and a perpendicular bar on its top and left respectively. To respond to the challenge, the user shot or drags the bars to align the pre-selected pass-square of the image with the login indicator.

4) Repeat step 2 and step 3 for each pre-selected pass image.

5) The transmission module gets user account information from the server.

6) Finally, for each image, the password substantiation module verifies the alignment between the pass square and the login indicator. Only if all the alignments are correct in all images, the user is allowed to log into PassMatrix.

V. TECHNIQUES USED:

User authentication is an essential component in computer security context. There are various techniques used for authenticating the user. Such as recognition based authentication, recall based authentication, pure recall based authentication. Most common method for authentication is alphanumeric password authentication. In which sequence of alphabet and numbers used as password. It is simple and easy to use but susceptible to various attacks such as dictionary attack, brute force attack etc., to overcome these drawback Graphical password were introduced. Graphical passwords are easy to memorize by user and also resistant to dictionary attack, brute force attack, etc. some authentication technique are discuss below.

- PassPoint is a technique in which only one image is selected during the registration. From that image, appropriate part of image or cue of image are selected as the password. User can select multiple cues randomly from the image but user should memorize the sequence of cued entered at the time of registration. During the login time preselected image will appear on the screen. User has to enter the preselected cued of images in the same order as they selected during registration. As human mind can memorize images better than text so this method is easy to remember. But this method suffers shoulder surfing attack.

- CCP refers to Cued Click Point is authentication technique coming from passpoint. In which during the enrollment certain number of images are selected in the particular order. From each image only one cued click point will be selected. During the login time first image will appear on the screen, user has to identify the correct cued and should select as password. If the preferred cued is correct then it will open the next image. same procedure is applied for all the images. But if any one image cued is wrong then it will not display the next image. This method is easy to memorize by the user and unbreakable. But this method undergoes shoulder surfing attack.

- Security Aspect in Authentication Technique

- Dictionary Attack

This attack is a assumption type of attack. in which attacker has a list of string contain likely words or letter combinations. By using this combinations attacker try to guess the password.

- Brute Force Attack

It consists of regularly checking all possible keys or passwords until the correct one is found. In the worst case, this would involve traversing the unified search space.

- Guessing

Attacker can guess the password by trying the personal information of the user.

- Shoulder Surfing Attack

In Shoulder surfing attack, attacker can detect password directly or trap password using any device. It is most commonly occurring attack.

VI. IMPLEMENTATION

- Registration

- Text Based Registration

At this stage user creates an account using required credential. However this acts as the first stage of registration of the system.

- CCP Registration

After the first phase, user needs to login using user name and password.CCP registration needs to be done where user is asked to select number of images and splits. User needs to select images from the set of images. The user needs to select one point from each image for CCP registration. This point will be recorded in the database of the system. After that the user will have to wait for the approval/rejection from admin.

- Login

- Normal Login

After registration process, user needs to provide simple login details such as user id followed by password. User is directed to graphical login window.

- Graphical Login

Authorized user will select one click point per image. Each point selection will display another image associated with the address of click point.

VII. CONCLUSION:

Security is most essential factor for any system authentication. Firstly pass point method is proposed but due to all click point on the same image minimize the security of system. To conquered this problem, we proposed a shoulder surfing resistant authentication system based on graphical passwords. In CCP technique more images with separate click point on it is used. Authentication is required to provide the better security to the user. Textual password authentication is well known authentication technique. it is simple and easy but vulnerable to various attacks. Later graphical password is invented. This is simple and easy to memorize to the user. But undergo various problem such as, it require greater storage space, some are complex and time consuming. A session authentication technique which may help to reduce the shoulder surfing attack. The paper provides a good solution for the shoulder surfing attack and also it makes the better way to prevent the shoulder surfing attacks in every place where the authentication is required.

VIII. REFERENCES:


