Integration of Sound Signature In Graphical Password Authentication System

Mr. Prakash Kumar M[1], Ms. Anushree C S[2], Ms. Divya Priya S[3], Ms. Ishwarya V[4], Ms. Santhiya S[5]
[1, 2] Dept of Computer Science and Engineering
[3]Guide & Assistant Professor, Dept of Computer Science and Engineering
[4, 5]Dept of Information Technology
[1, 2, 3, 4, 5] Narasu's Sarathy Institute of Technology, Tamilnadu, India

Abstract- *With the increasing capabilities of good devices, keeping them secure has become a significant concern. To mitigate that concern, over the previous few years, many new categories of authentication schemes are projected. Graphical Authentication (GA) is one in all those categories and is that the focus of this project. The GA schemes area unit additional in style and preferred for good devices thanks to their heavily graphics-oriented nature, higher memorability over text-based schemes, and no further hardware demand. However, most of those GA schemes area unit unable to resist many outstanding attacks, particularly shoulder aquatics, smudge, and brute force. Therefore, during this paper, a replacement hybrid authentication theme is projected that seamlessly integrates 2 freelance however in style authentication schemes Pass points and Press bit Code or PTC. The aim of this new theme is to make sure the next level of security by resisting those outstanding attacks. The projected theme is enforced on the humanoid package and is tested on Huawei P9 and device, a pressure sensitivity screen enabled device, that is obligatory for the PTC theme. The performance of the projected technique is evaluated for security, practicality, and value. Once it's compared with different similar schemes, it outperforms the present schemes*

Keywords- Authentication Schemes, Graphical Authentication Scheme, Pass Points, Press Touch Code.

I. INTRODUCTION

In this project, the authentication or security is provided by means of the image processing. Here the users are registered and their passwords are generated with the help of axis co-ordination in the picture. The values of x and y axis are combined to generate a password for the user. If the user forgets his axis (password) another option of sound file is given for recalling the password. The matching process is done with the help of the Hash Visualization Algorithm.

Passwords are used for :-

a. Authentication (Establishes that the user is who they say they are)
b. Authorization (The process used to decide if the authenticated person is allowed to access specific information or functions) and
c. Access Control (Restriction of access-includes authentication & authorization).

Mostly user select password that is predictable. This happens with both graphical and text based passwords. Users tend to choose memorable password, unfortunately it means that the passwords tend to follow predictable patterns that are easier for attackers to guess. While the predictability problem can be solved by disallowing user choice and assigning passwords to users, this usually leads to usability issues since users cannot easily remember such random passwords. Numbers of graphical password systems have been developed; Study shows that a text-based password suffers with both security and usability problems. According to a recent news article, a security team at a company ran a network password cracker and within 30 seconds and they identified about 80% of the passwords .It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic.

II. LITERATURE SURVEY

D. Gibson, "Understanding the Three Factors of Authentication,"

Authentication is the first step in access control, and there are three common factors used for authentication: something you know, something you have, and something you are. This article provides you with good understanding of the three factors of authentication and how they can be used together with multifactor authentication.

S. Azad, M. Rahman, M. S. A. N. Ranak, B. M. F. K. Ruhee, N. N. Nisa, N. Kabir et al., "Vap code : A secure graphical password for smart devices,"

In parallel to the increasing purchase rate of the smart devices, attacks on these devices are also increasing in an alarming rate. To prevent these attacks, many password-based authentication schemes are proposed. Among them, graphical password schemes are preferred on these devices due to their limited screen size and a lack of full sized keyboard. Again, existing graphical password schemes are susceptible to various attacks, among which shoulder surfing, smudge attack, and brute force attack are the most prominent. Hence, in this paper, we propose *Vibration-And-Pattern (VAP)* code, a new graphical password scheme that is resilient against these three major attacks. To evaluate the usability of our proposed scheme, a usability study has been conducted on 122 participants of various age groups from different demographics.

S. Kostromina and D. Gnedykh, "Students' psychological characteristics as factor of effective acquisition of visual information in e-learning,"

This article is motivated by the fact that teachers choose a form of visualization basing on their subjective views on the ways to make multimedia presentation or on the existing standards, not taking into account that effective acquisition of visual information equally depends on psychological characteristics of students. The main purpose of this research is to identify psychological characteristics assisting students' effective acquisition of information presented in different visual forms (text, charts, comics) in e-learning. The methods used included, firstly, experiment in an educational setting, secondly, control tasks created on the basis of Bloom's taxonomy, and, finally, psycho diagnostic techniques studying: cognitive and met cognitive skills, learning motivation, and self-organization. The findings allow us to identify which forms of electronic visual information are more suitable for students of certain psychological types. These results can help teachers to create conditions for students' more effective absorption of visual information by taking into account their psychological characteristics.

O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical user authentication system resistant to shoulder surfing attack,"

User authentication is one of the most significant issues in the field of Information Security. The most common and convenient authentication method used is the alphanumeric password which has significant drawbacks. To overcome the vulnerabilities of traditional methods, graphical password schemes have been developed as possible alternative solutions to text-based scheme. A potential drawback of graphical password schemes is that they are more vulnerable to shoulder surfing than conventional alphanumeric text passwords due to their visual interface. To overcome the shortcoming of existing graphical password schemes this project focuses on developing a graphical authentication system that is resistant to shoulder surfing attack.

III. EXISTING METHOD

A user clicks on several previously chosen locations in a single image to log in. The user chooses several predefined regions in an image as his or her password. To log in the user has to click on the same regions. The problem with this scheme is that the number of predefined regions is small. Another problem of this system is the need for the predefined regions to be readily identifiable. In effect, this requires artificial, cartoon-like images rather than complex, real-world scenes. Cued Click Points (CCP) is a proposed alternative to Pass Points. In CCP, users click one point on each of 5 images rather than on five points on one image. It offers cued-recall and introduces visual cues that instantly alert valid users if they have made a mistake when entering their latest click-point (at which point they can cancel their attempt and retry from the beginning). It also makes attacks based on hotspot analysis more challenging. Each click results in showing a next-image, in effect leading users down a "path" as they click on their sequence of points. A wrong click leads down an incorrect path, with an explicit indication of authentication failure only after the final click. Users can choose their images only to the extent that their click-point dictates the next image.

DISADVANTAGES

a. This scheme is that the number of predefined regions is small.
b. The predefined regions to be readily identifiable.
c. An explicit indication of authentication failure only after the final click.

IV. PROPOSED METHOD

In the proposed work we have integrated sound file to help in recalling the password. No system has been devolved so far which uses sound file in graphical password authentication. That sound file or tone can be used to recall facts like images, text etc.It is very useful to recalling an object by the sound related to that object.The proposed system creates user profile as follows Master vector,(User ID, Sound File frequency, Tolerance),Detailed Vector - (Image, Click Points) As an example of vectors - Master vector (Smith , 2689, 50) Detailed Vector enters User ID and select one sound file which he want to be played at login time, a tolerance value is also selected with will decide that the user is legitimate or an imposter.To create detailed vector user has to select sequence of images and clicks on each image at click points of his choice.After creation of the login vector, system calculates the Euclidian distance between login vector and profile vectors stored.Finally fetch the user profile vector and find the click points, if all points are get match and show the authenticated user profile.

ADVANTAGES

a. We have integrated sound file to help in recalling the password.
b. That sound file or tone can be used to recall facts like images, text etc.
c. It is very useful to recalling an object by the sound related to that object.
d. To create detailed vector user has to select sequence of images.
e. All points are get match and show the authenticated user profile.

V. MODULE DESCRIPTION

A. User Registration

In this module a new user gets registered with his details and his password is generated according to the values at the x and y axis of the particular point.

B. **Login**

Here the registered users are trying to logging in with their registered user name and the password.

C. Profile Matching

In this module the entered login details is matched with the existing details with the help of Hash Visualization Algorithm

D. Login Confirmation

In this module after matching the data's with the help of hash visualization algorithm the login of the particular user is confirmed and he is permitted to enter the specific region.

VI. ARCHITECTURE

System architecture is a conceptual model that defines the structure,behavior and views of a system. Here a architecture gives a detailed process of user registration. At initial a user enters a complete details in a login form. The form includes a selected image co-ordinates and adding sound signature. Then all details are stored in a database. Before a login process is finished, a graphical process recognition system makes a match the mouse points and fetch a user profile. Then finish a login process. If a process is done, it shows the user profile. Otherwise it shows a re-login process.

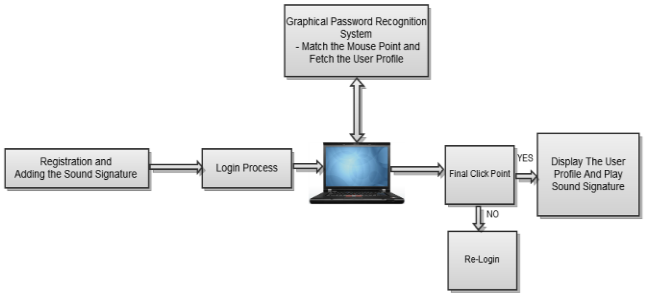
Graphical Password Recognition System
- Match the Mouse Point and Fetch the User Profile
Registration and Adding the Sound Signature
Login Process
Final Click Point
YES
Display The User Profile And Play Sound Signature
NO
Re-Login

Figure 1 : System Architecture Diagram

VII. WORKFLOWFLOWCHART

The flowchart shows a registration process and login process.

Registration Process :

a. Get unique ID from user
b. Then select a sound signature, tolerance level, image by a pass point
c. Repeat a process upto given images
d. Then its create a user profile vector

Login Trial :

a. Read a user unique ID
b. Then a Database fetch a user profile vector based on a unique ID
c. Detect a mouse position on image then it produce a sound signature
d. A mouse position is match, then it move to next image with a correct sound signature
e. Otherwise, it move to random image and sound signature then it shows re-login
f. Finally a login is done when all mouse position is matched

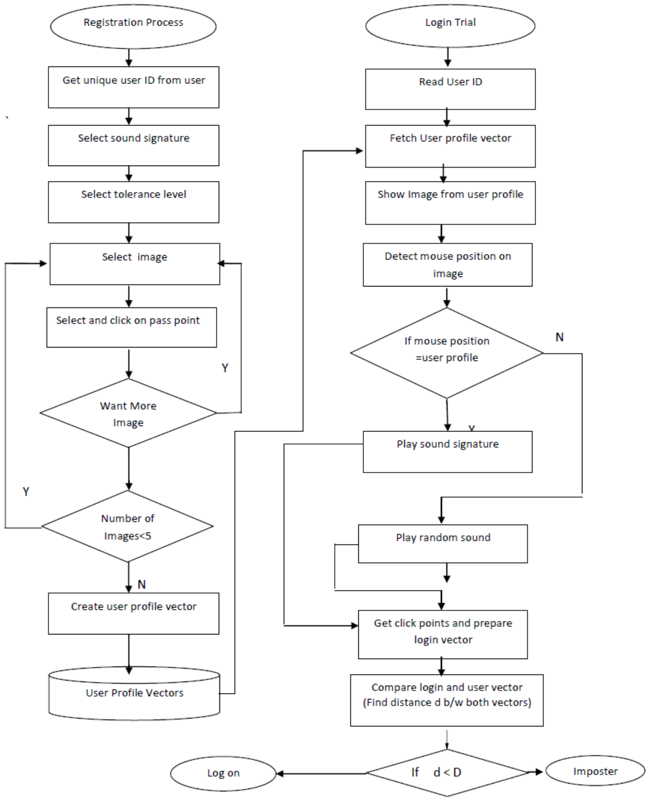
Registration Process
Get unique user ID from user
Select sound signature
Select tolerance level
Select image
Select and click on pass point
Want More Image
Y
Number of Images<5
Y
N
Create user profile vector
User Profile Vectors
Login Trial
Read User ID
Fetch User profile vector
Show Image from user profile
Detect mouse position on image
If mouse position =user profile
N
Y
Play sound signature
Play random sound
Get click points and prepare login vector
Compare login and user vector (Find distance d b/w both vectors)
If d < D
Log on
Imposter

Figure 2 : Login Process Flowchart

VIII. METHODOLOGY

HASH VISUALIZATION ALGORITHM

We have prototyped a user authentication system that utilizes “visual hashes” in place of text based passwords. One proposed hash visualization algorithm is Random Art, a technique that converts meaningless strings into abstract structured images . Instead of having to memorize a password, the user is able to create an image “portfolio”, by selecting some desired number of images, which he must memorize for future recognition. During authentication, the user is presented with a different set of images, some of which are from the portfolio and others which are chosen randomly. To login, the user must correctly identify all of his or her portfolio images. Another variation on this idea uses a fixed database of real photographs instead of Random Art images.

The security of image authentication will depend on how many images are in the user's portfolio and how many the user is presented with. Suppose that the portfolio contains P images and that for authentication, the system presents a total of T images. This gives us T!/[(T-P)! P!] possible combinations. For example, a 4 digit credit card PIN that is four digits long results in 10,000 possible combinations. To achieve an equivalent result with images, we could use P=5 and T=20 which gives us 15,504 possible combinations. The optimal combination of P and T will depend on the level of security and performance time desired. One security advantage of images, especially of Random Art images, is that they are harder to write down and to share with others than passwords and PINs. A vulnerability of this system is that an attacker might try to discover the image portfolio by making repeated login attempts and taking the intersection of images that are presented. Such attacks need to be taken into consideration during system design.

IX. CONCLUSION

Shoulder surfing resistant graphical authentication system has been successfully developed and implemented with a high degree of awareness and competence with the environment. The system was tested for a range of inputs and found to be error free. User with minimum computer awareness can easily operate this system, as the system is user friendly and menu driven. The forms have a very high technology of handling the records in the database The overall objective of efficiency and maintenance has been achieved particularly. All the information regarding this system have been documented and east to modify with less effort.

X. FUTURE ENHANCEMENT

The future enhancement of this project is that sound file or tone can be used to recall facts like images, text etc. It is also very useful to recalling an object by the sound related to that object. To create detailed vector user has to select sequence of images. All points are get match and show the authenticated user profile. This is done with the help of Hash Visualization Algorithm.

REFERENCES

[1] D. Gibson, “Understanding the Three Factors of Authentication,” Jun. 2011. [Online]. Available : http ://www.pearsonitcertification.com/articles/article.aspx ?p=1718488

[2] S. Azad, M. Rahman, M. S. A. N. Ranak, B. M. F. K. Ruhee, N. N. Nisa, N. Kabir et al., “Vap code : A secure graphical password for smart devices,” Computers & Electrical Engineering, vol. 59, pp. 99–110, 2017.

[3] S. Kostromina and D. Gnedykh, “Students’ psychological characteristics as factor of effective acquisition of visual information in e-learning,” in Proc. of Procedia - Social and Behavioral Sciences, 2016, pp. 34–41.

[4] M. S. Ranak, S. Azad, N. N. H. B. M. N. Nor, and K. Z. Zamli, “Press touch code : A finger press based screen size independent authentication scheme for smart devices,” PLoS ONE, vol. 12, no. 10, 2017.

[5] W. Goucher, “Look behind you : The dangers of shoulder surfing,” Computer Fraud & Security, vol. 2011, no. 11, pp. 17–20, 2011.

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, “Smudge attacks on smartphone touch screens,” in Proc. of 4th USENIX Workshop on Offensive Technologies, 2010.

[7] P. Biocco and M. Anwar, “Grid authentication : A memorability and user sentiment study,” in Lecture Notes in Computer Science, vol. 11594. Springer, 2019.

[8] G. E. Blonder, “Graphical password, us patent 5559961,” 1996.

[9] H. Gao, W. Jia, F. Ye, and L. Ma, “A survey on the use of graphical passwords in security.” JSW, vol. 8, no. 7, pp. 1678–1698, 2013.

[10] A. H. Lashkari, R. Saleh, F. Towhidi, and S. Farmand, “A complete comparison on pure and cued recall-based graphical user authentication algorithms,” in Computer and Electrical Engineering, 2009. ICCEE’09. Second International Conference on, vol. 1. IEEE, 2009, pp. 527–532.

[11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, “Passpoints : Design and longitudinal evaluation of a graphical passwordsystem,” International journal of human-computer studies, vol. 63, no. 1, pp. 102–127, 2005.

[12] “Passlogix v-go sso.” [Online]. Available : https ://www.scmagazine.com/review/passlogix-v-go-sso/

[13] O. Osunade, I. A. Oloyede, and T. O. Azeez, “Graphical user authentication system resistant to shoulder surfing attack,” Advances in Research, vol. 19, no. 4, 2019.

[14] J.-C. Birget, D. Hong, and N. D. Memon, “Robust discretization, with an application to graphical passwords.” IACR Cryptology ePrint Archive, vol. 2003, p. 168, 2003.