Authentication Schemes for Session Password Using Sound Signature

Swati N. Sonune[#1] Prof. Sandeep Sahu*[2]

[#]*M.E., Department of Computer Science & Engg.*
Shri Ram Institute of Technology. Jabalpur.
RGPV University, Bhopal.
swatisonune@gmail.com

[*]Head, M.E. Department of Computer Science & Engg.
Shri Ram Institute of Technology. Jabalpur.
RGPV University, Bhopal.
sandeep.sahu12@gmail.com

Abstract--Current authentication systems suffer from many weaknesses. Textual passwords are commonly used. Users tend to choose their nick names, which make textual passwords easy to break. Many available graphical passwords have a password space that is less than or equal to the textual password space. Here a graphical password system with a supportive sound signature to increase the remembrance of the password is discussed. In proposed work a click-based graphical password scheme called Cued Click Points (CCP) is presented. In this system a password consists of sequence of some images in which user can select one click-point of a image. In addition user is asked to select a sound signature corresponding to each click point this sound signature will be used to help the user in recalling the click point on an image. System showed very good Performance in terms of speed, accuracy, and ease of use. Users preferred CCP to Pass Points, saying that selecting and remembering only one point per image was easier and sound signature helps considerably in recalling the click points.

Index Term—Sound Signature, Authentication, Textual Passwords.

I. INTRODUCTION

Authentication is the first step of information security. Authentication refers to the process of confirming or denying an individual's claimed identity. Authentication schemes require users to memorize the passwords and recall them during log-in time. The most common user authentication method is the text-based password scheme that a user enters a login name and a password. The vulnerabilities of this method have been well known. Users tend to pick short password or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. To resist brute force search and dictionary attacks, users are required to use long and random passwords. Unfortunately, such passwords are hard to remember. Furthermore, textual password is vulnerable to shoulder-surfing, hidden camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text. In addition, the possible password space of a graphical password scheme may exceed that of text based schemes and thus presumably offer higher level of security. It is also difficult to devise automated attacks for graphical passwords. As a result, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Due to these advantages, there is a growing interest in graphical password. However, existing graphical passwords are far from perfect. Typically, system requirements and communication costs for graphical passwords are significantly higher than text-based passwords. In addition, few graphical systems support keyboard inputs. More importantly, most current graphical passwords are more vulnerable to shoulder-surfing attacks than textual passwords. In this paper, Using pure recall-based techniques and Cued Recall Based Techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

These systems can involve users: a. identifying one or more images out of a group. b. Touching points of an image.

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).

It is well know that the human brain is better at recognizing and recalling images than text, graphical passwords exploit this human characteristic we have

use this following schemes for better Security purpose in Authentication.

Graphical Authentication

In this scheme, we use images for Authentication. When register the new user, first select the one or multiple images from given sequence of images and then click on particular points that is pixel values in sequence i.e CCP which stored in System Database. When user log's in, first select the proper images and click points in same sequence then system checks that image and click points are same or not. If incorrect then give the error and if it is correct then give permission for next authentication scheme.

Sound Signature

In this scheme, we use sound clips for Authentication. When register the new user, select one sound clip and play that clip then stored its pause time in System Database.

II. GRAPHICAL AUTHENTICATION MECHANISM

The following are main methods of authentications:

a. Token based authentication.
b. Biometrics based authentication.
c. Knowledge based authentication.

Token-based techniques, such as key cards, bank cards and smart cards are widely used. Many token-based authentication systems also use knowledge-based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Biometric based authentication techniques, such as fingerprints, iris scans, or facial recognition has been developed due to uniqueness properties of biometrics. These systems are very secure. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. Knowledge based techniques are the most widely used authentication techniques and include both text-based and picture-based passwords. The picture-based techniques can be further divided into two categories: recognition - based and recall-based graphical techniques. Using recognition-based techniques, a user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage. Using pure recall-based techniques and Cued Recall Based Techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

III. RELATED WORK

EXISTING SYSTEM:

In the existing system**,** Brostoff and sasse carried out an empirical study of passfaces, which illustrates well how a graphical password recognition system typically operates. Blonder-style passwords are based on cued recall. A user clicks on several previously chosen locations in a single image to log in. As implemented by Passlogix Corporation, 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 in effect, 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. 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.

DISADVANTAGES:

The problem with this scheme is that the number of predefined regions is small, perhaps a few dozens in a picture. The password may have to be up to 12 clicks for adequate security, again tedious for the user. Another problem of this system is the need for the predefined regions to be readily identifiable.

PROPOSED SYSTEM:

In the proposed work we have integrated sound signature to help in recalling the password. No system has been developed so far which uses sound signature in graphical password authentication. Study says that sound signature or tone can be used to recall facts like images, text etc. In daily life we see various examples of recalling an object by the sound related to that object enters User ID and select one sound frequency 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. Profile vector is created.

PROFILE VECTORS-

The proposed system creates user profile as follows-

Master vector - (User ID, Sound Signature frequency, Tolerance)

Detailed Vector - (Image, Click Points)

As an example of vectors -

Master vector (Swati, 2658, 60)

Detailed Vector

Image	Click points
I 1	(128,679)
I 2	(186,137)
I 3	(460,287)
I 4	(741,154)
I 5	(855,254)

IV. SYSTEM ARCHITECTURE

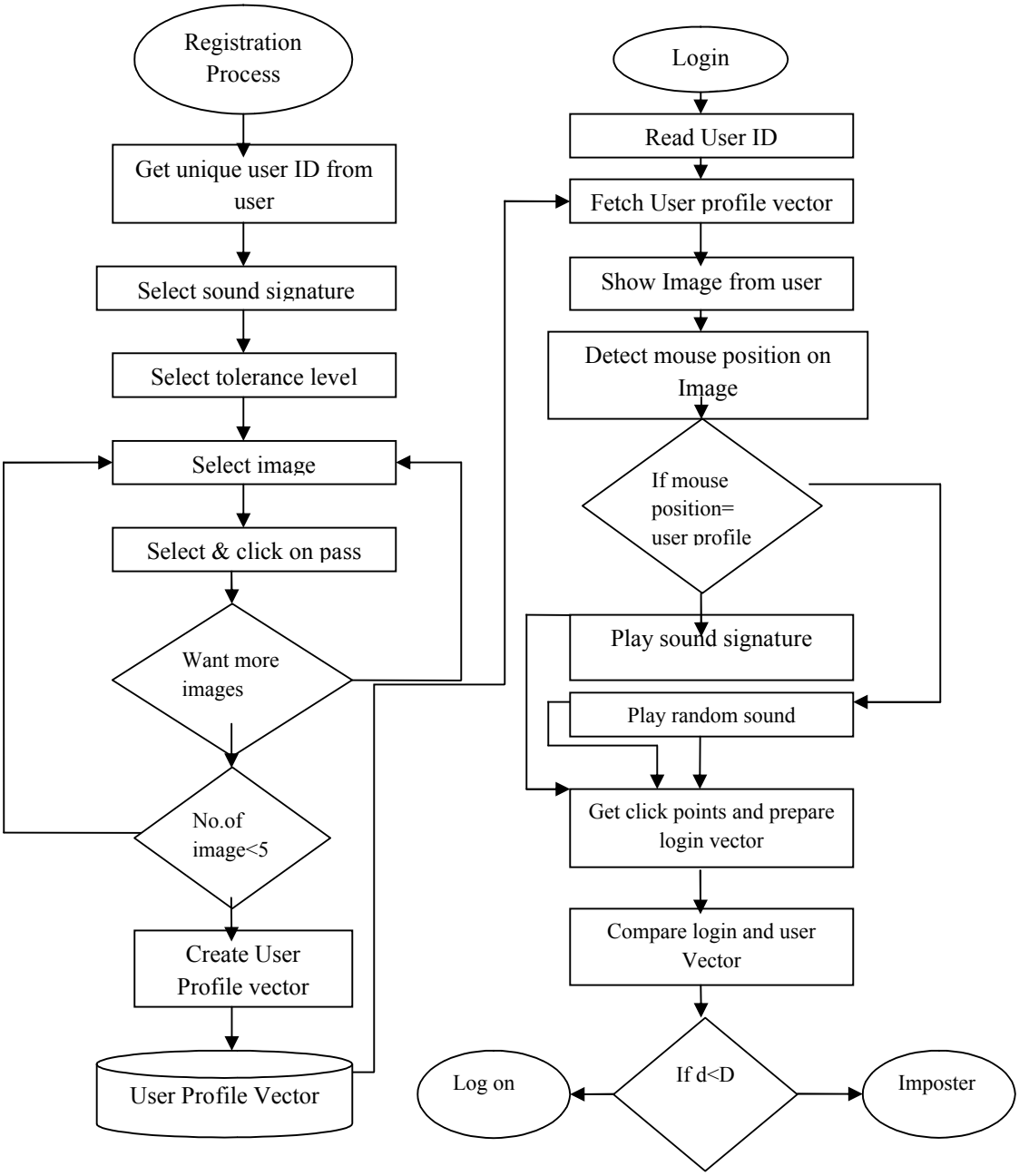

Fig. System Architecture

Working

➢ *Registration*

1. When new user registers, first enter the all details which give in registration form.
2. Then select any one image or sequence of images from multiple images and also click the points.
3. Then select any one sound clip, play and pause that clip at particular time.
4. This all interactions stored in database

➢ *Authentication*

1. Enter username and password.
2. Select proper image or images and their sequence of click points.
3. Select proper sound clip and their pause time.
4. All interactions fetch from database then compared one by one.

Then access granted to authorize user for access applications.

V. EXPERIMENTAL RESULTS

Data collected from 30 participants. Each participant was asked to register himself/herself and then each was invited for login trails. Participants were engineering students of age group 20-28 Y. Following Figure shows the detail of the registrations of the student.

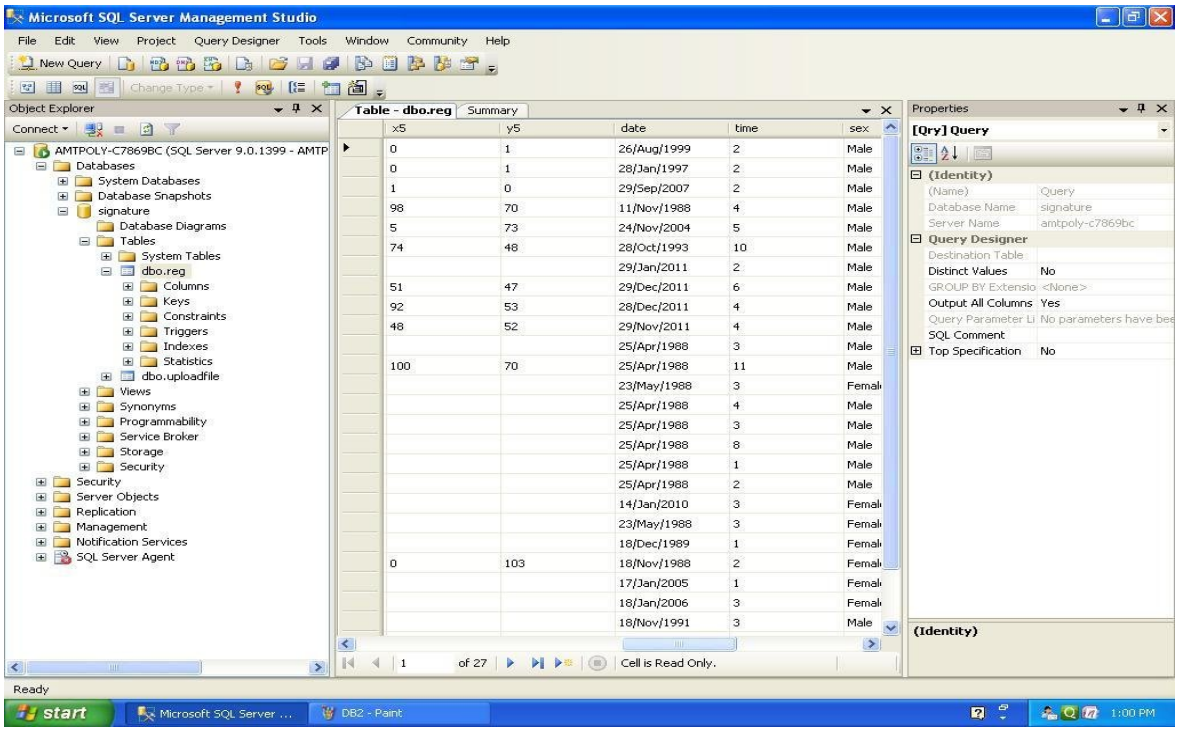

Figure 1: Database table showing registration fields of the student.

VII. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, Pure Recall-Based and Cued Recall-Based graphical password authentication algorithms were reviewed. From all these algorithms we were able to come up with a number of shortcomings that can allow attacks to be perpetuated. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques. The main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

VIII.FUTURE ENHANCEMENT

In future systems other patterns may be used for recalling purpose like touch of smells, or any other advanced signature mechanism, study shows that these patterns are very useful in recalling the associated objects like images or text.

VIII. ACKNOWLEDGMENTS

We would like to express our appreciation to our parents and all the teachers and lecturers specially Mr. T.N. Ghorsad who helped us to implement these research due to his knowledge, efforts and show us the best way to gain it.

IX. REFERENCES

[1] R. Dhamija, and A. Perrig. “Déjà Vu: A User Study Using Images for Authentication”. In 9th USENIX Security Symposium, 2000.
[2] Real User Corporation: Passfaces. www.passfaces.com
[3] Jermyn, I., Mayer A., Monrose, F., Reiter, M., and Rubin., “The design and analysis of graphical passwords” in Proceedings of USENIX Security Symposium, August 1999.
[4] Arash Habibi Lashkari may, 2010 “a new algorithm for graphical user authentication based on rotation and resizing”,
[5] G. E. Blonder, "Graphical Passwords," In *Lucent Technologies, Inc., Murray Hill, Nj*, U. S. Patent, Ed. United States, 1996.
[6] Passlogix, site http://www.passlogix.com
[7] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, “A New Graphical Password Scheme Resistant to Shoulder-Surfing.
[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon, “Design and longitudinal evaluation of a graphical password system”. International J. of Human-Computer Studies 63 (2005) 102127.
[9] Arash Habibi Lashkari1*, Abdullah Gani1, Leila Ghasemi Sabet2 and Samaneh Farmand1 “A new algorithm on Graphical User Authentication (GUA) based on multi-line grids”.
[10] M Sreelatha 1, M Shashi 2, M Anirudh 1, MD Sultan Ahamer 1, V Manoj Kumar, “Authentication Schemes for Session Passwords using Color and Images”.
[11] Xiaoyuan Suo Ying Zhu G. Scott. Owen, “Graphical Passwords: A Survey”
[12] D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," in *Proceedings of International conference on security and management*. Las Vergas, NV, 2004.
[13] S. Man, D. Hong, and M. Mathews, "A shouldersurfing resistant graphical password scheme," in *Proceedings of International conference on security and management*. Las Vegas, NV, 2003.
[14] Gajbhiye S.K.1* and Ulhe P.2, “Authentication Schemes For Session Passwords Using Color And Gray-Scale Images”