Graphical Password based Authentication System with Sound Sequence

Shabina Sayed
Assistant Professor, Department of Information Technology,
MHSSCOE
Mumbai

Aman Mohid
Student B.E, Department of Information Technology,
MHSSCOE
Mumbai

Manish Pal
Student B.E, Department of Information Technology,
MHSSCOE
Mumbai

Murtaza Haji
Student B.E, Department of Information Technology,
MHSSCOE
Mumbai

ABSTRACT
There have been many graphical password schemes proposed as alternatives to text passwords. Research and experience show that alpha-numeric passwords are inefficient with both usability and security issues which limit their application in today's life. Studies have showed that human brain is much better at recognizing and memorizing images than text. Graphical based passwords are intended to make use of this human characteristic with a goal to reduce the memory burden on users, along with a password space which is offered by images, more secure passwords can be produced and users will be spared of unsafe practices in order to cope. This paper focuses on a new click-based graphical password scheme which is known as Cued Click Points (CCP). It can be viewed as a combination of PassPoints, Passfaces and Story. A password comprises of one click-point per image from a sequence of images. The next image displayed is based on the previous click-point so that the users receive immediate feedback as to whether they are on the correct path when logging in. CCP offers better usability, efficiency and security. Users could quickly create and re-enter their passwords. Another feature of CCP is the immediate feedback telling the correct user whether their latest click-point was correctly entered.

Keywords
Graphical password, sound sequence, authentication

1. INTRODUCTION
Users are provided with many types of password such as alphanumeric passwords, biometric scanning, graphical passwords, cards (such as an ATM) etc. But there are many flaws in current authentication systems. When a user uses alphanumeric passwords, they choose passwords that are related to their nick names or favorite place names which can be guessed easily. Graphical passwords strength comes from the fact that users can memorize pictures better than words. Cards can easily be misplaced or lost or even get stolen. Biometric recognition scheme has its pros and cons based on various factors such as consistency, strength, uniqueness. The major drawback of using biometrics is its dependency on a user's personal and unique characteristic. Most of the biometric systems require the user's physical presence and a special scanning device for authentication, which is not applicable for Internet users

Passwords are used for Authorization, Authentication, and Access Control (AAA). Mostly the users tend to select passwords that are predictable and simple. This generally happens with both graphical and alphanumeric passwords. Users tend to choose passwords that are easy to remember password, unfortunately it results in the passwords that follow predictable patterns which makes it easier for attackers to guess. While the users can be assigned system generated passwords to reduce the predictability, this usually causes usability issues since users are unable to remember such random passwords.
Several of graphical based password systems have been developed. Study shows that alphanumeric passwords suffer with both security and usability problems. According to a recent article, a company ran a security test to crack passwords and in less than 60 seconds and they successfully identified about 75% of the passwords. It is well known that the human brain is better at memorizing and recalling graphics than words, graphical based passwords make use of this human characteristic.

2. EXISTING SYSTEMS
2.1 Need for the system
The idea is that using graphics and sound will lead to better memorability and reduce the tendency to choose simple and inefficient passwords that are easy to predict. This increases the overall password security and also secures the confidential information of the user. Several graphical password systems, have been developed and some HCI evaluation has been done. The problems with password arise from limitations of humans' long-term memory (LTM). Once a user chooses a password, they must be able to remember it to log in. But, humans have a tendency to frequently forget their passwords.

Human brain may not be able to recall the password if it is not frequently used and hence it may lock-out the user from their account. Furthermore, a complication is that users have unique passwords for computers, web sites, social media etc. The amount of passwords may interfere with the memory and may lead to forgetting or confusing passwords.

2.2 Comparison with Existing Systems
The advantages offered by this system are given below:

The system uses objects instead of human faces which can be used for selecting a password because during the latter phase,

the user has to select the same password and it is a much easier task to simple objects. The system is resistant against Brute-force attack as the password space is large. It is also less vulnerable to other attacks such as online and offline dictionary attacks. The system is better than Man et al scheme. It is because in that scheme the user needs to remember the objects string as well as the code.

In comparison with Van Oorschot's approach, the system is more secure and efficient since users not only select graphical password but also sound sequence as their password, making it difficult to hack. In the system, even if the alphanumeric password is compromised, the graphical password is difficult to be stolen or compromised.

The approach of this system protects the system and prevents the attackers from hacking the password and prevents them from executing attacks on the system. Thus the system is more secure, flexible and reliable than two step authentication system. An important issue of the system is that it is user dependent during authentication The attacks that can possible exploit alphanumeric passwords are Dictionary attacks, Brute force attack, Shoulder surfing, Guessing and social engineering. Graphical based passwords are less resistant to all such attacks than alphanumeric based passwords and it has been proved that it is difficult to crack graphical based passwords using various traditional attacks. The system is resistant to almost all the attacks on graphical passwords.

Graphical Password Schemes/ Systems	Type of Scheme	Resistant to Possible Attacks				
		Brute Force Attack	Dictionary Attack	Guessing Attack	Shoulder Surfing Attack	Phishing Attack or Social Engineering
Blonder's Scheme	Recognition Based	Y	N	Y	Y	N
BDAS	Pure Recall Based	N	-	-	-	-
Qualitative DAS	Pure recall Based	N	-	-	-	-
PassPoints	Cued Recall Based	Y	N	Y	Y	N
PassFace	Recognition Based	Y	Y	Y	Y	N
PassGo	Pure Recall Based	Y	-	-	-	-
Man et al Scheme	Recognition Based	Y	N	N	Y	N
Picture Password Scheme	Recognition Based	Y	N	Y	Y	N
Association based scheme	Recognition Based	-	-	-	Y	-
Déjà Vu	Recognition Based	Y	-	Y	-	-
Haptic Password Scheme	Pure Recall Based	-	-	-	Y	-
YAGP	Pure Recall Based	Y	-	Y	Y	-
Photographic Authentication	Recognition Based	-	Y	-	-	-
Two Step Authentication	Hybrid	-	-	-	N	Y
Our System	Hybrid	Y	Y	Y	Y	Y
Note: Y= Yes resistant to attack N=No not resistant to attack						

Figure 2.Comparison with Existing Systems

3. PROPOSED SYSTEM

This system integrates sound signature with the graphical password. Study says that sound signature can be used along with images or text to enhance security. In a research it has been found out that human can memorize images as well as sound tone with less difficulty. Users who register using graphical password and sound clip have better security overall and their data remains safe. It is very good for Graphical and sound clip password authentication system.

The next user study focused on the robustness of graphical password against a guessing attack by asking relatives of the participants to guess their graphical passwords in various attempts. The results showed that graphical passwords used with ambiguous decoys were easy to memorize than other graphical passwords with familiar decoys. However, the guidelines showed a significant impact on maintaining the capacity to memorize the passwords over time. The study also found that graphical passwords used with ambiguous decoys were more vulnerable to guessing attacks than graphical passwords with familiar decoys. The results in the end showed that graphical passwords that followed the provided guidelines were more secure.

3.1 Passpoints

In the passpoint technique, numbers of images are displayed to the user, out of which the user selects any one of the image. On the selected image user must select N click points during the time of selecting a password. During login, the user must select on accordance with the same sequence of click numbers. The user has to recall the number of clicks. The system has a certain degree of tolerance for the selected pixels. This makes the system secure and gives it a better usability.

3.2 Cued Click Points

A Cued Click point is a graphical password scheme based on clicks, a cued-recall graphical password technique. Users click on one pixel or one point per image for a sequence of images. The next image is based on the previous click-point. Performance of this is very good in terms of speed, efficiency, fault tolerance and security.

3.3 Sound Sequence

User must select a sound sequence at the time of registration. This sequence will then be saved in the database in an encrypted format. At the time of user login, the user will have to enter the sound pattern in the correct sequence in order to

gain access to the system, if the user is not able to do so then he will have to start the procedure all over again from the start.

4. IMPLEMENTATION

Figure 4.1 Signup for system

In fig. 4.1 The user is creating a new account. During account creation the user will have to enter his details such as login id, password, phone number, and the most important is sound signature. User has to enter ID and password during Signup.

Figure 4.2 Selecting Sequence of images as a password

User must select a sequence of images as their password along with the corresponding sound signature. Fig. 4.2 shows us that user has selected 4 images as their password.

Figure 4.3 Selecting click point on an image

After selecting sequence of images user has to select pixels and a corresponding sound signature on images as Password.

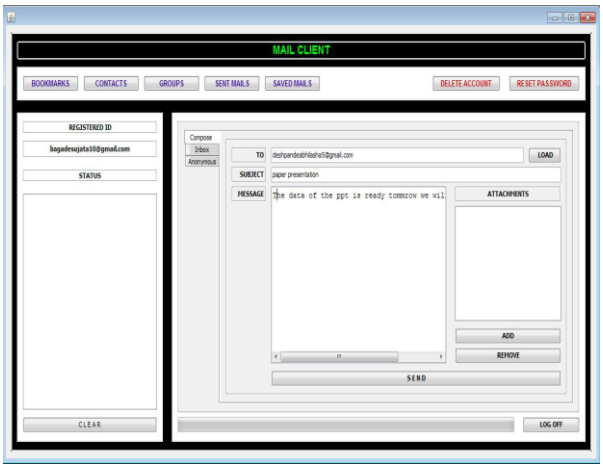

Figure 4.4 User Account

After logging in, the account will be shown to user. User can send file, message or any picture.

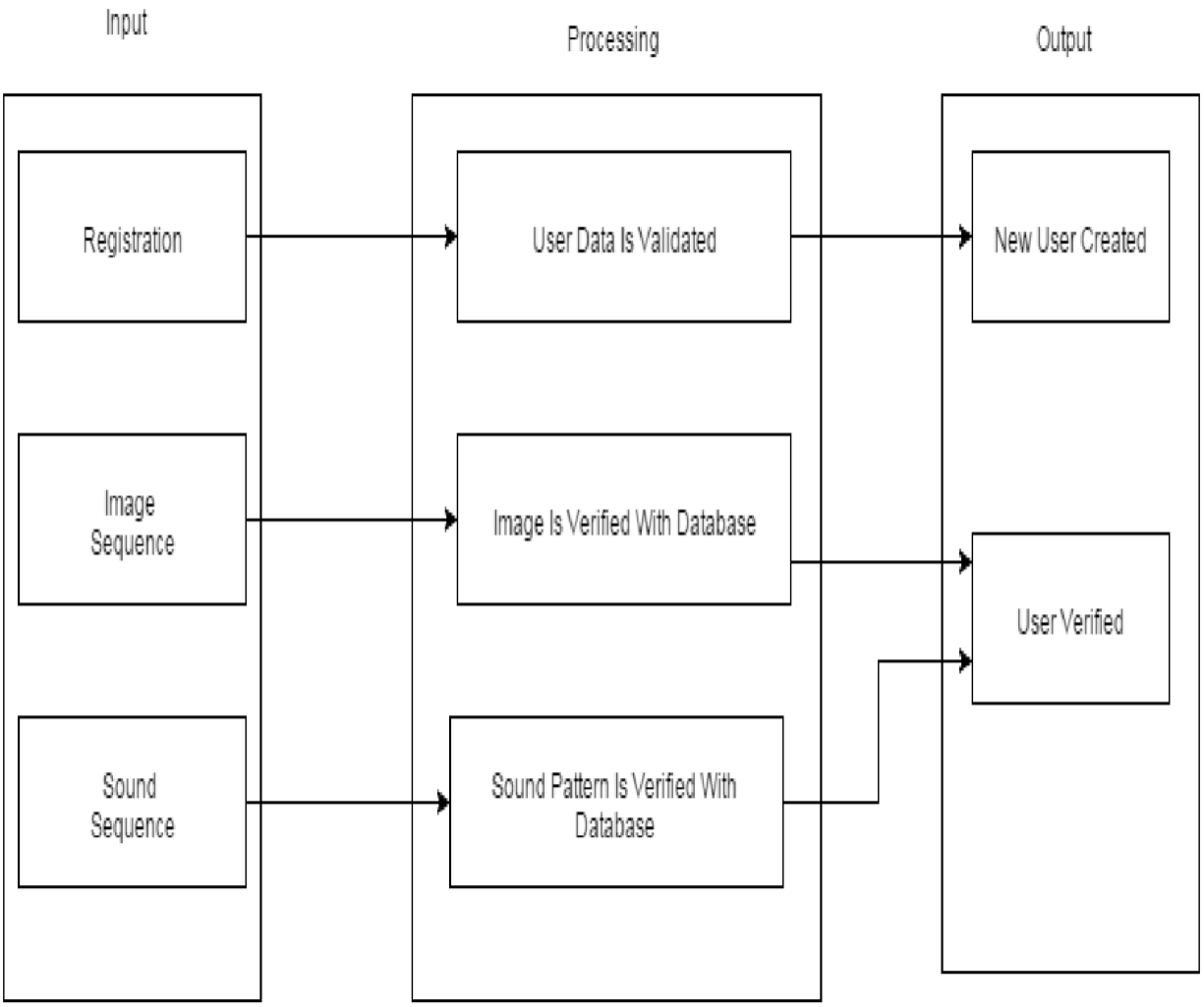

Figure 4.5 Block Diagram

Fig 4.5 starts with an input .In input registration of the user is done. During registration the user generates a new account by selecting a sequence of images and sound clips. The user selects a particular sequence of images and this sequence is stored in the database along with click points which the user has selected in those images.

After the image sequence is done the user is given list of sound clips. The user selects a sequence of sound clips and this sequence of sound clips is stored in the database. The registration of the user is stored in the database and a new user data is validated in the database which is done by the processing part. The output shows us that a new user is created.

During registration the user selects an image sequence and this particular image sequence is stored in the database and then it is verified with the database. If the user succeeds in proper image sequence then the system proceeds to the next phase. Now the user selects the particular sound sequence and then the sound sequence is verified with the database and if the sequence is correct the user is granted access to the system.

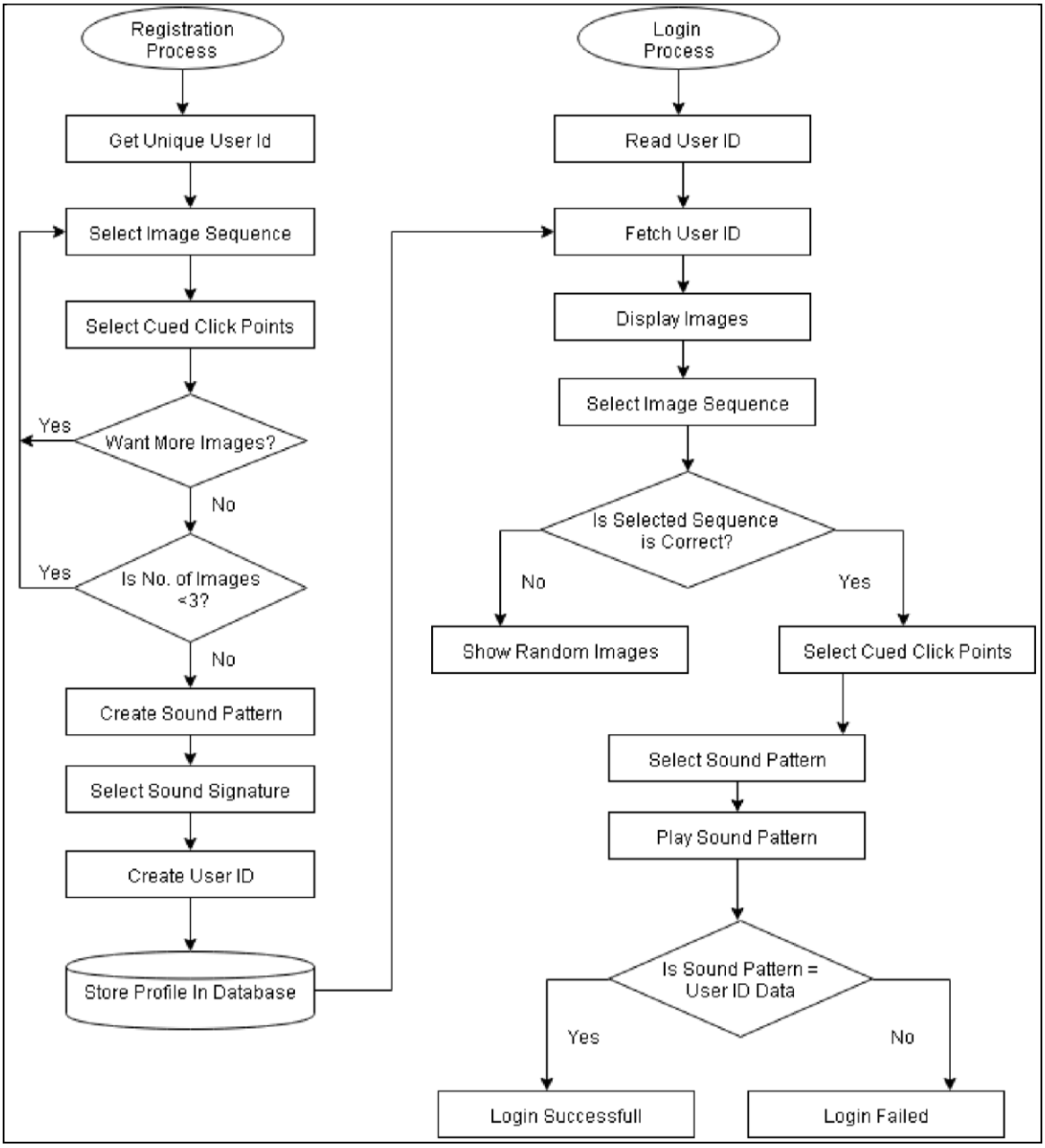

Figure 4.6 Flow Chart

Fig 4.6 Provides us the detailed description about how the system proceeds. The flow starts with a registration process if it is a new user. If the users already have an account then it will start with a login process. For a new user registration is done by selecting images and sound clips. During registration process the user is given a unique id.

5. RESULT ANALYSIS:

Data was collected from 10 different participants. Each participant was asked to register themselves and then each was given an invitation to login trail 5 times as legitimate user and 5 times as impostor randomly. Participants were users ranging from age group of 20-25 Years.

Table 1. Shows the detail of the data generated by legitimate users.

Users	Attempts	Rejected	Accepted
1	5	0	5
2	5	1	4
3	5	0	5
4	5	2	3
5	5	0	5
6	5	1	4
7	5	1	4
8	5	0	5
9	5	2	3
10	5	1	4

Table 2. Shows the detail of the data generated by Imposter users.

Users	Attempts	Rejected	Accepted
1	5	5	0
2	5	5	0
3	5	5	0
4	5	5	0
5	5	4	1
6	5	5	0
7	5	5	0
8	5	5	0
9	5	5	0
10	5	5	0

6. CONCLUSION

This application helps the user to increase the security of user account this web application could be a harbinger to the new world of Assistive Web Technologies. A CCP technique makes user easily recall the click points and requires less time and also produce an accurate result. Playing a sound file at the login time makes a system more interactive. A sound file simply plays a role of hint. In future systems other patterns may be used for recalling purpose like touch , study shows that these patterns are very useful in recalling the associated objects like images or text. The future scope of this software is that it could be used on mobile devices and tablets for greater security.

7. REFERENCES

[1] Badgude Puja, Ghorpade Hemlata, Ghadge Yogita, More Supriya , International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-4, Issue-1, March 2014

[2] International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 1 – Mar 2014

[3] Chippy.T, R.Nagendran "Defence Against Large Scale Online Password Guessing Attacks By Using Persuasive Click Points" International Journal of Communications and Engineering Volume-3, 01 March 2012

[4] S. Chiasson, E. Stobert, A. Forget, R. Biddle, and P. van Oorschot, "Persuasive cued click-points: Design, implementation and evaluation of a knowledge-based authentication mechanism," School of Computer Science, Carleton University ,Tech. Rep. TR-11-03, February 2011..

[5] S. Chiasson, A. Forget, R. Biddle and P.C. van Oorschot, &ldquo,User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords,&rdquo, Int',l J. Information Security, vol. 8, no. 6, pp. 387-398, 2009.

[6] Thorpe, J. and van Oorschot, P.C. "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords. USENIX Security" Symp. 2007.

[7] Nilesh Changune1 , Ganesh Shinde2 , Sagar Chaugule3 , Sandeep Helkar4 IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-730

[8] E. Stobert, A. Forget, S. Chiasson, et al. Exploring usability effects of increasing security in click-based graphical passwords. In Annual Computer Security Applications Conference (ACSAC), 2010

[9] Harsh Kumar Sarohi,Graphical Password Authentication Schemes: Current Status and Key Issues, International Journal of Computer Science Issues,2013, 437-443.

[10] S.Singh, G.Agrawal "Integration of sound signature in graphical password authentication system" Invertis University Bareilly,India, January ,2011.