RESEARCH ARTICLE OPEN ACCESS

Pattern Point Based Graphical Authentication

Anshul Nema[1], Amit Ranjan[2]

[1]M.Tech. Scholar, Shri Ram Institute of Science & Technology, Department of CSE, Jabalpur, M.P., India.
[2]Asst. Prof. Shri Ram Institute of Science & Technology, Department of CSE, Jabalpur, M.P., India

Abstract:

Internet services such as social networks, e-banking, email, cloud services, blogs, all require some form of security like user authentication. Despite the availability of advanced authentication technologies such as smart cards, biometrics or USB tokens, passwords and PINs are still the most prevalent form of user authentication. Graphical passwords are a form of user authentication on which a lot of research has been undertaken over the past decade and a variety of alternative password schemes proposed. Proposed system develops image based and pattern based authentication method. It provides user to select image and grid pattern for making pattern password. It was found that brute-force attacks were largely ineffectual in terms of time required although image analysis had a profound impact on the effective password space. Password generated by this algorithm is more memorable than pass point mechanism. Proposed system is user friendly, effective, efficient, multifactor and multilayer authentication system. It keeps resistance against information leaks, brute force attack, phishing attacks, replay attack and man-in-the-middle attack.

Keywords — Security, Authentication, Multifactor authentication, Graphical Password, Image Pattern, PassPoints

I. INTRODUCTION

The idea of graphical password as an alternative to text based approach was proposed by Blonder in 1996 motivated by the fact called as "picture superiority effect" i.e. tendency of human brain to memorize images far better than text [1]. Graphical passwords can be classified under three categories namely, recognition, recall, and cued-recall. Recognition schemes operate by requiring the user to recognize visual data. Recall schemes require the users to reproduce something that was created earlier during registration, and finally, cued-recall schemes provide the users with some clues to aid recollection. Application examples for graphical password use as an authentication mechanism emerge in social media, online commerce, and also in the management of critical infrastructure such as smart micro-grids. In all of these applications, the underlying access control model is discretionary, and so the onus of protecting one's content from adversarial access lies with the user who is making the content available. Recognition schemes operate by requiring the user to recognize visual data. Recall schemes require the users to reproduce something that was created earlier during registration, and finally, cued-recall schemes provide the users with some clues to aid recollection. Application examples for graphical password use as an authentication mechanism emerge in social media, online commerce, and also in the management of critical infrastructure such as smart micro-grids. In all of these applications, the underlying access control model is discretionary, and so the onus of protecting one's content from adversarial access lies with the user who is making the content available. Graphical password authentication schemes can be classified into two types: Recognition-based and Recall-based graphical techniques.

A. Recognition Based Methods: 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. There are many graphical password authentication schemes which designed by using recognition-based techniques. We

only introduced two typical methods. The first one is PassFaces which was developed by Real User Corporation. The user will be asked to choose four or more images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight cheat faces (figure 1.1). The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures.

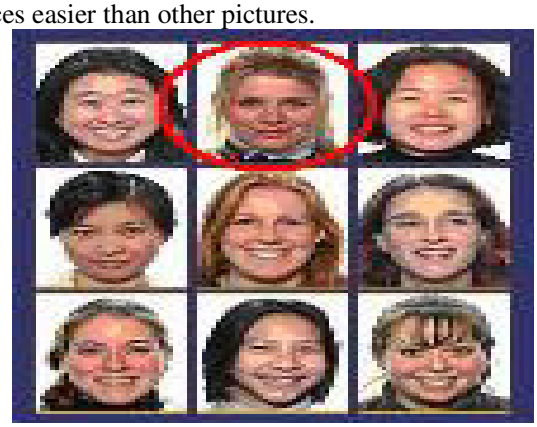

Figure 1.1: Example of PassFaces.

Another recognition-based scheme is Pass-Objects which were developed by Sobrado and Birget [2]. The system will display a number of pass-objects among many other objects. Then, to authenticate, the program shows a variety of similar objects on the screen, and the user is asked to click inside the area that the selected objects make. For instance, if you chose three Pass-Objects, when those three objects are displayed on the screen, it will form a triangle. What a user will then do is click inside of this newly formed invisible triangle for authentication. It will then ask for the same action again, but with the icons on the screen in different positions. Figure 1.2. is an example of this method.

The emerging requirement is to provide better security solutions that could efficiently cater-for the possible risks and loopholes endangering security of smart phone users. In the following section we, in brief explain the domain of our research, perform a survey of various security issues, existing user authentication techniques for cloud and discuss the growth as well as scope of authentication system in cloud computing.

Figure 1.2: An example of Pass-Objects.

1.3 Authentication Requirements:

In general authentication is the process of validating someone as authentic and claims they made are true. In client-server architecture, validation is generally done using the login username and password. Knowledge of the password is adopted to ensure that the tenant is authentic. Each tenant registers first or gets registered by someone else on cloud server and using an assigned or self-stated password. During each successive use, the tenant must know and use the already declared password. The weakness of this system is that passwords can often be stolen, unintentionally revealed or forgotten.

Graphical passwords have become popular due to the proliferation of touch screen devices, in particular Smartphone's and tablets. The prevalent approaches are based on simple graphical passwords, which can be easily remembered and reproduced by potential attackers. In this work, we study user authentication based on image selection and pattern selection from pattern grid and image grid. Authentication is based on features extracted from the dynamics of the image-grid and pattern grid.

As a consequence, a potential attacker would have to copy not only *what* the user selects, but also *how* the user draws it. Unfortunately, graphical passwords tend to be much simpler than signatures and are not composed, in general, of previously learned or heavily practiced movements. This can lead to a higher intrauser variability (i.e., variations between samples produced by the same person) than in the case of signatures or may cause users to forget part of or the whole graphical password. There are a couple of possible authentication attacks describing in Table 1.1.

Type of Attack	Description
Password guessing attack	This includes multiple attacks, including brute force, common passwords and dictionary attacks, which aim to obtain

	password of the user. The attacker can try to guess a specific user's password, Try common passwords to all users or use an already made list of passwords to match against the password file, in their attempt to find a valid password.
Replay attack	The attacker tracks the authentication packet and replays this information to get an unauthorized access to the server.
Man-in-the-middle attack	The attacker passively puts himself in between the user and the verifier in an authentication process. The attacker then attempts to authenticate by pretending to be as the user to the verifier and the verifier to the user.
Masquerade attack	The attacker pretends to be the verifier to the user to obtain authentication keys or data that may be used to authenticate fallaciously to the verifier.
Insider assisted attack	The systems managers intentionally compromise the authentication system or thieve authentication keys or relevant data of users.
Phishing attack	Social engineering attacks that use fake emails, web pages and other electronic communications to encourage the user to disclose their password and other susceptible information to the attacker.
Shoulder-surfing attack.	Social engineering attacks definite to password systems where the attacker secretly directs observing the password when the user enters it.

II. RELATED WORK

2.1 Types of Authentication:

Everyday user authentication commonly uses passwords, based on"something the user knows" for computer authentication. There have been many studies that highlight the problems associated with password authentication, most of them boiling down to the illegitimate acquisition of passwords, thus granting access to resources, to the wrong users [3]. In addition, Kemp stated that Moore's Law of doubling every two years is directly applicable to the continuous growth of password authentication complications [4].

This means that as more and more passwords are created and used, more countermeasures are required to mitigate the ever-growing threats. Authentication through" something the user is" has recently been more prevalent for computer authentication in the forms of fingerprint recognition and facial recognition biometric systems. Lai et al. identified that authentication through face recognition has, however, been affiliated with problems such as irrevocability, potentially compromising its future use [5]. Furthermore, authentication through fingerprint recognition has been implemented by systems such as the Windows 10 Hello feature, even though it has not been extensively implemented due to apparent reasons such as the cost of implementation. From the previously mentioned authentication techniques (facial and fingerprint recognition), passwords are currently the most prominent method used, due to various advantages that in most cases outweigh the disadvantages.

Gesture-based authentication typically combines, "something the user knows", as well as "something the user is", which attempts to provide a stronger authentication system. Current systems make use of technologies such as accelerometers and wearable sensors for user authentication. However, these systems again face problems regarding implementation, as well as rigorous testing in order to be seen as viable alternatives to passwords. Figure 2.1 below shows the basic types of authentication used.

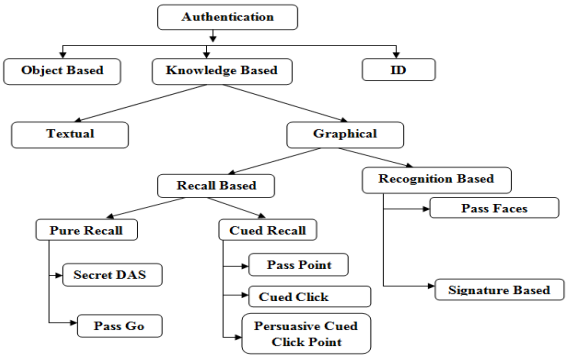

Figure 2.1 Authentication Types.

Authentication is defined as the process which positively verifies the user identity, device, or other entity in a computer system, in order to allow access to resources in the system.

Authentication is divided into three categories which are as follows Knowledge based authentication, Object based Authentication (Token), ID based authentication.Figure1 shows the classification of authentication mechanism. The problem with text based password is that user creates memorable password which can be broken easily and also the password space is small. Biometric based authentication techniques are slow ,expensive, and unreliable thereby not preferred by many .No doubt that Token [6] based authentication provides high security, accessibility and usability then the others but if token get lost, the security also get lost. Therefore the most preferable technique that can be used to improve the security is Knowledge based authentication technique. Knowledge based technique includes Graphical Password which is categorized into

Recognition based and Recall based. In Recognition based techniques user has to recognize or reproduce the things during the login where as in case of recall based technique user has to recall the things during the login in such a way that whatever they selected during the password creation they have to recall it in the same manner.

In 2015, Doiphode et al [7] proposed a scheme that combines Captcha and graphical password. For example, suppose the password is "Mango". During sign in user see the Captcha challenge. The m, a, n, g, o are at different locations and there are different alphabets too. User clicks on the locations of the m, a, n, g, o in correct sequence (see Fig. 2.2).

Advantage

• It is prevents from the attacks of bots and guessing [8].

Disadvantage

• It is non-resistant to shoulder-surfing attack.

In [9] the author proposed the Graphical Password (GP) approach for authenticating the legitimate user in Online Social network. Graphical Password is a picture based authentication. The combination of pictures is increasing by selecting images from distinct levels. Due to this, password space of this approach may overshoot the space limitation of text based password approach.

In [10] the author proposed Presents a new scheme for graphical password that uses images that are unexplainable and have larger password space. The user selects 10 images from 50 images that are shown to her/him and assigns a character to each image. In this case adversaries cannot realize what character is assigned to each image unless watches login several times.

In [11] the research group Proposed a novel authentication system PassMatrix, based on graphical passwords to resist shoulder surfing attacks. With a one-time valid login indicator and circulative horizontal and vertical bars covering the entire scope of pass-images, PassMatrix offers no hint for attackers to figure out or narrow down the password even they conduct multiple camera-based attacks.

In [11] the authors proposed a new secure graphical password technique of authentication, which conceals information about the user's password without sacrificing the usability. The technique exploits indirect entry of password image by creating a delusion to select nearby neighbour which makes it difficult for a shoulder-surfer to identify the user's actual password.

III. PROPOSED WORK

3.1 Proposed Model

Proposed system provides the high security level by providing three level authentications. It consists of user name authentication and integrates the image password system with graphical pattern password to authenticate a user. Proposed system architecture is divided into two main modules- password creation and authentication, shown in figure below:

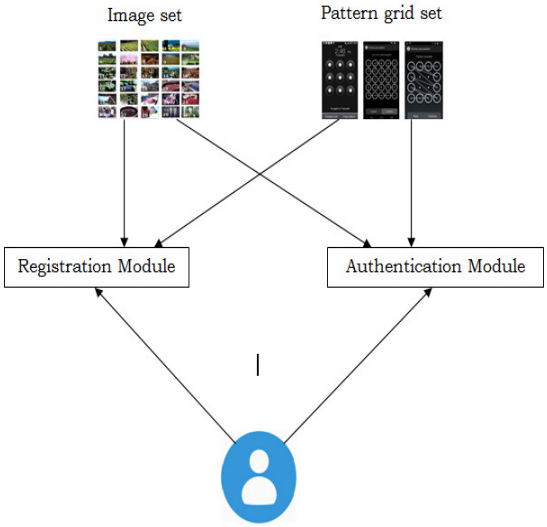

Figure 3.1: Proposed architecture.

In this module, main task is to produce password. User has to select one image from displayed set of images and select type of pattern grid from provided types, than draw a pattern. Every image in image set and pattern grid in pattern grid set has a unique code associated with it. Points in pattern also have unique code. According to ordered selection of image, pattern grid and sequence of pattern point a password string will be produced with concatenation of corresponding unique codes, than it will be encrypted into hash code. This hash code will be stored in database, which will be utilized at the time of authentication.

Following are steps in the registration module:

Step-1: Input user details.

Step-2: Load image set.

Step-3: User selects one image and remembers it. Unique code of image will be stored as key string.

Step-4: Load pattern grid set.

Step-5: User select one pattern grid, its unique code will be concatenated to key string.

Step-6: User draw pattern on grid by selecting pattern points in some sequence. Pattern will be confirmed and unique code of pattern points (in sequence) will be concatenated in key string.
Step-7: A hash will be generated by encrypting key string and that will be stored in database.

3.3 Authentication Module

For authentication, firstly user clicks on login button and enter user name that will be matched with stored user name. If found than user generate password by applying same process as at the time of registration, than generated password will be matched with stored password. If matched than user will be authorized, otherwise not.

Steps for the process are as follows:

Step-1: Input user name.
Step-2: Verify user name, if matched than go to next step.
Step-3: Load image set.
Step-4: User selects same image selected at the time of registrationt. Unique code of image will be stored as key string.
Step-5: Load pattern grid set.
Step-6: User select pattern grid selected at the time of registration, its unique code will be concatenated to key string.
Step-7: User draw pattern on grid by selecting pattern points in some sequence. Pattern will be confirmed and unique code of pattern points (in sequence) will be concatenated in key string.
Step-8: A hash will be generated by encrypting key string and will be matched with stored hash in database. If matched than user will be authorized, otherwise not.

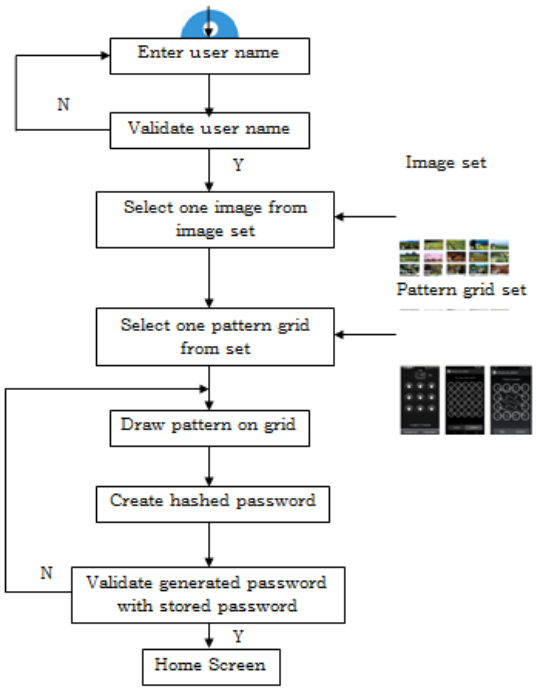

Fig 3.3: Working of authentication module.

IV. RESULTS

5.1 Results & Evaluation

For OTP authentication using proposed method snapshot is shown below:

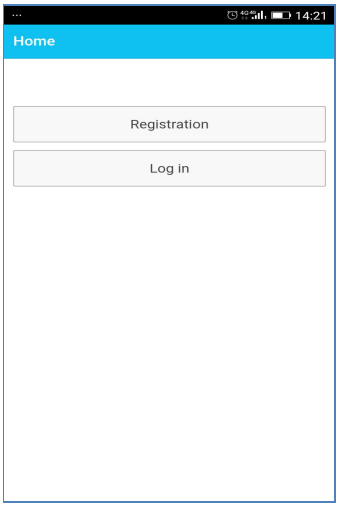

Figure 5.1: Registration Page.

5.2 Evaluation

The proposed model for authentication solves following issues for authentication using multifactor approach. It keeps resistance against the following security hazards and susceptibility:

1. Probing, information leaks
2. Shoulder Surfing
3. Phishing attacks
4. Token theft
5. Replay Attack
6. Eavesdropping
7. Man-in-the-middle attack

Following are points that kept in mind for threat prevention:

- Password must be minimum of 5 points pattern in length which increases password space
- Only test password in its entirety against the stored hashed password which saves from information leaks
- Password will be stored securely in hashed form using Java PBKDF2 hashing implementation, which is difficult to crack

Some important concepts that are kept in mind at the time of developing proposed system:

- Randomness in password generation
- More usability
- More reliability
- Better experience
- Ease in remembering password

Proposed system is also evaluated with existing graphical password authentication system. Graphical password system uses pass point method. In this method user should select an image and select five random points for creating password. The main limitation of this method is to remember these five points on image. It also takes more time to authenticate and more time to input.

In Figure 5.1 From the responses to the questionnaire we noted that users found the Proposed Graphical passwords simplest to remember and more user friendly than Click-Point and Text-based schemes.

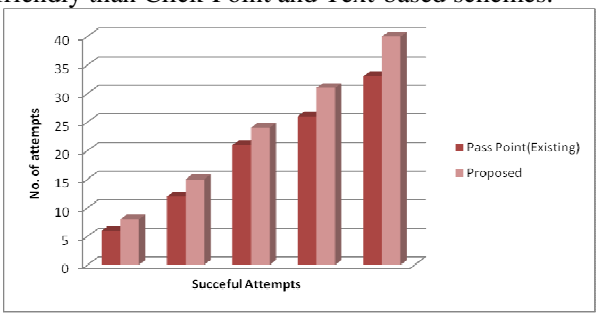

Figure 5.1 Comparisons of Login.

V. REFERENCES

[1]. *M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defences against large-scale online password guessing attacks," IEEE Transaction on Dependable and Secure Computing, vol. 9, no. 1, pp. 128-141, Jan./Feb. 2012.*

[2]. *X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., "A Novel Cued-recall Graphical Password Scheme", In sixth International Conference on Image and Graphics (ICIG), pp. 949-956, 2011.*

[3]. *P. Andriotis, T. Tryfonas, G. Oikonomou and C. Yildiz, "A pilot study on the security of pattern screen-lock methods and soft side channel attacks", Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks - WiSec '13, 2013.*

[4]. *T. Kemp,"The Problems with Passwords", Forbes.com, 2011. [Online]. Available: http://www.forbes.com/sites/tomkemp/2011/07/25/theproblems- with-passwords/. [Accessed: 08- Aug- 2016].*

[5]. *K. Lai, J. Konrad and P. Ishwar,"Towards Gesture-Based User Authentication", 2012 IEEE Ninth International Conference on Advanced Video and Signal-Based Surveillance, 2012.*

[6]. *M Anwar and A Imran, "A comparative study of graphical and alphanumeric passwords for mobile device authentication," In MAICS 2015, pp. 13-18.*

[7]. *Elham Darbanian, Gh. Dastghaiby fard," A Graphical Password against Spyware and Shoulder-surfing Attacks", IEEE 2015.*

[8]. *J.C. Birget, D. Hong, and N.Memon, "Graphical Passwords Based on Robust Discretization," IEEE Transactions on Information Forensics and Security 1(3), 20016, pp.395-399.*

[9]. *Jina Marin Bijoy, Kavitha.V.K, Radhakrishnan.B," A Graphical Password Authentication for Analyzing Legitimate User in Online Social Network and Secure Social Image Repository with Metadata. " IEEE-2017.*

[10]. *Elham Darbanian, Gh. Dastghaiby fard," A Graphical Password Against Spyware and Shoulder-surfing Attacks." IEEE 2015.*

[11]. *Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Cheng," A Shoulder Surfing Resistant Graphical Authentication System" IEEE-2016.*

[12]. *Swaleha Saeed, M Sarosh Umar," PassNeighbor:A Shoulder Surfing Resistant Scheme. "NGCT-2016.*