Research and Development of User Authentication using Graphical Passwords: A Prospective Methodology

Reshma, G. Shivaprasad

Abstract*: Nowadays in information security user authentication is a very important task. In most of the computer, user authentication depends on the alphanumeric username and password. It means text-based password. But, this is not highly secure because of hackers can easily break the password. Brute force attack, dictionary attack, guessing attack etc. these all are some possible attacks on the password. If the user chooses a difficult password to prevent the system from the attackers which is very much harder for the user to remember such a difficult password. So, to resolve this problem introduced a new technique called graphical password authentication. This paper presents a detailed survey of user authentication techniques using a graphical password. It contains basically two type approaches. They are recognition-based and recall-based approaches. This survey discusses the different techniques about Graphical password authentication and their advantages and limitations. The survey provides a roadmap for the development of new graphical authentication scheme.

***Index Terms*: Authentication, CaRP, Cryptography, Cued click, Graphical passwords, Security.**

I. INTRODUCTION

Information security is a very crucial task to protect the data or information. This data authentication is possible by the application of password. The alphanumerical passwords are being used in user authentication since very long time. Nowadays, most of the devices need a password which controls the access to the data. A small, and weak password for the security can be easily hacked by the attackers. If the user has a strong password, then it's harder to remember it often. The normal alphanumeric password has some drawbacks. An article in computer world tells that within 30-second a hacker can guess the 80% text passwords because it is not highly secured. For the high-security, a new technology is invented. Instead of the alphanumeric password, the users can use a graphical password. Psychology studies say that a person can easily remember images in a long time rather than alphabets and numbers. It leads to propose a graphical password. Here, instead of typing an alphanumeric password, the user can just click on the images to authenticate themselves. An authentication method can be classified into mainly three categories.

Revised Manuscript Received on July 22, 2019.

Reshma, Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India.

G. Shivaprasad, Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India..

They are

- Authentication based on Token
- Authentication based on Biometric characteristics
- Authentication based on Knowledge

Key card, bank card and smart cards widely used in token-based authentication. To enhance the security, token-based authentication combines with the knowledge-based authentication. For example, generally, ATM card used with a pin number. Here, ATM card is token-based and pin number is knowledge-based authentication. Fingerprints, face recognition and iris scan etc., are used in biometric-based authentication. This is an expensive authentication technique. Also, the process of identification is slow, but has high-level security technique.

Knowledge-based authentication technique is a widely used authentication method. It includes passwords consisting of both text and picture. There are two main categories of techniques in password schemes involving picture. They are based recognition and based on recall technique. In techniques based on recognition, a user must select some image as his password from a collection of images. Later, the user should identify those images considered as his password for authentication. The recall-based technique can be either pure recall or cued recall. In the pure recall, the user selects some image as his password in the registration stage. Later, he should remember or recall that password without clue or hint. It is highly secure as compared to recognition but also difficulty in remembering the password. In cued recall, user generates a password with the help of hint.

The graphical password technique is used for various purposes. It also has various advantages and disadvantage. This survey answers to the following questions, like

i.Is graphical password more secure than the alphanumeric password?

ii. What are the drawbacks of prevailing graphical password techniques?

This review leads to the development of new authentication techniques that substitute and stronger than authentication techniques based on text password

II. LITERATURE SURVEY

In order to build a better authentication scheme, a new method called Pass-Matrix authentication [1] is proposed. This method contains several phases. In that, first one is user registration phase. In this phase user has to register by giving his name, user id, password etc. After this, system assigns three random images to the user and the user should select the coordinates squares of the image as his/her password. Next, these three pictures are combined and replaced by

hash code. The second phase is user Login. If the user wants to log in to the system, the user first enters his user id and password. If it is valid, the system will send One Time Password (OTP) to the user mail. OTP contains vertical, horizontal sides coordinate points of three images in a random pair. If OTP coordinates match with user choose coordinate at password setting time, then the user can log in. This method protects the system from shoulder surfing attack.

An image authentication system which works on the basis of recognition, Select-to-spawn is proposed in [2]. Here, the user selects one image from a group of images. The image chosen will be further divided into 4*4 invisible grid cells, in a new window. Clicking on any of the grid cells will results into a new image with 16 cells along obscure grid lines. The selection process may continue depending on the user and the selected image becomes the part of the password. In addition, provision for backtracking is also provided.

In reference [3] at registration page user load an image and then chooses several point-of-interest (POI) in that image. Each point-of-interest described by a circle with an associated word which is typed by the user. In next login page for authentication users enter the username, then the system displays the registered image. Next, the user has to correctly choose the POI and also type associated words, it will match then only successfully log in.

Authentication technique on the basis of persuasive cued click points is proposed in [4]. A user is provided with series of images depending on last click. This will pose more challenge for an intruder. Persuasive helps to select a strong password.

A graphical authentication method based on graphical coordinates and time interval between successive clicks is proposed in [5]. The factors affected by this approach are the number of clicks, its order, time intervals between two clicks and tolerance. This approach reduces the possibility of dictionary attack, brute force attack and malware attack. This technique can be employed in ATMs, personal computers, etc.

In [6], an image sequence-based authentication technique is presented. Here, a special purpose computer game is used to generate secret password. Narrative constructs composed of cartoon image sequences is used to generate user specific secret key. The durability of generated password and authentication process during the reconstruction process is validated. This method avoids the possibilities of attacks by strengthening sign in security.

An improved graphical password authentication system is proposed in [7]. It is based on the cued click point system. In this process, the user will upload an image, which could be from the database. During registration, depending on the RGB values of chosen points, a system generated text password is sent to user mail. The user should key-in the password received during login for authentication. This way a second level of security is provided. User will receive an attentive message in the case of any hacking attack.

An authentication scheme based on cued clicks is presented in [8]. This scheme is difficult to break by non-authenticate user. This mainly consists of two stages. They are Registration and log in. In registration phase, a user should mention his details, and select image(s) from the database and choose a point in the image as a cue. Next, a color rating for the displayed colors has to be mentioned by the user. A unique password per session is generated using the color rating. The login phase, contains three stages. In the first stage, i.e., Cued click, user must select the cued point which was selected during registration. In the second stage, i.e., Session password, right color rating should be entered by the user to clear the authentication test. The third stage consists of Text-based graphical password using the circular ring. A circular ring with six equal sectors of different colors is displayed with each sector containing 6 unique characters. A total of 36 characters including 26 alphabets and 0-9 numbers are displayed and user should confirm when the i^{th} pass character of password falls into designated color sector. This technique robust against key logging and shoulder surfing attack.

In [9], Grid-based authentication system using a pattern called Auth-Pattern to authenticate a user is proposed. To register in the system, a user needs to select a unique user name and select Auth-Pattern as password, which is formed by placing images in grid boxes. The order of the images in the grid is a security metric. The system ensures security by generating random and encrypted password for each login.

An authenticate system based on text-based graphical password technique is proposed in [10]. Using this technique, it resists the shoulder surfing attack and minimizes the password image searching time. Here it contains mainly three phases. They are registration, login and change password space. In the registration phase system displays 16 images to the user. The user should select any five images as his password. In the login phase, the user must select those registered images then only he can successfully login to the system. And also, the user can able to change the password as his wish. This project was implemented using the android studio in android application.

Image Recognition based password authentication scheme (Image Pass) is proposed in [11]. This ImagePass process consists of username, selection of graphical password and authorization of graphical password. First, the user name is entered by the user. After the user name is validated, a graphical password is selected by the user. Given a set of images, user clicks on some image to set as a graphical password. For password confirmation user again selects those images from a large set of images. These correct sequences of image entered successfully allow the user to access system. This process requires less effort to recall and prevents password attacks.

In [12], usage of false image in authentication is proposed. This technique mainly consists of two steps. In registration stage, user enters the username and email following which he/she must select some image categories from the list. Then he/she select one image in each category and also need type some alphanumeric character. These are stored in the database as a graphical password. In authentication or login stage, user must enter a username and select an image which is available in each different category. If an image is not available, there is a false image (i.e., not my password) in each category. The user should select a false image to ignore that category and these false images are considered as a real image. This scheme resists the shouldering surfing attack.

Pass Positions- A secure and user-friendly graphical authentication system is proposed in [13]. In graphical password selection, some positions on the image are converted as a graphical password. If the user cannot

select correct absolute position on correct order, it will give rise to problem in the recognition phase. Pass Positions helps in choosing the click point easily. When a user chooses the positions instead of click point by the thick pointer, PassPositions automatically finds the center point of the position and that is a click point. This PassPositions also remember the directions of the current point. Pass Positions is user-friendly, and it will prevent the password space problem.

In [14], the necessity of storing user password in host is eliminated. In this technique, a derivative password is created and stored using the bitmap image uploaded by the user during registration process. During login, the user must upload the image and password. The image will be compared by the system with image uploaded earlier. Next, the system derives password by using the stored image and verifies it against the password entered by the user. This method provides security against key logging, shoulder surfing and hidden camera attacks.

Authentication systems consisting of graphical password-based captcha is proposed in [15]. This contains both the captcha and the graphical password. Captcha as gRaphical Password (CaRP) includes objects like alphanumeric character, similar animals, flowers etc. In CaRP challenge, each time alphabets and similar animals are randomly arranged. It's a challenge to user to choose the correct similar image. CaRP contains schemes based on Recognition and Recognition-recall. In recognition based scheme, it includes Click Text, Animal Grid and Shuffle Text. Recognition-recall scheme includes TextPoints4CR. CaRP provides solution to the dictionary attack, online password guessing attack and relay attacks.

The Graphic-Based Cryptographic Model (GBCM) [16] consists of mainly two-stages- registration and verification. This technique takes the benefits of cued, recognition and pure recall. To enhance the security, operator and scrambling of grid cells is employed in addition to secret key. This will bring in 3-level authentication. During registration, the user must mention the username and then select different images, three times from system displayed images. In secret key selection, user must select operator and multiplier. During verification, user must enter user name and select the registered image on the grid and execute operation using secret key on grid cell ID. Results have shown that GBCM is secure and a user-friendly.

An authentication system based on decoy image of original image is proposed in [17]. In registration phase, a password image is created by choosing one image from the mobile device. The user also chooses its level of complexity. In the login phase, the system displays the original sub-image of the previously chosen image along with the decoy sub-images. To successfully login, the original sub-image must be chosen by the user. This scheme resists the shoulder surfing attack and avoids brute force attack. Also, the scheme is more user-friendly.

An authentication system suitable for online examinations wherein live video of user is captured in real time is proposed in [18]. At registration phase, self-image is captured from the live video and positions on the self-image is selected and cropped and set as a password for the security system. These passwords are used in the online examination system. To login to the system, user must hit on the image location and if it matches, login is successful. After that, user can take the online test. Here authentication technique is applied in the real-time application. It takes less time and reduces the errors, and also it avoids the shoulder surfing attack.

To provide high security to business data, banking details and personal data, a new method using pictorial password and indirect pin injection to the system is proposed in [19]. Login indicator used to protect the original password. In registration phase, user enters the required data and uploads one image. The server splits that image to a grid cell. Then, the user selects one grid cell as pass point. During login, user is provided with a Login Indicator (temporary password. Then, a grid password image with horizontal and vertical bar of alphabet and numeral is displayed to the user. Temporary password will be a combination of alphabet and digit. This method resists the shoulder surfing attack.

In [20], analysis of knowledge-based graphical password authentication systems is presented. Knowledge-based authentication consists of schemes based on recognition and recall. The paper analyzes both the techniques. It was shown that recognition-based techniques are useful in terms of password characteristics, as they are less time consuming and easy to remember. Recall based technique are very effective for security issues.

Various graphical passwords applied in online applications are analyzed in [21]. The CaRP approach, which uses the benefits of both Captcha and graphical password technology is also proposed. In this method proposed a four model. The approach consists of four modules -registration, authentication, verification stage using CaRP and image. In registration, a user fills the required details and uploads an image, then set it as his/her password by clicking on the image. It is saved in the system database. In login, user sends the required details to the system and the system validates the credentials. Next, the verification is done by the CaRP. The system displays the image and user should select correct pixels in that image. In verification using image, user must select the registered image among hundreds of image displayed by the system. This method preserves the user account from brute force attack, dictionary attack, guessing attack, relay attack, and shoulder surfing attack.

In [22], the authors qualitatively analyzed more than 200 graphical passwords for patterns other than the classically reported hotspots. The analysis concluded that significant percentage of passwords fall into a small set of patterns. These patterns can be used to form attack models against graphical passwords. Also, they are useful a thumb rule in future password selection.

A survey of different graphical schemes is presented in [23]. The alphanumeric password has a lot of disadvantages. So, a graphical password authentication is proposed. Here graphical password mechanism applied to mobile devices. It also contains 2 phases. One is the registration phase and another one is the login phase. In registration, user enters the required details and upload one image of their choice and clicks grid point on that image in the sequence. In login, user enters required details and again selects same image grid point. The server checks this data with stored data and if it matches then login is successful. The main advantage of this method is system security is very high. It prevents from dictionary attack and brute force attack. People can easily remember image-based password long time as compared to the text-based password.

In [24], a new algorithm proposed for authentication based on image. Here a grid-based approach is used for authentication. In registration, the user enters his/her details and upload one image. After that, the uploaded image will appear on the page with transparent grid layer. Then, the user selects some grids as his/her password for authentication. To avoid shoulder surfing attack, a Shoulder Surfing Resistant shield (SSR) is developed. In SSR, multiple fake pointers moved randomly on the image. It looks like as the original pointer. It will be confusing for the attacker to break security. The main advantage of this method is a fast mechanism to resistant shoulder surfing attack and also it is user-friendly.
An authentication method for web account access is achieved by recognition based graphical password through watermarking [25]. It is a process of embedding a type of mark in images. This method begins with the registration phase. In that, user has to enter user id and set password by selecting any images from a set of images and then enter corresponding code. This image is embedded with watermark code, which will be extracted by the system and stored in the database. In login phase, user has to enter user id and a password by selecting images and enter corresponding code. The system will extract watermarked data and compares with the user information in the database. If there is a match, user is allowed access the web account. This method provides security against password cracking and shoulder surfing attacks.

III. RESULTS & DISCUSSIONS

Graphical password authentication system contains various password authentication systems. These methods authenticate the user using graphical images in association with other techniques. A comparison of different graphical password schemes proposed by various authors is presented in Table 1.

The techniques discussed in literature differ in various aspects. It may be its technology, algorithms, result etc. In that, some algorithm and some schemes in a paper will be resistant to some attacks while non-resistant to other attacks. Table.2 gives a comparison of different attack resistance.

Table.1 Comparison of Different Password Authentication Systems

Password Authentication System	Security	Cost	Usability	User-friendly	Availability
Token-Based	Less	Less	Easy	Yes	All time
Biometric-Based	High	High	Complex	No	Not all time
Knowledge-Based	Very high	Less	Easy	Yes	All time

Table.2 Comparison of Various Algorithms Based on their Attack Resistance

Reference Paper No.	Algorithm/ Schemes	Resistance to attack	Non-resistance to attack
[1]	Image Segmentation	Guessing attack	Brute force, Dictionary attack
[2]	Select-to-spawn	Brute force attack	-
[4]	Persuasive Cued Click Point	Hotspot, Shoulder surfing attack	-
[5]	Time interval-based approach	Shoulder surfing, Dictionary, Spyware attack	-
[7], [8]	Cued Click-Points	Keylogging, Shoulder surfing attack, Dictionary attack	Brute force attack
[9]	Grid-Based Authentication (GAS)	Dictionary attack, Social engineering attack, Brute force attack	-
[10], [15], [21]	Captcha as Graphical Password	Dictionary attack, relay attack, Shoulder surfing attack	-

Table.2 (Continued).

[12]	Falsification	Shoulder surfing	-
[14]	2-way authentication	Shoulder surfing, Hidden camera, keystroke attack	-
[18], [24]	Graphical own image password scheme	Shoulder surfing	-
[23]	Cued Click	Dictionary attack, Brute force attack	-
[25]	Watermarking copyright technique	Dictionary, Brute force attack, shoulder surfing attack	-

Every authentication scheme has some advantage over other scheme. Each paper helps a researcher to invent or research on a new technique. They have adopted some knowledge from previous papers and also try to resolve the drawbacks. The advantages and disadvantages of various graphical authentication schemes are presented in Table.3

Table.3 Various Graphical Password Authentication Techniques with their Advantages and Disadvantages

Reference paper No.	Algorithm/ Schemes	Advantage	Disadvantage
[1]	Image Segmentation	1) Large password space and user-friendly.	1) Take a long time to register and login phase
[2]	Select-to-spawn	1) Secure, robust, user-friendly 2) High-security space 3) Time efficient	-
[4]	Persuasive Cued Click Point	1) Provide a better password and its space 2) Security success rate is high	-
[5]	Time interval-based approach	1) High Password space 2) Secure, robust user-friendly	-
[7], [8]	Cued Click-Points	1) Very secure, flexible to use. 2) This is very cheap and user-friendly.	-
[9]	Grid-Based Authentication (GAS)	1) Provide high security 2) User-friendly 3) System can be accessed from everywhere	-
[10], [15], [21]	Captcha as Graphical Password	1) Provide high security 2) Application in Desktop and Android smartphone	-

Table.3 (Continued).

[12]	Falsification	1) High security	-
[14]	2-way authentication	1) Provide security against an un-authorized person 2) Robust in password security mechanism	1) Increase the complexity of user authentication 2) User need to remember both text and image passwords
[18], [24]	Graphical own image password scheme	1) More secure, robustness 2) Reduce the task performance time and reduce error rate	-
[23]	Cued Click	1)Provide high security 2) User-friendly	-
[25]	Watermarking copyright technique	1)Provide high security 2) Provide security to web account access	-

IV. CONCLUSION

This paper conducts an exhaustive study of authentication systems based on graphical passwords. Graphical passwords are difficult to crack and hence more secure compared with text password and biometric-based passwords. This authentication system is resistant to more attacks and also most of its techniques are user-friendly. This authentication system reduces the difficulty in remembering a password to a user. It is difficult for hackers to break the graphical password by the traditional attacks like dictionary attack, brute force attack etc. Overall the study shows that the graphical passwords provide a high-level security to authenticate the system.

REFERENCES

1. S. Tabrez and D. J. Sai, Pass-matrix authentication a solution to shoulder surfing attacks with the assistance of graphical password authentication system, In: Intelligent Computing and Control Systems (ICICCS), 2017 International Conference on, IEEE, 2017, 776-781.
2. M. S. Umar and M. Q. Rafiq, Select-to-Spawn: A Novel Recognition-based Graphical User Authentication Scheme, In: Signal Processing, Computing and Control, 2012 IEEE International Conference on, IEEE, 2012, 1-5.
3. A.Almulhem, A graphical password authentication system, In: Internet Security (WorldCIS-2011), London, 2011 World Congress on, IEEE, 2011, 223-225.
4. S. Kaja and D. Gupta, Graphical password scheme using persuasive cued click points, In: Smart Technologies For Smart Nation (SmartTechCon), Bangalore, 2017 International Conference On, IEEE, 2017, 639-643.
5. M. S. Umar, M. Q. Rafiq and J. A. Ansari, Graphical user authentication: A time interval based approach, In: Signal Processing, Computing and Control, Waknaghat Solan, 2012 IEEE International Conference on, IEEE, 2012, 1-6.
6. P. Chellaiah, B. Nair, K. Achuthan, S. Diwakar, Using Theme-based Narrative Construct of Images as Passwords: Implementation and Assessment of Remembered Sequences, International Journal of Online Engineering 13(11) (2017) 77-93.
7. Bhand, V. Desale, S. Shirke and S. P. Shirke, Enhancement of password authentication system using graphical images, In: Information Processing (ICIP), Pune, 2015

International Conference on, IEEE, 2015, 217-219.
8. S. S. S. Ahmed and N. M. Shekokar, Cued click authentication, In: Wireless and Optical Communications Networks (WOCN), Mumbai, 2017 Fourteenth International Conference on, IEEE, 2017,1-5.
9. Gowraj N., Avireddy S., Prabhu S., GAS: A Novel Grid Based Authentication System, In: Quality, Reliability, Security and Robustness in Heterogeneous Networks, QShine, (Singh K., Awasthi A.K.), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, Berlin, Heidelberg, 115, 2013, 578-590.
10. K. Irfan, A. Anas, S. Malik and S. Amir, Text based graphical password system to obscure shoulder surfing, In: Applied Sciences and Technology (IBCAST), 2018 15th International Bhurban Conference on, IEEE, 2018, 422-426.
11. M. Mihajlov, B. Jerman-Blazič and M. Ilievski, ImagePass - Designing graphical authentication for security, In: Next Generation Web Services Practices, 2011 7th International Conference on, IEEE, 2011, 262-267.
12. L. Chee Yeung, B. Lee Weng Wai, C. H. Fung, F. Mughal and V. Iranmanesh, Graphical password: Shoulder-surfing resistant using falsification, In: 9th Malaysian Software Engineering Conference (MySEC), IEEE, 2015, 145-148.
13. G. Yang, PassPositions: A secure and user-friendly graphical password scheme, In: Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on, IEEE, 2017, 1-5.
14. S. Biswas and S. Biswas, Password security system with 2-way authentication, In: Research in Computational Intelligence and Communication Networks (ICRCICN), 2017 Third International Conference on, IEEE, 2017, 349-353.
15. K. Kolekar and M. B. Vaidya, Click and session based — Captcha as graphical password authentication schemes for smart phone and web, In: Information Processing (ICIP), 2015 International Conference on, IEEE, 2015, 669-674.
16. B. K. Alese, A. Akindele, F. M. Dahunsi, A. F. Thompson and T. Adesuyi, A graphic-based cryptographic model for authentication, In: Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), 2017 International Conference On, IEEE, 2017, 1-10.
17. M. R. Albayati and A. H. Lashkari, A New Graphical Password Based on Decoy Image Portions (GP-DIP), In: Mathematics and Computers in Sciences and in Industry, 2014 International Conference on, IEEE, 2014, 295-298.
18. M. Mathapati, T. S. Kumaran, A. K. Kumar and S. V. Kumar, Secure online examination by using graphical own image password scheme, In: Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2017 IEEE International Conference on, IEEE, 2017, 160-164.
19. R. Sudha and M. Shanmuganathan, An Improved Graphical Authentication System to Resist the Shoulder Surfing Attack, In: Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference on, IEEE, 2017, 53-55.
20. G. Agarwal, S. Singh and A. Indian, Analysis of knowledge based graphical password authentication, In: Computer Science & Education (ICCSE), 2011 6th International Conference on, IEEE, 2011, 588-591.
21. P. S. S. Princes and J. Andrews, Analysis of various authentication schemes for passwords using images to enhance network security through online services, In: Information Communication and Embedded Systems (ICICES), 2017 International Conference on, IEEE, 2017, 1-8.
22. J. S. Vorster, R. P. van Heerden and B. Irwin, The pattern-richness of Graphical passwords, In: Information Security for South Africa (ISSA), 2016 Conference on, IEEE, 2016, 69-76.
23. Chiasson S., van Oorschot P.C., Biddle R. Graphical Password Authentication Using Cued Click Points, In: Computer Security – ESORICS, (Biskup J., López J.), Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 4734, 2007, 359-374.
24. Almulhem, A graphical password authentication system, In: Internet Security (WorldCIS-2011), 2011 World Congress on, IEEE, 2011, 223-225.
25. H. Lashkari, A. A. Manaf and M. Masrom, A Secure Recognition Based Graphical Password by Watermarking, In: Computer and Information Technology, 2011 IEEE 11th International Conference on, IEEE, 2011, 164-170.