International Journal of Innovations & Research Analysis (IJIRA)
ISSN : 2583-0295, Impact Factor: 5.449, Volume 02, No. 03(II), July- September, 2022, pp 93-100

STUDY OF SECURITY ENHANCEMENT USING TEXT AND GRAPHICAL PASSWORDS

Dushyant Singh*
Baldev Singh**

ABSTRACT

The growth of the online applications and the concept of online working have increased the growth of data, which is of importance to a person or even for the whole of the organization. As the volume of data is increasing online, its raising the need that the data should protected from unauthorized access. Hackers and intruders, always in the attempt to hack or gain unauthorized access to the data. As a result, password authentication methods are also changing. One way to process the data is by authenticating the users trying to access the information. The authentication method most often used for security is password authentication. Several password-based authentication mechanisms have been proposed to counteract these attacks. Text password-based authentication mechanism is known for selection of a weak and easy to remember passwords. Now, if we compare with the graphical password, they are more interactive for users and less prone to attacks like dictionary attacks, brute force attacks and more. Our study of existing Text pass and word graphical authentication systems shows that several of them compromise their security while making the authentication process simpler, which could lead to perpetration of numerous attacks like shoulder surfing, hidden camera, smudge, and many other attack. Furthermore, a few of them sacrifice performance while targeting security alone. In this paper, we reviews the various research works which are done in the field of the text passwords, graphical password and captcha passwords, and also summarized the work they presented.

Keywords: *Computer Security, Usability, Security Attack, Text Password, Graphical Password.*

Introduction

In the modern age, with increasing data growth of technology, the demand for the data security is also increasing. In order to discuss, the ways to implement the data security, first it is important to get aware about what is data security [1]. Data Security in simple terms we can say that, it is the concept which deals with the security of data from the unauthorized users and hackers. Data security ensures that the corporate information and forestalling information with the help of unapproved access from the user. This results in information shielding from assaults that can encode or obliterate information, for example, ransom ware has the ability to change or ruin the information of a user. Information security guarantees the accessibility of Information to anybody who approaches it. [1] The data security is beneficial in many ways some important benefits are discussed below:

- Protects important data: It doesn't allow leakage of sensitive data. Weather it is bank clients' details or a patients' data; these are critical data that are not supposed to be shared with anyone else. Information security keeps this data precisely without any unknown intervention [2].
- Significant for your standing: Any association which is able to maintain user's private information assists with building certainty among all associates together with clients, and makes them realizes that their information is free from any danger[2]
- Advertising and strategic advantage: By storing private data from unlawful access and divulgence keeps you in front of your rivals. Forestalling any admittance to your future turn of events or development plans is key in keeping up with your upper hand [2].

* Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, Rajasthan, India.
** Department of Computer Science & Engineering, Vivekananda Global University, Jaipur, Rajasthan, India.

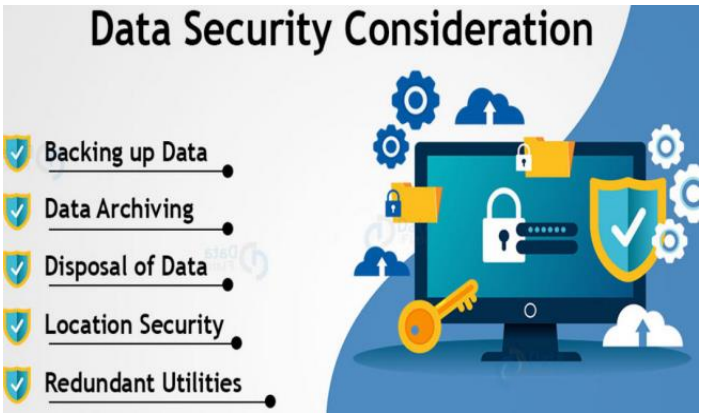

Fig. 1: Data Security Requirements

The fig 1 shows requirement related data security like backing up of data, data archiving and more. The next section, we will focus on how the data security can be implemented. Authentication of users has the important prospective in implementation of data security. Thus, this section is devoted on understanding the concept of authentication.

Data Security Characteristics

- **Authentication of Users**

User authentication is the process by which we authorize the users which are trying to gain the access to the sensitive data. If the user authentication is not up to the mark or not secure then the cyber criminals can gain access to the sensitive data.[3] Intruders accessed Yahoo client records to take contacts, schedules and private messages somewhere in the range of 2012 and 2016. The Equifax information penetrate in 2017 uncovered Visa information of in excess of 147 million purchasers. Without a safe verification measure, any association could be in danger [3].

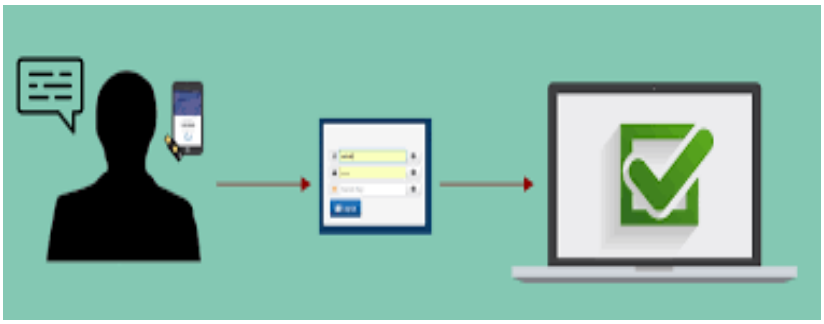

Fig. 2: Authentication of Users

Cybercriminals consistently work on their assaults. Therefore, security groups are confronting a lot of verification related difficulties. This is the reason organizations are beginning to carry out more complex episode reaction methodologies, including validation as a feature of the cycle. [3]

In the process of the authentication, the most common method of verification is password based authentication, in this way of authentication Passwords are the most well-known strategies for confirmation. They can be as a series of letters, numbers, or exceptional characters. For securing the data of a user, he/she is required to create solid passwords that incorporate a mix of every single imaginable choice [3].

- **Password Characteristics**

In the mechanisms, which are knowledge-based authentication, there are the two major characteristics like taking the example of graphical passwords authentication. The usability security should not be seen as a one-dimensional trade-off. However, graphical password schemes seems to be the best way to improve and enhance security systems without any risk and thus, makes it more safer and reliable.

- **Security:** Several aspects regarding user security must be considered in the mind while creating and designing these user authentication techniques and schemes which consists of store passwords and many more characteristics.
- **Theoretical Password Space:** It's an indicator which determine the total number of unused passwords. Equiprobable password distribution is contained in theoretical password space. The number of characters determines the size of theoretical password space which are also available in password lengths for text passwords. The character element determined by the visual elements in the case of graphical passwords. The password length is related to recall sequence or length of recognition.
- **Usability:** PINs and text passwords are the most common forms of security measures for substitute authentication process. Therefore, graphical passwords match the ability and reliability as text passwords. Usability can be assessed qualitatively or
- **Quantitatively:** User satisfaction and insights are some of the characteristic methods which are provided by these security systems while qualitative methods provides effective usability to the users. Efficiency, effectiveness, and memorability are quantitative metrics of password usability, as they are affected by design features.
- **Efficiency:** Efficiency is work on the entry time which required by a user to complete a login task. To facilitate efficient authentication, entry time should be low and must be balanced against security requirements. For easy and efficient felicitation of authentication, balance against security requirements and low amount of entry time should me mandatorily required. But they are too long in the terms of practical usability when compared with graphical passwords.
- **Effectiveness:** Effectiveness is the ability of a user to perform a specific task with the help of a mechanism. In case of password schemes, legitimate users should be able to authenticate without error. The success rate is a common metric for effectiveness for obtaining a correct password which contains no passwords.
- **Easy to Remember:** According to the studies, graphical passwords are considered as memorable over long intervals but the problem related to password interference arises sometimes when user uses similar or multiple graphical passwords. This can be supported by applying prior knowledge rather than asking users to remember their chosen passwords and information.

- **Password Authentication**

Password Based Authentication is the authentication which is performed using the pattern which can be directly the series of characters, some random numbers, or even the graphical password [4].

In order to perform the review-based research on the approaches suggested by various researchers, we have grouped the review analysis in three main categories,

- Text Based Password
- Graphical Passwords

Research Works on Various Authentication Types

In this section, we explore the research work by various researchers in the field of authentication types, in our study we categorized then in text passwords, graphical password and captcha based passwords.

- **Text Passwords**

In the case of text authentication, users either input the string which act as the password, like name of celebrity, date of birth, or even some random combination of the numbers and text [5].

F. Z. Glory et. al suggested the process of authentication of the user using the algorithm which generates the password using the random combination of the words and numbers. Password which generated is based on the dynamic inputs like the favorite name of the novel, the number of grandmother's children, secret dates etc[6].

J. Song et. al. suggested the interested concept of generating the password by writing strokes on the keyboard. They simulate the letter on the keyboard and then either take all the key symbols as password or some of the key symbols as the password pattern[7].Just like in fig. 3 the simulations of the alphabets A or a is shown so the key symbols which are forming the symbols are taken into consideration, i.e. for A it is 4es4rfer , including all symbols which forms A.

Fig. 3: Alphabet Simulation

W. Zheng and C. Jia et. al introduced the simple authentication system with the simple routine passwords which are traditionally used by the users, apart from that authors introduced the concept of counting the blanks in the password. The user with the specification of password, also specifies the number of spaces which are to be given by the user while entering the password. If the specification is 00300100 means that 0 means no space actual character, 3 means then three spaces are required and so on. Thus, in this way using the simple password, more secure way of authentication of user is implemented[8].

M. Taufiq and D. Ogi et. al Introduced the technique One-time password by making using of the One-Way Hash function and also the random permutation functions. The concept involves generation of the various sub-passwords and sum of these sub-password hash was used for the generation of OTP. Authors performed tests on OTP by applying reply attacks but the OTP overcome these attacks[9].

S. I. Yusuf et.al. proposed the dynamic changing password, in this the password is the simple 4 digit password which is entered in the 4 text fields, and the two parameters which control the whole process are the change factor which is required to specify the time period in which the password required to change and change column fields which specifies in which digits the change is performed and the updated password then informed to the registered user. Thus, such a system is more reliable in case an intruder came to know the password, as the next time the password will automatically get changed and the intruder will not able to access the system[10].

Nikita Zujevset.al.. suggested the graphical password based scheme. In this method several images are shown in a single picture At the time of registration. There are many pictures of same type. The picture is chosen as a password by a user in this case. It's also give option of deleting or inserting an image in the given picture. The user will have to recognize his chosen picture and during login time, he/she have to choose the selected picture from multiple images which appears on the screen. The disadvantage of this method is that it stored these passwords in a database, and match the of the symbols hash with the hash of the symbols stored during registration process [11]. When person insert their passwords in a open place, there may be a risk of leakage of sensitive information and passwords by the attacker. Shoulder-surfing attack happen by direct surveillance method, like come across over user shoulder, to get PINs, passwords, and other sensitive information. There are 14 million plaintext passwords, are cracked out of 60 million LinkedIn plaintext passwords.

Furthermore, textual password can be guessed by applying certain methods and algorithms. Key-loggers, Dictionary attack, and social engineering, hidden-camera shoulder surfing, and spyware attacks are common examples of it. An attacker can get a password by direct observation or by recording the authentication session as a result of the drawbacks associated with the use of textual passwords.

- **Graphical Password**

In case of the graphical password, either the graphics or picture is directly users as the password or the graphic organization and selection form the basis for the generation of the password or pattern. Such concept of generation of pattern is interactive and eases to use.

H. Macíaset.al Introduced a PassPoints technique like to Blonder, that requires the use of photos and well-defined tolerance circles. This scheme needs to define an effective area around the enrolment points to carry out successful verification process[12]. . Authors proposed a scheme of in which effective grid must be 19x19 approximately the point of enrolment to decrease login failures but exploit key-space[13].

B. Yao et. al devised the concept of the graphical password, which begin with taking some small circles, these circles are then joined in order to form the topological structure, after that the edges are joined and circles are numbered.

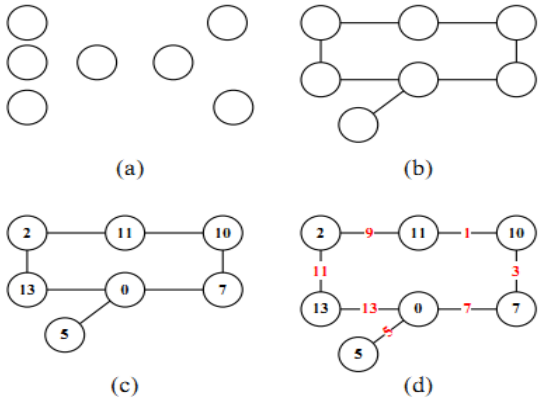

Fig. 4: Topological Concept Password Generation

Then authors have used the concept of difference calculation in between the edges to form the password pattern. The main advantage of their approach is the unpredictability of password and less storage requirement[14]. The fig 4. Shows the procedure for the formation of the password via the use of circle.

Y. Mu et.al suggested the concept of forming the strong graphical password by forming the Hanzi-Graphs. They first directly input Chinese characters and then the Hanzi-graphs for those characters are formed using the small circles and edges. They using the concept of labeling and absolute variation of two vertex labels of the edge, the password pattern is formed. The main advantage is for the Chinese users to get easiergraphical passwords and no down tracking or pattern guessing algorithms available for Hanzi-Graphs[15].

Bilal et. al. proposed a 2-D graphical password method, in which, a user i draw a graphical password during the time of registration or logging in process. The GP is mapped on a textual password and stored in the database and during sign-in process user has to keep in mind the same 2-D graphical password shapes and sketch it in the same shape as drawn in registration time. Authors declare that this method is secure against both dictionary attack, and brute force attack. Author did not concern about computational speed and required login time[16].

G. Yang et. al proposed the PassPositions for graphical passwords. In this the user chooses three points on the screen, if the point is precise using stylus then that pixel position is taken otherwise if user press on screen using finger then center point of area pressed is taken. Authors then used the absolute values of the points selected to form the password pattern. The pattern form on basis of the coordinate of current point is up, down, left or right as compared to the previous point[17].

- **Captcha Based Passwords**

In the CAPTCHA based techniques either the captcha is a randomly generated image or some graphic pattern which needs to organized or arrange in some way. Artificial Intelligence is used for security reasons in this scheme. One problem which occurs with this entire scheme is that they are completely dependent on the present technology. This scheme can overthrow by new method. Other authors also proposed as password recovery for secondary security.

Almuairfi et.al. introduced the concept of arranging the image into the grid pattern and according to the grid pattern , they have mapped the area on the basis of the text password , so when the user click on the particular area , the location or coordinated of that areas are captured and on the basis of the object identified by that coordinate , the password is generated [18].

N. Asmat and H. S. A. Qasim et. al. proposed Conundrum-Pass graphical password. In this author let user to select the picture and divide that picture into grid based on square matrix. Then on the basis of the picture chunks in grid and how they are arranged in grid, the password pattern is formed. Such concept of graphical password helps in overcoming the password guessing attacks. The fig 5 shows how the picture selected is divided in the grid based on square matrix, chosen by the user[20].

H. Sun et.al makes the use of graph structures and number theory for generation of graphical passwords. Authors proposed Topsnut graphical password which was based on graphs with number labelled vertices and edges. These are joined and labelled by users to generate password. The main advantage is that the given set of vertices can be joined in variety of ways to form the graphical structure. [21].

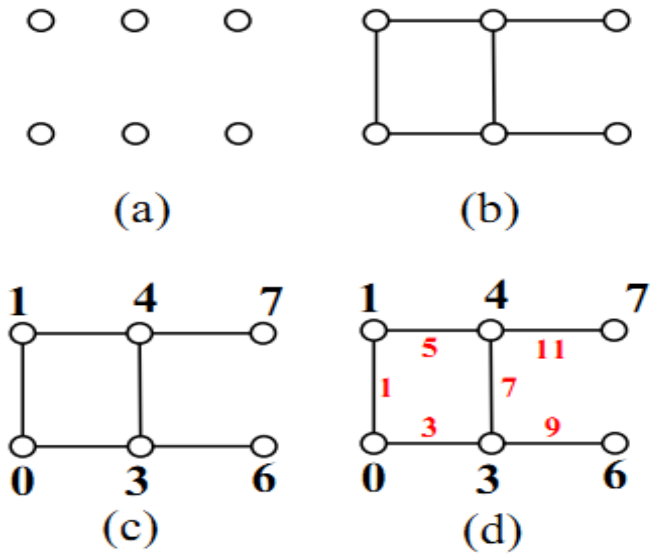

Fig. 5: Topsnut Password Generation

A. Khan and A. G. Chefranov et. al projected combined Click Symbols Alphabet into one entity. The Alphanumeric (A) and the Visual (V) symbols (CS-AV) give the Captcha-based password logic scheme which they have integrated with the recall-based n ×n grid points, in which the user is able to draw the shapes or the various pattern using the meeting point of grid points.

Fig. 6: Captcha Password

This helps in overcoming shoulder surfing attacks on cell phone. The fig 6 shows the proposed concept[22].

S. Sadeghi et. al. proposed Evolutionary Authentication System is being introduced to eliminate Shoulder surfing vulnerability. In this way the graphical password is uploaded by the user and extracted from that particular graphic design. When logged in, this drawing will be displayed along with other designs which can only be recognized by knowing the original image[23].

Conclusion

This paper has reviewed the various concepts proposed by the researchers for the text and graphical based passwords. However, the hackers and intruder's device each day the new way of hacking the data. But still the idea of the graphical passwords is found to be more interactive and more defensive against the password recognition attacks. The graphical password has the option of more versatility as compared to text passwords. Seeing the advantages of graphical password, we will also like to extend our research in this direction

References

1. Kaka, J. G., Ishaq, O. O., & Ojeniyi, J. O. "Recognition-Based Graphical Password Algorithms: A Survey". in 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), pp. 44-51.
2. Devi, G. R., & Kumar, D. A,. "Analytical study on data security for graphical password authentication using drops", Journal of Critical Reviews, vol. 7, pp. 3157-3162.
3. V. Venkateswara Rao and A. S. N. Chakravarthy, "Analysis and bypassing of pattern lock in android Smartphone," in 2017, IEEE International Conference. Res. ICCIC, pp. 1–3.
4. Sonwalkar, M. M. S. "Captcha: Novel approach to secure user", Pramana Researcj Journal., vol. 10, pp. 106-114.
5. A. Khan, &A. G. Chefranov, "A new secure and usable captcha-based graphical password scheme," in 2018, IEEE International Conference on International Symposium on Computer and Information Sciences, Springer, Cham., September, 2018, pp. 150-157.
6. F. Z. Glory, A. Ul Aftab, O. Tremblay-Savard and N. Mohammed, "Strong Password Generation Based On User Inputs," in 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2019, pp. 0416-0423.
7. J. Song, D. Wang, Z. Yun and X. Han, "Alphapwd: A Password Generation Strategy Based on Mnemonic Shape," in IEEE Access, vol. 7, pp. 119052-119059, 2019, doi: 10.1109/ACCESS.2019.2937030.
8. W. Zheng and C. Jia, "Combined PWD: A New Password Authentication Mechanism Using Separators Between Keystrokes," in 2017 13th International Conference on Computational Intelligence and Security (CIS), 2017, pp. 557-560.
9. M. Taufiq and D. Ogi, "Implementing One-Time Password Mutual Authentication Scheme on Sharing Renewed Finite Random Sub-Passwords Using Raspberry Pi as a Room Access Control to Prevent Replay Attack," in 2018 International Conference on Electrical Engineering and Informatics (ICELTICs), 2018, pp. 13-18.
10. S. I. Yusuf, M. M. Boukar, A. Mukhtar and A. D. Yusuf, "User Define Time Based Change Pattern Dynamic Password Authentication Scheme", in 2018 14th International Conference on Electronics Computer and Computation (ICECCO), 2018, pp. 206-212.
11. Nikita Zujevs "Authentication by Graphical Passwords Method 'Hope'", in 2019, International Conference on Computing, Electronics & communication Engineering, 2019, pp. 94-99.
12. Herrera-Macías, J. A., Suárez-Plasencia, L., Legón-Pérez, C. M., Piñeiro-Díaz, L. R., Rojas, O., & Sosa-Gómez, G. "Effectiveness of Some Tests of Spatial Randomness in the Detection of Weak Graphical Passwords in Passpoint", In 2020, International Conference on Computer Science and Health Engineering,2020, pp. 173-183. Springer, Cham.
13. F. Alt, S. Schneegass, A. S. Shirazi, M. Hassib, and A. Bulling, "Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes," in 2015, Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services. ACM, 2015, pp. 316–322.
14. Yao, H. Sun, M. Zhao, J. Li, G. Yan and B. Yao, "On coloring/labeling graphical groups for creating new graphical passwords," in 2017 IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 2017, pp. 1371-1375, doi: 10.1109/ITNEC.2017.8285020.
15. Y. Mu, Y. Sun and B. Yao, "New Techniques for Topological Graphic Passwords Made by Chinese Characters," in 2018- IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC), 2018, pp. 1904-1907.

16. Bilal Eid “A New Password Authentication Mechanism Using 2D Shapes “in 2018- 8th International Conference on Computer Science and Information Technology (CSIT) ISBN: 978-1-5386-4152-1

17. G. Yang, "Pass Positions: A secure and user-friendly graphical password scheme," in 2017- 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), 2017, pp. 1-5.

18. S. Almuairfi, P. Veeraraghavan, and N. Chilamkurti, “A novel image-based implicit password authentication system (ipas) for mobile and non-mobile devices,” Mathematical and Computer Modelling, vol. 58, no. 1, pp. 108–116, 2013.

19. P. C. van Oorschot and J. Thorpe, “Exploiting predictability in click-based graphical passwords,” Journal of Computer Security, vol. 19, no. 4, pp. 669–702, 2011.

20. N. Asmat and H. S. A. Qasim, "Conundrum-Pass: A New Graphical Password Approach," 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE), 2019, pp. 282-287.

21. H. Sun, X. Zhang and B. Yao, "Construction of New Graphical Passwords with Graceful-Type Labellings on Trees," 2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2018, pp. 1491-1494.

22. A. Khan and A. G. Chefranov, "A Captcha-Based Graphical Password with Strong Password Space and Usability Study," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, pp. 1-6.

23. Sadeghi, S., Manochehri, K., & Jahanshahi, M. (2021). Use of Digital Image Watermarking to Enhance the Security of Graphical Password Authentication. Journal of Algorithms and Computation, 53(1), 165-180.

□❍□