International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 07 | July -2020 ISSN: 2582-3930

Graphical Password System To Avoid Shoulder Surfing Attacks

Mrs Chaya P[1], Preeya D[2], Rashmi K A[3], Reshma S [4], Sandhya G S Ramu[5]

[1] *Mrs Chaya P, Assistant Professor, Information Science and Engineering, GSSSIETW*
[2]*Preeya D,Information Science and Engineering, GSSSIETW*
[3]*Rashmi K A,Information Science and Engineering, GSSSIETW*
[4]*Reshma S,Information Science and Engineering, GSSSIETW*
[5]*Sandhya G S Ramu,Information Science and Engineering, GSSSIETW*

Abstract -Passwords provide security mechanism for authentication and protection against access to resources. The traditional password schemes which are textual passwords are a string of alpha-numeric characters (which include alphabets, numbers and special characters). These text-based passwords are most likely and widely used in present. But these are not fully secured and face security issues by using textual passwords. In our paper we have considered these and tried to overcome by implementing Graphical Password System. Graphical password allow users to remember images/pictures instead of string of characters which is helpful for them to memorize the password easily. Graphical Password Scheme are likely vulnerable to shoulder surfing attacks, for which we have implemented Advanced Encryption Standard(AES) Rijndael algorithm for high level authentication.

Key Words **:**TraditionalPasswords, Graphical Password, Authentication, Shoulder Surfing, Advanced Encryption Standard(AES) Rijndael algorithm,

1.INTRODUCTION

User authentication is the process of verifying a user's identity and determining whether the user should be authorized to access information or not. Information Security and Authentication is now an important in the world. Traditional Password schemes such as textual passwords are most likely to be used mechanism for authentication. But these are vulnerable to a dictionary, brute force, shoulder surfing attacks and guessing attacks. Although biometrics- based authentication are considered very secure, but they are too expensive and not reliable.

These issues can be resolved by using Graphical Password, which is more secure, reliable technique for authentication. This technique i.e., Graphical passwords allow users to remember images or graphical pictures instead of string of characters which helps users to remember and memorize the passwords easily. Graphical password system is more recognizable and has less cognitive load.

In this paper, however, we focus on graphical user authentication which is utilizing images/pictures as passwords. Graphical password authentication schemes have been proposed as another alternative to the traditional password authentication schemes. It is partially motivated by the fact that humans are more capable of remembering pictures or images better than texts. Graphical pictures or images are generally much easier to be recognized than textual character. But these are also vulnerable to the shoulder surfing attacks. To overcome shoulder surfing we have implemented the encryption algorithm which is Advanced Encryption Standard (AES) Rijndael Algorithm which ensures high level authentication.

1.1 Textual Authentication

The traditional authentication method is to use alphanumerical username and passwords. Textual based password authentication scheme are most widely and likely used method because it is simple, inexpensive compared to other techniques and easy to implement. But these are more vulnerable to attacks such as dictionary, brute force, shoulder surfing attacks and guessing attacks. The main drawback of passwords are (1) Password should be remembered easily, and user authentication protocol should be executable quickly. (2) Passwords should be secure, i.e., they should have high security. To address the problems of textual passwords, Graphical passwords are introduced.

1.2 Graphical Password

A graphical password is an authentication system that works by the user select from images, implemented in a graphical user interface (GUI). Graphical passwords may be an alternative to text-based password. The technique was first described by Greg Blonder [G. Blonder, Graphical Passwords, United States Patent 5559961 (1996)], is to let the user click (with a mouse or a stylus) on a few regions in an image that appears on the screen. To log in, the user has to click in the same regions again. Our design allows the use of random images in grid form. Moreover, we let users choose any images; which are easier to remember. However, allowing the user to choose images from grids which are inclined to shoulder surfing assaults. So we have included Encryption Decryption technique by using Advanced Encryption

Standard (AES) Rijndael Algorithm which will reduce shoulder surfing. For passwords, human aspects (usability of the system, learnability and long-term memorability of the passwords, avoidance of unsafe practices, and user satisfaction) are of crucial importance.

The main objective of the project are as follows:

- To provide the graphical passwords and will reduce the chances to forget the password.
- To protect from shoulder surfing attack by encrypting and decrypting the graphical password using Advanced Encryption Standard (AES) Rijndael algorithm.
- The correct login rate for multiple images with movable frame is 15% more than text password schemes thus a better solution to protect shoulder surfing.

2. LITERATURE REVIEW

Text-based passwords have a vital importance to provide access control to privileged entities. However, text-based authentication systems have some deficiencies. While users prefer faster and easier authentication processes, security experts want to apply stricter and more compulsive rules. Graphic passwords can be a good option for meeting the deficit of text based passwords. [1] This paper, they conducted a comprehensive survey of the existing graphical password techniques. They classified the password techniques into two categories: recognition-based and recall-based approaches and they discuss the strengths and limitations of each method and point out the future research directions in this area. [2] Directional Based Graphical Authentication is proved to be shoulder- surfing-proof authentication system because user will not click to their images directly, users clicked into image that satisfies direction of their images. [3] Basak Bilgi , Bulent Tugrul proposed an graphical authentication method which is a solution to the problem of shoulder surfing. Hybrid images are used to provide two different impression depending on the distance instead of regular images.[4] R. Sudha, M. Shanmuganathan proposed improved graphical authentication application system resists the shoulder surfing attacks. Secures the bank account from hackers by blocking, when the mobile was lost.

3. METHODOLOGY

For implementing the Graphical Password System we have taken the scenario of Banking sector. We have created a Graphical user interface for Banking sector, in which we have used Graphical password technique. Banking sector needs high level authentication for the process of verifying a user's identity. We can Also use our system in other high security needed sectors such as, for military sectors, government sectors etc.

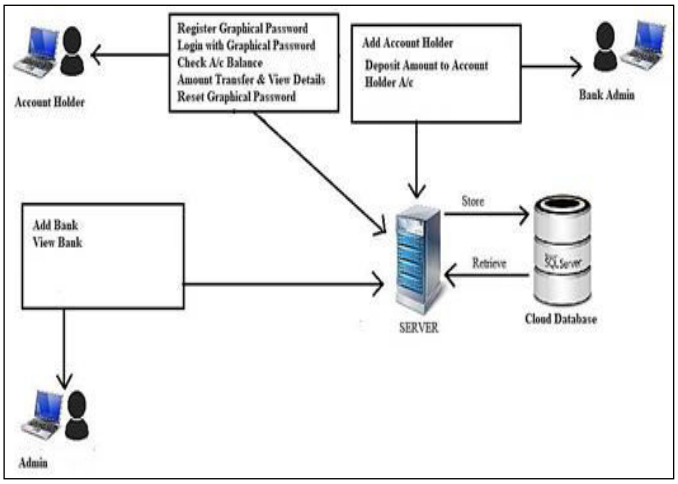

Fig -1: System Architecture of Graphical Password System

The above figure shows the architecture of Graphical Password System Using Movable Frames, here we have three modules namely admin, Bank admin and Account holder. New user can register by providing user details that are stored in database. Later system generates image grid from which the user has to select the password. Selected images are stored in database. The authenticated user can login to the application by entering the graphical password selected by him/her previously. The image grid in the login page will be moving horizontally using movable frame schema.

3.1 Proposed System

The proposed system includes the Graphical interface for identification and authentication by displaying a grid of graphical images. Detailed working of the system is explained using registration, login phase and change password phase. In the Registration phase, user must first enter the account number and password which is been set to the users mail once beingaddedbythebankadmin.Laterthescreendisplaysagridwhere 9randomGraphicalimages areshowntotheuserinwhichhe must chooseany5imagestosetagraphicalpassword.Oncethe Graphical password is set, the selected images will be identified by the id's and are comma separated. This id is encrypted and stored in the database using AES Rijndael Algorithm to give multi-levelsecurity.

In the Login phase user must first enter the account number and password. Once its done it will be directed to a page which asks the Access key which is sent to user's mail once the 5 selected images are encrypted. Once access key is entered graphical image's id will be decrypted and user must login by selecting the correct 5 images chosen during registration phase.

There will be 3 attempts to get the access key or graphical password correct. Once it exceeds 3 attempts the account will be blocked and the user will be blocked to perform any transaction.Hecanresetpasswordifhehasforgotthepasswordbygi

vingtheaccountnumberand password and the steps are same as in registrationphase.

System Modules:

- **Admin**

Login: There will be unique id and password for the Admin through which they can login and perform following functions.

Manage Bank: Admin have option to add bank details

- **Bank Admin**

Login: There will be unique id and password for the Bank Admin through which they can login and perform following functions.

Manage Account Holder: Bank Admin have option to add Account holder details, provide unique Account No and Password to Account holder.

Manage Account Holder Amount Deposit: Bank Admin have option to deposit amount to the account of Account holder.

- **Account Holder**

Register Graphical Password: Account Holder Registers graphical password by selecting 5 images out of 9 images display, inputs account number to set images as graphical password. Selected Graphical Password images Id's are encrypted using AES Rijndeal algorithm and generatesAccesskey,whichwillbe mailedtotheaccountholderandstoredincloudDBfor securepurpose.

Login: Account holder should enter the unique Account No. and Password, which will be redirected to graphical password page where he/she has to select the Graphical Password images I.e., 5 registered graphical password images out of 9 images by inputting the Access key. Based on Access key decryption takes place and the graphical password images Id's selected in login phase will be compared with graphical password images. If both are same thennavigatetoaccountholderhomepage, elsedisplayinvalidgraphicalpassword.Account holder are provided 3 times to choose right graphical password images. If account holder failstochoosegraphicalpasswordimagesin3chances,thengraphi calpasswordoptionwill be blocked. Account holder have to Reset Graphical password by choosing 5 new set of graphical password images to get unblock oractive.

Reset Graphical Password: Account holder have option to reset graphical password by selecting 5 images out of 9 images display, input account no. to set images as graphical password.SelectedGraphicalPasswordimagesId'sareencrypted andgeneratesAccessKey which will be mailed to the account holder and will be updated to cloud DB for secure purpose.

Check Account Balance: Account Holder can view the details of the deposit and can check the details of the account balance.

*AmountTransfer:*AccountHolderhaveoptiontotransferamountt ootherregisteredaccount holder in the application, also have option to view transfer amountdetails.

4. CONCLUSIONS

In graphical password schemes, pictures are utilized rather than alphanumeric characters. Client must recollect a lot of pictures to effectively login. The conspicuous downside of such a plan is having an enormous word reference of such one of a kind pictures put away in a memory however on the off chance that the quantity of potential pictures is adequately enormous, the conceivable secret phrase space of a graphical secret word apparently offer better protection from lexicon assaults.

Password authentication system will encourage less predictable and strong password while maintaining memorability and security. The correct login rate for multiple images with movable frame is 15% more than text password schemes thus a better solution to protect shoulder surfing. Proposed system avoids the problem with remembering random strings of characters. User can easily remember images better than text-based password. Our current system is highly secure and hard to guess the graphical password.

REFERENCES

[1] Suo, Xiaoyuan, Ying Zhu, and G. Scott Owen. "Graphical passwords: A survey." Computer security applications conference, 21st annual. IEEE, 2005.

[2] Noor Ashitah Abu Othman, Muhammad Akmal Abdul Rahman, Anis Shobirin Abdullah Sani, Fakariah Hani Mohd Ali " Directional Based Graphical Authentication Method with Shoulder Surfing Resistant", IEEE, 2018

[3] Basak Bilgi, Bulent Tugrul ,"A Shoulder- Surfing Resistant Graphical Authentication Method", IEEE, 2018.

[4] R. Sudha, M. Shanmuganathan, "An Improved Graphical Authentication System to Resist the Shoulder Surfing Attack",IEEE,2018

[5] Sobrado, Leonardo, and Jean-Camille Birget. "Graphical passwords."The Rutgers Scholar, an electronic Bulletin for undergraduate research 2002.

[6] Khandelwal, Ankesh, Shashank Singh, and Niraj Satnalika. "User Authentication by Secured Graphical Password Implementation. "International Journal of Computer Applications pp 115- 120, 2010.

[7] Ugochukwu, Ejike Ekeke Kingsley, and Yusmadi Yah Jusoh. "A review on the graphical user authentication algorithm: recognition-based and recall-based."

International Journal of Information Processing and Management 4.3 pp 238-252., 2013.

[8] Shah, Amish, et al. "Shoulder-surfing Resistant Graphical Password System." Procedia Computer Science 45, 2015.

[9] Dhamija, Rachna, and Adrian Perrig. "Deja Vu-A User Study: Using Images for Authentication." USENIX Security Symposium. Vol. 9.2000

[10] K. Gilhooly, “Biometrics: Getting Back to Business”, in Computerworld, (May, 2005).

[11] R. N. Shepard, "Recognition memory for words, sentences, and pictures," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp. 156-163, (1967).

[12] Real User Corporation, Passfaces TM “http//:www.realuser.com,” Accessed on June 2007.

[13] Jansen, Wayne, et al. "Picture password: a visual login technique for mobile devices." NIST Interagency/Internal Report (NISTIR)-7030 2003.

[14] Takada, Tetsuji, Takehito Onuki, and Hideki Koike. "Awase-e: Recognition-based image authentication scheme using users' personal photographs." Innovations in Information Technology, 2006. IEEE, 2006.

[15] Davis, Darren, Fabian Monrose, and Michael K. Reiter. "On User Choice in Graphical Password Schemes." USENIX Security Symposium. Vol. 13. 2004.

[16] Man, Shushuang, Dawei Hong, and Manton M. Matthews. "A ShoulderSurfing Resistant Graphical Password Scheme-WIW." Security and Management. 2003.

[17] N. Wakabayashi, M. Kuriyama and A. Kanai, "Personal authentication method against shoulder-surfing attacks for smartphone," 2017 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas.

[18] Xingjie Yu, Zhan Wang, Yingjiu Li, Liang Li, Wen Tao Zhu, Li Song, EvoPass: Evolvable graphical password against shoulder-surfing attacks, Computers & Security, Volume 70, Pages 179-198, 2017.

[19] Mrs. Aakansha S. Gokhale, Vijaya S. Waghmare, The Shoulder Surfing Resistant Graphical Password Authentication Technique, Procedia Computer Science, Volume 79, Pages 490-498, 2016.

[20] Shah, Amish, et al. "Shoulder-surfing Resistant Graphical Password System." Procedia Computer Science 45, 2015.