

Three Level Password Authentication System

¹Prof. Veena Katankar, ²Pranjali Fating, ³Apoorva Mamarde, ⁴Mansi Lokhande, ⁵Kritika Agrawal

Abstract— Authentication is one of the most important security services provided to the system by the different authentication schemes or algorithms which must be provided so that only authorized persons can have the right to use or handle that system and data related to that information system securely. Techniques used include text-based, image-based as well as graphical-based. Despite these, no single mechanism is efficient and effective to provide adequate security for computing resources such as programs, files, messages, printers, the internet, etc. A 3 – level authentication is proposed in this paper that is more confidential for ensuring adequate security. The 3-level password authentication system is an authentication scheme that combines the benefits of authentication schemes in existence to form the 3-levels of security. The proposed system in this paper would provide a more secure authentication technique than the existing one, overcome the drawbacks and limitations of previously existing systems (such as textual passwords, graphical passwords. etc.) and combine more than one authentication technique.

Keywords— Text-Based Password, Authentication, Color Code Detection, Bot Attack Recognition, Graphical Password

I. INTRODUCTION

The paper is an authentication system that validates users for accessing the system only when they have input the correct password. The project involves three levels of user authentication. It contains three logins having three different kinds of a password system. The password difficulty increases with each level. The project comprises text passwords i.e. passphrase, image-based passwords, and graphical passwords for the three levels respectively. The paper is based on the verification and validation methodology for user authentication. The proposed system verifies the legitimate user if he or she claims to be. The security system

has three levels to crack through before a successful login. Authentication is the proper validation and rights management of the user for accessing the resources of any information system. It is now beyond any doubt that user authentication is the most critical element in the field of Information Security. Authentication is one of the most important security services provided to systems by the different authentication schemes or algorithms. To protect any system, authentication must be provided so that only authorized persons can have the right to use or handle that system and data related to that system securely. Authentication processes may vary from simple password-based authentication systems too costly and computation intensified authentication systems. One of the approaches normally in use is the common authentication procedure in which a user needs only a user name and password, in other to make use of an authentication and authorization system in which every client has the right to access the data and applications which are only appropriate to his or her job. A password is a secret word or phrase that gives users access to computer resources such as programs, files, messages, printers, internet, etc. Passwords are more than just a key. They ensure our privacy, keeping our sensitive information secure. They also enforce nonrepudiation, preventing us from later rejecting the validity of transactions authenticated with our passwords. Our username identifies us and the password validates us. Often, individuals tend to use key that can easily be remembered.

The aim of this paper is to evaluate the effectiveness of using a three-level authentication system to improve the security system. The objectives are as follows:

1. To design implementation of password authentication that gives the highest security in authenticating users.
2. To implement the applications/system that is more user-friendly.
3. To test and evaluate the authentication scheme in preventing unauthorized access.
4. The main objective of the three-level security system is to provide advanced security to the web applications, prevent unauthorized access, and make the applications more user-friendly.

Manuscript Received April 25, 2022; Revised 15 May, 2022 and Published on June 08, 2022

Prof. Veena Katankar, Department of Computer Engineering, Suryodaya College of Engineering and Technology, RTMNU Nagpur, Maharashtra, India. Mail Id:

Pranjali Fating, Apoorva Mamarde, Mansi Lokhande, Kritika Agrawale, Department of Computer Engineering, Suryodaya College of Engineering and Technology, RTMNU Nagpur, Maharashtra, India. Mail Id: pranjaliating35@gmail.com, appumamarde@gmail.com, mansilokhande14@gmail.com, agrawalkritika055@gmail.com

II. RELATED WORK

Ahmad Almulhem et al. have proposed an alternate method for the text passwords. They suggested replacing text passwords with graphical passwords, which makes passwords more memorable and easier for people to use. In addition, the graphical password is more secure.

Ahmet Emir et al. proposed the confirmation framework Pass Points Graphical Password, which comprises a succession of snap focuses (express 5 to 8) that the client picks in a picture. The picture is shown on the screen by the framework.

A few papers were inspected and observed unique views to execute the feasible method for encryption and unscrambling calculation for safety.

In 2018 Aparna M and Anjusree CM proposed a “Three-level security system using Image-based Authentication”. This paper introduces OTP (one-time password) concept password as their third level. They recommended using image choice Authentication where the user can select a particular image from given options as a second level. The author has proposed different types of Authentication systems, which are secured highly. In June, 2020 Rahul Chourasia proposed “Three-level password authentication system”. This paper proposed a trading approach for textual content passwords. They recommended changing textual content passwords with the aid of using graphical passwords, which makes easy to remember and less difficult for humans to use. In addition, the graphical password is greater security.

In December 2022 Gouri Sankar Mishra, Pradeep Kumar Mishra and Parma Nand proposed “User Authentication:

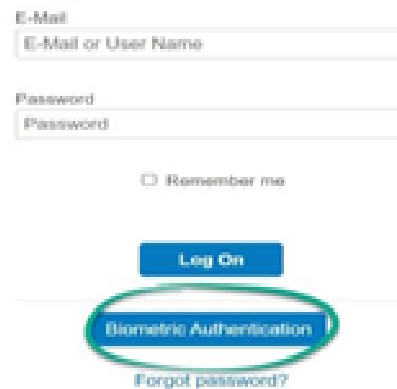
A Three-level password Authentication Mechanism”. This paper is based on the Users Authentication for Verification and Validation methodology. They proposed a method where the system verifies user if he or she claims to be by using Three-level password verification.

III. LEVELS PASSWORD AUTHENTICATION SYSTEM

A. First Level

The first level is a conventional password system i.e. text-based password or a passphrase. Users would have to set a text password initially based on some specifications. Text-Based Password the first phase of this application is basic authentication with validations for fields and length. Basic authentication includes entering a user id and user password, which is text-based authentication. This is the most traditional approach in use for the last 3 to 4 decades. The reason for this is that it is very easy to implement, cost-effective, simple, and familiar to almost everyone. Text password contains case-sensitive alphabet characters, numbers, and special symbols too. Combining this becomes a secret pass code for every user, which he or she should never share to anyone.

Log On

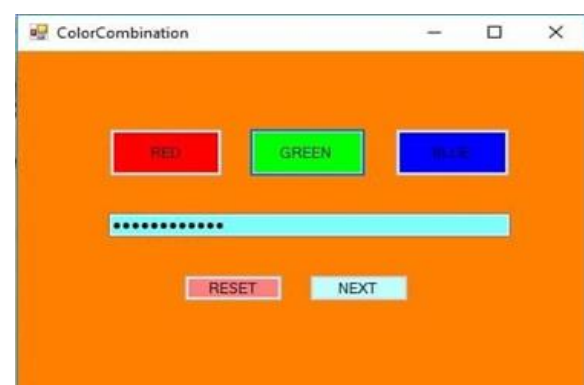


The image shows a web-based login form titled "Log On". It contains two input fields: "E-Mail" with a placeholder "E-Mail or User Name" and "Password" with a placeholder "Password". Below the password field is a checkbox labeled "Remember me". A blue "Log On" button is positioned below the checkbox. A green oval highlights the "Log On" button and a link labeled "Forgot password?" below it.

Figure 1: Text Based

B. Second Level

The second level is an image-based password where users have to set passwords based on some color combinations through RGB button combinations. : Image-Based Password The second level of this project Color Code Detection In this level user needs to enter the color code that was set during the time of registration. The password. There are a total of five colors and the user needs to pick any three colors in a particular sequence. Then during the time of logging in user will have to enter the same code and in the same sequence. The order of colors will always appear in random order, so the user must remember the code, hit and try will simply not work as there are a total of 120 combinations of color in this security check. Where the user will have only one chance to fill the correct order, the moment pattern mismatches the user will send it back to login. The overall procedure of authentication is based upon the textual password verification in the first level. This verification is static in nature. After successful verification, the users are asked to draw a pattern that is a dynamic one.



The image shows a software window titled "ColorCombination". It has an orange background. At the top, there are three colored buttons: "RED" (red), "GREEN" (green), and "BLUE" (blue). Below these buttons is a light blue horizontal bar with a series of dots, representing a password input field. At the bottom, there are two buttons: "RESET" (pink) and "NEXT" (light blue).

Figure 2: image-based password Authentication

C. Third Level

The third level is a graphical password method where users: Graphical-Based Password: In this level, the user can upload any image related to itself or its own image and that image will be cropped into 9 small images while logging into the final level User needs to arrange all 9 combinations of images by selecting each image or can drag and drop it, after arranging user can finally login into the system. The third level is an image-based password where users can upload their desired image into the system and then create a password by segmenting it and assigning them a block During login process the system will automatically disperse the image segmentations and users have to select the block.



Figure 3: Graphical Password Method

CONCLUSION

The three-level security approach applied for a framework makes it exceptionally secure alongside being easier to understand. It has been set up to increase security, prevent password cracking and identify theft, and also focuses on a better user-friendly interface. The goal is to provide the importance of user authentication and how it can be used to protect users during the login process. Authentication is the proper validation and rights management of the user for accessing the resources of any information system and is the most critical element in the field of Information Security. Yet, no single mechanism is efficient and effective to provide adequate security for computing resources such as programs,

files, messages, printers, the internet, etc. On that note, the paper proposes a 3 - level authentication technique that employs textual passwords, pattern lock, and biometrics, hereby combining the benefit of the three techniques/methods to enhance the security of computer resources. The three-level authentication system had been applied to the above system which makes it highly secure along with more user-friendly. This system will help with Man-in-the-middle attacks and Brute-force attacks on the user's side. A three-level security system is a time-consuming approach since the user needs to enter details carefully for all three security levels and at last, the user can add any image for its final level Authentications.

REFERENCES

- [1] A. A. Hassan (2005): Database security and auditing, protecting data integrity and accessibility. 1st edition, course technology
- [2] A. T. Akinwale and F. T. Ibharalu (2009): Password authentication scheme with secured log in interface. Annals. Computer Science series 7th tome 2nd Fasc.
- [3] Akazue M. 1 and Efozia, N. F. (2010): A Review Of Biometric Technique For Securing Corporate Stored Data
- [4] Bob Savage (2012): 'Science and Industry: Working Together for Economic Recovery', <http://www.siliconrepublic.com/cloud/item/24428-cloud-mostsignificant-tranlast> retrieved 02.08.2012.
- [5] Brunelli R.: Template Matching Technique in Computer Vision: Theory and practice. <http://www.enterstageright.com> (2009). Retrieved Sept. 2009.
- [6] Grover Aman and Narang Winnie (2012): 4-D Password: Strengthening the Authentication Scene. International Journal of Scientific & Engineering Research, Volume 3, Issue 10, October- 2012.
- [7] H.-W. Kim, J.-H. Kim, D. J. Ko, E.-H. Song, and Y.-S. Jeong, (2013): "8- Way lock for personal privacy of smart devices based on human-centric," in Proceedings of the 40th Conference of the KIPS, vol. 20, pp. 735-737, KIPS, November 2013.
- [8] Himika Parmar, Nancy Nainan and Sumaiya Thaseen (2012): Generation of secure one-time
- [9] Jae Dong Lee, Young-Sik Jeong, and Jong Hyuk Park (2014): A Rhythm-Based Authentication Scheme for Smart Media Devices. Hindawi Publishing Corporation, Scientific World Journal K. Gilhooly (2005), "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.
- [10] Lalu Varghese, Nadiya Mathew, Sumy Saju, Vishnu K Prasad (2014): 3-Level Password Authentication System. International Journal of Recent Development in Engineering and Technology, Volume 2, Issue 4, April 2014) 9