World Journal of Engineering Research and Technology
WJERT
www.wjert.org SJIF Impact Factor: 5.924

THREE-LEVEL IMAGE PASSWORD AUTHENTICATION SYSTEM

***P. L. Narayanan, R. Sathish Kumar, M. Dilip Kumar and P. Chandrasekar**

Dr. M.G.R. Educational and Research Institute, University, Chennai, India.

Article Received on 12/03/2022 Article Revised on 02/04/2022 Article Accepted on 22/04/2022

***Corresponding Author**
P. L. Narayanan
Dr. M.G.R. Educational and Research Institute, University, Chennai, India.

ABSTRACT

A security breach can put national secret data, as well as the private information of an organization or a person, at risk. Text-based passwords are the most common type of security password. However, these passwords are readily cracked, and one's personal information might fall into the wrong hands. Security issues connected to logins and accesses have become a key concern as cyber-crime has increased. Furthermore, just a single security authentication method is insufficient to keep you safe from cyber-attacks. As a result, in order to improve security, we created a Three-Level Password Authentication system that ensures that only authorized users have access to the system or data. This system has three levels of logins, each with three separate password methods. A text-based password, image-based segmentation password, and graphical password are included in the project. With each level, the password difficulty rises, making access more secure. This PHP-based Three Level Authentication System will assist customers to protect their data from hackers and cyber dangers in this way. Users will be requested to create three-level passwords upon user registration in this system for security reasons. The first level is the text-based password system, the second level is the image-based password system, and the third level is the graphical password technique. Users must log in to check the security of the system by submitting a three-level password authentication. As users begin to submit passwords, the first level will authenticate the user by matching the data recorded in the database upon registration, and the second and third levels will authenticate the password supplied by the user, respectively.

KEYWORDS: Three-Level, Graphical Authentication, Text-Based Authentication, Image

Authentication, PHP.

INTRODUCTION

The project is built on a user authentication verification and validation approach. If a user claims to be authentic, the suggested system checks that assertion. Before a successful login, the security system must be cracked through three layers. There have already been several password schemes that appear to have failed due to bot assaults. As a result, this system concentrates mostly on bot assaults. One of the three stages is entirely dedicated to bot assaults in order to avoid system hacking via bots. As a result, the suggested system is built to provide the highest level of user authentication security.

The login process is divided into three stages. With each step, the login parameters get more complex. The user must successfully complete all steps in order to log into the system for the first time. If the user makes a mistake in the second or third step, the user will be immediately sent to the first phase. New users may create an account and choose their own password and color scheme. The three phases are simple login id and password-based security, which is basic authentication. After that, the system will move on to the second phase, bot attack detection, where the system will determine whether you are a real human user or a bot and if you pass, the third and final phase, color-code-based password authentication, will be implemented. The chances of breaking into the application are next to none because it includes three distinct phases. The system cannot be broken into by a simple bot assault or a fictitious user.

The new methodology combines the advantages of both technologies by applying the new technology to older systems. The suggested system has three levels of security: textual password, bot-attack recognition, and color code detection. Previously, textual and graphical passwords were used separately, but in the suggested method, they were integrated to reduce the security hazard. Furthermore, the bot attack identification module protects against programmed assaults.

LITERATURE SURVEY

[1] User Authentication: A Three-Level Password Authentication System (2020)

Gouri Shankar Mishra, Pradeep Kumar Mishra, Rani Astya, Amrita

Simple basic authentication using text-based user id and password. Now With the benefit of having three-level password authentication, we can check a bot and user security code so we cover all three major fields of security. However, time complexity can be high but security is also high and there are regions where you can compromise with a little bit of time complexity but not at all with data security.

[2] Three Level Password Authentication (2020)

Aachal Khadke, Anushka Dhanve, Ashwini Bansode, Prof. S.N. Shitole

To implement a modern system of password authentication, we will design the system with high security. Then levels in the system for authentication will be tough to crack. We use a one-time password authentication process in one of the levels.

[3] Multi-level Graphical Password Authentication Scheme for Cloud (2019)

Vijayakumari Rodda, Gangadhara Rao Kancherla, Basaveswara Rao Bobba

Cloud computing is the most happening thing in the present digital era. In this context, a strong and secure authentication mechanism is direly needed to protect cloud resources from malicious users. The method proposed in this chapter is a promising one that validates a user in two levels. This method also shields the user's personal information during transmission along the wire. It is resistant to almost all possible attacks. As the method uses randomization of grid and images in the grid, it withstands shoulder-surfing attack vigorously.

[4] Three Level Password Authentication System (2017)

Swarna Lakshmi M, Roobini S, Shalie Monicka A, Saraswathi V, Ms. N. Radha

This paper describes the importance of multi-factor authentication in overcoming security threats and this system can be used in high-security applications like Internet Banking. The Limitation of this paper is that it may be time-consuming for the user to cross multiple levels to log in successfully. Keeping this limitation aside and considering the security, a high level of security can be achieved through the successive levels of authentication. Several new authentication methods which emerge day-to-day and those which tighten security can be combined to form levels of authentication in the future.

[5] Three-Level Password Authentication (2015)

Mughele Ese Sophia

Authentication is the proper validation and rights management of the user for accessing the resources of any information system and 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 locks, and biometrics, hereby combining the benefit of the three techniques/methods to enhance the security of computer resources.

[6]A Simple text-based shoulder surfing resistant Graphical Password scheme (2013)
Chen et al

In this paper, we have proposed a simple text-based shoulder surfing resistant graphical password, in which the user can easily and efficiently complete the login process without worrying about shoulder surfing attacks. The operation of the proposed scheme is simple and easy to learn for users familiar with textual passwords. The user can easily and efficiently to log in the system without using any physical keyboard or on-screen keyboard. Finally, we have analyzed the resistances of the proposed scheme to shoulder surfing and accidental login.

[7]A Graphical Password Authentication (2011)
Ahmad Almulhem

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples and highlighted important aspects of the system.

[8] Graphical Password Authentication using cued Click-Points (2007)
Sonia Chiasson et al

The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each image is shown and having to remember only one click point per image appears easier than having to remember an ordered series of clicks on one image. In our small comparison group, users strongly preferred CCP

[9] Enhancing Security and privacy in biometrics-based authentication system (2001)
N.K.Radha, J.H.Connell, R.M.Bolle

Biometrics-based authentication has many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forge. We have shown that the intrinsic bit strength of a biometric signal can be quite good, especially for fingerprints, when compared to conventional passwords.

[10] Déjà Vu: A user study using images for Authentication (2000)

Rachna Dhamija, Adrian Perrig

A user study which compares Déjà Vu to traditional password and PIN authentication. Results indicate that image authentication systems have potential applications, especially where text input is hard (e.g., PDAs or ATMs), for infrequently used passwords or in situations where passwords must be frequently changed. Since the error recovery rate was significantly higher for images, compared to passwords and PINS, such a system may be useful in environments where high availability of a password is paramount and where the difficulty to communicate passwords to others is desired. Further study is required to determine how user performance and error rate will vary with the frequency of use, over longer time periods, and with large or multiple portfolios.

Disadvantages

- Time Complexity.
- Performance and Error Rate is high.
- Not Effective enough to provide adequate security for computing resources.
- User needs more knowledge.

PROPOSED METHODOLOGY

Three levels of security are included in this one-of-a-kind and simple-to-understand 3-Level Security System. Security at this level has been required by using Text-based secret phrases (with unique characters), which is a conventional and currently a chronologically incorrect approach, where the previous level must be passed to progress to the next level. The Color Combination password has been used to enforce security at this level. By clicking on the three colours red, green, and blue (RGB), the user may create numerous colour combinations.

The 3-Level security system will be Picture Password when the above two levels have been cleared successfully. At first, the user must choose an image in jpg format to use as a secret word, and then the client can set the secret phrase by tapping on the picture in different locations. At the time of log in, the user must choose a similar picture to use as a secret phrase, and then the client must click at similar spots where he/she clicked at the time of setting the secret word.

Advantages

- Resistant to all posible attacks.
- High level of security.
- Easy to use.

OVERALL SYSTEM ARCHITECTURE

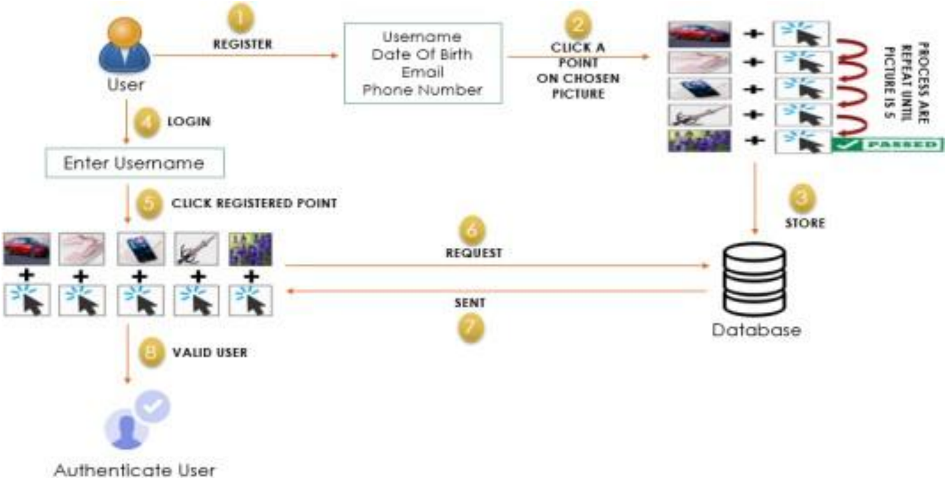

Fig. 3.1: Overall Architecture.

This Project includes three degrees of security

1. Security at this level has been required by using Text-based secret phrases (with unique characters), which is a conventional and currently a chronologically incorrect approach, where the previous level must be passedto progress to the next level.
2. The Color Combination password has been used to enforce security at this level. By clicking on the three colours red, green, and blue (RGB), the user may create numerous colour combinations.
3. The 3-Level security system will be Picture Password when the above two levels have been cleared successfully. At first, the user must choose an image in jpg format to use as a secret word, and then the client can set the secret phrase by tapping on the picture in different locations. At the time of log in, the user must choose a similarpicture to use as a secret phrase, and then the client must click at similar spots where he/she clicked at the time of setting the secret word.

CONCLUSION

Authentication is the most important factor in the field of information security since it involves the correct validation and administration of the user's rights for accessing the resources of any information system. However, no one technique is efficient or effective enough to ensure acceptable security for computer resources including programs, files, communications, printers, the internet, and so on. The importance of multi-factor authentication and randomization in overcoming security threats is discussed in this project, and this system may be used in high-security applications such as Internet banking. The different tiers of authentication can be used to obtain a high level of security.

Future Scope: The user is notified when they successfully authenticate using three levels and begin using the application by fixing the invalid count. Increasing the number of levels by using some techniques (biometric, face recognition) to increase the level of security.

REFERENCES

1. Gouri Sankar Mishra, Pradeep Kumar Mishra, Parma Nand, Rani Astya, Amrita, “User Authentication: A Three Level Password Authentication Mechanism” Conference Series, Volume 1712, International Conference On Computational Physics in Emerging Technologies 1 August, Mangalore, India, 2020.
2. "Three Level Password Authentication", International Journal of Emerging Technologies and Innovative Research, ISSN: 2349-5162, March-2020; 7(3): 68-72.
3. Rahul Chourasia, Dr. N.Partheeban” Three Level Password Authentication System, 2020; 8(6).
4. Vijayakumari Rodda, Gangadhara Rao Kancherla, Basaveswara Rao Bobba, “Multi-level Graphical Password Authentication Scheme for Cloud (MGPASC)” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, September 2019; 8(3).
5. Mughele Ese Sophia “THREE – LEVEL PASSWORD AUTHENTICATION” European Journal of Computer Science and Information Technology, November 2015; 3(5): 1-7.
6. C.T. Li and M.-S. Hwang, “An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards,” J. Network and Computer Applications, 2010; 33(1): 1- 5.
7. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon study on Design evaluation of a graphical password system. International J. of Human-Computer Studies, 2005; 63: 102- 127.
8. S. Man, D. Hong, and M. Mathews, “shoulder surfing resistant to graphical password scheme in International conference on security and management”. Las Vegas, NV, 2003.

9. J. Goldberg, J. Hagman, V. Sazawal, "Doodling Our Way To Better Authentication", CHI '02 extended abstractson Human Factors in Computer Systems, 2002.
10. R. Dhamija, A. Perrig paper based on Study Using Images for Authentication in 9th USENIX Security Symposium, 2000.