THREE LEVEL PASSWORD AUTHENTICATION

K.Jyoshna Priya, Assistant Professor, Department of Computer Science and Engineering
DVR and Dr.HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India.
G.Pratyusha, ,Assistant Professor, Department of Computer Science and Engineering
DVR and Dr.HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India
U.Sarvani, V.Likitha, MD.Abdul Rahaman and V.Rakesh, UG Student
Department of Computer Science and Engineering, DVR and Dr.HS MIC College of Technology, Kanchikacherla, Andhra Pradesh, India

Abstract:

In an organizational network, when the control of resources is given to more than one user, the identity of users must be verified and then granted access to their entitlements. That can be done with the help of a password, as it has long been one of the preferred ways to validate one's identity and relies on one's ability to authenticate oneself by presenting the correct credential.

But as the password is simply text-based, it is very easy for the attacker to get hold of a user's password and impersonate the user and gain access to the organizational resources to which the user is entitled.

So to protect the organizational resources and data from hackers and malicious software, single security authentication is not sufficient enough. Therefore, needs something for secure and user-friendly authentication schemes to overcome this problem. This paper presents a 3-level password authentication scheme to overcome the problem. The three different levels used in the **3-level password authentication scheme** are text password, one-time password (OTP), and image-based password. The main objective is to provide a high level of security to the organization's resources or applications from hackers and secure the resources from unauthorized users.

Keywords: Authentication, Simple Text-based password, three-level authentication, OTP password, Image-based password.

1. Introduction:

Three-level password authentication is a security mechanism that provides a high level of protection for sensitive data and systems of organizations. It involves using three levels of passwords, each with increasing levels of complexity and access privileges.

The purpose of using three-level password authentication is to ensure that only authorized users can access and use critical systems and data. Each level of password provides a different level of access, and the combination of all three passwords provides the highest level of security.

The first level of password is usually a simple password that is easy to remember and is used to access less sensitive data and systems. The second level of password is more complex and is used to access more sensitive data and systems. The third level of password is the most complex and is used to access the most sensitive data and systems.

By requiring three passwords, the system can ensure that only users with the highest authorization level can access and use the most sensitive data and systems. This helps to prevent unauthorized access and reduces the risk of data breaches and other security incidents.

Three-level password authentication is commonly used in government agencies[10], financial institutions, and other organizations that handle sensitive data and systems. It is an effective way to ensure that critical information is protected and only accessible to authorized users.

2. Related work:

In the existing model, only text-based security is used. Where usersuse login and simple text as Passwords for accessing the data of the organizationalsoftware or applications. In which the simple password can be easily cracked by hackers or simply by the common people who are close to

DOI: 10.36893.DRSR.2023.V13I04.0040-0047

them causing the resources to leak outside of the organization or can easily be hacked by malicious software. Here the main drawback is less security.

- 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[12]". 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 the second level. The author has proposed a different type of Authentication system, which is secured highly.
- In June 2020 Rahul Chourasia proposed a 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[11], which makes them 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 the user if he or she claims to be by using Three level password verification.

3.Proposed Method:

Authentication acts as the first line of defense to allow access to valuable data only to those who are approved by the organization and the Security[13] of all resources in the organization lies in the complexity and secrecy of the password. In the existing model, a simple text can easily predict and more possibility oflosing the data.

Hence to increase the level of security, In this project, we have tried to extend the protection by involving a 3-level security approach, involving text-primarily based at Level one,automatically generated one-time password at Level two, and Image-based Authentication at Level three.

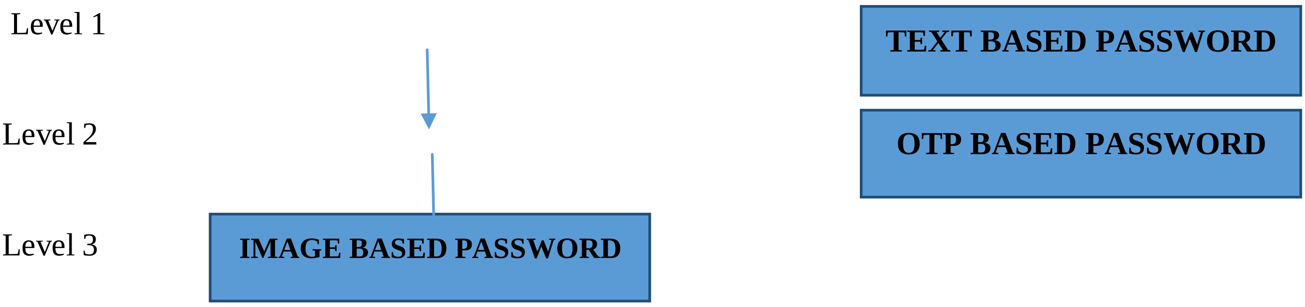


Figure: Security Levels

In this proposed model the user has 2 Modules,

- Registration Module
- Login Module

3.1 Registration Module:

In this phase, the user first needs to register with the system or application. To register, the needs need to submit the authentication details such as user name, Password, and mobile number and select an Image for the third phase of authentication. All the details at the registration were matched with details of login to authenticate the user. If all the details are correctly matched then only the user can successfully access the data.

3.2 Login Module:

In this phase, the user needs to face three levels of authentication.

Level 1:

It is simple text-basedand contains a username and simple password. While registering User creates a simple text format password that contains the alphanumeric characters along with the special characters.Simple text-based Passwords are

- It should contain at least 10 characters long.
- At least one charter should be a capital letter.
- At least one special character must be used.
- Should not use a name as a password as it is simple to guess.

Figure 3.2.1: Text Based Password

Level 2:

It is one-time password-based. After a successful session of level 1, the user will receive OTP (random sequence of digits) to the registered mobile number which is given at the registration phase. If the mobile number is matched and OTP provided is correct then only the level is authenticated[14] successfully.

Figure 3.2.2: OTP Based Password

Level 3:

After the successful completion of the above 2 levels, the user enters into the level 3 phase. It is an image-based password, the user needs to select the image which is given at the time of registration. If both images are matched, then the user is authenticated. The same image needed to be selected, if you select the compressed image of the same input image, then the image will not authenticate.

DOI: 10.36893.DRSR.2023.V13I04.0040-0047

Figure 3.2.3: Image Based Password

3.3Working Process of Three-Level Password Authentication:

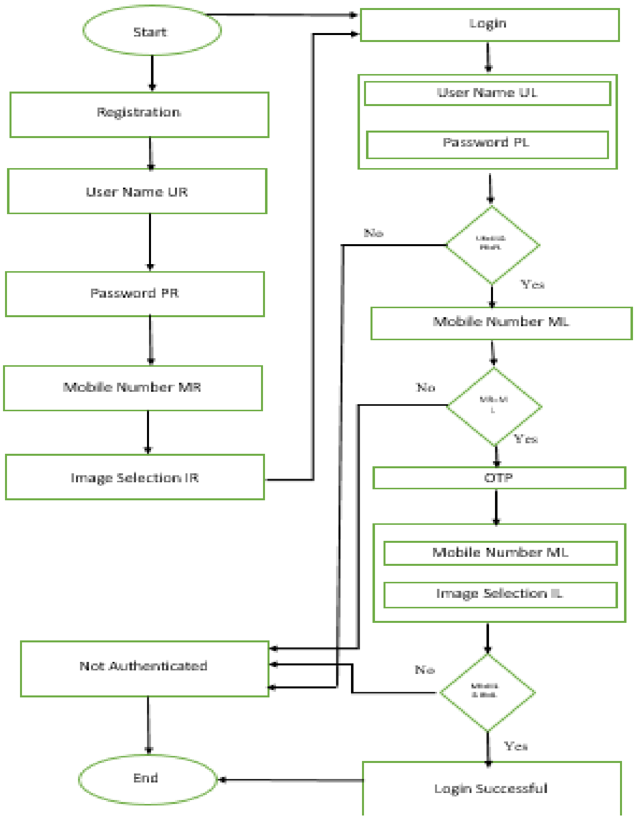


Figure:Process Flow Diagram

3.4 Comparison of Authentication Mechanisms:

The experimental results of the 3-tier authentication are found to be achieving 98.39% accuracy. This methodology is also found to be more reliable in comparison to the methodologies previously implemented namely biometric authentication, image-based authentication, and graphical, shape, and text-based authentication mechanisms. The comparison of these methodologies is given in Fig. Here the execution is carried out for a 3-tier authentication for an application. The user requires to be authorized to Appeal services from the system. Earlier a user can be attested to the system, he accepts to register with the system for the beginning time. This procedure is called registration. Therefore, for a new user, the user must register with a system and then authenticate before he can request a service. The first level of authentication is a Text based authentication where verification is performed using text.

DOI: 10.36893.DRSR.2023.V13I04.0040-0047

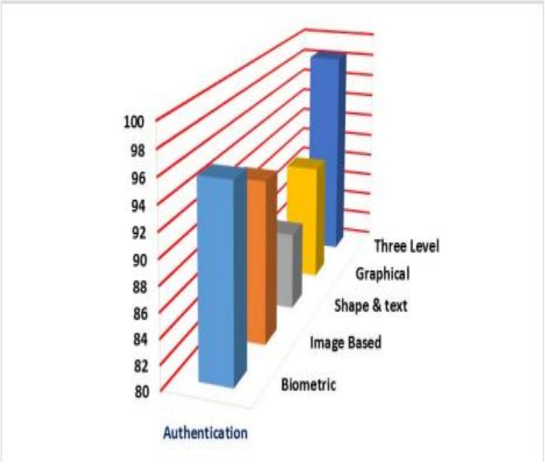


Figure: Comparison of Authentication Levels

The second level is Time Password authentication when verification is executed using a Random Sequence generated by the system. And the third level of authentication is Image password authentication, where to choose an image for authentication. Verification is executed to keep up privacy and it provides protection too. User Verification can be ameliorated by employing both text passwords and images. From the analysis of results in can be recommended that sensitive data accessing systems deploy three level authentication model.

4.Results:

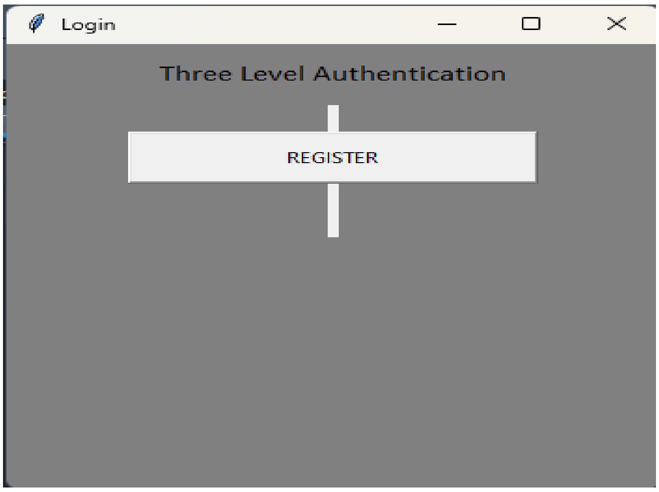


Figure 1: Home Page

DOI: 10.36893.DRSR.2023.V13I04.0040-0047

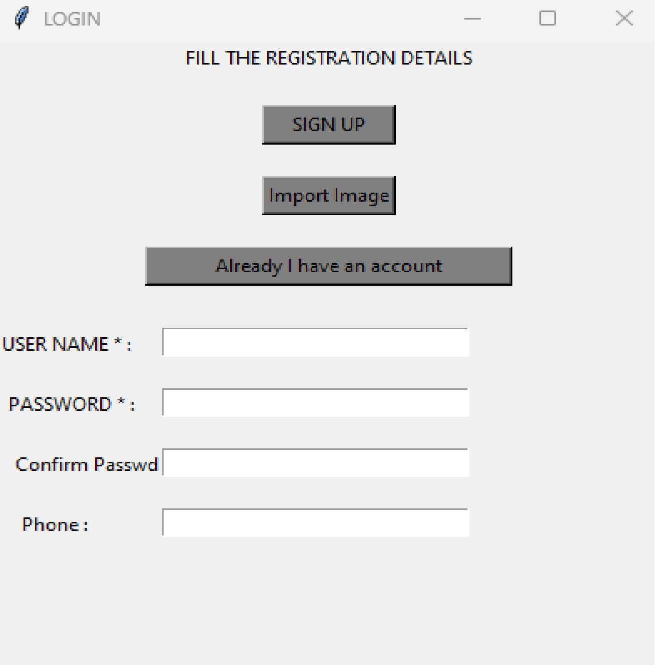


Figure 2: Registration Page

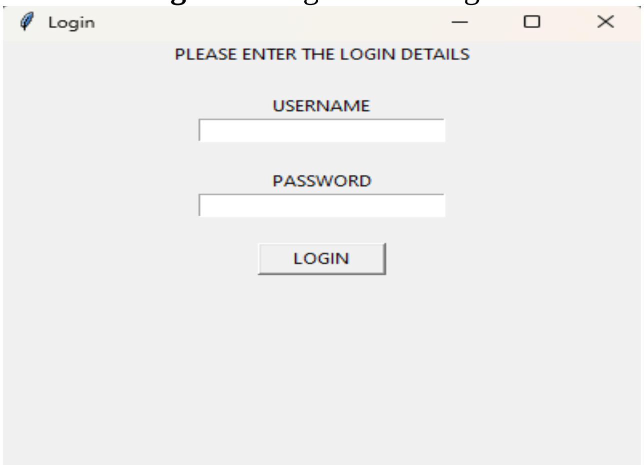


Figure 3: Level 1

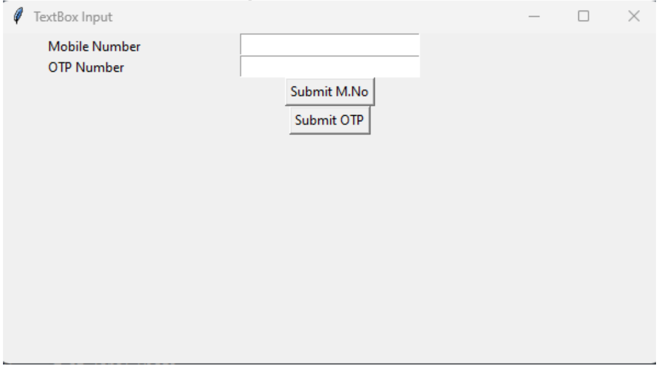
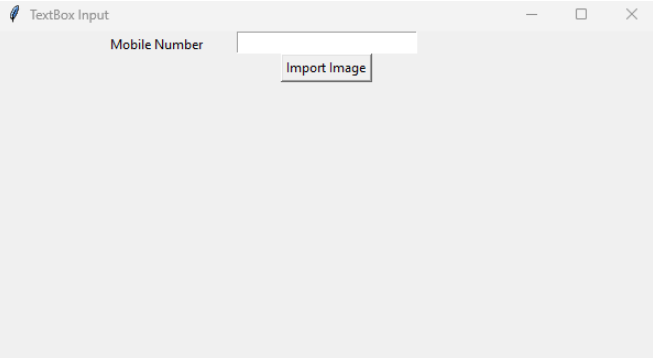


Figure 4: Level 2

DOI: 10.36893.DRSR.2023.V13I04.0040-0047



Mobile Number

Figure 5: Level 3

5. Conclusion:

Based on the research, providing a 3-level authentication password scheme is better than a single-factor authentication because it needs to pass through the 3 levels to authenticate successfully. The main reason proposed this scheme is to enhance the security of computer systems.

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. Therefore, this system is unsuitable for security since it takes time to fill in all three security-level details.

But it will be helpful in high-security levels where the security of data is a primary concern and time complexity is secondary.The main objective of this project is to improve the security level of the systems for many survey papers where researched. It is found that a three-level authentication system helps to provide more security compared to one-level and two-level authentication systems. Three levels are more important because the user needs to enter critical details and login with three different levels of authentication.

6.Reference:

[1] A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM, vol. 42, pp.40–46, 1999. Article (CrossRef Link)

[2] R. N. Shepard, "Recognition memory for words, sentences and pictures 1," Journal of Verbal Learning and Verbal Behavior, vol. 6, pp.156–163, 1967. Article (CrossRef Link)

[3] Aviv, Adam J. Gibson, Katherine, Mossop, Evan, Blaze, Matt, Smith, Jonathan M., "Smudge Attacks on Smartphone Touch Screens," in Proc. of 4th USENIX Workshop on Offensive Technologies. Article (CrossRef Link)

[4] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, pp. 102-127, 2005. Article (CrossRef Link)

[5] T. Seong, G.-W. Park, and Y.-S. Byun, "A Study on Graphical Passwords," in Proc. of 26th KIPS Fall Conference, vol. 13, no. 2, 2006. Article (CrossRef Link)

[6] J.-W. Kim, S.-H. Kim, K. Kim, and H.-G. Cho, "A Shoulder-Surfing Resistant Graphical Password Using Hangul Choseong," in Proc. of KISS Fall Conference, vol. 37, no. 2(A), pp. 95-96, 2010. Article (CrossRef Link)

[7] J.-W. Kim, S.-H. Kim, K. Kim, and H.-G. Cho, "Improvement of the Grid-based Password System Resistant to Shoulder-Surfing Attacks, "Journal of KISS, vol. 17, no. 4, 2011. Article (CrossRef Link)

[8] G. Moon, J. Kim, and M. Hong, "A Graphic Password Scheme using Eulerian Path," in Proc. of the Korea Computer Conference, vol. 38, no. 1(D), 2011. Article (CrossRef Link)

DOI: 10.36893.DRSR.2023.V13I04.0040-0047

[9] G. Moon, J. Kim, and M. Hong, "A Graphical Password Scheme Resistant to Shoulder-Surfing Attack in Mobile Environments," Journal of KISS, vol. 18, no. 1, 2012. Article (CrossRef Link)

[10] T. Kim, S. Kim, E. Park, and J.H. Yi, "Minesweeper Game Based Password Authentication Scheme Resistant to Shoulder-Surfing Attack," in Proc. of 37th KIPS Spring Conference, vol. 19, no. 1, pp. 654-657, 2012. Article (CrossRef Link)

[11] G.Sai Chaitanya Kumar, Dr.Reddi Kiran Kumar, Dr.G.Apparao Naidu, "Noise Removal in Microarray Images using Variational Mode Decomposition Technique " Telecommunication computing Electronics and Control ISSN 1693-6930 Volume 15, Number 4 (2017), pp. 1750-1756

[12] V. S. Rao, V. Mounika, N. R. Sai and G. S. C. Kumar, "Usage of Saliency Prior Maps for Detection of Salient Object Features," 2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021, pp. 819-825, doi: 10.1109/I-SMAC52330.2021.9640684

[13] G. S. C. Kumar, D. Prasad, V. S. Rao and N. R. Sai, "Utilization of Nominal Group Technique for Cloud Computing Risk Assessment and Evaluation in Healthcare," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021, pp. 927-934,doi: 10.1109/ICIRCA51532.2021.9544895

[14] . N. R. Sai, G. S. C. Kumar, M. A. Safali and B. S. Chandana, "Detection System for the Network Data Security with a profound Deep learning approach," 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1026-1031, doi: 10.1109/ICCES51350.2021.948896