International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2429 - 2432
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0332

Three Level Password Authentication System

Dr. Shameena Begum[1], K. Sri Sravani[2], K. Sai Mounika[3], V. Durga Saranya[4], M. Dhanush Kumar[5]
[1,2,3,4,5]Computer Science & Engineering (Cyber Security), RCE, Eluru-AP, 534462, India.
Emails: *cse-cshod@rcee.ac.in[1], srisravani812@gmail.com[2], saimounika.paladugu@gmail.com[3], saranyavandanala@gmail.com[4], dhanushmarrapu@gmail.com[5]*

Abstract
Password authentication remains widely used but vulnerable. Our three-way system enhances security by combining alphanumeric passwords, RGB colour combinations, and image-based passwords. During registration, users go through three levels of authentication to log in to the system or the main page of the website. The system uses HTML, CSS, JavaScript for the front end, and Python with Django for the back end, with MySQL for the database. This multi-factor approach significantly improves security, preventing unauthorized access and data breaches.

Keywords: *Python; HTML; CSS; Django; Three-level Authentication.*

1. Introduction
Nowadays, we know that computer security mostly depends on passwords to verify and authenticate users. There are many authentication schemes proposed and most of them still have weaknesses. Some of them are based on the physical and behavioural properties of the user such as voice recognition, and some others are based on knowledge of the user such as textual and graphical passwords. However, these schemes are still not secure enough and allow attackers to steal the data easily. Our python-based Three-Level Password System is designed to overcome the problem. It is an authentication system that only allows users to access the system if they have entered the correct password. The project includes three levels of user authentication – Textual, Image and Graphical. That way there would be negligible chances of the bot or anyone else cracking the passwords, even if they crack the first or second level it would be impossible to crack the third. [1-3]

1.1. Scope
The scope of the Three-Level Password System is to provide a multi-layered approach to security that makes it more difficult for unauthorized users to gain access to sensitive information or systems. By implementing this system, organizations can improve the security of their data and systems by requiring multiple levels of authentication before granting access. This can help prevent unauthorized access, data breaches, and other security-related incidents that can compromise the integrity of the organization's operations.

1.2. Objective
The objective of the Three-Level Password System is to provide an additional layer of security that enhances the overall security of the organization's data and systems. With three different levels of passwords required to access the system, it becomes more challenging for unauthorized users to gain access. Additionally, the system can help detect and prevent unauthorized access attempts, as any failed login attempts can be monitored and flagged for further investigation. [4-7]

1.3. Expected Outcome
1.3.1. Problem with the Current Scenario
Nowadays, access to sensitive and private information has become easy. It leads to the problem of unauthorized access, security breaches or data theft.

1.3.2. Drawbacks of the Existing System
The existing password system has several drawbacks that can compromise the security of user accounts and sensitive information. Many systems still rely solely on a username and password for authentication, which is not secure enough.

1.4. Proposed System
Our Python-based multi-factor authentication system boasts a single user module, aptly named "User". This

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2429 - 2432
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0332

module empowers users to register by creating a strong, conventional alphanumeric password. To bolster security further, we've implemented a second-level authentication layer that leverages colour combinations. During registration, users can establish a unique password composed of RGB button combinations. Imagine pressing a specific sequence of coloured buttons on a keypad to grant access – it's like a secret handshake translated into the digital realm! For the ultimate defence, users can configure a third-level authentication factor. This layer entails uploading a personal image into the system. Upon login, the system will scramble the image into a jumbled puzzle. To gain access, users must correctly identify the correct pattern or combination of the image, starting from the top-left corner and navigating through the distorted layout. This approach adds a layer of familiarity and recognition, making it difficult for unauthorised individuals to bypass security even if they possess the email address and password. The frontend uses HTML, CSS, and JavaScript for a user-friendly interface, while Python, MySQL, and Django handle backend functionality. This project offers a secure, user-friendly authentication method, utilizing layered defences and diverse technologies for robust security.

2. Method

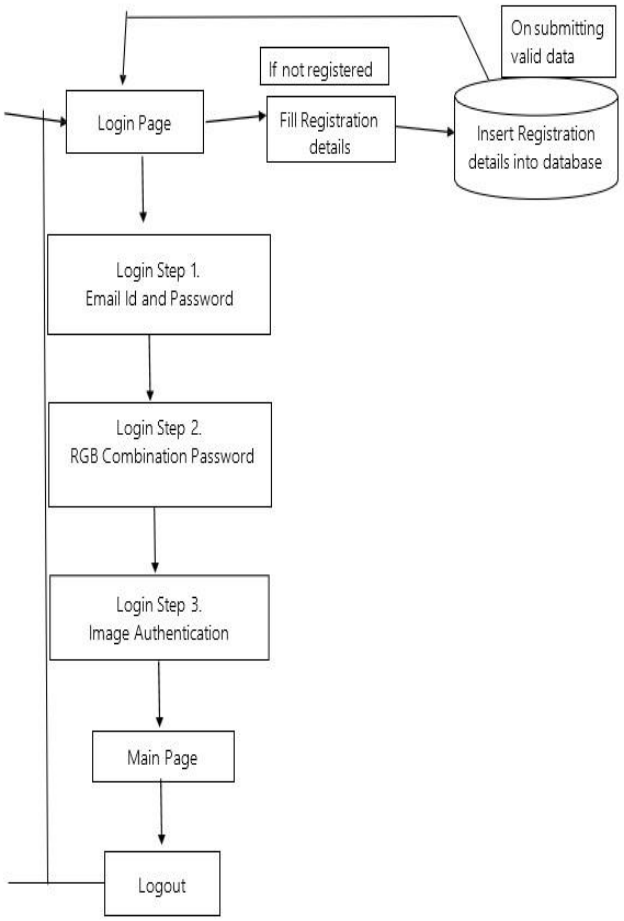
This three-level password authentication system offers three levels of highly secured mechanisms. The user has to first register into the system by providing their personal details like name, email id, mobile number, password, etc,. Then the user must go through three levels of login process to access the contents of the website. (Refer Figure 1)

i. **Username and Password:** In the first level of the login process, the user must enter their email-id and password. Upon entering valid data, the user is taken to the second level of login.

ii. **RGB Colour Combination:** In the second level, there are three colours present and the user has to click on the correct combination of colours which they have entered at the time of registration. A code is generated for each colour and stored into the database and verified with the data in the database. If the combination is correct, then the user is directed to the third level of login.

iii. **Image Authentication:** In the third level, an image uploaded by the user is displayed in the form of a puzzle which must be solved by the user to get the correct image. If the image is valid, then the home page of the website can be accessed.

Even if the first two levels are hacked by the intruders, the third level is highly difficult to bypass. Therefore, a secure password authentication system is provided.



Figures 1 Method

3. Results and Discussion

3.1. Results

The results show the Registration phase, the three phases of login and main page of the website which are the key components of this three-level authentication system. (Refer Figure 2, 3, 4, 5, 6)

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2429 - 2432
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0332

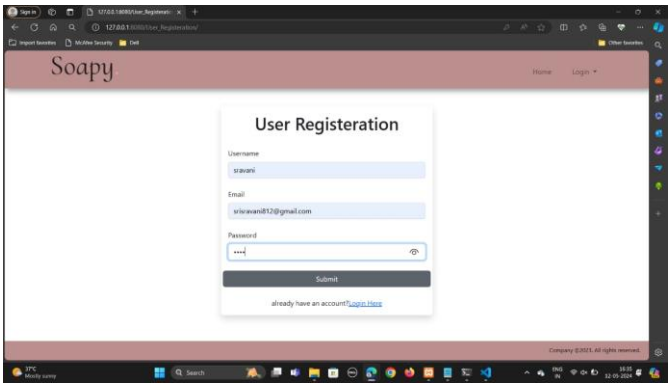


Figure 2 Registration Phase

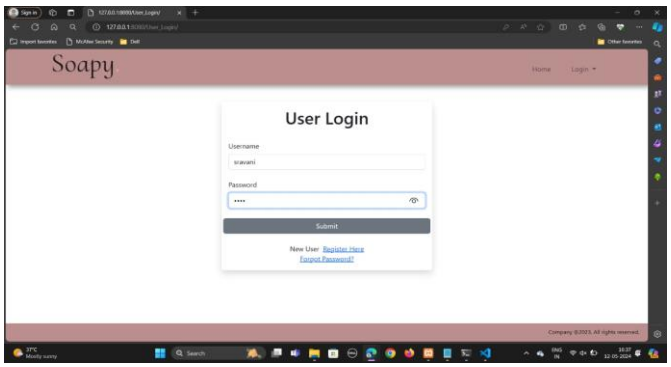


Figure 3 Level 1

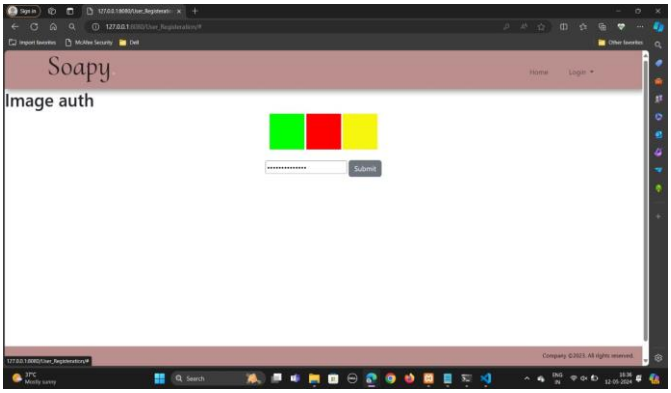


Figure 4 Level 2

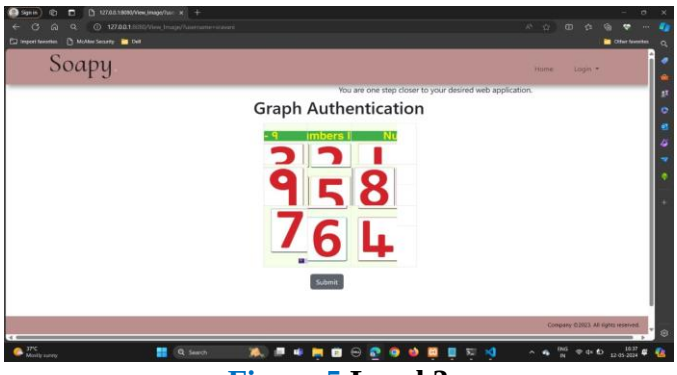


Figure 5 Level 3

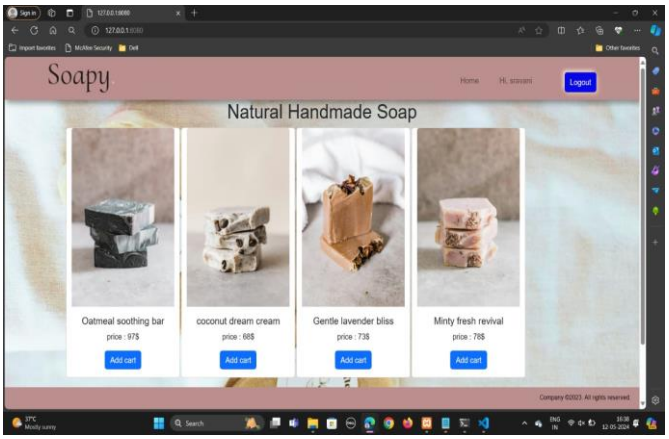


Figure 6 Homepage

3.2. Discussion

Users must go through three levels of login process to access the contents of the website. Test results serve as a critical mechanism for identifying defects, prioritizing corrective actions, and validating that the software meets specified requirements and quality standards.

Conclusion

This proposed approach has its advantages like High level of security, load balancing, Easy Accessibility, User friendly approach, Efficiency and reliability, Ease of Maintenance and Usability. While multi-level authentication offers a significant security boost, it can come at the cost of user convenience. Going through multiple steps to verify your identity can be time-consuming. However, this drawback shouldn't overshadow the security benefits. Each additional layer of authentication makes it exponentially harder for unauthorized access. Even if a hacker obtains one piece of information, like user's password, they'd still need to crack the other layers to gain entry. This layered approach is especially important for protecting sensitive data. By implementing different authentication levels for varying degrees of data sensitivity, you can achieve a balance between robust security and a user-friendly experience.

Acknowledgements

We wish to take this opportunity to express our deep gratitude to all the people who have extended their cooperation in various ways during our project work. It is our pleasure and responsibility to acknowledge the help of all those individuals.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 09 September 2024
Page No: 2429 - 2432
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0332

References

[1]. Student Portal with 3 Level Passwords Authentication System - Journal by B. Lakshmi Praveena1, M. Anitha2, J. Supriya3 T. Lakshmi Priya4 1,2,3,4 Dept. of Information Technology, Vvit, Ap

[2]. Three Level Password Authentication System - Ijrct.Org Journal By 1 Rahul Chourasia, 2 Dr. N.Partheeban Galgotias University, Uttar Pradesh , 203201 , India

[3]. Three Level Password Authentication System, Ladychampionz April 18, 2020 Information and Cyber Security Projects Topics and Materials

[4]. Varghese, L., Mathew, N., Saju, S., & Prasad, V. K. (2014). 3-Level Password Authentication System. International Journal of Recent Development in Engineering and Technology, 2(4), 127-131.

[5]. Edition, W. S. F. (2023). Cryptography And Network Security.

[6]. Computer Security: Principles and Practice (3rd Edition) by M. E. Whitman and Herbert Mattord

[7]. Krause, M. (Ed.). (2006). Information Security Management Handbook on CD-ROM (Vol. 27). CRC Press.