iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.69782

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Secure Three Level Authentication System

Pratyush Kumar[1], Pavan[2]
Bachelor of Technology Computer Science and Engineering, School of Engineering and Technology, CMR University, India

Abstract: ***This paper presents the design, development, and evaluation of a three-level authentication system. The increasing prevalence of cybercrimes has heightened the need for secure and efficient authentication systems to safeguard sensitive data. Traditional authentication mechanisms such as single factor or two factor systems, relying on text-based passwords, tokens, or biometric data, have been found to have vulnerabilities. This paper introduces a robust and user-friendly Secure Three Level Authentication System that combines text-based passwords, colour pattern recognition, and image-based authentication. By integrating these three methods, the system ensures a multilayered defines against common security threats such as phishing, brute force attacks, and shoulder surfing. The first layer utilizes a passphrase-based text password, designed for ease of use while maintaining complexity. The second layer involves a graphical password using RGB colour patterns, leveraging visual memory for added security. Finally, the third layer employs image-based authentication, where users segment and rearrange a chosen image for secure access. The system is implemented using PYTHON, CSS, and HTML, ensuring a seamless and efficient user experience. Designed with the waterfall model, the authentication process involves registration and login phases, where each layer must be passed sequentially for access. This three-level system addresses the vulnerabilities of conventional methods by increasing password difficulty at each stage. While slightly more time-consuming, it offers significant advantages for applications requiring high security standards, such as corporate environments, sensitive data repositories, and critical infrastructures. Future iterations aim to enhance the system's adaptability and user customization. The proposed system represents a significant advancement in authentication technology, providing a balance between usability and security to protect against evolving cyber threats.***

Keywords: Authentication, Multilevel Security, Text Based Password, Graphical Password, Image Based Authentication, Cybersecurity, RGB Color Pattern, Secure Login, Waterfall Model, Phased System

I. INTRODUCTION

In an era where digital connectivity governs personal, professional, and governmental operations, ensuring data security through reliable authentication systems is more crucial than ever. Traditional single-factor and two-factor authentication mechanisms—relying on text-based passwords, tokens, or biometrics—often fall short in delivering comprehensive protection against sophisticated cyber threats such as phishing, brute-force attacks, and data breaches. These methods are either vulnerable to common attack vectors or introduce usability challenges that hinder adoption. This project presents a Secure Three-Level Authentication System that addresses these shortcomings by combining three distinct yet complementary authentication methods: text-based passwords, colour pattern recognition, and image-based puzzle. By layering these techniques, the system increases resistance to unauthorized access while maintaining a user-friendly interface. Each authentication level leverages different aspects of user cognition—textual, visual, and spatial memory—making it significantly harder for attackers to bypass all stages. Developed using PYTHON, HTML, and CSS, and structured under the Waterfall model, the system ensures modular development and scalability. Its design prioritizes not only robust security but also accessibility, aiming to strike a balance between technical integrity and ease of use. The solution is particularly suited for high-security applications, such as protecting sensitive corporate or governmental information. As cyberattacks grow in scale and complexity, there is a pressing need for advanced authentication solutions that evolve alongside these threats. This project contributes to that objective by delivering a multi-layered, adaptable, and secure system, offering an innovative approach to authentication in an increasingly connected digital world.

II. LITERATURE REVIEW

Authentication is a fundamental component of information security, serving as the first line of defence against unauthorized access. Over the years, researchers and developers have explored various authentication mechanisms, including single-factor, two-factor, and multi-factor approaches. However, as cyber threats evolve, traditional methods have proven inadequate in mitigating modern attacks. Single-factor authentication (SFA), which typically relies on text-based passwords, remains the most widely adopted technique due to its simplicity and ease of implementation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

However, studies have consistently shown that SFA is vulnerable to dictionary attacks, brute-force attacks, and phishing schemes. Users often create weak passwords or reuse them across platforms, further compromising system security (Florêncio & Herley, 2007).To improve upon SFA, two-factor authentication (2FA) emerged, combining knowledge-based factors (e.g., passwords) with possession-based factors (e.g., tokens or one-time passwords). While 2FA enhances security, it still faces challenges such as token theft, SIM swapping, and user inconvenience (Bonneau et al., 2012). Moreover, its reliance on external devices can introduce operational complexities and additional costs. Graphical password systems, which use images or visual patterns instead of text, have been proposed to counter the limitations of traditional methods. Studies have demonstrated that users tend to remember images more effectively than text, making graphical passwords both secure and user-friendly (Wiedenbeck et al., 2005). Similarly, image-based authentication, such as CAPTCHA or puzzle-based techniques, introduces a layer of cognitive interaction that is difficult for automated attacks to bypass. Recent literature emphasizes the benefits of multi-factor and multi-modal systems, which combine several independent methods of authentication to build layered security. These systems are more resilient to single-point failures and provide robust protection against a wide range of attack vectors. However, balancing security with usability remains a challenge. This project builds upon existing research by integrating three distinct authentication layers—text, colour pattern recognition, and image segmentation—into a cohesive system. By doing so, it addresses known vulnerabilities in conventional methods and responds to the growing demand for systems that offer both strong security and a positive user experience.

III. SYSTEM ARCHITECTURE AND DESIGN

A. Architectural Overview

The proposed Secure Three-Level Authentication System is designed with a modular and layered architecture that enhances security by requiring users to sequentially pass through three distinct authentication stages. The system follows the Waterfall development model, ensuring a systematic and well-documented design process.

B. User Interface Layer (Frontend)

Developed using HTML and CSS the user interface is designed to be intuitive and responsive. It provides separate interfaces for registration and login. Each authentication level is presented sequentially, ensuring a clear and structured flow for users.

C. Application Logic Layer (Backend)

Implemented in PYTHON, this layer handles the core authentication logic. It processes user inputs, manages session states, and communicates with the database to verify credentials. It ensures that each authentication level is passed successfully before granting access to the next stage.

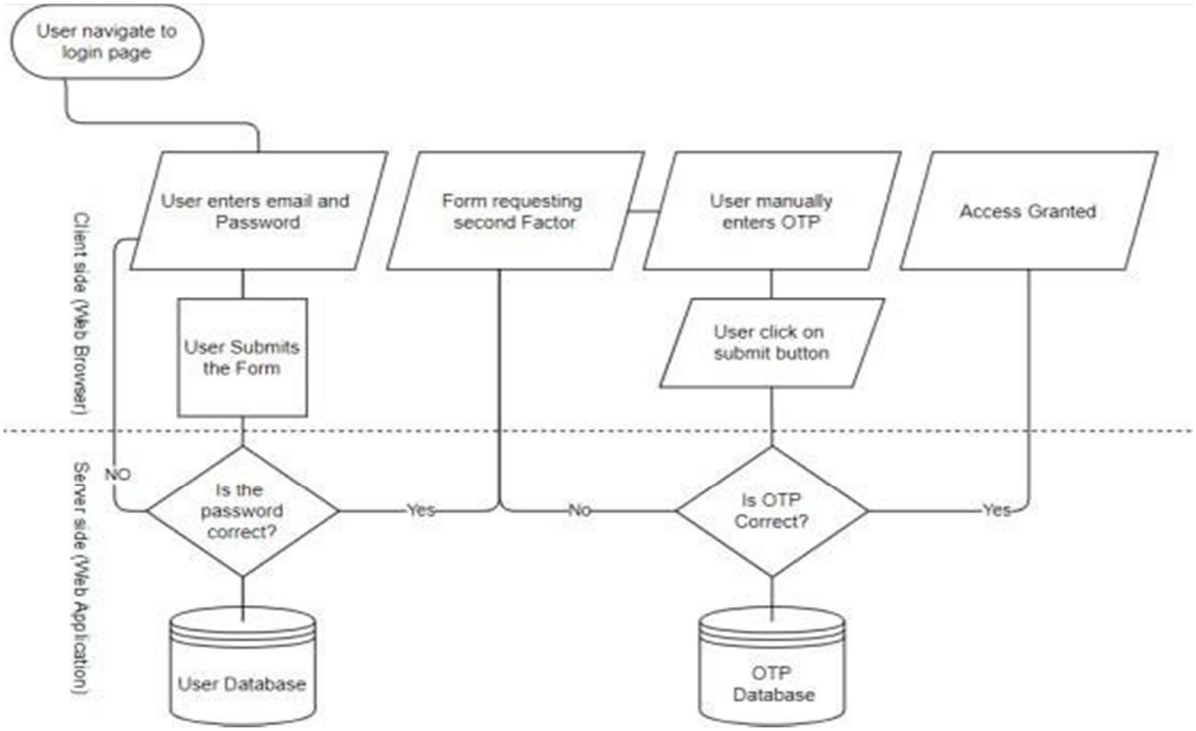
D. Data Storage Layer (Database)

The database, powered by local server, stores encrypted user credentials, including:
Hashed text passwords
Encoded color pattern sequences
Image segment arrangement data
The use of encryption and hashing mechanisms ensures that stored data is secure and resistant to unauthorized access.

E. Authentication Workflow

The system follows a sequential validation process during login:
Level 1 – Text-Based Password
The user enters a passphrase, which is verified against a hashed value stored in the database.
Level 2 – Colour Pattern Recognition
The user selects a predefined RGB colour sequence. This graphical password is matched with the stored encoded pattern.
Level 3 – Image-Based Puzzle Authentication
The user reassembles a scrambled image, previously chosen during registration. Correct segment arrangement is verified against the stored configuration.
Only upon successful validation at all three levels is the user granted access. Failure at any level results in termination of the login attempt, ensuring maximum security.

F. Existing System Architecture



G. Proposed System Architecture

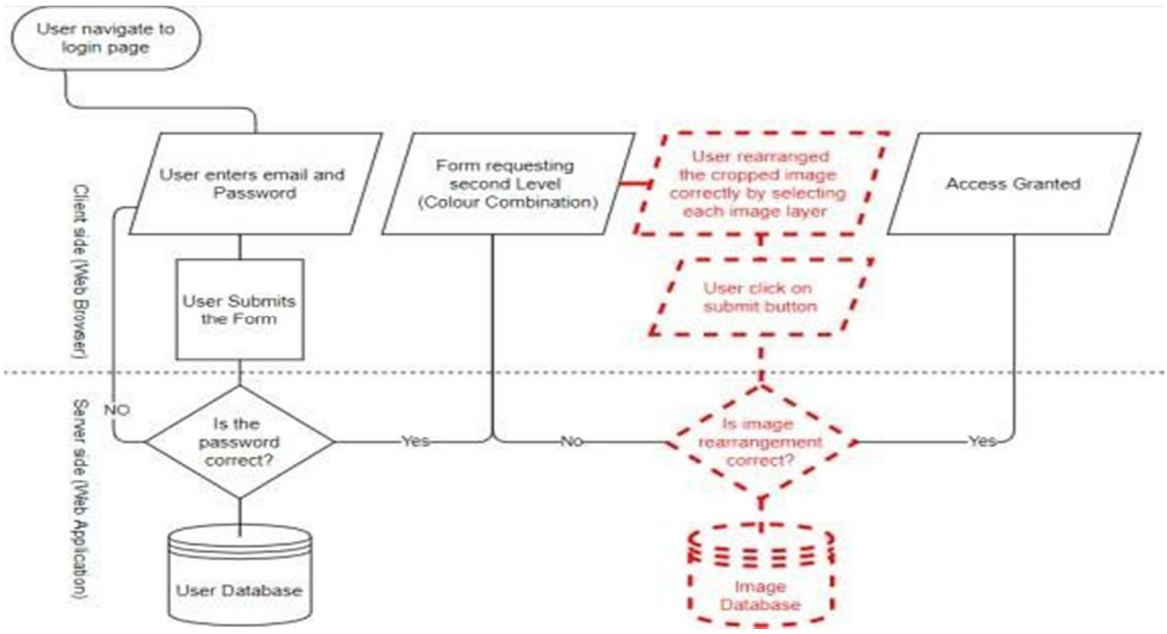


Fig.1 System Design

IV. IMPLEMENTATION

The Secure Three-Level Authentication System is implemented using open-source technologies including PYTHON, HTML and CSS. The system is built following the Waterfall Model, which allows for a structured and systematic development cycle—progressing through requirement analysis, system design, implementation, testing, deployment, and maintenance.

A. *Development Environment*

The project is developed using a local server environment set up with Python as the primary backend programming language. The system is executed locally without the use of MySQL or PHP. Instead of a traditional database, file-based storage (such as JSON or text files) is used to store user credentials, colour patterns, and image puzzle configurations securely.

B. *Registration Module*

The registration process includes three steps:

1) Text-Based Password Entry: Users provide a username and a secure password. The password is hashed using PHP's password hash() function before storing it in the database to prevent plain-text password storage.
2) Colour Pattern Selection: A grid or sequence of colours (RGB-based) is presented using buttons or visual tiles. Users must select a colour pattern in a specific sequence. This selection is stored in the database as a serialized or JSON string, which will later be used for authentication during login.
3) Image Puzzle Configuration**:** Users upload or choose a default image which is divided into a grid (e.g., 3x3). The user is required to rearrange the segments into the correct order, essentially solving a puzzle. The final arrangement (i.e., tile positions) is stored in the database for future comparison during login.

C. *Login Module*

During the login process, each authentication level is presented in the same sequence. The user must successfully pass all three levels to gain access:

1) Text Password Validation: The entered password is verified against the stored hash using PHP's password verify() function. If the password is valid, the system moves to the next layer.
2) Colour Pattern Verification: Users must select the same sequence of colours they chose during registration. The system compares the submitted pattern with the one stored in the database. This layer enhances resistance to shoulder surfing and brute force attacks.
3) Image Puzzle Authentication: The user is presented with a scrambled version of their image puzzle. They must rearrange the segments correctly. JavaScript handles the UI interaction, while the final tile arrangement is sent to the server for validation against the stored correct configuration.

D. *Frontend Experience*

The user interface is clean and responsive. JavaScript is used for dynamic UI updates and validations without refreshing the page. Transitions between layers offer feedback (e.g., success messages or error prompts), guiding the user through the authenticating on stages smoothly.

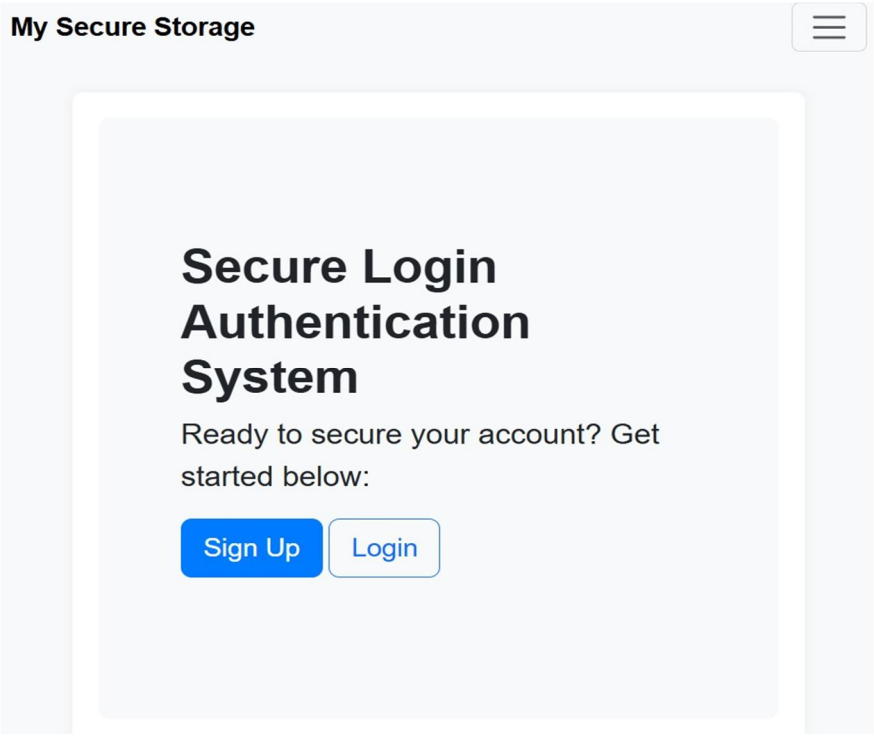
V. RESULT

The Secure Three-Level Authentication System was successfully developed and tested, demonstrating a significant improvement in login security without greatly compromising user convenience. The system was evaluated on the basis of functionality, user experience, and security robustness. During testing, the authentication flow performed as expected across all three layers. Users were required to correctly input their registered text-based password, match the selected color pattern, and finally solve the image-based puzzle. Only upon successful completion of all three stages was access granted. If any single layer was failed, the authentication process was terminated, thereby ensuring high security and strict access control.

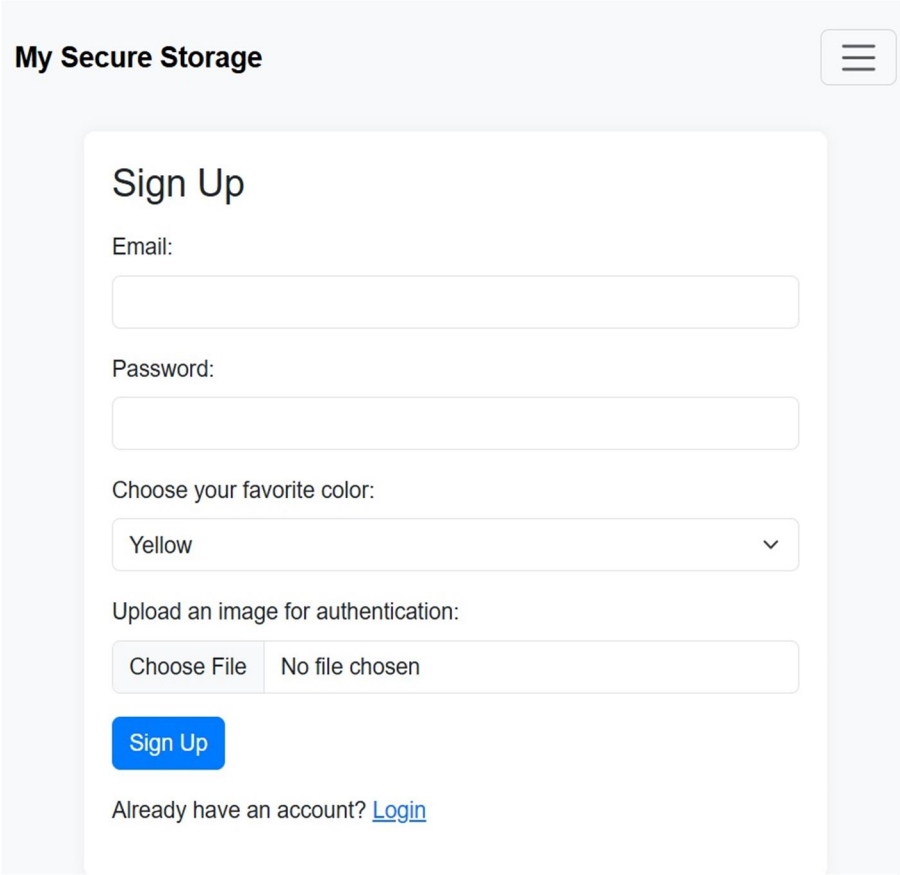
The password authentication layer effectively validated user credentials using PHP's hashing mechanisms, offering protection against brute-force and dictionary attacks. The colour pattern recognition layer provided a unique visual element that leveraged the user's memory, making it difficult for attackers to guess or replicate, especially against threats like shoulder surfing. The image puzzle layer proved to be the most secure, as it added a cognitive challenge that would be extremely hard to bypass without prior knowledge. User testing showed that while the system took slightly longer to log in compared to traditional single or two-factor systems, users adapted quickly and appreciated the enhanced sense of security. The interface was rated user-friendly, with intuitive transitions between authentication layers. The system was also evaluated against common attacks. Simulated brute force and phishing attempts failed to bypass the layered authentication. Furthermore, storing image and colour data in non-obvious formats (e.g., encoded strings) added an extra layer of obfuscation.

Overall, the system effectively meets its goal of providing a multi-layered, user-friendly, and secure authentication solution suitable for high-security applications like corporate systems, personal data vaults, and sensitive access portals.

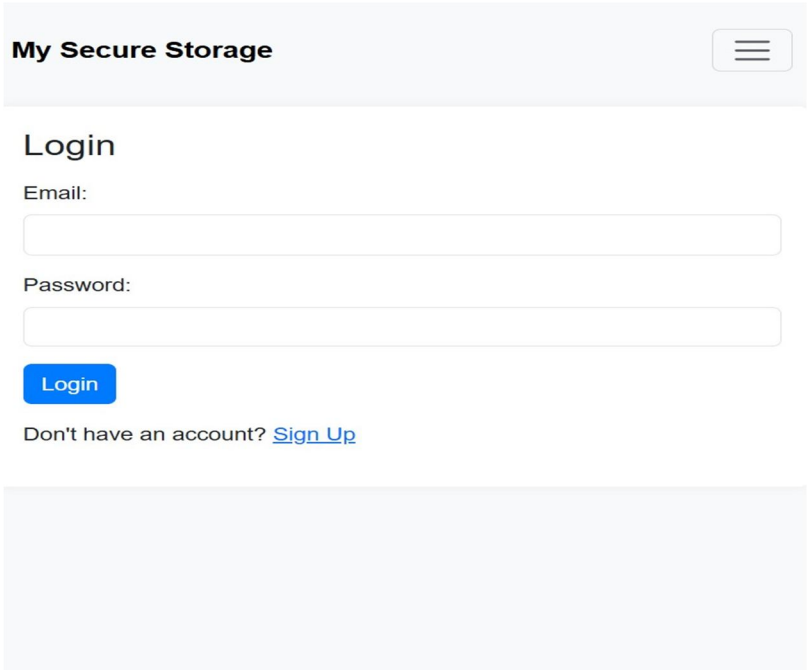
User Authentication Interface



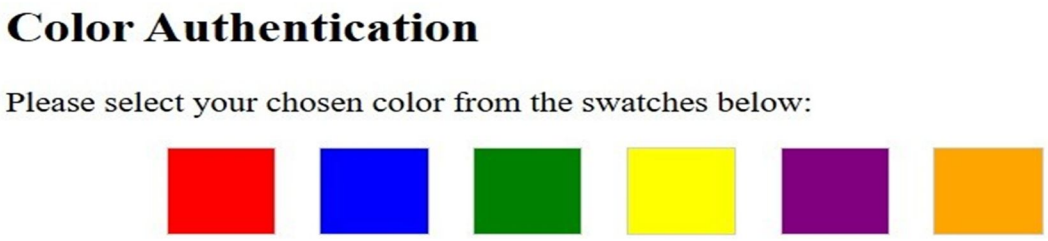
User Authentication Interface



User Signup Interface



User Color Authentication Interface



Rearrange Authentication Interface

User Local Storage

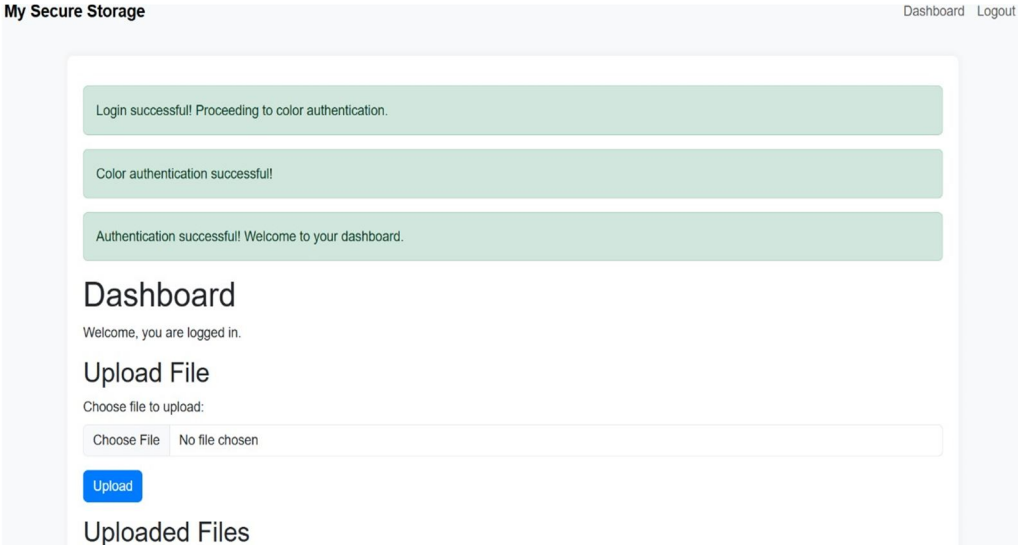


Fig.2 Three level authentication system

VI. CONCLUSION

In an era where cyber threats are increasingly sophisticated and persistent, the need for secure and reliable authentication mechanisms has become more critical than ever. This project presents a Secure Three-Level Authentication System that combines traditional text-based passwords, color pattern recognition, and image-based puzzle authentication to provide a multi-layered defense against unauthorized access.

Each level of the system is uniquely designed to address the limitations of conventional authentication methods. The text-based password offers a familiar first layer of protection. The graphical color pattern adds a cognitive and visual challenge, making it resistant to common threats like shoulder surfing and brute force attacks. Finally, the image puzzle layer incorporates an element of visual memory and interaction, greatly enhancing security while maintaining usability.

Through practical implementation using PYTHON, CSS and HTML, the system demonstrated robust performance and user acceptance. Although the process involves slightly more time than standard login methods, the trade-off is justified by the significantly increased security.

The system proves especially effective for applications where sensitive data or secure access control is essential—such as corporate portals, academic records, or personal data storage. It balances the need for user-friendliness with advanced protection, showing that security does not have to compromise usability.

Future improvements could include mobile app integration, biometric extensions, or AI-driven pattern anomaly detection. Overall, the project contributes a valuable step forward in the field of cybersecurity and user authentication.

VII. ACKNOWLDGEMENT

I would like to express my heartfelt gratitude to all those who have supported and guided me throughout the completion of this capstone project, "Secure Three-Level Authentication System."

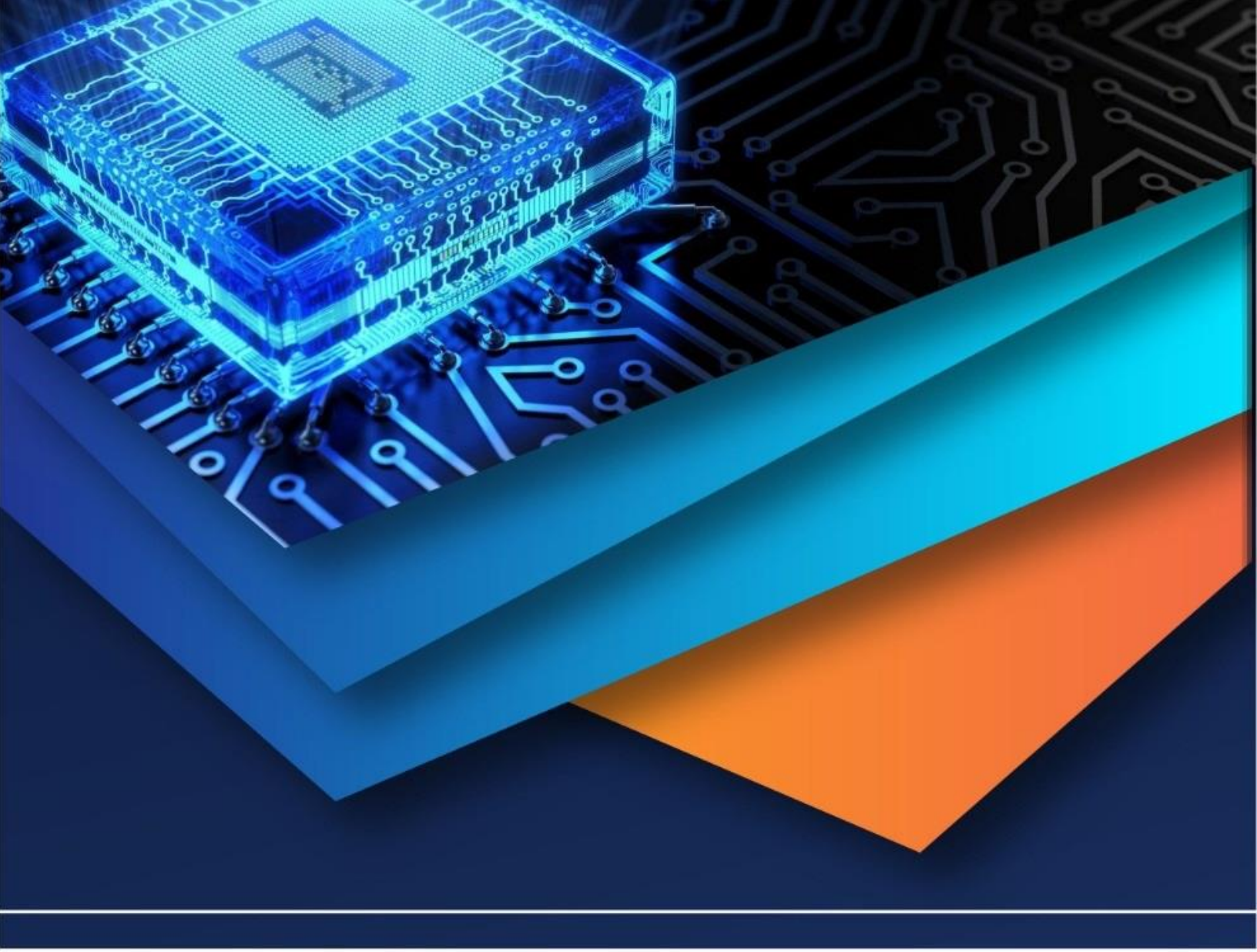
First and foremost, I sincerely thank my project guide Prof. Prabhakar K from the Department of Computer Science and Engineering, CMR University, for their invaluable guidance, constant encouragement, and insightful suggestions at every stage of the project. Their support was crucial in shaping this work from concept to completion. I would also like to thank the Head of the Department and the faculty members of the School of Engineering and Technology for providing the necessary resources and infrastructure, and for fostering a conducive environment for academic growth.

Special thanks to my peers and friends who provided feedback during testing and helped me evaluate the user experience and effectiveness of the system. Their input played an important role in refining the final implementation.

Lastly, I am deeply grateful to my family for their unwavering support, patience, and motivation throughout the course of this project. Their belief in me has been a source of constant strength. This project has been a tremendous learning experience, and I appreciate everyone who contributed, directly or indirectly, to its success.

REFERENCES

[1] Ahmad Amulet (2011) Computer Engineering Department King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia: A Graphical Password Authentication System.
[2] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. International Journal of Human-Computer Studies, 63:128–152, July 2005.
[3] Babich, A, 2012, Biometric Authentication, Type of Biometric Identifier
[4] Cynthia Kuo, Sasha Romanosky, Lorrie Faith Cranor; 2006; Human Selection of Mnemonic Phrasebased Passwords.
[5] Lackey, A. E., Pandey, T., Moshiri, M., Lalwani, N., Lall, C., & Bhargava, P. (2014). Productivity, part 2: cloud storage, remote meeting tools, screen casting, speech recognition software, password managers, and online data backup. Journal of the American College of Radiology, 11(6), 580-588.
[6] Li, Z., He, W., Akhawe, D., & Song, D. (2014). The emperor's new password manager: Security analysis of web-based password managers. In 23rd {USENIX} Security Symposium ({USENIX} Security 14) (page. 465-479).
[7] Petsas, T., Tritanomalies, G., Athanasopoulos, E., & Ioannidis, S. (2015, April). Two-factor authentication: is the world ready? Quantifying 2FA adoption. In Proceedings of the eighth European workshop on system security (page. 1-7).
[8] Weaning Yang, Jinghui Li, Omar Chowdhury, Aiping Xiong, Robert W. Proctor; 2016; An Empirical Study of Mnemonic Sentence-based Password Generation Strategies
[9] Weaning Yang, Jinghui Li, Omar Chowdhury, Aiping Xiong, Robert W. Proctor; 2016; An Empirical Study of Mnemonic Sentence-based Password Generation Strategies.
[10] Lackey, A. E., Pandey, T., Moshiri, M., Lalwani, N., Lall, C., & Bhargava, P. (2014). Productivity, part 2: cloud storage, remote meeting tools, screen casting, speech recognition software, password managers, and online data backup. Journal of the American College of Radiology, 11(6), 580-588.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY