

A PBL-II Report on
“Three Level Password Authentication System”

By

ROLL NO

NAME

15

Sanskar Darekar

05

Ritesh Auti

23

Hrishikesh Garje

24

Abhishek Gavand

Guided By

Prof. A. A. PATEL



विद्या ददाति विनयं, विनयाद् याति पात्रताम्।

Department of Computer Engineering
TSSM'S
Padmabhooshan Vasantdada Patil Institute of Technology,
Bavdhan, Pune-21

TSSM'S
Padmabhooshan Vasantdada Patil Institute of Technology, Bavdhan, Pune-21



विद्या ददाति विनयं, विनयाद् याति पात्रताम्

CERTIFICATE

This is to certify that Mr/Ms.

Sanskar Darekar

Ritesh Auti

Hrishikesh Garje

Abhishek Gavand

with Exam Seat No.

S190484224 S190484209

S190484233 S190484203

has successfully completed the Dissertation entitled

“Three Level Password Authentication System”

under my supervision, in the partial fulfillment of SE - Computer Engineering of Savitribai Phule Pune University.

Date :

Place :

Prof. AEMAN PATEL
Mentor,
Department of Computer Engineering

Prof. G. S. Wayal
Head,
Department of Computer Engineering

Dr. R . S . Pawar
Principal,
Padmabhooshan Vasantdada Patil Institute of Technology, Pune

Place : Pune

ACKNOWLEDGEMENT

First of all, we express our deep gratitude to our project guide Prof. A.A.Patel for her valuable support, help & guidance from time to time during the project work. We are also grateful to our Head of Department ,Prof.G.S.Wayal for giving us this opportunity to present this project report.

Last but not the least; we would like to thank our entire teaching and non-teaching staff who assisted us directly or indirectly throughout the duration of this project.

Name of student	Exam Seat No.
Sanskar Darekar	S190484224
Ritesh Auti	S190484209
Hrishikesh Garje	S190484233
Abhishek Gavand	S190484203

Index

SR.NO	Contents	PAGE NO.
1	Introduction	06
2	Literate Survey	07
3	Software Requirement	09
4	Project Scope	10
5	Assumptions and Dependencies	11
6	System Features	12
7	User interface	13
8	Safety Requirement	14
9.	Algorithm And Technologies Used	15
9	Outputs	16
10	Advantages	19
11	Disadvantages	21
12	System Block Diagram	23
13	Summary	24
14	Conclusion	25
15	References	26

ABSTRACT

Multi-Factor Authentication is an electronic authentication method in which a computer user is granted access to an application or a website only after successfully presenting two or more factors, or pieces of evidence.

It is the first step to protect systems against intruders since the traditional log-in methods (username and password) are not completely protected from hackers, since they can guess them easily using tools. Current Systems use additional methods to increase security.

The system incorporates user credentials, color-based passwords, and graphical-based passwords as successive layers of authentication, each adding a unique dimension to the overall security framework. By combining multiple authentication factors, the system offers enhanced protection against unauthorized access and security threats

This report introduces a comprehensive three-level password authentication system designed to provide robust security measures while ensuring user convenience and usability. The report outlines the methodology, features, advantages, disadvantages, software requirements, project scope, assumptions, and safety requirements of the proposed authentication system.

INTRODUCTION

Authentication is considered a very important verification method when someone is trying logging into computer resources, such as networks, applications, or devices. Several popular web services such as google and amazon employ multi-factor authentication as an optional feature that is deactivated by default. In IT industry, developers also face serious challenges for securing their systems, wherein unauthorized persons may easily damage many hours of software development, and since fall into consequences of breaking down the system. Consequently, authentication is the process or the action that decides whether a person or an application is allowed to access the system or not

Psychological research and modern practices support that humans can retrieve pictures faster and easier than words. When you read, for example, a car or a book, you automatically draw a picture of it in your mind, while if you mention words such as ‘amount’, ‘level’, ‘ease’, you may not draw anything and will only remember them as word

In an era marked by escalating cybersecurity threats, Traditional password-based authentication systems often fall short in providing protection, as they are susceptible to various vulnerabilities and attack vectors. Multi-factor authentication (MFA) systems address these shortcomings by requiring users to provide multiple forms of identification, thereby adding layers of security to the authentication process. This report presents a novel three-level password authentication system that combines user credentials, color-based passwords, and graphical-based passwords to establish a robust authentication framework. By leveraging diverse authentication factors, the system aims to enhance security while preserving user experience and ease of use.

LITERATURE SURVEY

Extensive research in the field of cybersecurity has underscored the limitations of traditional password-based authentication mechanisms and advocated for the adoption of multi-factor authentication solutions. Studies have explored a wide range of authentication methods, including biometrics, tokens, smart cards, and behavioral biometrics, highlighting their efficacy in enhancing security and mitigating the risk of unauthorized access.

Additionally, research has emphasized the importance of usability, user acceptance, and system efficiency in the design and implementation of authentication systems. By reviewing existing literature and best practices, this report aims to inform the development of a robust and user-friendly authentication system.

Advantages of traditional authentication:

1.Familiarity: Traditional authentication systems are widely known and understood by users. Most people are familiar with the concept of creating a username and password to access accounts and services.

2. Ease of Implementation: Implementing traditional authentication systems is relatively straightforward. Many programming languages and frameworks offer built-in support for username/password authentication, making it easy for developers to implement.

3.Low Cost: Traditional authentication systems typically require minimal infrastructure and resources, making them a cost-effective option for many organizations.

4.Flexibility: Traditional authentication systems can be adapted to various use cases and security requirements. Organizations can enforce password complexity rules, account lockout policies, and other security measures to enhance protection.

Disadvantages of traditional authentication :

- 1.Security Risks:** Username/password authentication has several security vulnerabilities, including password theft, phishing attacks, and brute-force attacks. Weak passwords, password reuse, and lack of multi-factor authentication (MFA) can increase the risk of unauthorized access.
- 2.User Experience:** Remembering multiple usernames and passwords for different accounts can be challenging for users. As a result, they may resort to using weak or easily guessable passwords, which compromises security.
- 3.Password Management:** Users often struggle with password management, such as creating strong passwords, securely storing them, and updating them regularly. Password reset processes can also be cumbersome and time-consuming for both users and support teams.
- 4.Single Point of Failure:** Traditional authentication systems rely on a single factor (password) for authentication. If a user's password is compromised, it can lead to unauthorized access to multiple accounts and services.

SOFTWARE REQUIREMENT

- **Development Environment:**

Software: Integrated Development Environment (IDE) such as Visual Studio Code, PyCharm.

Purpose: Write, test, and debug the application code.

- **Web Development:**

Software: Languages like HTML, CSS and Javascript.

Purpose: Develop web interfaces for user registration, login, and authentication.

- **Hashing and Encryption Libraries:**

Software: bcrypt, Argon2 (for password hashing), OpenSSL (for encryption).

Purpose: To Hash and encrypt sensitive information.

PROJECT SCOPE

The project scope encompasses the following key aspects:

- **System Design and Architecture:** Designing an intuitive and scalable architecture for the authentication system, including frontend and backend components, data storage, and communication protocols.
- **Authentication Algorithms:** Developing algorithms for generating color-based passwords and graphical-based passwords, ensuring randomness, uniqueness, and security.
- **User Interface Design:** Creating an intuitive and user-friendly interface for guiding users through the authentication process, providing feedback, and facilitating error handling and recovery procedures.
- **Backend Implementation:** Implementing backend functionality for user authentication, session management, account management, and database operations, adhering to security best practices and regulatory requirements.
- **Testing and Validation:** Conducting comprehensive testing and validation to assess the reliability, security, and performance of the authentication system under various scenarios and usage conditions.

ASSUMPTIONS AND DEPENDENCIES

The successful implementation and operation of the authentication system are contingent upon the following assumptions and dependencies:

- **Availability of Internet-Connected Devices:** Users have access to internet-connected devices such as smartphones, tablets, or computers capable of accessing the authentication system through web browsers.
- **Secure Storage and Transmission of Credentials:** The system relies on secure encryption techniques and protocols to protect the confidentiality and integrity of user credentials during transmission and storage.
- **User Compliance:** Users are expected to adhere to security best practices, including safeguarding their login credentials, promptly reporting any suspicious activity, and updating their passwords regularly.
- **Effective Error Handling and Recovery Mechanisms:** The system incorporates robust error handling and recovery mechanisms to address common issues such as login failures, forgotten passwords, and account lockouts effectively.

SYSTEM FEATURES

- **User Credential Authentication:** Users can create, manage, and authenticate their credentials (username and password) for accessing the system securely.
- **Color-Based Password Authentication:** Users select a sequence of colored balls to generate a password based on the chosen pattern, adding an additional layer of security beyond traditional alphanumeric passwords.
- **Graphical-Based Password Authentication:** Users arrange photos of chocolates in the correct order based on a dynamically generated sequence, leveraging visual cues and memory recall to authenticate successfully.
- **Account Management:** Users can perform account-related tasks such as password resets, account recovery, profile updates, and security settings customization.
- **Security Measures:** The system implements various security measures, including encryption, hashing, salting, session management, rate limiting, and intrusion detection, to mitigate security risks and safeguard user accounts and sensitive information.

USER INTERFACE

The user interface is designed to be intuitive, responsive, and user-friendly, catering to users of varying technical proficiencies and accessibility needs. Key features of the user interface include:

- **Clear Instructions:** Concise and easy-to-understand instructions are provided to guide users through the authentication process at each level.
- **Visual Feedback:** Visual cues, animations, and feedback mechanisms are incorporated to provide real-time feedback on user actions and authentication status.
- **Error Handling:** Clear and informative error messages are displayed to assist users in resolving issues such as incorrect inputs, password mismatches, or authentication failures.
- **Accessibility:** The user interface is designed to be accessible to users with diverse abilities, supporting keyboard navigation, screen readers, and other assistive technologies to ensure inclusive user experiences.

SAFETY REQUIREMENT

To ensure the safety and security of user accounts and sensitive information, the authentication system adheres to the following safety requirements:

- **Data Encryption:** User credentials, authentication tokens, and sensitive data are encrypted using strong cryptographic algorithms and protocols during transmission and storage.
- **Secure Communication:** Secure communication channels (e.g., HTTPS) are employed to protect data exchanged between clients and servers, mitigating the risk of eavesdropping and man-in-the-middle attacks.
- **Access Controls:** Access controls and permissions are enforced to restrict unauthorized access to system resources, APIs, and administrative functionalities, preventing privilege escalation and unauthorized data manipulation.
- **Audit Trails:** Comprehensive logging and auditing mechanisms are implemented to track user activities, system events, and security-related incidents, facilitating forensic analysis, compliance monitoring, and incident response.
- **Regular Security Updates:** The system undergoes regular security updates, patches, and vulnerability assessments to address emerging threats, software vulnerabilities, and compliance requirements, ensuring ongoing protection and resilience against security risks.

ALGORITHM AND TECHNOLOGY USED

- **Color-Based Password Algorithm:** The system utilizes a custom algorithm to map selected colors to alphanumeric characters, generating unique passwords based on the chosen color sequence. The algorithm ensures randomness, uniqueness, and security while allowing users to create memorable and visually distinctive passwords.
- **Graphical-Based Password Algorithm:** A dynamic algorithm generates sequences of chocolate photos, which users must arrange in the correct order based on a predetermined pattern. The algorithm leverages visual memory cues and spatial reasoning to create an engaging and secure authentication method that is resistant to common attacks such as shoulder surfing and brute force.
- **Technology Stack:** The system is built using a modern technology stack comprising frontend and backend technologies, including HTML, CSS, JavaScript, Node.js, Express.js, MongoDB, and cryptographic libraries. The choice of technologies emphasizes scalability, performance, security, and developer productivity, enabling the efficient implementation and operation of the authentication system.

OUTPUTS:

Register

Select Security Question

Register

Already have an account? [Login](#)

Login

Login

Forgot Password?

Don't have an account? [Register](#)

Create Color Pattern Password



Reset

Register

Chocolates Preference Authentication

Order Names:

5star, Dairymilk, Ferrero Rocher, Snickers, Kitkat

Refresh Order


Preference:



1



1



1



1



1

Reset Preferences

Login

ADVANTAGES

1. **Enhanced Security:** The utilization of multiple authentication factors significantly reduces the likelihood of unauthorized access and strengthens the overall security posture of the system.
2. **User Convenience:** Despite the added layers of security, the authentication system is designed to be intuitive and user-friendly, minimizing friction in the login process and enhancing user satisfaction.
3. **Adaptability:** The system offers flexibility in accommodating various authentication factors, allowing organizations to tailor the authentication process to their specific security requirements and user preferences.
4. **Resilience to Attacks:** By incorporating diverse authentication factors, the system mitigates the risk of common attack vectors such as brute force attacks, password guessing, and credential theft, thereby enhancing resilience against security breaches.
5. **Enhanced User Confidence:** The implementation of advanced authentication methods instills confidence in users regarding the security of their accounts and sensitive information, fostering trust and loyalty towards the system or platform.
6. **Customization and Personalization:** The system allows for customization and personalization of authentication processes, enabling organizations to tailor authentication methods based on user preferences, security requirements, and industry regulations.

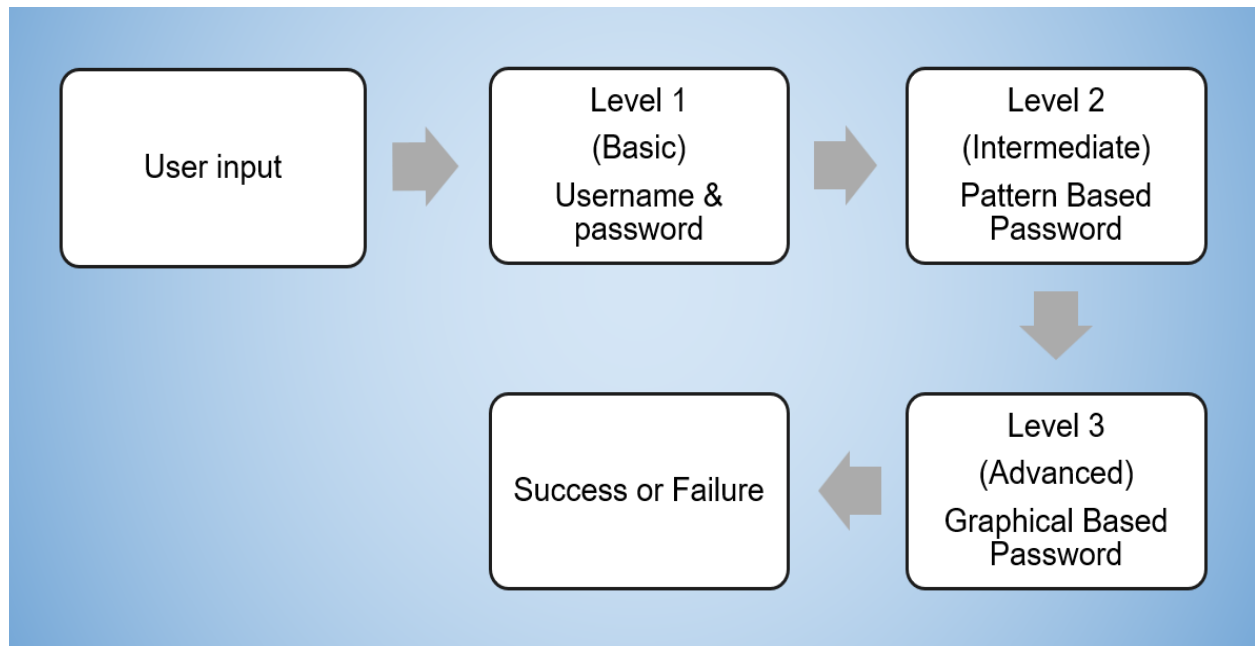
7. **Adoption of Industry Best Practices:** Incorporating industry best practices such as two-factor authentication (2FA), multi-factor authentication (MFA), and risk-based authentication (RBA) elevates the security posture of the system, aligning it with global standards and benchmarks.

DISADVANTAGES

1. **Complexity:** Implementing and managing a multi-level authentication system may entail additional complexity in terms of system architecture, maintenance, and user training, potentially posing challenges for organizations with limited resources or technical expertise.
2. **User Training:** Users may require training and guidance to familiarize themselves with the authentication process and understand the significance of multi-factor authentication in safeguarding their accounts, necessitating ongoing education and awareness initiatives.
3. **Risk of Lockout:** Inadvertent errors or forgotten credentials could lead to user lockout or account suspension, necessitating robust account recovery mechanisms and user support services to address such incidents promptly and efficiently.
4. **User Education and Training:** Educating users about the importance of robust authentication practices and guiding them through the authentication process is vital. Comprehensive training programs can enhance user awareness and compliance, minimizing the risk of security breaches due to human error.
5. **Scalability and Performance Optimization:** As user populations and transaction volumes grow, ensuring scalability and optimal performance of the authentication system becomes critical, necessitating load testing, performance tuning, and scalability enhancements to meet evolving demands.

6. **Regulatory Compliance Burden:** Compliance with evolving regulatory requirements and industry standards imposes a significant burden, necessitating continuous monitoring, updates, and adherence to compliance frameworks to mitigate legal and regulatory risks

SYSTEM BLOCK DIAGRAM



SUMMARY

In summary, the proposed three-level password authentication system represents a significant advancement in user authentication techniques, offering a robust and user-friendly solution for securing online accounts against unauthorized access and security threats.

By integrating multiple authentication factors, leveraging advanced algorithms, and adhering to best practices in software engineering and cybersecurity, the system provides a secure, reliable, and flexible authentication framework that meets the evolving needs of users and organizations in an increasingly digital world.

CONCLUSION

A multi-factor authentication system that combines the ease of use and the low-cost factors is proposed. The system did not need any special settings or infrastructure. It was designed depending on graphical passwords. In registration phase, the user might choose and memorize three or more images. In the login phase, the user needed only to choose the correct images that he has chosen during the registration process in a specific order. The proposed system might overcome many different security threats, such as key-loggers, screen capture attack or shoulder surfing.

The three-level password system is a smart way to keep online accounts safe. By using multiple layers of security, it's much harder for bad guys to get in. Even though it's more secure, it's still easy for you to log in. It's a good solution for anyone who wants to protect their online stuff better.

REFERENCE

Research papers:

1.Multi factor authentication by Bandar Omar ALSalee published in 2021

2.IRJMETs - Three level Password Authentication System by N Chaitra ,Pratibha,Dr. Rajashree V Biradar published in 2022.