**LOGIN-AUTHENTICATION**

A MINI PROJECT REPORT

Submitted by:

*G -26A*

Mohd.Arshad Malik-2210990580

Mohd.Ishaan – 2210990581

Monalika – 2210990582

Mona Kumar - 2210990583

in partial fulfillment for the award of the degree of

BACHELEOR OF ENGINEERING

***in***

COMPUTER SCIENCE & ENGINEERING

****

**CHITKARA UNIVERSITY**

**CHANDIGARH-PATIALA NATIONAL HIGHWAY**

**RAJPURA (PATIALA) PUNJAB-140401 (INDIA)**

**04/2023**

###### TABLE OF CONTENTS

|  |  |  |
| --- | --- | --- |
| Sr.no | Section | Page no |
| 1 | Introduction | 1 |
| 2 | Problem Statement | 1 |
| 3 | Case study | 2 |
| 4 | Technical details | 3 |
| 5 | Objectives | 3 |
| 6 | Methodology | 4 |
| 7 | Project Advantages | 5-6 |
| 8 | Results | 7 |
| 9 | Future scope | 7 |

**1.Introduction**

**The title of the project is “Login Authentication” and the team member’s names are:**

1. **Mohd Arshad Malik,**
2. **Mohd Ishaan,**
3. **Monalika**
4. **Monu Kumar**

**Login authentication is the process of verifying the identity of a user who is trying to access a system or application. It is a crucial security measure to ensure that only authorized users can access sensitive data or perform actions within the system. In this project report, we will discuss the implementation of a login authentication system using a web application as an example.**

**This project aims to develop a secure and reliable system that verifies the identity of users before granting them access to a protected platform or application. The system will authenticate user credentials such as usernames and passwords, ensuring that only authorized individuals can access the system's resources.**

**2.Problem Statement**

In this project, we will be designing a simple log-in-authentication system. Authentication is a process of validating a user, hence it requires a username and password like any web system we use. Authentication is an activity to authenticate the person credential that wishes to perform the activity. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user.In this project,there is a website’s login authentication bar- where users enter their email ID/username and password to log in to the site. In simple words,it is the way of confirming the identity of a user while they access their profile on a particular platform.

**Case study**

**1.Project Goals:**

* Develop a secure and reliable login authentication system for the e-commerce platform.
* Implement strong password policies and encryption techniques to safeguard user credentials.
* Prevent unauthorized access and protect user accounts from brute-force attacks.
* Provide a password recovery mechanism to assist users who forget their passwords.
* Maintain a secure session management system to protect against session hijacking.

**2. System design**

* User Registration: A registration module where users can create new accounts by providing their personal details and creating a password.
* Login Process: A login module that verifies user credentials against stored data and grants access to authorized users.
* Password Security: Implementation of password policies, including complexity requirements, hashing, and salting techniques to protect stored passwords.
* Account Lockout: Mechanism to lock user accounts temporarily after multiple failed login attempts within a specified time frame.
* Password Recovery: Secure options for users to recover their passwords, such as email-based password reset links or security questions.

**3. Results and Benefits:**

* The implementation of the login authentication system will significantly enhance the security of the e-commerce platform, protecting user accounts and sensitive data.
* User confidence and trust in the platform will increase, leading to improved customer satisfaction and increased usage of the e-commerce services.

**Technical details**

1.We will first create the simple structure with HTML and then move to make it look great with CSS.

2.A login page in HTML collects information from the user and log in button to send the details for server-side operations.

**Objectives**

The main objective of this project is to develop a login authentication system that will ensure that only authorized users can access the web application. The system shouldbe secure, easy to use, and should provide a seamless user experience.

**Methodology**

The login authentication system will be developed using the following steps:

**Step 1: User Registration**

The first step is to allow users to register on the web application. During the registration process, users will be required to provide their name, email address, and a strong password. The password will be encrypted and stored in a secure database.

**Step 2: Login Page**

The login page will allow users to enter their email address and password. The email address and password will be verified against the database to confirm that the user is authorized to access the web application.

**Step 3: Session Management**

Once the user has successfully logged in, a session will be created that will allow the user to navigate through the web application without having to re-enter their credentials for every page. The session will be terminated automatically after a set period of inactivity or when the user logs out.

**Step 4: Password Reset**

In case a user forgets their password, the system will provide an option to reset the password. This will involve sending a password reset link to the user's email address, which will allow them to create a new password.

**Advantages:**

There are several advantages of implementing login authentication in a web application or system, including:

**1.Security**: The primary advantage of login authentication is the security it provides. By requiring users to provide valid login credentials, such as a username and password, the system can verify their identity and ensure that only authorized users have access to sensitive information or functionality within the system.

**2.User Accountability**: Login authentication helps to establish user accountability. By requiring users to login with their unique credentials, the system can track their activity within the system and identify who performed specific actions or accessed particular data.

**3.Personalization:** Login authentication allows the system to personalize the user's experience by providing them with customized content, settings, and preferences based on their login credentials and activity history.

**4.Access Control**: Login authentication enables access control, which means that the system can restrict access to certain areas or functions based on the user's login credentials or user group membership. This helps to ensure that users only have access to the information and functionality that they need to perform their job or task.

**5.Data Protection:** Login authentication helps to protect sensitive data from unauthorized access. By requiring valid login credentials, the system can verify that the user has the appropriate permissions to access the data, and can encrypt or restrict access to the data to prevent unauthorized use or disclosure.

Overall, login authentication is a critical security measure that provides several benefits, including increased security, user accountability, personalization, access control, and data protection.

**Results:**

The login authentication system will provide a secure and user-friendly experience for users. The system will ensure that only authorized users can access the web application and that their data is protected from unauthorized access. The system will also provide a seamless user experience, with automatic session management and password reset functionality.

**Future Scope:**

The future scope of login authentication is continuously evolving, and new technologies are being developed to enhance security and improve user experience. Here are some of the potential future developments in login authentication:

**1.Biometric Authentication:** Biometric authentication, such as fingerprint or facial recognition, is becoming more prevalent as a login authentication method. Biometric authentication can provide a higher level of security and convenience than traditional username and password login methods.

**2.Multi-factor Authentication (MFA):** MFA is a method of authentication that requires users to provide multiple forms of identification before accessing a system. This could include a combination of a password, a physical token, and biometric authentication.

**3.Passwordless Authentication:** Passwordless authentication is a newer authentication method that eliminates the need for a password. Instead, users are authenticated through alternative means such as biometric authentication, email verification, or SMS verification.

**4.Blockchain Authentication**: Blockchain technology is being explored as a potential authentication method. The decentralized nature of blockchain could provide a high level of security and prevent unauthorized access to a system.

**5.Adaptive Authentication:** Adaptive authentication is a method that assesses the risk of a login attempt and adjusts the authentication requirements accordingly. This could include requesting additional authentication factors for high-risk login attempts.

Overall, the future scope of login authentication is focused on enhancing security and user experience through new technologies and methods. As technology continues to evolve, it is likely that new authentication methods will emerge that provide even greater security and convenience for users.

**Conclusion:**

A login authentication system is an essential security measure for any web application that requires user authentication. By implementing a secure and user-friendly login authentication system, we can ensure that only authorized users can access the system, protecting sensitive data from unauthorized access. The system can be further improved by adding two-factor authentication or implementing a password policy that ensures users create strong passwords.