USER AUTHENTICATION MODULE (OS)

Submitted by: Dheeraj Kumar
Registration ID: 12417074
Roll NO: 17
Course: Computer science and Engineering(B.tech)
Batch: 2024 -28

Signature: *Dheeraj Kumar*

Submitted to: Amandeep kaur
Date: 17 December, 2025

DECLARATION

I hereby declare that the project work entitled "USER AUTHENTICATION MODULE IN OS" is an authentic

record of my own work carried out as requirements of Project for the award of B. Tech degree in Computer Science and Engineering from Lovely Professional University, Phagwara, under the guidance Amandeep Kaur, during January to December 2025. All the information furnished in this project report is based on my own intensive work and is genuine.

NAME: Dheeraj Kumar
ID: 12417074

17th December, 2025

Acknowledgement

I would like to express my sincere gratitude to my faculty and guide for their valuable support, guidance, and encouragement throughout the development of this User Authentication Module project. Their insights helped me understand core operating system concepts such as security, password management, and access control. I am also thankful to my friends and family for their motivation and feedback. This project enhanced my practical skills and deepened my interest in system security and software development.

Aim of This Project

The aim of this project is to design and develop a secure user authentication module for an operating system that

ensures only authorized users can access system resources. It focuses on implementing user registration, password verification, and account protection techniques to enhance system security. The project aims to provide practical understanding of authentication principles, secure data handling, and system access control mechanisms.

System Requiredments

Hardware

RAM, Processor and Disk Space

Softwares

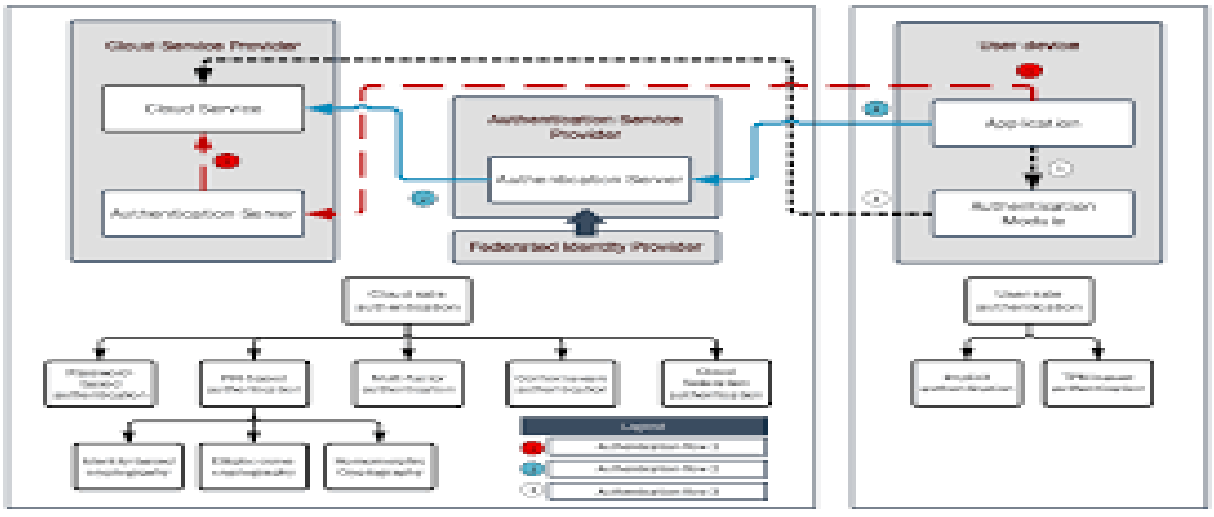
C and code editor, vs Code and Ubuntu Linux

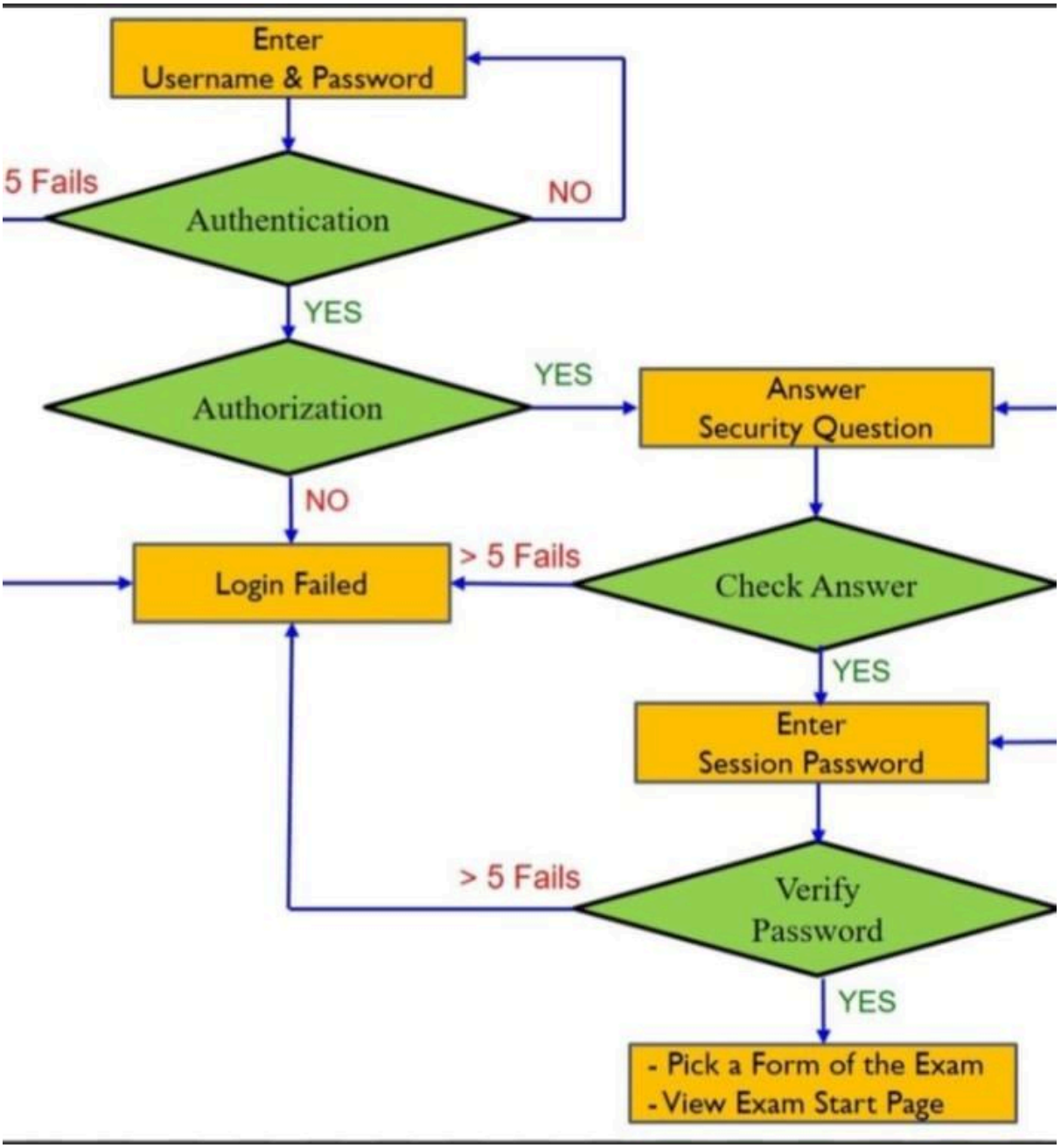
System Design

Architecture Design

Flowchart

ER Diagram





Abstract

This project presents a User Authentication Module designed to ensure secure access within an operating system. It includes user registration, password management, login verification, and security checks to

prevent unauthorized usage. By implementing encryption and validation techniques, the module enhances system protection while improving user experience. The project demonstrates practical understanding of authentication principles and secure software development.

Introduction

User authentication is a vital aspect of operating system security, ensuring that only authorized users can access system resources. This project focuses on designing a secure authentication module that manages user registration, login validation, password handling, and basic security controls. It aims to provide hands-on understanding of OS security concepts while demonstrating how authentication mechanisms protect data, enhance system reliability, and support safe computing environments.

Working Principle

The User Authentication Module works on the principle of identity verification and access control. When a user registers, their details such as username, password, and security information are securely stored after hashing and salting the password. During login, the entered credentials are compared with stored encrypted values. If they match, access is granted; otherwise, the system denies entry. The module may include security

questions, OTP verification, or lockout features to prevent brute-force attacks. It maintains session validity to track logged-in users and ensures only authenticated users can change or delete passwords. The module enhances system security by preventing unauthorized access, safeguarding user data, and ensuring accountability within the operating system environment.

Implementation

1. Modules / Components Used

Explain parts of your project, example for OS authentication project:

✔ User Registration Module – stores new user credentials
✔ Login Authentication Module – verifies username & password
✔ Password Hashing Module – secures password
✔ Database/File Handling Module – stores user data
✔ Security & Error Handling Module – prevents invalid access

The registration module collects username, password, security question, and stores hashed credentials.
➡ The login module compares entered password hash with stored hash and allows access.
➡ File handling module reads & writes encrypted user data securely.

Output

```
root@DESKTOP-PA9N2QK:~# ./RaaZ

==== USER AUTHENTICATION MODULE ⚙️ ====
1. Register New User:
2. Login (2FA):
3. Recover Password:
4. Change Security Question:
5. View all Logs:
6. List all Users:
7. Delete User:
8. Exit
➡️ Select Option From 1 to 8: 1

--- New User Registration 📝 ---
➡️ Enter username: dheeraj
➡️ Enter strong password: Kumar@123
➡️ Enter security question: raaz
➡️ Enter answer: raaz
✅ User registered successfully.

==== USER AUTHENTICATION MODULE ⚙️ ====
1. Register New User:
2. Login (2FA):
3. Recover Password:
4. Change Security Question:
5. View all Logs:
6. List all Users:
7. Delete User:
```

8. Exit
➡️ Select Option From 1 to 8: 2

--- User Login 🔑 ---
➡️ Enter username: dheeraj
➡️ Enter password: Kumar@123

[Simulated OTP Sent] 📧 -> 533153
➡️ Enter OTP: 533153
✅ Login successful! Welcome dheeraj. 🚀

==== USER AUTHENTICATION MODULE ⚙️ ====
1. Register New User:
2. Login (2FA):
3. Recover Password:
4. Change Security Question:
5. View all Logs:
6. List all Users:
7. Delete User:
8. Exit
➡️ Select Option From 1 to 8: 6

--- User List 👥 ---
👤 - dheeraj
👤 - raaz
👤 -
👤 - amit
👤 - rahul
👤 - himanshu

👤 - shami

==== USER AUTHENTICATION MODULE ⚙️ ====
1. Register New User:
2. Login (2FA):
3. Recover Password:
4. Change Security Question:
5. View all Logs:
6. List all Users:
7. Delete User:
8. Exit
➡️ Select Option From 1 to 8: 7

--- Delete User 🗑️ ---
➡️ Enter username: amit
✅ User deleted.

==== USER AUTHENTICATION MODULE ⚙️ ====
1. Register New User:
2. Login (2FA):
3. Recover Password:
4. Change Security Question:
5. View all Logs:
6. List all Users:
7. Delete User:
8. Exit
➡️ Select Option From 1 to 8:

Conclusion

The project successfully ensures secure user access through password protection, verification, and data integrity. It strengthens system security by preventing unauthorized access, improving reliability, and demonstrating how authentication mechanisms safeguard sensitive information within an operating system environment.

Future Scope

The user authentication module can be enhanced with biometric login, AI-based fraud detection, cloud-based authentication, and multi-factor security. Future upgrades may include role-based access control, encryption improvements, mobile integration, and real-time monitoring. These advancements will increase security, improve user experience, and ensure adaptability for modern operating systems and enterprise applications.

Reference

1. Abraham Silberschatz, Peter B. Galvin, Greg Gagne, Operating System Concepts, Wiley Publications.

2. Andrew S. Tanenbaum, Modern Operating Systems, Pearson Education.

3. Research articles on authentication and security techniques from IEEE Xplore Digital Library.