Secure Software Design & Engineering

(Week 3 Deliverable)

Group Members:

Arsalan Khan - 2022115

Saad Ali - 2022512

Submitted to: Dr. Zubair Ahmad

TA: Ma'am Jazia

March 21, 2025

1 Introduction

This project aims to develop a secure ride-hailing platform that enables users to book rides, communicate with drivers, and track ride history. The security framework focuses on authentication, encryption, and access control to protect sensitive data and user interactions.

2 System Architecture

The system consists of the following components:

- **Client Applications:** Includes user, driver, and optional admin interfaces.
- **Backend Services:** Manages authentication, ride booking, and real-time chat.
- **Databases:** Stores user credentials, ride data, and chat logs securely.
- **External Services:** Handles geolocation and payment processing.

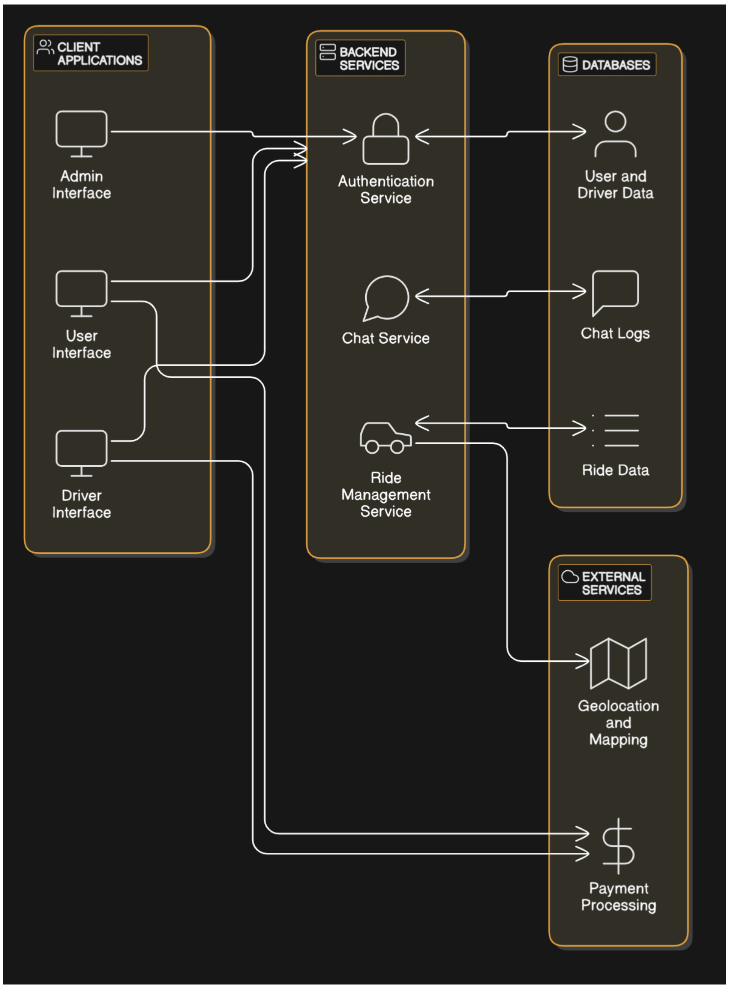

Figure 1: System Architecture Diagram

3 Security Controls

The security design implements the following controls:

3.1 Authentication

- Password hashing using bcrypt.
- JWT-based session management.

3.2 Encryption

- Encrypt sensitive data in transit and at rest.
- Secure chat messages.

3.3 Access Control

- Role-based access control (RBAC).
- Restricted admin access.

3.4 Input Validation and Sanitization

- Prevent SQL injection and XSS attacks.
- Use prepared statements for queries.

3.5 Secure Communication

- Enforce HTTPS.
- Secure real-time chat features.

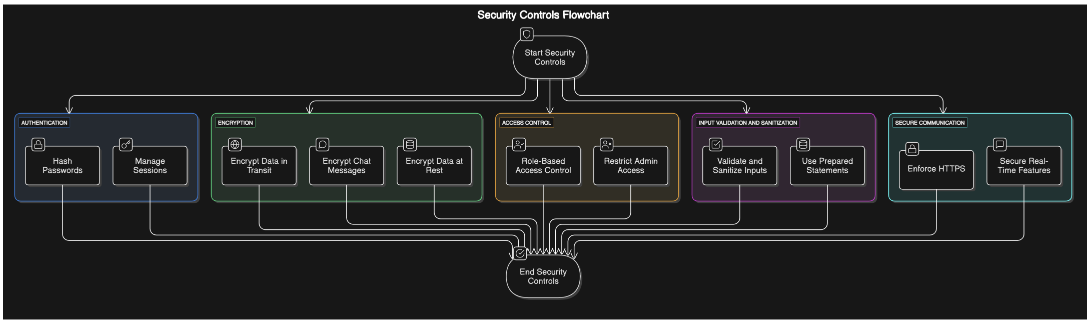

Figure 2: Security Controls Flowchart

4 Security Design Measures

To enhance security, we implement:

- **Regular Security Audits:** Periodic vulnerability assessments.
- **User Awareness:** Educating users on secure login practices.
- **Incident Response Plan:** Protocols to handle security breaches.
- **Compliance:** Adherence to GDPR and security best practices.

5 Conclusion

This report outlines a secure system architecture for the ride-hailing platform. With strong authentication, encryption, and access control, the platform ensures a safe environment for users and drivers. Future improvements will include advanced monitoring and AI-driven threat detection.