# CS 255 System Design Document Template

Alondra Paulino Santos

October 19, 2025

## UML Diagrams

### UML Use Case Diagram

A diagram of a diagram

AI-generated content may be incorrect.

### UML Activity Diagrams

A diagram of a process

AI-generated content may be incorrect.

A diagram of a test

AI-generated content may be incorrect.

### UML Sequence Diagram

A diagram of a software application

AI-generated content may be incorrect.

### UML Class Diagram

A diagram of a server

AI-generated content may be incorrect.

## Technical Requirements

The DriverPass system shall be developed as a secure, web-based application designed to provide a reliable and user-friendly experience for students, instructors, secretaries, and administrators. These technical requirements outline the hardware, software, security measures, and infrastructure necessary to ensure the system’s performance, scalability, and data protection.

**Hardware and Infrastructure Requirements**

• The system shall be hosted in a cloud-based environment such as AWS or Microsoft Azure to ensure scalability, reliability, and uptime.

• Web and application servers shall require a minimum of 2 virtual CPUs and 4–8 GB RAM to maintain consistent performance during peak hours.

• A relational database instance (PostgreSQL 14+ or MySQL 8.0+) shall manage lesson schedules, user profiles, and transactions.

• Automated backups and multi-zone replication shall protect against data loss and maintain service continuity.

**Software and Operating Systems**

• Client-side support: Windows 10+, macOS 12+, iOS 15+, and Android 12+.

• Server environment: Linux (Ubuntu 22.04 LTS) or Windows Server 2019 for hosting.

• Supported browsers: Latest versions of Chrome, Edge, Firefox, and Safari.

• Frontend technologies: HTML5, CSS3, JavaScript, and React for responsive, accessible interfaces.

• Backend framework: Java Spring Boot to handle scheduling, authentication, and API communication.

**Security Requirements**

• All communications between users and the server shall be encrypted using TLS 1.3.

• User credentials shall be protected through bcrypt hashing, and all sensitive data shall be stored using AES-256 encryption.

• The system shall rely on third-party payment processors (Stripe or Braintree) that comply with PCI-DSS standards for secure financial transactions.

• Regular security audits shall be conducted to address emerging threats and maintain compliance.

**Integration and Connectivity**

• DriverPass shall synchronize with Department of Motor Vehicles (DMV) databases via secure APIs to ensure that study materials and test requirements reflect current laws.

• The system shall provide automated reports and real-time updates for administrators, instructors, and students.

**Tools and Maintenance**

• Development and version control shall be managed through GitHub, with CI/CD pipelines automating testing and deployment.

• Developers shall use Eclipse IDE or IntelliJ IDEA for backend work and Visual Studio Code for frontend development.

• System performance shall be monitored through AWS CloudWatch or Azure Monitor to ensure reliability and uptime.

**Summary of Key Technical Requirements**

• Cloud-hosted web system compatible with Windows, macOS, iOS, and Android.

• Backend implemented using Java Spring Boot with PostgreSQL/MySQL databases.

• Secure DMV integration and API-based data synchronization.

• High availability (99% uptime) and data protection via encryption standards (TLS 1.3, AES-256).

• Automated backups, scalability, and centralized monitoring for performance stability.

Implementing these technical requirements shall allow DriverPass to operate as a secure, efficient, and scalable web-based solution that aligns with the organization’s goals of improving student access, instructor coordination, and administrative oversight. This technical foundation ensures long-term maintainability, data protection, and consistent performance across all supported devices.