# CS 255 System Design Document Template

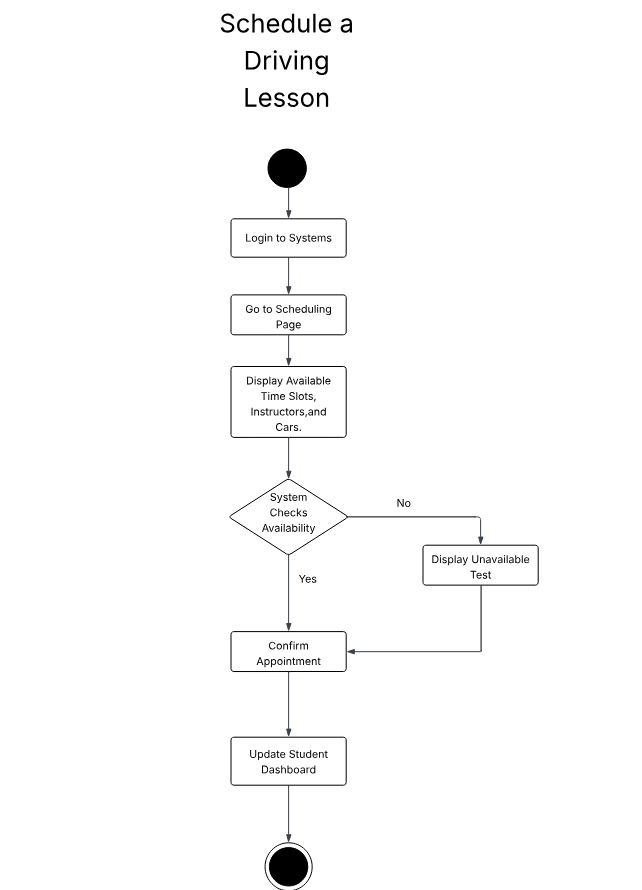
## UML Diagrams

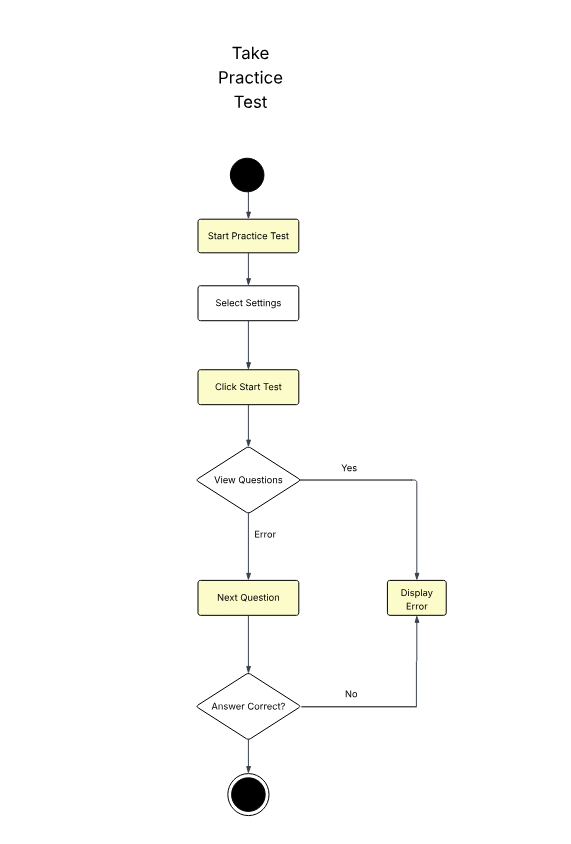
### UML Use Case Diagram

*A diagram of a diagram

AI-generated content may be incorrect.*

### UML Activity Diagrams

**

**

### UML Sequence Diagram

A screen shot of a diagram

AI-generated content may be incorrect.

### UML Class Diagram

A diagram of a student

AI-generated content may be incorrect.

## Technical Requirements

*A secure, scalable, and responsive online application is how the DriverPass system is intended to function. The system needs a cloud-hosted infrastructure, such Google Cloud Platform, Microsoft Azure, or Amazon Web Services (AWS), to enable its capability. Both the relational database and the backend services will be housed in the server environment, guaranteeing scalability and high availability. Students, teachers, and administrators will use contemporary desktop or mobile devices with dependable internet access to access the system. Automated backups and a redundant failover server setup are advised to preserve data integrity and system dependability.*

*The system will make use of common web technologies on the software side. HTML5, CSS3, JavaScript, and perhaps a responsive framework like Angular or React will be used to build the front end. A stable programming language like Python (with Flask or Django), Java, or Node.js will be used to construct the backend logic. A secure MySQL or PostgreSQL database hosted in the cloud will house the data. In order to provide users with updates and appointment confirmations, the backend will also interface with an email delivery provider like SendGrid or Mailgun.*

*An integrated development environment (IDE) like Visual Studio Code or IntelliJ IDEA, a version control system like Git (with repositories hosted on GitHub or GitLab), and tools like Lucidchart for modeling UML diagrams will all be used in the system's creation and upkeep. Jenkins and GitHub Actions are two examples of technologies that may be used to automate testing and deployment procedures for continuous integration and deployment (CI/CD).*

*Role-based access control (RBAC) and a secure authentication method utilizing OAuth 2.0 or JSON Web Tokens (JWT) will be integrated into the system from an infrastructure standpoint. SSL/TLS encryption will be used to secure all client-server communications. Tools like AWS CloudWatch or the ELK (Elasticsearch, Logstash, Kibana) stack will be used for security and performance monitoring. When combined, these technologies will help the DriverPass system achieve its functional objectives while adhering to strict security, scalability, and usability guidelines.*