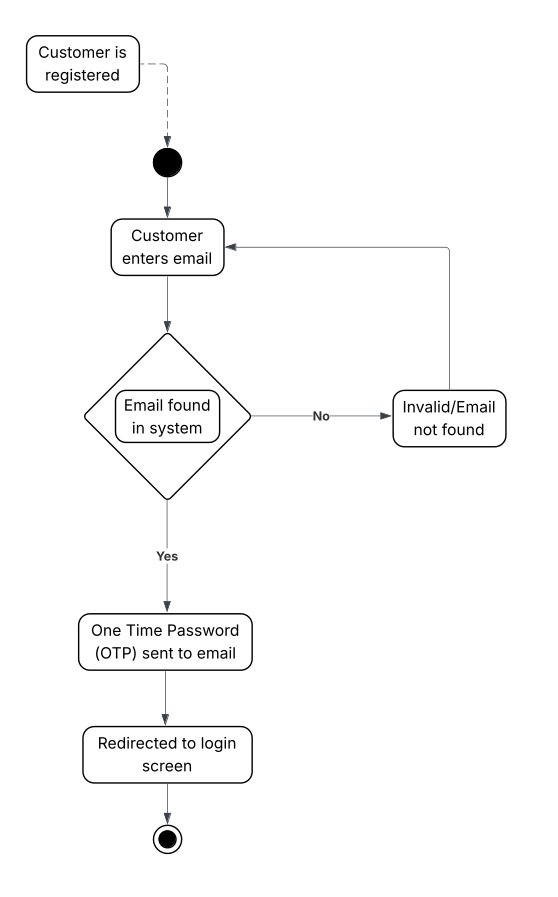
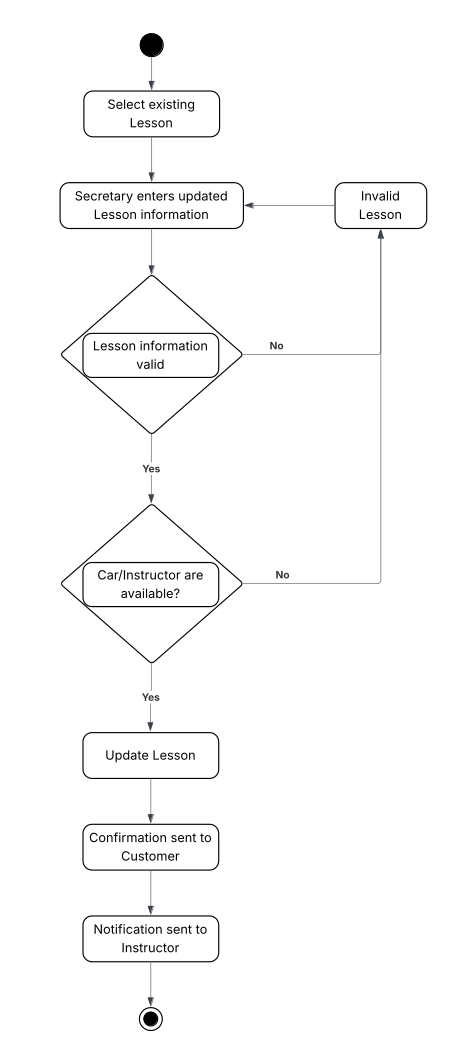
# CS 255 System Design Document Template

## UML Diagrams

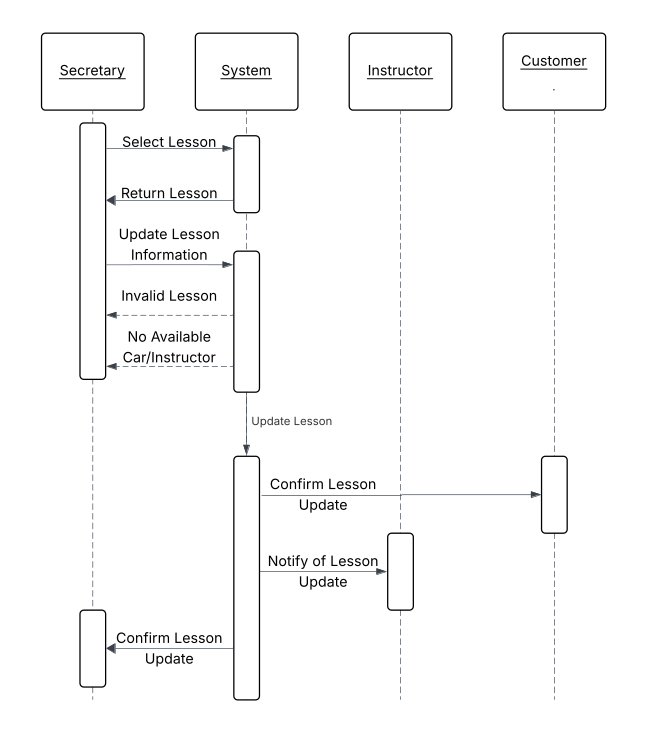
### UML Use Case Diagram

### 

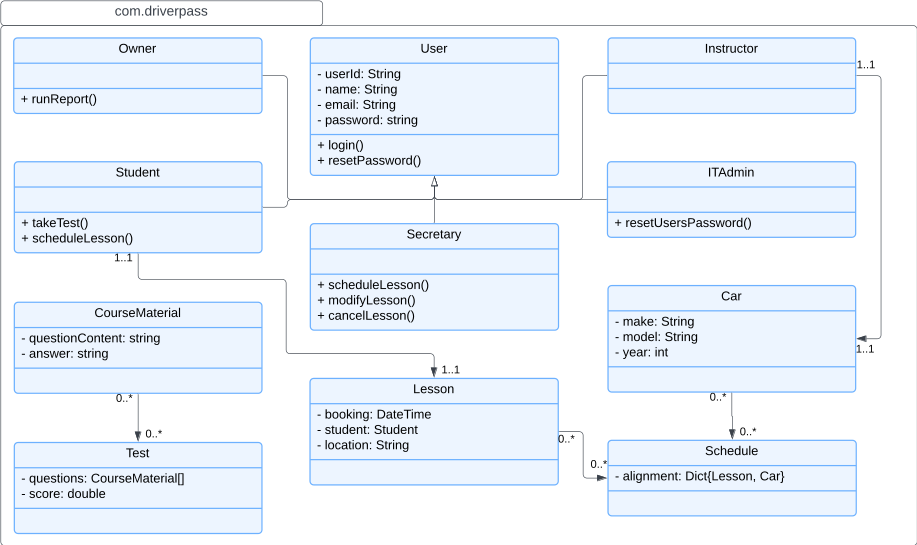
### UML Activity Diagrams



### UML Sequence Diagram



### UML Class Diagram

**

## Technical Requirements

The technical foundation for DriverPass is a fully cloud-native architecture. This approach completely removes the need for you to purchase, manage, or maintain any physical server hardware, directly addressing your desire to focus on business operations rather than IT overhead. We've designed the system to be highly accessible for both your staff and customers; they will only need a device with a modern web browser and a reliable internet connection. This strategy ensures the system is easy to use and future-proofs it against changes in technology, all while leveraging a providers infrastructure for top-tier scalability and reliability.

On the software side, your application will be built upon a robust and scalable open-source stack. The backend services will run on a Linux operating system and utilize a managed database service (like SQL Server or PostgreSQL) to handle all of your data, including user accounts, schedules, and test results. By using a managed database, critical tasks like backups and security patching are automatically handled by the cloud provider. The application itself will be developed using a modern framework to ensure compatibility across all major web browsers. To meet your compliance needs, the required integration with the DMV will be handled through a secure API, ensuring your system can reliably receive notifications and updates.

The entire system will be securely deployed and managed using services designed for high performance and security. Your web application can be hosted on serverless instances, which allows for automated updates and dynamic scaling to handle user traffic. We can isolate your network within an virtual network, with access strictly controlled by firewall rules. Security is a top priority; all data transmitted between users and the server will be encrypted. The critical requirement for Role-Based Access Control (RBAC) can be implemented, allowing you to manage distinct permissions for each user type. Finally, the infrastructure will be continuously monitored, providing your IT Officer with real-time alerts for any performance issues or security threats, ensuring your business operations run smoothly.