

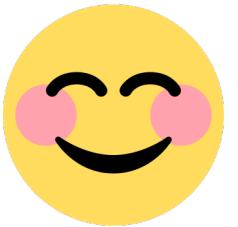
Educloud

Cloud Computing Project Presentation

BY TEAM 1



Team Member



Shital Hinge



Caihui Yang



**Akshat
Jangam**



**Dhruv
Basnotra**



Leni Jin



Atilla Karaali



**Maheswar
Barrenkala**



Qiong Zhang



Xu Liu



Project Overview

Objective

Provide an efficient, user-friendly course registration and account management system targeting the education sector for students, staff, and administrators.

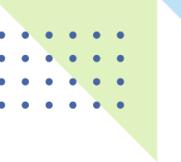
Background

With the rise of online education, schools need an efficient and secure system to manage user accounts and course registrations.

Target Audience

- Students
- Educational staff
- Administrators





Key Functionalities

Login Functionality

- **Account Sign-Up:** Supports creating accounts with distinct roles for students, staff, and administrators with specific access privileges.
- **Role-Specific Login:** Secure login system supporting multiple user roles with role-specific dashboards and permissions.

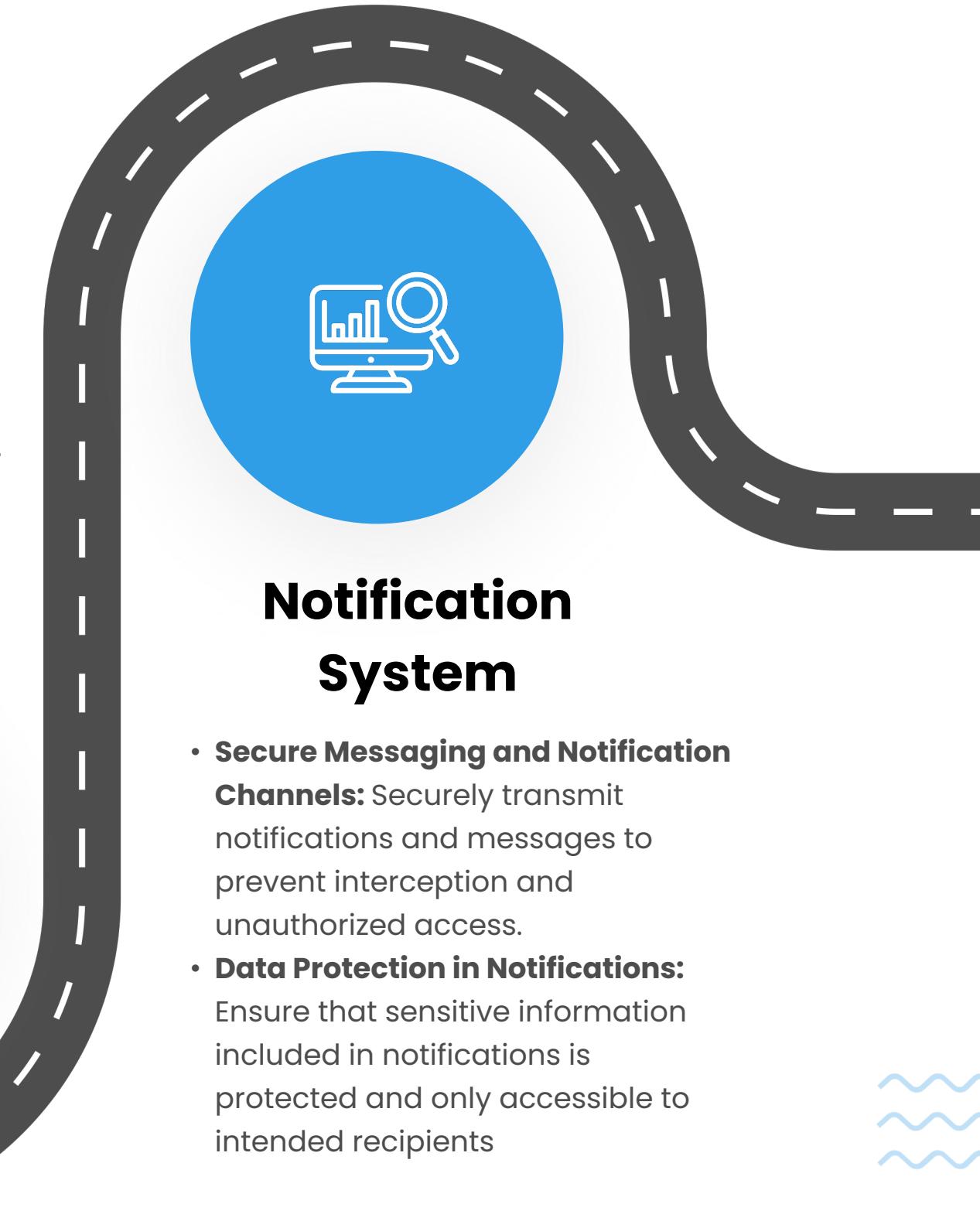


Course Registration System

- **Manual Course Registration:** Allows users to register for courses through a dropdown list, simplifying the registration process.
- **Future Improvements:** Plans for API integrations and a more advanced user interface.

Logout Functionality

- **Secure Session Termination:** Ensures user sessions are securely terminated to prevent unauthorized access.



Architecture Design Overview

System Architecture

Includes web server, API gateway, authentication service, course management service, notification service, and database services.

Microservices Architecture

1. Auth Service: Manages authentication, uses Amazon RDS for user data.
2. Course Upload Service: Stores course data in DocumentDB and Amazon S3.
3. Course Search and Registration Service: Uses ElasticSearch for search, stores data in relational databases and Cassandra, utilizes cache for performance.
4. Notification Service: Sends notifications using Kafka for event-driven communication.

01

02

03

04



Design Topology

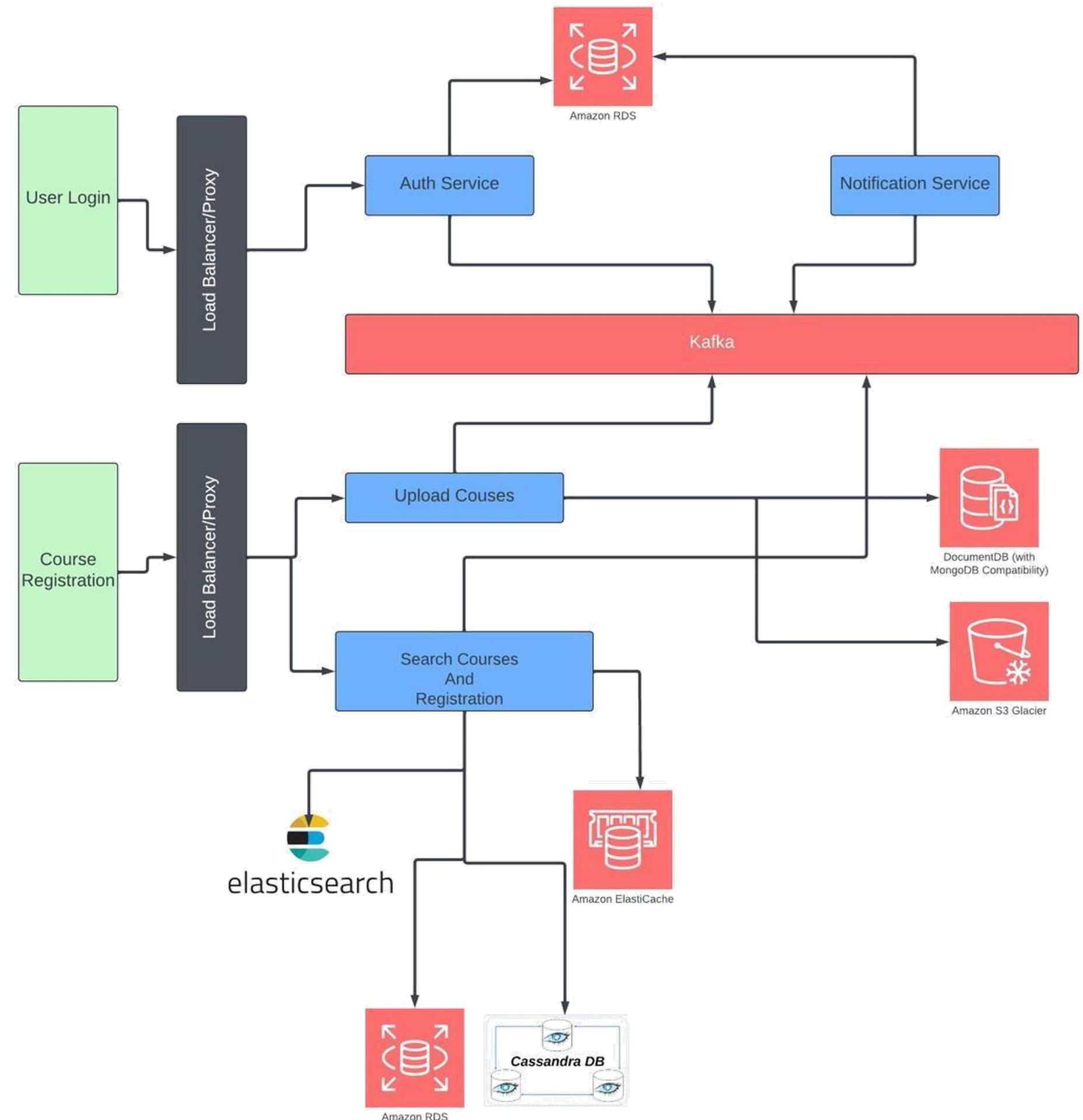
1. User task flow diagram from login to course registration and logout.
2. Service interaction sequence diagrams.

Cloud Deployment

1. Uses AWS services (EC2, RDS, DocumentDB, S3).
2. Managed by Kubernetes for high availability and automatic scaling.



Design Architecture Topology



Color Coding

Microservices

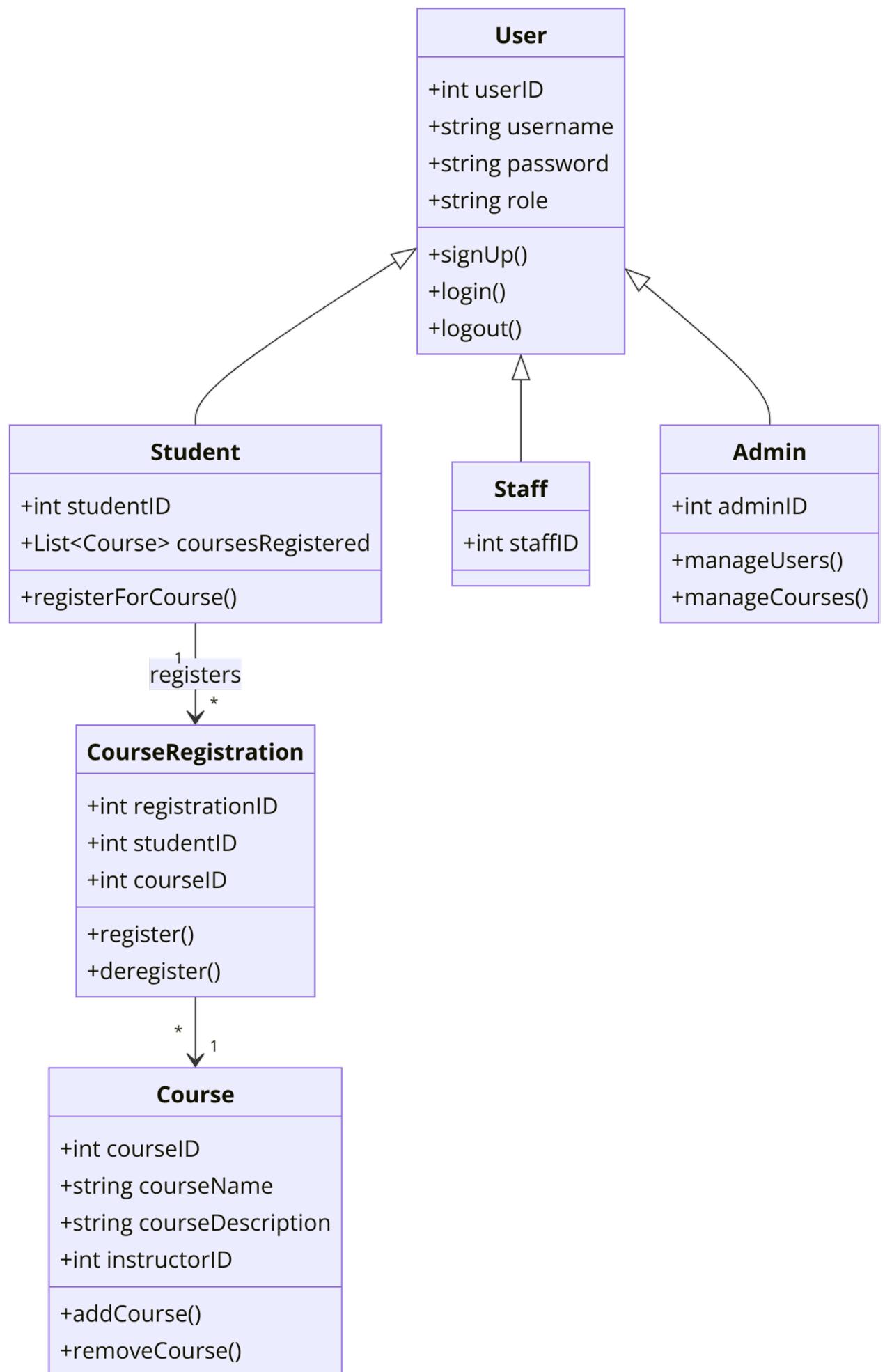
UI Components

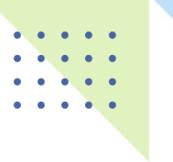
Data Storage Components

Load Balancer/ Proxy

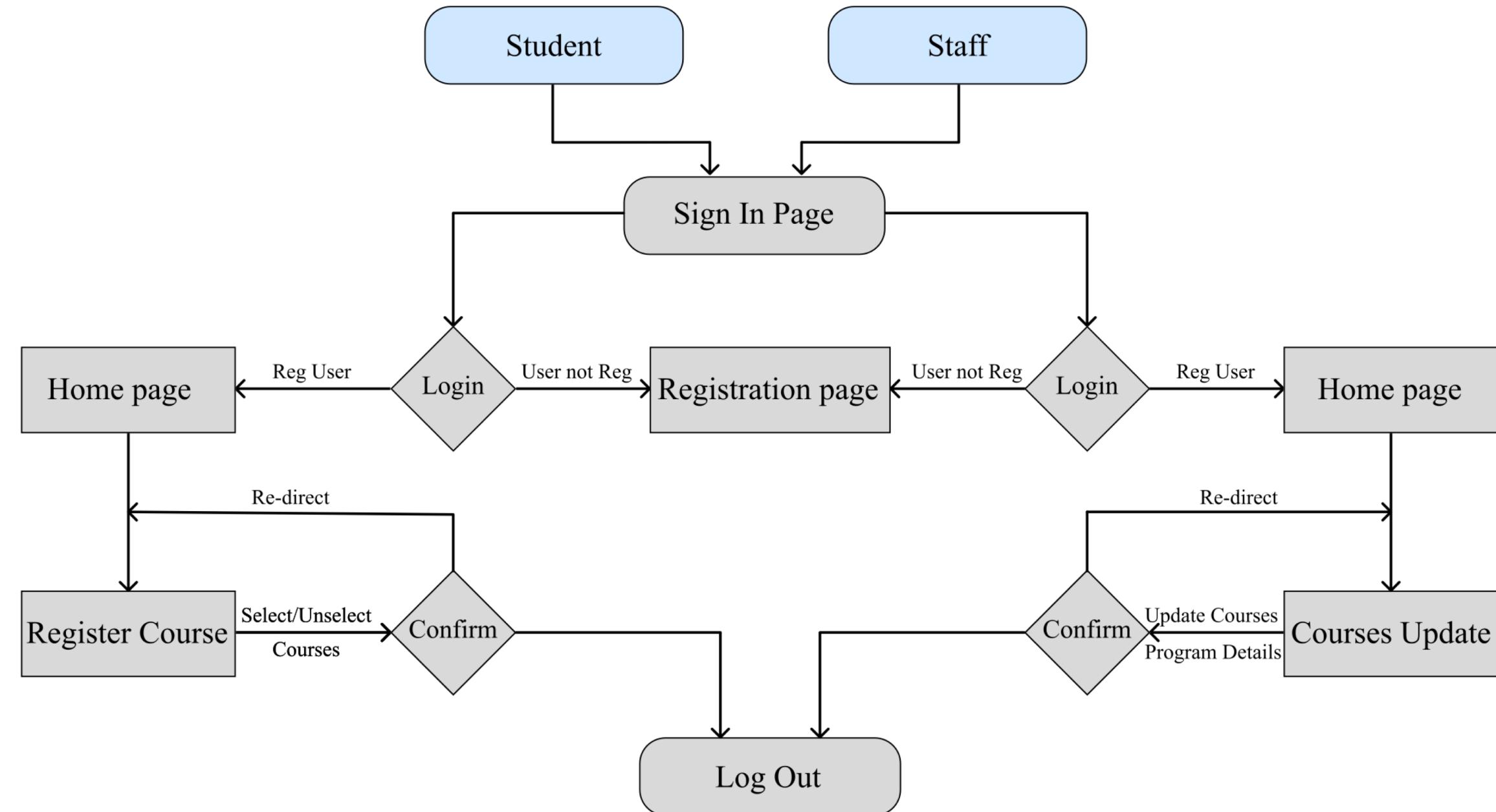


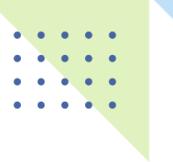
UML



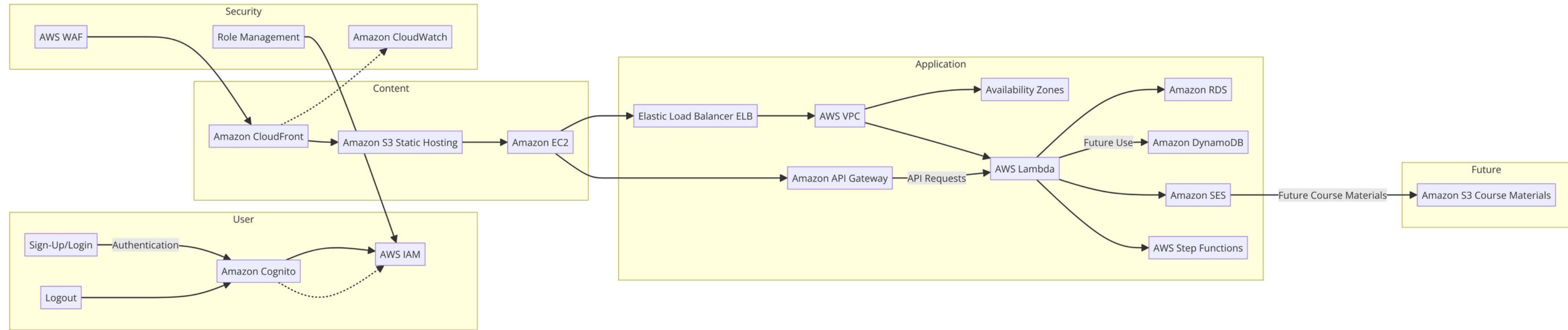


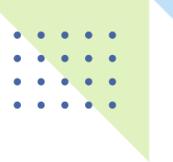
User Task Flow Diagram



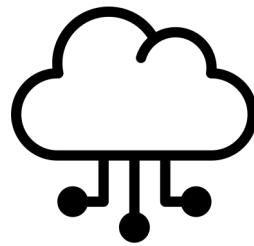


Design Architecture Topology





Estimating Cloud Resources



Compute Resources

- 3 Web server instances (AWS EC2 r5.large) for handling frontend and API gateway
- 13 microservice instances (AWS EC2 r5.large) for running various microservices



Storage Resources

- RDS: 25GB for Auth service
- MongoDB: 10GB for Course Upload service
- Amazon S3: 500GB for storing course materials
- RDS: 50GB for Course Registration service
- Cassandra: 50GB for Course Registration service
- ElastiCache: 1 instance (AWS ElastiCache cache.r5.large)



Network Resources

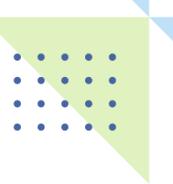
- 2 Load Balancers (AWS Network Load Balancers)



Additional Resources

- 1 Message Queue (Kafka) for inter-service communication





Orchestration with Kubernetes

- **Web Application Deployment**

Purpose: Manages three replicas to ensure high availability and robustness against failures.

File: [web-deployment.yaml](#)

- **Database Deployment**

Purpose: Maintains a single, persistent database pod to guarantee data integrity and continuous availability.

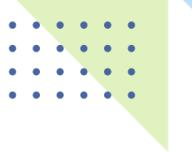
File: [db-deployment.yaml](#)

- **Web Service Configuration**

Function: Directs traffic to web pods and facilitates external access via ingress, ensuring seamless connectivity.

File: [web-service.yaml](#)





Security and Compliance Strategies

- Security Measures -

Authentication and Authorization

- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)



01



Secure Development Practices

- Code Review and Testing
- Vulnerability Management



Data Encryption

- Encryption in Transit (TLS)
- Encryption at Rest (AES-256)



03



Network Security

- Firewalls
- Intrusion Detection and Prevention Systems (IDPS)





Security and Compliance Strategies

- Compliance Strategies -

Regulatory Frameworks

- FERPA (Family Educational Rights and Privacy Act)
- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)

Data Privacy

- Student Data Protection
- Data Retention Policies

Accessibility Compliance

- Student Data Protection
- Data Retention Policies





Application-Specific Security Measures

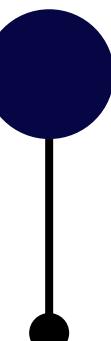
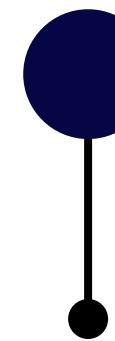
Our application-specific security measures are designed to ensure the confidentiality, integrity, and availability of critical educational data.

By implementing robust security protocols for the course management, grading, notification, and analytics systems, we ensure that all user interactions and data transactions are secure and compliant with industry standards.

This holistic approach to security helps protect sensitive information and enhances the overall trust and reliability of the system.



Implementation Plan



Security Policies

Develop and enforce security policies defining the security requirements and procedures for the application.

Training and Awareness Programs

Regularly conduct training and awareness programs to promote security best practices and compliance.

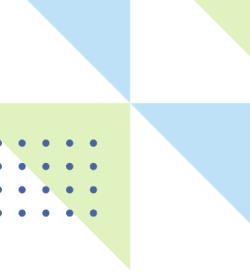
Monitoring and Improvement

Implement continuous monitoring and improvement processes to ensure the application remains secure and compliant with evolving regulations and threats.





California
Science and Technology University

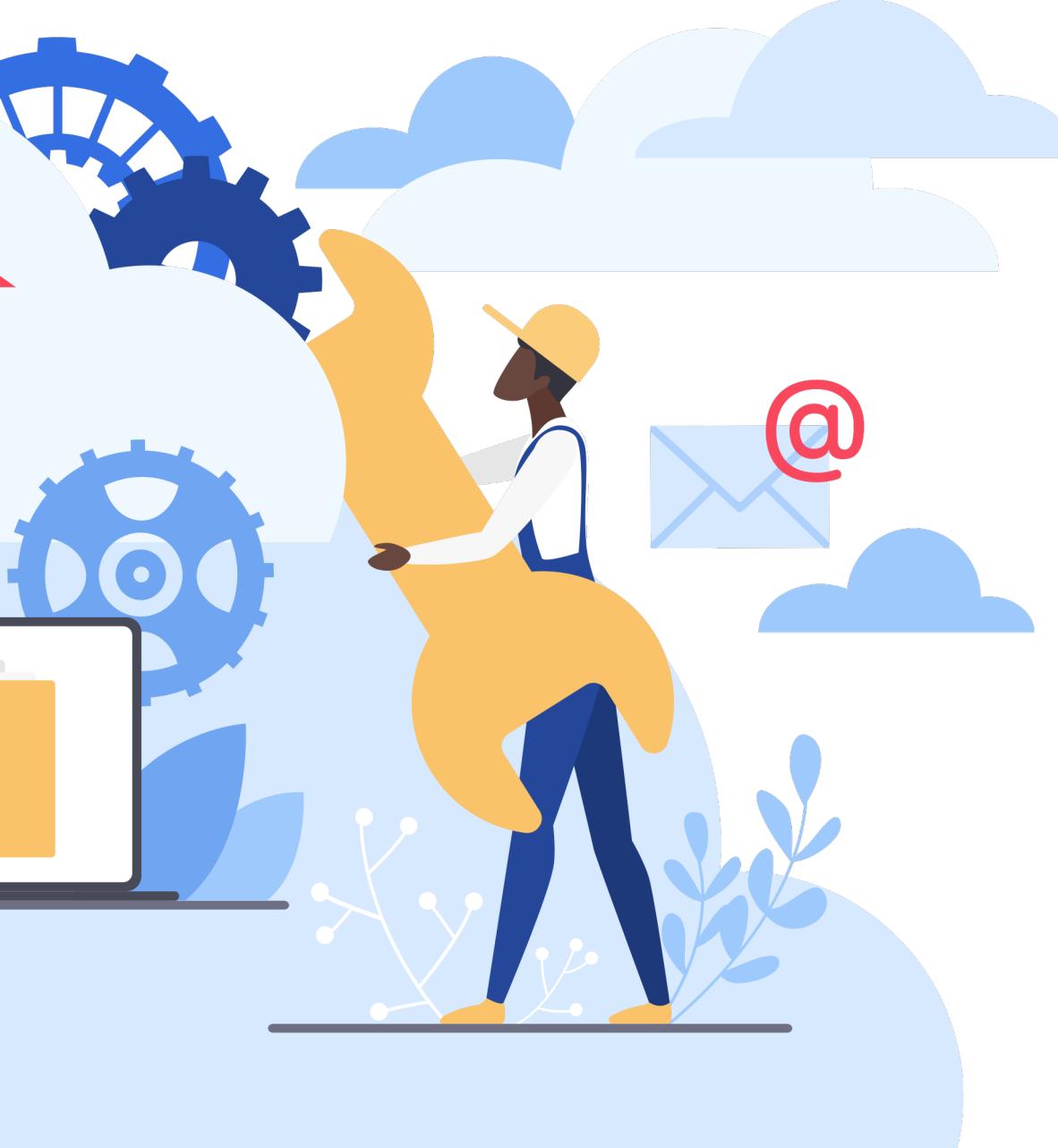


Question and Answer...





California
Science and Technology University



Thanks For Your Listening!

BY TEAM 1

