SLIIT | DEPARTMENT OF COMPUTER SCIENCE & SOFTWARE ENGINEERING | FACULTY OF COMPUTING

Module - Current Trends in Software Engineering (SE4010) | 2025 | Semester 1

Cloud Computing Assignment

Objective:

Design and implement a prototype of a secure, microservice-based application component using fundamental DevOps practices and cloud capabilities.

Assignment Overview:

Your group is tasked with creating a prototype for a single, key component of a larger microservice-based application. This should be deployed on a public cloud service provider. You have the option to choose from any cloud service provider of your choice. The final deliverable should demonstrate basic DevOps practices, and security considerations including DevSecOps practices, and cloud capabilities.

Specific Tasks:

Design a Simple Microservice (LO1, LO3)

- Choose a core component of a larger application idea (e.g., user authentication, product catalog for e-commerce, etc.).
- Outline the functionality and endpoints of this microservice.
- You can choose any programming language/ framework of your choice.

Implement Basic DevOps Practices (LO1, LO2)

- The code should be hosted in the version controlling system. Make sure it's a public repository.
- Use CI/CD pipelines to automate the build and deployment process for the microservice.

Containerize the Microservice using Docker (LO3, LO4)

- Your microservice should be containerized.
- Use any existing container registry service to host your container image. The application deployment should consume the container image from the container registry.

Deploy the Microservice (LO2, LO4)

- Use managed container orchestration services provided by your cloud service provider to deploy the containerized microservice.
    - You can use cloud specific services like ECS (Elastic Container Service)/ Azure Container Apps etc..
    - You have the freedom to even use managed Kubernetes services provided by your chosen cloud service provider.

- Ensure the microservice is accessible over the internet.
- Ensure that you can showcase how you have secured your application.

Integrate Basic Security Measures (LO2, LO4)

- Implement basic security best practices (like using IAM roles, security groups etc,,).
- Ensure the microservice handles data securely and follows principles of least privilege.
- Integrate managed SAST tools like SonarCloud or Snyk to enable DevSecOps practices to your microservice development. Use free versions here.

Deliverables:

Project Report (should only cover following components):

- Architecture diagram of the microservice.
- Description and rationale of the chosen microservice.
- Overview of the DevOps and security practices implemented.
- Any challenges faced and how they were addressed.

Code Repository:

- Access to the version-controlled repository with all source code.

Demonstration (Limited to 10 minutes):

- A working prototype of the microservice deployed on chosen cloud service provider.
- Demonstration of the CI/CD process.

Assessment Criteria:

First 90% (except report marks) will be covered during the viva sessions.

- Practicality and functionality of the microservice. (10%)
- Effective implementation of basic DevOps practices and cloud computing capabilities. (40%)
- Application of security measures in the microservice including DevSecOps practices. (20%)
- Code quality and adherence to best practices. (20%)
- Clarity of the project report and demonstration. (10%)

Notes:

- Focus on depth rather than breadth; a well-implemented single microservice is more valuable than several poorly implemented ones.
- Document all design decisions and challenges encountered during the project.
- When using cloud service provider services always ensure you are within Free Tier.