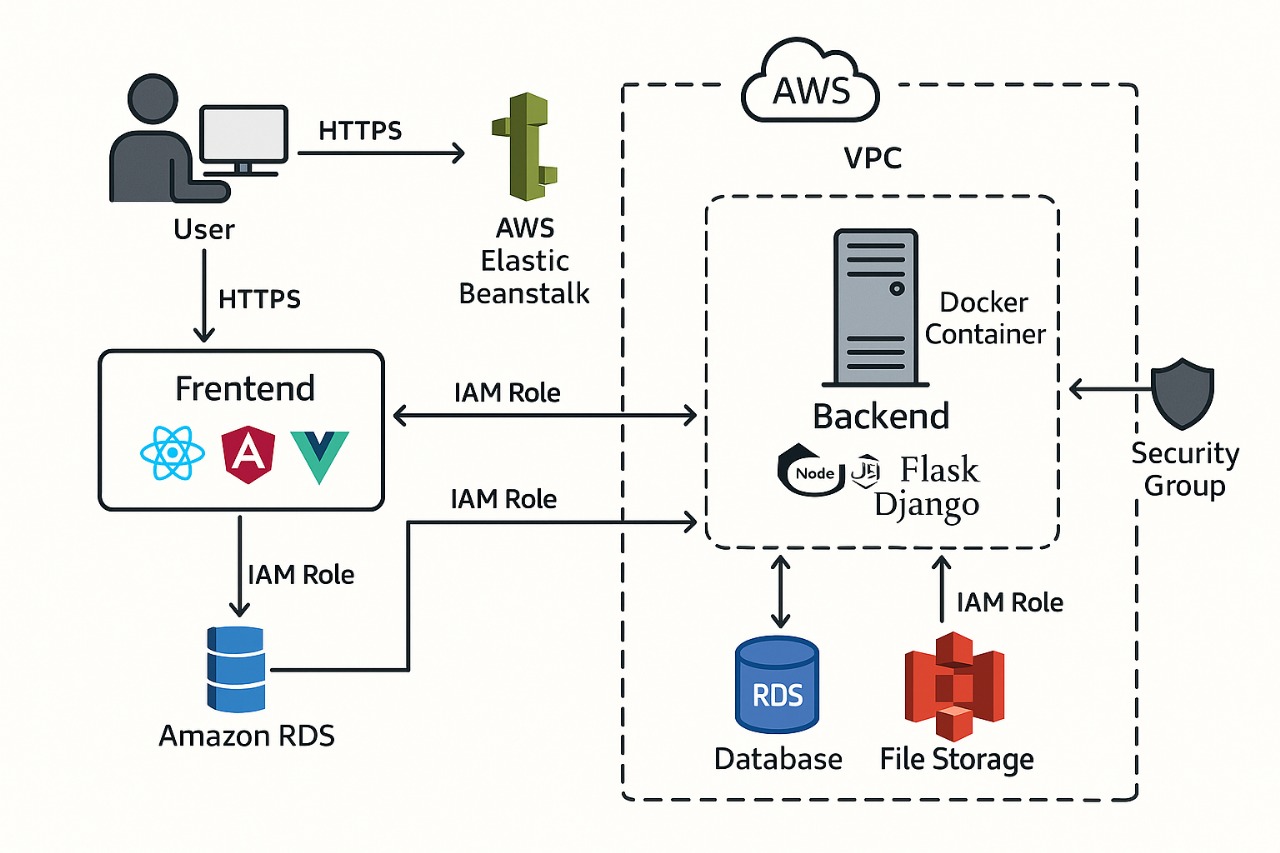
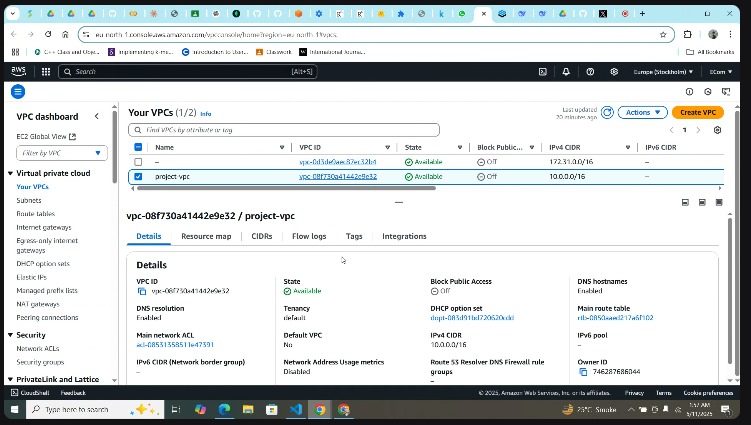
# Report Project

This project aims at hosting a cloud-native web application on AWS infrastructure with the integration of new generation architectural patterns for security and scalability. The solution has a decoupled frontend (hosted on Elastic Beanstalk) and backend (deployed through Docker on EC2), integrated with a managed database (RDS/DynamoDB) and S3 for file storage. Secure access controls are prioritized, such as IAM roles, security groups, and enforcement of HTTPS. The application has user authentication, CRUD functionality, and media upload with support for AWS best practices. The deployment is explained with architecture diagrams, screenshots of policies, and a reproducible step-by-step guide. This deployment shows a production environment in AWS based on the least-privilege security model.

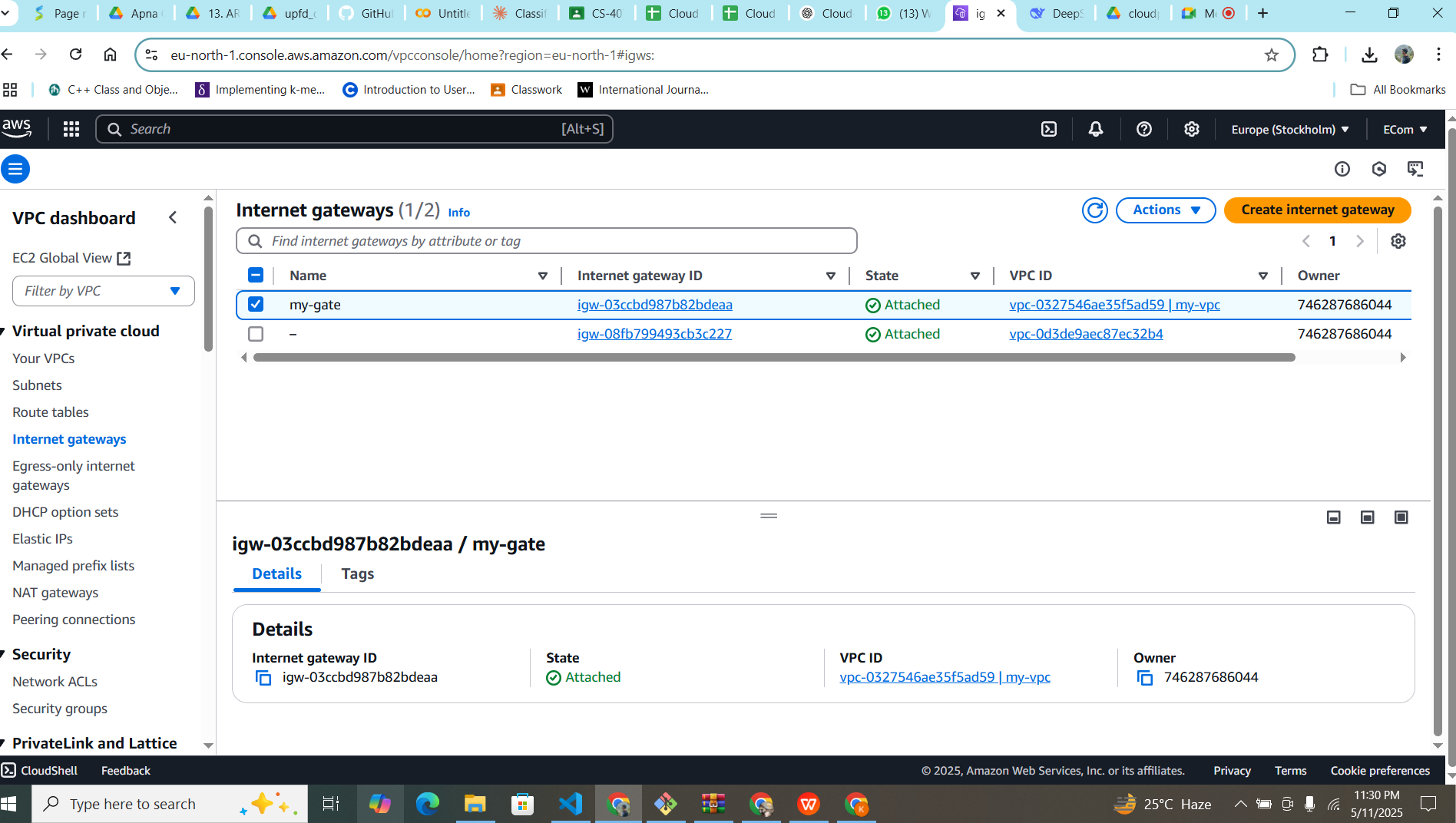
Architecture diagrame for our deployment of Personel Info Application with front end in React and backend in Express js



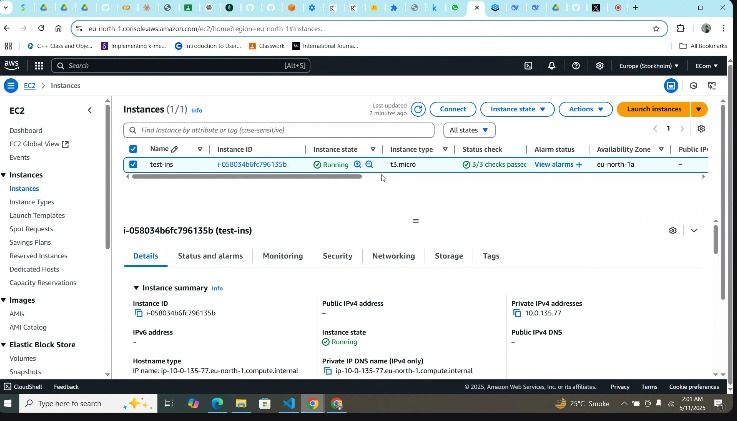
First we created an vpc subnet as shown in below picture



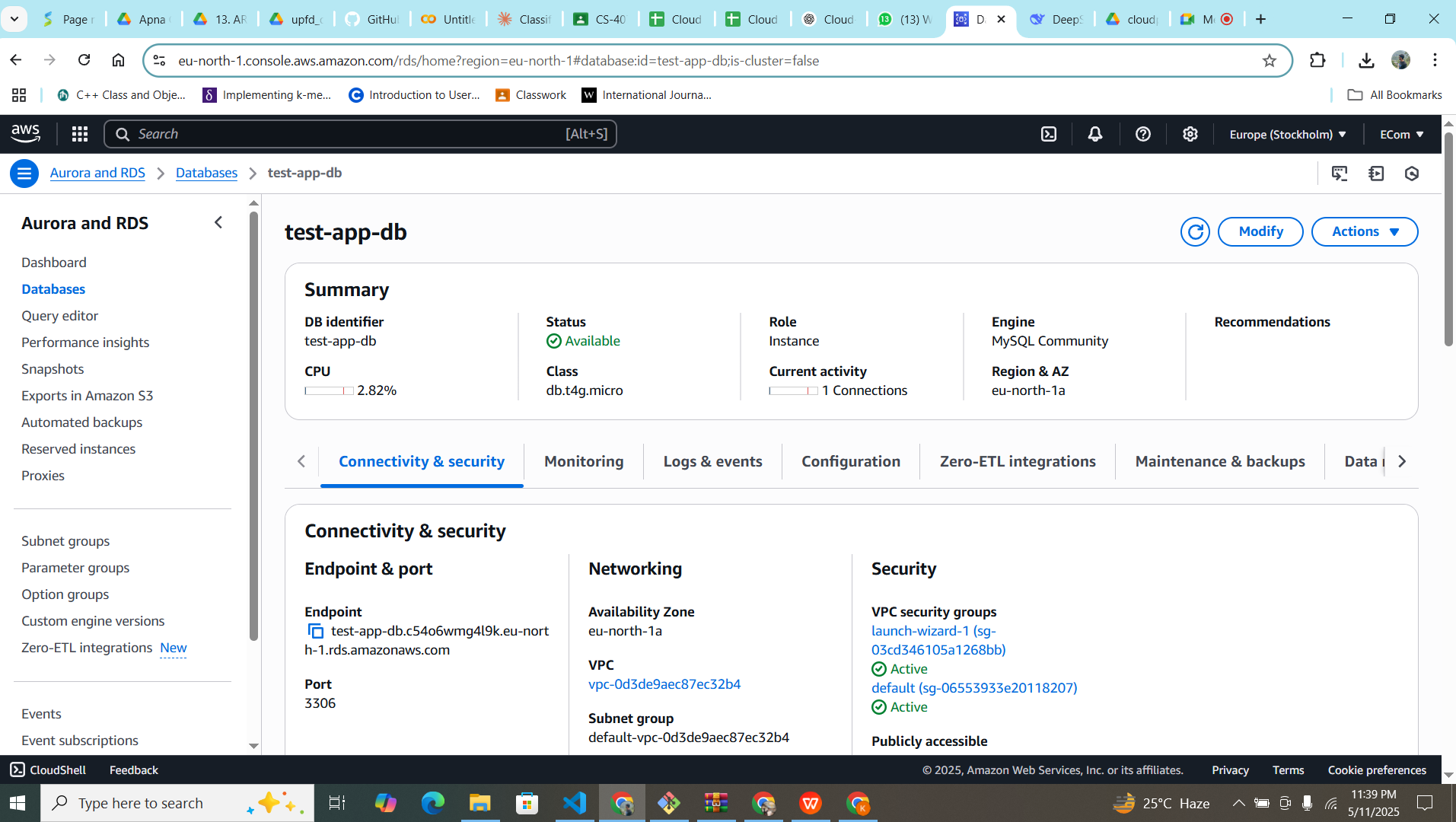
Then we set internet gateway which enables your resources (like EC2 instances) to communicate with the internet



Then we created an ec2 instance which run inside in public subnet of vpc



Then we created rds database to keep our personel information from our application



Then we have created an s3 bucket to keep the images which are coming from our application.

