Cloud Computing Security

Notes:

Security concerns:

* Data Breaches
* Unauthorised Access
* Data Loss (transfer/system failure)

Five factors determine the major component of security concerns:

* Network Related
* Confidentiality and privacy
* Data-related issues
* Virtualization-related issues
* Others

Cloud Security Frameworks are a collection of rules, standards.

Issues:

* Confidentiality
* Integrity
* Availability

Cloud Computing security entails guaranteeing confidentiality, integrity and availability of applications and data in a cloud environment.

Tech Stack:

Frontend: React.Js

Backend: Spring Boot

Database: Postgres

Cloud Service Provider: AWS and AZURE

Docker Compose is used to define this multi container project

Password Storage:

Using Spring Boot’s Security’s DelegatingPasswordEncoder to help remedy the issue of changing password storage requirements. It accomplishes this by encoding new password using current password storage recommendations while still validating passwords in legacy formats. It accomplishes this by using the format:

{id}encodedPassword

Where the id identifies the password encoder used and the rest is the encoded password. For instance.

{bcrypt}$2a$10$dXJ3SW6G7P50lGmMkkmwe.20cQQubK3.HZWzG3YB1tlRy.fqvM/BG

The current recommendation is to use the BCryptPasswordEncoder implementation which uses the bcrypt algorithm which is a slow hash algorithm that uses a random 16 byte salt value.

Data Storage and Encryption: