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: AES/CBC-128-bit encryption

Cloud Computing Security:

Overview of latest developments:

Today in cloud computing the adoption of Zero Trust Architecture (ZTA) since with cloud computing you cannot guarantee a trusted network. ZTA involves 3 basic principles never trust always verify, least privilege, and assume breach. There is also a move towards compliance and regulatory changes and designing systems that can easily evolve with these changes. Micro segmentation of containers using docker

Latest developments:

* AI
* Using zero trust models
* Zero trust architecture

Some of the more recent developments of Cloud Computing Security is the adoption of Zero Trust cybersecurity paradigms. This is because in Cloud Computing network location is no longer a factor in the security of resources and so permitter security is not viable. According to \cite{NIST\_SP\_800\_207}, Zero Trust Architecture (ZTA) emphasizes a principle of 'never trust, always verify,' shifting the security paradigm from perimeter-based trust assumptions to a model where no user/entity is implicitly trusted regardless of their location on the network and must always be continuously verified. Another important development is the use of micro-segmentation where the network is divided into smaller segments where access is restricted between them. According to \cite{Joo\_et\_al\_2023} this mitigates the spread of threats/damage across the network. One development specific to data privacy has been the use of homomorphic encryption of sensitive data which allows computations of encrypted data without decrypting it.\spa Cloud Computing Security entails guaranteeing the confidentiality, integrity and availability of data and applications in the cloud though techniques and procedures that are independent of the physical infrastructures location(s) and other users of said cloud resources.

Recent advancements in cloud computing security include the ever growing adoption of Zero Trust Architecture (ZTA), which shifts the security paradigm from perimeter-based trust assumptions to continuous verification of users and entities regardless of their network location \cite{NIST\_SP\_800\_207}. Micro-segmentation is another important development where by dividing the network into smaller segments with restricted access to mitigate the spread of threats and damage across the network (Joo et al., 2023). Additionally, the use of homomorphic encryption for sensitive data allows computations on encrypted data without decryption, enhancing data privacy and security.

Cloud computing security entails ensuring the confidentiality, integrity, and availability of data and applications in the cloud, independent of physical infrastructure locations and other cloud resource users.