Assignment 4 - REST Service with secure distributed storage

The challenges of a authentication and authorization in a distributed system is to ensure that only authorized users has access to the distributed system. Properties applied to system to ensure this would include: passwords, encryption, multi-factor authentication or detached systems. This can be challenging to implement due to the multifaceted system requirements in terms of complexity, flexibility and vulnerability to potential threats attempting to exploit such systems.

Functional Requirements

It is therefore essential to keep in mind the properties; confidentiality, integrity, availability and traceability for implementation. Availability is handled by applying a distributed database using Apache Cassandra. However, systems or part of systems can become unavailable due to overloading the system, DDoS attacks and other database errors. One solution for this is to invest in redundancy and/or high capacity database servers in exchange for cost.

Confidentiality is applied where the database can only be accessed through authorised users/employees to safeguard the data through “Spring Security”, alternatively Apache Cassandra Authenticator. Integrity and Traceability is handled through the use of authentication and logging services to ensure all changes are recorded in addition to by who and/or when. The password should be stored with encryption and the user database should be separated from clients’ database for login detail storage.

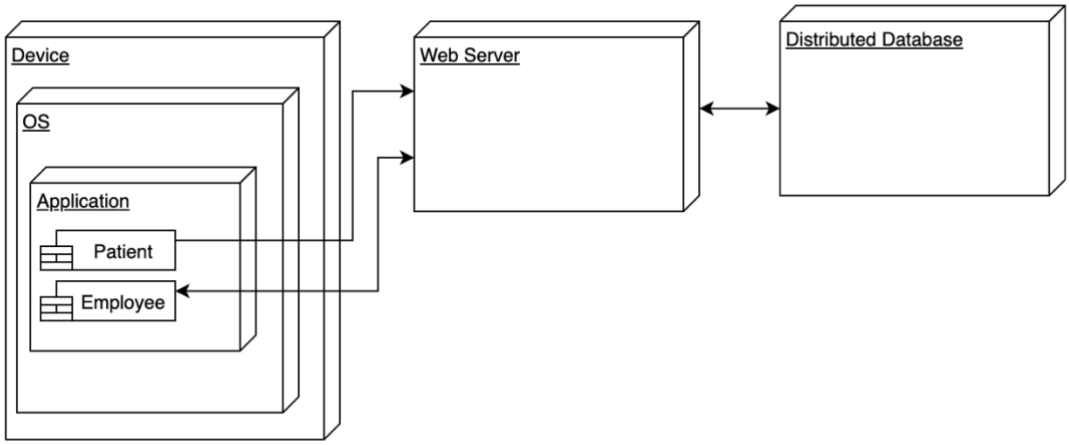

Figure 1 Deployment Diagram