**Design Diagram**

Database

DAO

Service

Controller

Web / Mobile Request

**Security**

For securing the API, we could have a config file with api username and password encrypted. Everytime with api request, we can send the credentials. Validate the credentials and authorize the request. To add a second level of security, we can have different set of credentials stored in database to validate the authenticity between API and DB i.e, basic authentication between the application and API as well as API and DB. It can be implemented once per session to improve the performance. Using OAuth, we could use tokens to authorise the requests.

Design