**Frontend (Android App)**

**Technologien:**

**Android Studio:**

* + Als Hauptentwicklungsumgebung.

**Kotlin oder Java:**

* + Als Programmiersprachen. Kotlin wird von Google empfohlen und bietet moderne Sprachfeatures.

**Jetpack Libraries:**

* + Bietet nützliche Tools und Bibliotheken, die die Entwicklung von Android-Apps vereinfachen, z.B. Room für die Datenbankinteraktion, ViewModel für die Datenhaltung und Navigation Component für die Navigation zwischen App-Bereichen.

**MVVM-Architektur:**

* + Das Model-View-ViewModel (MVVM) Muster unterstützt eine klare Trennung von Belangen und erleichtert die Entwicklung und Wartung.

**Backend (Server)**

**Technologien:**

**Spring Boot:**

* + Für die Erstellung des Backend-Services, bietet Unterstützung für die Entwicklung von RESTful Web Services.

**Sicherheitsmechanismen:**

* + OAuth2 für Authentifizierung und JWT für sichere Übertragung von Informationen zwischen Client und Server.

**Datenbank:**

* + PostgreSQL für relationale Datenhaltung oder MongoDB, falls eine NoSQL-Datenbank bevorzugt wird. Dies hängt von deinen spezifischen Anforderungen ab (z.B. Beziehungen zwischen Daten, Skalierbarkeit).

**Hibernate ORM:**

* + Für die Abbildung von Java-Klassen auf Datenbanktabellen, falls eine relationale Datenbank verwendet wird.

**Architekturübersicht:**

1. **Client-Schicht (Android App):** Nutzerinteraktionen, UI/UX, Anfragen an das Backend.
2. **Business-Logik-Schicht (Backend):** Verarbeitung von Geschäftslogik, Authentifizierung, Autorisierung, Datenverarbeitung.
3. **Datenzugriffsschicht (Backend):** Datenbankoperationen, ORM / Datenbankzugriff, Modelldefinitionen.
4. **Datenschicht (Datenbank):** Speicherung von Benutzerdaten, Transaktionen, Beiträgen etc.

**Kommunikation:**

* Die Kommunikation zwischen der Android App und dem Backend erfolgt über RESTful APIs. Das Backend stellt Endpunkte zur Verfügung, über die die App Daten abfragen oder senden kann.
* Daten werden typischerweise im JSON-Format ausgetauscht.
* Sicherheitsaspekte wie Authentifizierung und Autorisierung sind über das Backend zu regeln, wobei Technologien wie HTTPS, OAuth2 und JWT zum Einsatz kommen.