## **Titel Ideen:**

1. Sichere Finanzmanagement-App mit JWT und Multi-Faktor-Authentifizierung
2. Sichere Finanzverwaltung: JWT gestützte Authentifizierung mit Muli-Faktor-Schutz
3. Sichere Finanzanwendung: Integration von JWT und Multi-Faktor-Authentifizierung zur Datensicherheit

## **Abstract**

Die Sicherheit von Finanzdaten ist in der digitalen Welt von großer Bedeutung. Immer mehr Menschen nutzen Apps, um ihre Finanzen zu verwalten und ihre Ausgaben im Blick zu behalten. Diese Projektarbeit entwickelt eine Finanzmanagement-App, die JSON Web Tokens (JWT) für die Authentifizierung verwendet und eine Multi-Faktor-Authentifizierung (MFA) integriert. Das Hauptziel des Projekts besteht darin, eine sichere Anwendung zu schaffen, die Benutzer vor unbefugtem Zugriff schützt. Hierbei wird das Verhalten der Benutzer analysiert, um zu bestimmen, wann MFA erforderlich ist. Verschiedene MFA-Methoden werden eingesetzt, darunter SMS-OTP, biometrische Authentifizierung und adaptive Sicherheitsfragen. Diese Methoden erhöhen die Sicherheit und bieten einen zusätzlichen Schutz für sensible Daten. Der Ablauf des Projekts umfasst mehrere Schritte. Zunächst wird eine detaillierte Analyse der Sicherheitsanforderungen und Benutzerbedürfnisse durchgeführt. Diese Phase beinhaltet die Identifikation potenzieller Risiken und Schwachstellen in der Anwendung sowie die Festlegung der spezifischen Anforderungen an die Authentifizierung. Anschließend wird das System entworfen, wobei sowohl die Backend-Architektur als auch die Benutzeroberfläche berücksichtigt werden. In der Entwicklungsphase wird die App programmiert und die JWT-basierte Authentifizierung implementiert. Dabei wird darauf geachtet, dass die Tokens sicher generiert und verwaltet werden. Nach der Implementierung folgt eine umfassende Testphase, in der die Sicherheitsfunktionen validiert werden. Hierbei werden verschiedene Testszenarien durchgespielt, um sicherzustellen, dass sowohl JWT als auch MFA effektiv funktionieren. Die erwarteten Ergebnisse sind eine funktionierende Finanzmanagement-App, die sowohl sicher als auch benutzerfreundlich ist. Die App soll den Benutzern helfen, ihre Finanzen effizient zu verwalten und gleichzeitig das Risiko unbefugter Zugriffe zu minimieren. Darüber hinaus sollen neue Erkenntnisse über die Implementierung von MFA in JWT-basierten Systemen gewonnen werden, die für zukünftige Entwicklungen in diesem Bereich von Bedeutung sein könnten. Insgesamt trägt dieses Projekt dazu bei, das Bewusstsein für die Notwendigkeit robuster Sicherheitsmaßnahmen im Umgang mit sensiblen Finanzdaten zu schärfen.

## **Projektplan**

## **1. Anforderungsanalyse**

* Identifikation der Sicherheitsanforderungen für die Anwendung.
* Analyse der Benutzerbedürfnisse hinsichtlich Funktionalität und Benutzerfreundlichkeit.
* Untersuchung potenzieller Risiken und Schwachstellen in der Anwendung.
* Erstellung eines Anforderungsdokuments, das alle gesammelten Informationen zusammenfasst.

## **2. Systemdesign**

* Entwurf der Architektur der Anwendung, einschließlich Backend- und Frontend-Komponenten.
* Definition der JWT-Strategie für die Authentifizierung, einschließlich Token-Generierung und -Verwaltung.
* Planung der Multi-Faktor-Authentifizierung (MFA) mit Auswahl geeigneter Methoden (SMS-OTP, biometrische Authentifizierung).
* Erstellung eines UML-Diagramms, um die Systemarchitektur zu visualisieren.

## **3. Implementierung**

* Programmierung der Backend-Logik zur Verwaltung von Benutzerdaten und Authentifizierung.
* Implementierung der JWT-Generierung und -Validierung im Backend.
* Entwicklung des Frontends, das eine benutzerfreundliche Oberfläche für die Interaktion mit der Anwendung bietet.
* Integration der MFA-Methoden in den Anmeldeprozess.
* Sicherstellung, dass alle sicherheitsrelevanten Daten verschlüsselt gespeichert werden.

## **4. Dokumentation**

* Erstellung einer technischen Dokumentation, die alle Aspekte des Systems beschreibt, einschließlich Architektur, API-Spezifikationen und Datenbankdesign.
* Entwicklung eines Benutzerhandbuchs, das erklärt, wie die App verwendet wird, einschließlich Anweisungen zur Anmeldung und Nutzung der MFA.
* Dokumentation von Code und Implementierungsdetails zur Unterstützung zukünftiger Wartung und Weiterentwicklung.

**5. Testphase**

* Durchführung von Funktionstests zur Überprüfung aller App-Funktionen auf korrekte Arbeitsweise.
* Durchführung von Sicherheitstests, um sicherzustellen, dass die JWT-Implementierung und MFA effektiv sind.
* Dokumentation aller Testergebnisse sowie identifizierter Fehler und deren Behebung.

## **6. Ausarbeitung**

* Erstellung einer Projektpräsentation, die den gesamten Entwicklungsprozess zusammenfasst.
* Verfassen eines Abschlussberichts, der die Ergebnisse des Projekts dokumentiert, einschließlich Herausforderungen und Lösungen während des Entwicklungsprozesses.
* Zusammenfassung von Erkenntnissen über die Implementierung von MFA in JWT-basierten Systemen.

**Zeitplan**

| Arbeitspaket | Dauer (in Wochen) | Startdatum | Enddatum | Meilenstein |
| --- | --- | --- | --- | --- |
| Anforderungsanalyse | 1 | 13.12.24 | 20.12.24 | Abschluss Anforderungs-  analyse |
| Systemdesign | 2 | 13.12.24 | 10.01.25 | Abschluss Systemdesign |
| Implementierung | 3 | 20.12.24 | 24.01.25 | Abschluss Implemen-  tierung |
| Dokumentation | 2 | 24.01.25 | 05.02.25 | Abschluss Dokumentation |
| Testphase | 1 | 24.01.25 | 31.01.25 | Abschluss Testphase |
| Ausarbeitung | 1 | 31.01.25 | 05.02.25 | Abschluss Ausarbeitung |

## 

## 

## **Meilensteine**

1. **Abschluss Anforderungsanalyse** (20.12.2024)
   * Alle Anforderungen sind dokumentiert und genehmigt.
2. **Abschluss Systemdesign** (10.01.2025)
   * Das Systemdesign ist fertiggestellt und alle Diagramme sind erstellt.
3. **Abschluss Implementierung** (24.01.2025)
   * Die App ist vollständig entwickelt und alle Funktionen sind implementiert.
4. **Abschluss Dokumentation** (05.02.2025)
   * Alle technischen Dokumentationen und Benutzerhandbücher sind erstellt.
5. **Abschluss Testphase** (31.01.2025)
   * Alle Tests sind abgeschlossen und alle identifizierten Fehler wurden behoben.
6. **Abschluss Ausarbeitung** (05.02.2025)
   * Der Abschlussbericht ist fertiggestellt und das Projekt wird präsentiert.

**Wissenschaftliche Fragestellung:**

Wie kann die Sicherheit von Finanzdaten in mobilen Anwendungen durch die Implementierung von JSON Web Tokens (JWT) und Multi-Faktor-Authentifizierung (MFA) verbessert werden? Welche Herausforderungen und Best Practices gibt es bei der Integration dieser Technologien in eine Finanzmanagement-App?

## **Grundlagen**

1. **Tokenbasierte Authentifizierung:**
   * Erklärung der Funktionsweise von JWTs, einschließlich ihrer Struktur (Header, Payload, Signature) und der Sicherheitsmechanismen, die sie bieten.
   * Analyse der Vorteile von tokenbasierter Authentifizierung im Vergleich zu traditionellen Methoden, wie z.B. Sessions.
2. **Multi-Faktor-Authentifizierung (MFA):**
   * Definition und Bedeutung von MFA zur Verbesserung der Sicherheit in Anwendungen.
   * Übersicht über verschiedene MFA-Methoden, wie SMS-OTP, biometrische Authentifizierung und adaptive Sicherheitsfragen.
3. **Sicherheitsrisiken:**
   * Identifikation und Analyse von Risiken im Zusammenhang mit der Nutzung von JWTs, einschließlich potenzieller Angriffe wie Token-Manipulation oder Replay-Angriffe.
   * Diskussion von Best Practices zur Minimierung dieser Risiken.
4. **Benutzerverhalten:**
   * Untersuchung, wie Benutzerverhalten zur Entscheidung über die Notwendigkeit von MFA beitragen kann.
   * Analyse von Methoden zur Erfassung und Auswertung von Benutzerverhaltensdaten.

## **Aktuelle (Forschungs-)Arbeiten**

1. **M. A. Alzahrani et al. (2022)** - *Enhancing Security in Web Applications Using Multi-Factor Authentication and JWT*

* Diese Arbeit untersucht, wie die Kombination von MFA und JWT die Sicherheit von Webanwendungen verbessern kann. Es werden verschiedene Implementierungsansätze und deren Effektivität analysiert.

1. **R. K. Gupta et al. (2021)** - *A Study on Multi-Factor Authentication Techniques for Secure Access Control*

* Diese Studie befasst sich mit verschiedenen MFA-Techniken und deren Integration in bestehende Authentifizierungssysteme, einschließlich der Verwendung von JWTs zur Verbesserung der Sicherheit.

1. **A. M. Alhassan et al. (2020)** - *Token-Based Authentication: A Review of JSON Web Tokens and Its Security Implications*

* In dieser Arbeit wird die Sicherheit von JWTs untersucht, einschließlich der Herausforderungen bei der Implementierung von MFA in tokenbasierten Authentifizierungssystemen.

1. **Zhang, Y., & Zhao, H. (2019)** - *Research on the Application of Multi-Factor Authentication in Cloud Computing*

* Diese Forschung analysiert die Anwendung von MFA in Cloud-Computing-Umgebungen und diskutiert, wie JWTs als Teil dieser Sicherheitsarchitektur verwendet werden können, um den Zugriff zu sichern.

**Lastenheft**

**Funktionalitäten der Software**

* **Benutzerregistrierung und -anmeldung:** Benutzer können sich registrieren und anmelden, wobei JWT für die Authentifizierung verwendet wird.
* **Multi-Faktor-Authentifizierung:** Implementierung von MFA zur Sicherstellung eines höheren Sicherheitsniveaus bei der Anmeldung. Methoden umfassen SMS-OTP, E-Mail-Bestätigung und biometrische Authentifizierung.
* **Finanzverwaltung:** Benutzer können ihre Ausgaben verfolgen, Budgets erstellen und Berichte über ihre finanziellen Aktivitäten generieren.
* **Datenvisualisierung:** Grafische Darstellung der Ausgaben und Budgets zur besseren Übersichtlichkeit.
* **Benachrichtigungen:** Benutzer erhalten Benachrichtigungen über wichtige Ereignisse, wie z.B. das Erreichen von Budgetgrenzen oder ungewöhnliche Ausgaben.

## **Anwender-/Anwendungsproblem**

Die Software soll das Problem unzureichender Sicherheit bei der Verwaltung sensibler Finanzdaten lösen. Viele Benutzer verwenden einfache Passwörter oder keine zusätzlichen Sicherheitsmaßnahmen, was sie anfällig für Cyberangriffe macht. Durch die Implementierung von JWT und MFA wird ein höheres Maß an Sicherheit erreicht, das den Zugriff auf persönliche Finanzdaten schützt.

## **Nutzer-/System-Schnittstellen**

* **Benutzerschnittstelle (UI):** Eine intuitive Webanwendung, die es Benutzern ermöglicht, sich zu registrieren, anzumelden und ihre Finanzen zu verwalten. Mockups können einfache Layouts für Anmelde-, Registrierungs- und Dashboard-Seiten zeigen.
* **API-Schnittstelle:** Eine RESTful API, die es ermöglicht, Daten zwischen dem Frontend und Backend auszutauschen. Diese API wird Endpunkte für die Authentifizierung (JWT), Finanzdatenverwaltung und MFA-Anforderungen bereitstellen. **Beispiel für API-Endpunkte:**
  + POST /api/auth/register - Registrierung eines neuen Benutzers
  + POST /api/auth/login - Benutzeranmeldung und JWT-Generierung
  + POST /api/auth/mfa - MFA-Verifizierung

## **Technologien**

* **Programmiersprache:** Kotlin für das Backend
* **Frontend-Technologien:** Plain HTML und CSS für die Benutzeroberfläche.
* **Frameworks:**
  + **Backend:** ktor für die Erstellung der RESTful API.
  + **Datenbank:** MySQL für die Speicherung von Benutzerdaten und Finanzinformationen.
* **JWT-Bibliothek:** jsonwebtoken zur Erstellung und Verifizierung von JWTs.
* **MFA-Bibliotheken:** Verwendung von Bibliotheken wie speakeasy (für TOTP) oder Twilio (für SMS-Bestätigungen).

## **Eigenanteil**

**Vorhandene Komponenten:**

* Open-Source-Bibliothek “jsonwebtoken” für Kotlin

**Eigenentwicklung:**

* Die Entwicklung des gesamten Frontend mit HTML und CSS, um eine benutzerfreundliche Oberfläche zu schaffen.
* Die Implementierung der Logik zur Verwaltung von Finanzen, einschließlich Budgetierung und Ausgabenverfolgung in Kotlin.
* Die Integration der MFA in den Anmeldeprozess, einschließlich der Logik zur Analyse des Benutzerverhaltens zur Bestimmung der Notwendigkeit von MFA.

**Beschreibung der selbst programmierten Anteile:**

1. **Frontend-Anwendung:**
   * Entwicklung einer responsiven Benutzeroberfläche mit HTML und CSS, die eine einfache Navigation ermöglicht.
   * Implementierung von Formularen zur Registrierung, Anmeldung und Budgetverwaltung.
2. **Backend-Anwendung:**
   * Erstellung einer RESTful API mit Ktor zur Handhabung aller Anfragen vom Frontend.
   * Implementierung der JWT-Generierung und -Validierung sowie der Logik zur MFA.
3. **MFA-Integration:**
   * Entwicklung eines Moduls zur Verwaltung von MFA-Anforderungen basierend auf dem Benutzerverhalten.
   * Implementierung der Logik zur Versendung von OTPs per SMS oder E-Mail.