Bachelorthesis

Konzeption und Implementierung eines React-Frameworks zur flexiblen Erweiterung digitaler Datenbestände

Prüfer(in):
Prof. Dr. Christian Soltenborn

Verfasser(in):
Thomas Benjamin Hopf
101485

Heinrichstrasse 23
40764 Langenfeld

Wirtschaftsinformatik
Cyber Security

Eingereicht am:
10.06.2025

Sperrvermerk

Diese Arbeit enthält vertrauliche Informationen über die Firma Unternehmen GmbH. Die Weitergabe des Inhalts dieser Arbeit (auch in Auszügen) ist untersagt. Es dürfen keinerlei Kopien oder Abschriften - auch nicht in digitaler Form - angefertigt werden. Auch darf diese Arbeit nicht veröffentlicht werden und ist ausschließlich den Prüfern, Mitarbeitern der Verwaltung und Mitgliedern des Prüfungsausschusses sowie auf Nachfrage einer Evaluierungskommission zugänglich zu machen. Personen, die Einsicht in diese Arbeit erhalten, verpflichten sich, über die Inhalte dieser Arbeit und all ihren Anhängen keine Informationen, die die Firma Unternehmen GmbH betreffen, gegenüber Dritten preiszugeben. Ausnahmen bedürfen der schriftlichen Genehmigung der Firma Unternehmen GmbH und des Verfassers.

Die Arbeit oder Teile davon dürfen von der FHDW einer Plagiatsprüfung durch einen Plagiatsoftware-Anbieter unterzogen werden. Der Sperrvermerk ist somit im Fall einer Plagiatsprüfung nicht wirksam.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Listingverzeichnis

1 Einleitung

Relationale Datenbanken sind weiterhin die Standardlösung für die Speicherung und Verarbeitung betrieblicher Daten in Unternehmen. [1] Durch ihre rigide Struktur [2] ermöglichen sie eine klare Trennung zwischen Datenstruktur und Anwendungsebene, wodurch eine hohe Datenintegrität sichergestellt wird. Diese rigide Struktur kann jedoch auch zu Einschränkungen führen, insbesondere wenn Tabellen in Laufzeit erweitert werden müssten, um eine flexible und nutzerspezifische Erweiterung zu ermöglichen.

Auch im betrieblichen Ablauf der Bayer AG sind relationale Datenbanken, mitsamt ihrer Einschränkungen, allgegenwärtig. Dies gilt insbesondere für Abteilungen, die für Research and Development (R&D) zuständig sind. Alle Projekte, die im Rahmen von Forschungsaktivitäten durchgeführt werden, werden mitsamt zusätzlicher Attribute in einer Datenbank (Newport) hinterlegt, wodurch Budgetierung und Projekt-Planung effizient und effektiv möglich ist. Zwar besteht die Möglichkeit, dort viele Informationen zu hinterlegen, jedoch lassen sich die vorgegebenen Spalten nicht erweitern. Dadurch ist es nicht möglich, benutzerspezifische Informationen, die über den Horizont von Newport hinausgehen, zu speichern und weiterzuverarbeiten. Um dieses Problem zu lösen, soll eine Benutzeroberfläche entwickelt werden, die diese Speicherung ermöglicht.

Im Rahmen dieser Bachelor-Arbeit soll ein flexibles technisches Framework konzipiert und umgesetzt werden, mit welchem benutzerspezifische Attribut-Erweiterungen ermöglicht werden, ohne die bestehende Datenbankstruktur der Newport-Datenbank zu verändern. Dabei soll untersucht werden, wie sich die eingeführte Flexibilität mit den Anforderungen an Datenintegrität und Benutzerfreundlichkeit vereinbaren lassen.

Die Arbeit gliedert sich in folgende Kapitel: Zuerst sollen in Kapitel 2 wichtige grundlegende Konzepte und Begriffe rund um relationale Datenbanken und flexible Datenmodellierung erläutert werden. Daraufhin werden die Anforderungen an das zu entwickelnde Framework, sowie die Zielsetzung für das Projekt definiert werden. Die folgenden Kapitel widmen sich der technischen Konzeption und Implementierung des Front- und

[1] https://arxiv.org/abs/2301.00847

[2] `https://rebelsky.cs.grinnell.edu/Courses/CS302/2007S/Readings/codd-1970.pdf?utm_source=chatgpt.com`

Backends, sowie einer abschließenden Evaluation der Ergebnisse. Abschließend folgt ein Ausblick auf mögliche zukünftige Entwicklungen gegeben.

2 Grundlagen und Hintergrund

Für die Umsetzung des Projekts ist theoretisches Wissen rund um Datenspeicherung -verarbeitung und -verteilung sowie Webdesign notwendig. Während grundlegendes Informatisches Fachwissen vorausgesetzt wird, werden alle weiteren für das Verständnis dieser Arbeit relevanten Konzepte im Folgenden erläutert.

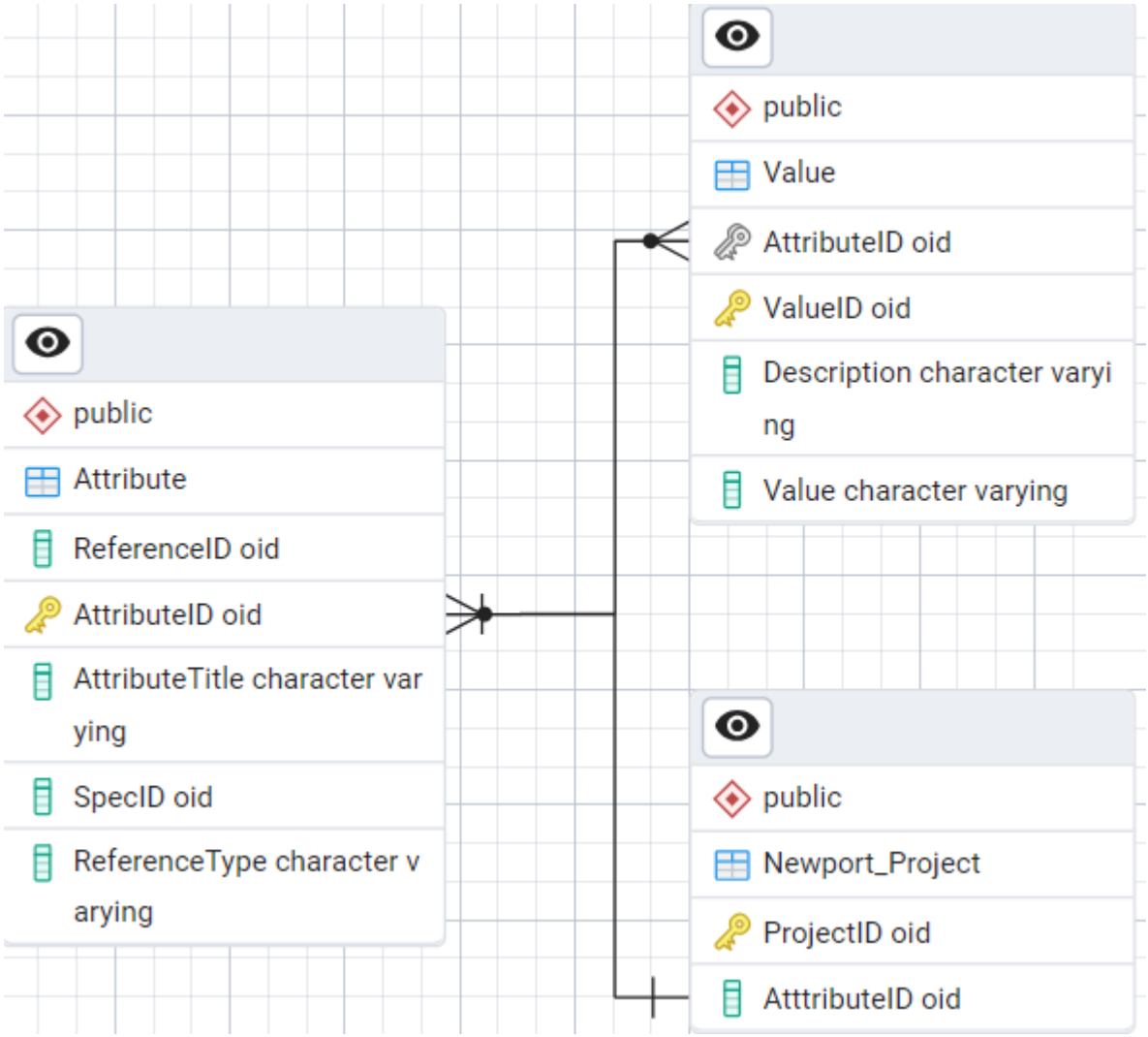
2.1 Fixed-Schema Datenbanken

Die Newport-Datenbank hat aufgrund ihrer großen Datenmenge und Nutzerbasis ein unveränderbares Schema. Das bedeutet, dass die vorgegebenen Spalten nicht bearbeitet, und auch keine neuen Spalten hinzugefügt werden können. Dadurch wird verhindert, dass die Anzahl an Spalten der Datenbank unkontrolliert wächst, was sich negativ auf Recheneffizienz und Übersichtlichkeit auswirken könnte. [3] Ein Nachteil dieses Konzepts ist jedoch die geringere Flexibilität. Ohne die Möglichkeit, neue Spalten hinzuzufügen, sind Nutzer auf die zum Zeitpunkt der Erstellung der Datenbank vorgesehenen Informationen beschränkt. Im Rahmen dieses Projekt soll diese Flexibilität durch Verwendung des Ättribute-Value-Pair=Modells in einer umschließenden Architektur gewährleistet werden, ohne aber die Vorteile einer Fixed-Schema Datenbank zu mindern

2.2 Attribute-Value-Pair Modell

Im Rahmen des Attribute-Value-Pair Modells (In Zukunft AVPM) werden Attribute, durch welche ein Objekt genauer beschrieben wird, in eine eigenständige Tabelle ausgegliedert. Diese Tabelle ist über einen Fremdschlüssel mit dem jeweils tragenden Objekt verbunden. Die Attribute sind in der Tabelle als Schlüssel-Wert-Paare gespeichert. Diese Struktur ermöglicht eine flexible Erweiterung der Attribute, ohne dass die Struktur der Datenbank verändert werden muss:

[3] quelle bitte



2.3 Technologischer Rahmen

Um dieses Modell im Backend umzusetzen, und dann im Front-End nutzbar zu machen, bedarf es verschiedener Technologien. Im Backend werden die Daten in einer Aurora PostgreSQL Datenbank gespeichert[4]. Aurora PostgreSQL (Im Folgenden Aurora) ist ein Dienst, der die Erstellung von relationalen Datenbanken ermöglicht. Auf dieser relationalen Datenbank ermöglicht eine in NodeJS [5] erstellte API den Zugriff auf und die Bearbeitung der gespeicherten Daten. Auf diese API greift dann widerum eine React-App zu, die dann ermöglicht, durch eine Benutzeroberfläche die API zur Kommunikation

[4]Diese Wahl beruht auf Standards im Unternehmen. Dazu mehr in der Evaluierung
[5]Bessere Kompatibilität mit React als alternativen

mit der Datenbank zu benutzen. Die Architektur ist bewusst mehrgliedrich gehalten, um Erweiterungen wie Daten-Redundanz zu ermöglichen [6] Die Wahl dieses technologischen Rahmens beruht auf vorhandenem Wissen und Infrastruktur im Unternehmen, sowie auch Abwägung der Entwicklungsgeschwindigkeit. Grundsätzlich stehen Enwticklern in der Web-Entwicklung jedoch viele Möglichkeiten zur Verfügung

2.4 Alternative Technologien

Für die Datenbank wäre es denkbar gewesen, anstatt einer relationalen auf eine sogenannte NoSQL Datenbanken zurückzugreifen. Eine solche Lösung wird auch im AWS-System angeboten. Der Grund, warum sich gegen diese Option entschieden wurde, liegt in der Natur der Datengrundlage. NoSQL eignet sich vor allem für große Mengen unstrukturierter Daten, während traditionelle Datenbanken besser mit strukturierten Daten umgehen können [7] Im Rahmen der Anwendung muss zwingendermaßen eine strenge Typisierung von Daten gegeben sein, da auf dessen Basis unter anderem Grafiken erstellt werden sollen. Aus diesem Grund ist eine strukturierte Datenbank für den speziellen Zweck des Projekts besser geeignet.

Die Entscheidung, NodeJS für die API zu verwenden, beruht hauptsächlich auf der zeitlichen Komponente der Entwicklung. React basiert auf einem NodeJS-Environment, weshalb es sich anbietet, die gleiche Umgebung für die APi zu verwenden. Grundsätzlich hätte auch jede andere Umgebung zur API-Erstellung ihren Zweck erfüllt, und diese Entscheidung beruht eher auf Bequemlichkeit. React hingegen als Umgebung wurde mit dem Hintergedanken der Modularität gewählt. Da das Projekt nicht nur eine einzene Anwendung, sondern eher einen Komplex kleinerer Tools beherbergen soll, bietet sich ein modulares Framework wie React an, wodurch dieses schon zu Beginn als Anforderung feststand, und als Basis aller weiteren Entscheidungen verwendet wurde. Zudem wird React unternehmensintern immer häufiger für verschiedenste Anwendungen verwendet, weshalb die Infrastruktur für das Deployment bereits aufgebaut ist.

[6] Unter anderem sollen die Daten in ein großes Daten Warehouse der Bayer Cropscience kopiert werden
[7] nosql source

3 Anforderungen und Abgrenzung

Die Anforderungen dieses Projekts gehen auf konkrete Bedürfnisse einer Nutzergruppe zurück, die im Arbeitsalltag intensiv mit dem System „Newport“ arbeitet. Aus diesen Bedürfnissen ergibt sich das zentrale Ziel dieser Arbeit.

3.1 Zielsetzung

Im Rahmen dieser Bachelor-Arbeit soll das Minimum Viable Product (MVP) des Projekts erarbeitet werden, also einer ersten lauffähigen Version mit den Kernfunktionen, die von der Nutzergruppe als unverzichtbar herausgearbeitet wurden. Entsprechend liegt in der Anforderungskonzeptiond er Fokus auf den sogenannten "Must-HaveAnforderungen, ohne welche die Anwendung ihren Zweck verfehlen würde.

Die durch interne Gespräche erfassten Nutzeranforderungen lassen sich in zwei Kategorien einteilen. An erster Stelle stehen die funktionalen Anforderungen, die sich direkt auf die Interaktion mit der Anwendung beziehen. Ebenfalls wichtig sind jedoch auch nicht-funktionale Anforderungen, die sich auf Qualität, Sicherheit, Performance und Wartbarkeit der Lösung beziehen.

3.2 Funktionale Anforderungen

Im Rahmen des Minimum Viable Products (MVP) wurden folgende funktionale Anforderungen als unverzichtbar identifiziert. Sie bilden die Grundlage für die Nutzung des Systems durch Fachanwendende ohne tiefgehendes technisches Vorwissen.

- **Anlegen neuer dynamischer Attribute:** Nutzer*innen sollen die Möglichkeit haben, eigene Attribute anzulegen, die einem bestehenden Projektelement (z. B. einer Formulierung oder einem Projekt) zugewiesen werden können. Hierbei müssen folgende Angaben möglich sein:
- **Zuweisung von Attributen zu Datenobjekten:** Bereits definierte Attribute sollen spezifischen Datenbankeinträgen zugeordnet und durch nutzerspezifische Werte ergänzt werden. Dies umfasst:

  Auswahl eines vorhandenen Attributs

Angabe	Pflichtfeld
Name des Attributs	Ja
Beschreibung	Nein
Datentyp (z. B. Text, Zahl, Datum)	Ja

Tabelle 1: Erforderliche Angaben beim Anlegen eines neuen Attributs

Eingabe eines entsprechenden Werts

Validierung des Werts entsprechend des Datentyps

- **Bearbeiten und Anzeigen von Attribut-Werten:** Im Benutzerinterface sollen alle bereits zugewiesenen Attribute mitsamt ihren Werten für ein bestimmtes Projektelement angezeigt und editierbar sein. Die Darstellung soll dynamisch erfolgen und sich an der Anzahl und Art der zugewiesenen Attribute orientieren.
- **Löschen von Attribut-Zuweisungen:** Nutzer*innen sollen die Möglichkeit haben, bestehende Attribut-Wert-Paare wieder zu entfernen, ohne dabei das globale Attribut selbst zu löschen. Dadurch bleibt das Attribut für andere Einträge verfügbar.
- **Benutzerführung und Validierung:** Die Oberfläche muss durch verständliche Beschriftungen, Platzhaltertexte, Tooltips oder andere visuelle Hinweise den Nutzer bei der Eingabe unterstützen. Validierungsfehler sollen unmittelbar und verständlich angezeigt werden.

3.3 Nicht-Funktionale Anforderungen

Neben den funktionalen Anforderungen, die die direkten Systemfähigkeiten betreffen, wurden verschiedene nicht-funktionale Anforderungen identifiziert. Diese beschreiben die Qualitätsmerkmale des Systems und sind essenziell für den erfolgreichen Betrieb in einem unternehmenskritischen Umfeld wie dem von Bayer.

- **Performance:** Das System muss eine hohe Reaktionsgeschwindigkeit aufweisen, um eine flüssige Nutzererfahrung zu gewährleisten.

  Die Ladezeit für die Anzeige eines Projektelements inklusive dynamischer Felder soll unter 500 ms liegen (bei bis zu 20 zusätzlichen Attributen).

Schreiboperationen (z. B. Hinzufügen eines Attribut-Werts) sollen ohne spürbare Verzögerung erfolgen.

- **Skalierbarkeit:** Die Lösung soll so ausgelegt sein, dass sie mit wachsender Datenmenge und Nutzerzahl ohne grundlegende Umstrukturierung betrieben werden kann.

  Die Datenbankstruktur muss große Mengen an dynamischen Attribut-Werten performant verarbeiten können.

  Die Architektur (Frontend, Backend, Datenbank) muss eine horizontale Skalierung ermöglichen (z. B. API-Lastverteilung).

- **Datenintegrität:** Es muss sichergestellt werden, dass sämtliche gespeicherte Daten vollständig, korrekt und konsistent sind.

  Alle Eingaben durch die Nutzer:innen müssen auf Plausibilität und Formatkonformität geprüft werden.

  Die Datenbank muss durch Constraints und Foreign Keys inkonsistente Zustände verhindern.

- **Wartbarkeit:** Die Codebasis soll modular und verständlich strukturiert sein, sodass zukünftige Weiterentwicklungen oder Fehlerbehebungen effizient durchgeführt werden können.

  Der Quellcode muss dokumentiert sein (Kommentare, Readmes, API-Spezifikationen).

  Wiederverwendbare Komponenten und Services sollen sauber gekapselt sein.

- **Sicherheit:** Das System muss grundlegende Sicherheitsanforderungen erfüllen, um unberechtigte Zugriffe zu verhindern und sensible Daten zu schützen.

  Schreibende Aktionen (z. B. das Anlegen neuer Attribute) sollen nur autorisierten Nutzern erlaubt sein.

  Die API muss gegen typische Angriffe (z. B. SQL-Injection, CSRF) abgesichert sein.

  Benutzerfreundlichkeit (Usability) Die Benutzeroberfläche muss so gestaltet sein, dass auch nicht-technische Anwender:innen effektiv mit dem System arbeiten können.

Komplexe Prozesse wie das Anlegen neuer Felder sollen durch schrittweise geführte Dialoge unterstützt werden.

Fehlerzustände (z. B. ungültige Eingaben) müssen klar und nachvollziehbar kommuniziert werden.

3.4 Abgrenzung

Es ist zwingend notwendig, sich im Rahmen dieser Bachelorarbeit auf das MVP der Anwendung zu fokussieren, um eine abschließende Evaluation zu gewährleisten. Dementsprechend gibt es relevante Anforderungen an das fertige Produkt, die im Rahmen dieser Bachelorarbeit nicht umgesetzt werden. All diese Anforderungen sollen im Folgenden der Vollständigkeit halber aufgeführt und begründet werden.

- **Rollen- und Berechtigungssystem:** Viele verschiedene Nutzer werden für ihre jeweiligen Vorhaben in dieser Anwendung Attribute anlegen, und diesen Werte zuweisen. Da künftig auch vertrauliche Daten gespeichert werden könnten, ist perspektivisch ein Berechtigungssystem erforderlich. Vorerst werden Nutzer jedoch angewiesen, keine solcher Daten zu speichern, bisdieses System fertig implementiert ist, was vorraussichtlich erst nach Ende des Bearbeitungszeitraums dieser Arbeit geschehen wird. Daher wird ein solches System in der Implementierung nicht beachtet.
- **Internationalisierung:** Das fertige Produkt soll, wie auch in vielen anderen Anwendungen der Fall (bspw. SAP), in vielen verschiedenen Sprachen verfügbar sein. Das soll erreicht werden, indem dynamische Language Files eingesetzt werden, die auch eigens von Nutzern bereitgestellt werden können. Eine solche Implementation ist jedoch zeitaufwendig und aufgrund der Sprachkenntnisse der Nutzer nicht von elementarer Wichtigkeit, wird deshalb in dieser Arbeit keine Verwendung finden.
- **Integration in andere Systeme:** Das Projekt soll zwar publiziert werden, insbesondere um Nutzer-Rückmeldungen erhalten zu können, jedoch soll es noch nicht in die restliche IT-Landschaft integriert werden, da das über lange Zeit und unter großer Vorsicht geschehen muss, um Kompatibilität zu garantieren.

Zusätzlich zu den hier aufgeführten Anforderungen wurden Erfolgskriterien definiert, anhand derer die Zielerreichung in Kapitel 4 überprüft wird.

4 Erfolgskriterien und Evaluation

In erster Linie gilt das Projekt als gescheitert, sollten die funktionalen und nichtfunktionalen Kriterien nicht erfüllt sein. Demnach ist es zwingend erforderlich, dass Nutzer die Anwendung zweckgemäß nutzen können, sowohl in Anbetracht der Funktionalität, als auch der Performanz. Um diese Kriterien in der Evaluation bewerten zu können, werden im Folgenden (soweit möglich) KPIs (Key Performance Indicators) definiert.

4.0.1 Funktionale Zielerreichung

Hierfür soll in erster Linie ein Abgleich zwischen den durch die Nutzer gestellten Anforderungen und der Anwendung durchgeführt werden. Die Anwendung hat alle definierten "Must-HaveAnforderungen zu erfüllen.

4.0.2 Nicht-Funktionale Zielerreichung

Bei durchschnittlicher Nutzung sollte sich die Response-Time der Anwendung in verhältnismäßigen Bereichen bewegen. Diese sind unabhängig vom Endgerät des Nutzers, da es sich um eine Cloud-Applikation handelt, und sollten 2 Sekunden nicht überschreiten.

4.0.3 Zukunftstauglichkeit und Wartbarkeit

Zusätzlich zu der imminenten Funktionalität des Programms muss gewährleistet sein, dass die Instandhaltung, sowie eventuelle Erweiterungen der Anwendung in Zukunft möglich sind. Hierfür ist es wichtig, dass die Codebasis modular und verständlich strukturiert ist, was durch eine saubere Trennung von Frontend und Backend, sowie durch die Verwendung von Frameworks, die eine klare Struktur vorgeben erreicht wird. Über

diese Arbeit hinaus muss demnach eine Dokumentation gegeben sein, mitdessen Hilfe der Code der Anwendung verständlich ist.

5 Systemdesign und Herausforderungen

Die Architektur ist im Sinne der Übersicht und Erweiterbarkeit klar in drei Teile aufgeteilt. Zur Datenspeicherung wird eine Aurora-Datenbank verwendet, mit welcher über eine NodeJS API von einem in React erstellten User Interface kommuniziert werden kann. Die Datenbank soll in der Lage sein, Attribut-Wert-Paare flexibel beherbergen zu können, und dabei die bestmögliche Performanz aufweisen.

5.1 Datenbankarchitektur

Um die Erweiterbarkeit der Anwendung zu garantieren, muss die Datenstruktur fest sein. [8] Trotzdem muss die Datenbank aber in der Lage sein, flexibel unterschiedliche Attribute und Werte speichern zu können. Das soll folgende Datenstruktur erreichen:

[8] quelle bitte

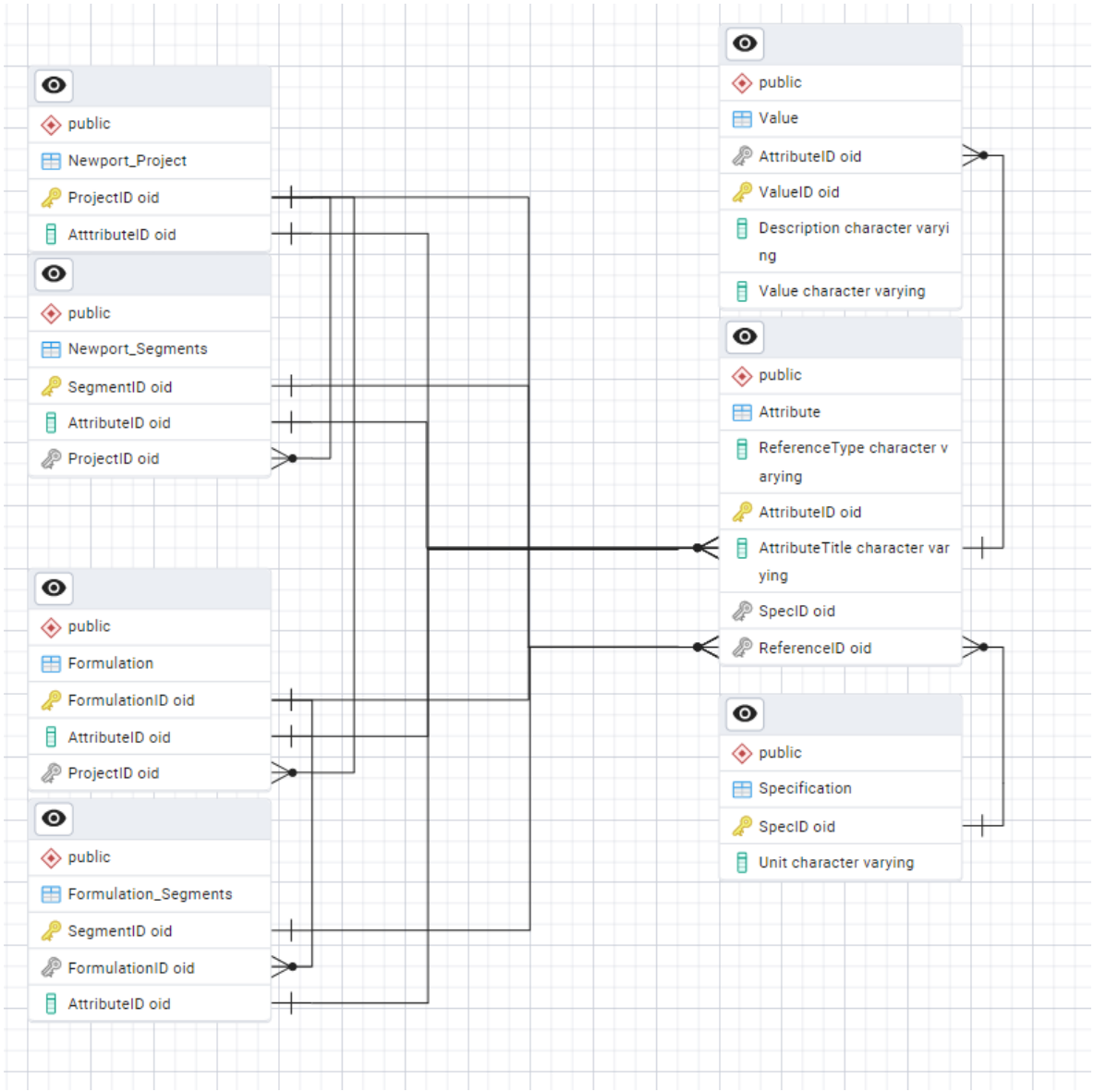


Abbildung 1: Modell der Datenbank

Die Datentruktur lässt sich in drei wesentliche Schichten aufteilen: An erster Stelle stehen die festen Datenobjekte, welche gleichlautend aus der bestehenden Infrastruktur übernommen werden. Diese Schicht bildet das Bindeglied zwischen der bereits existierenden Datenlandschaft und der von dieser Anwendung angehängten flexiblen Daten. Darauf folgt die dynamische Attributzuordnung, die über Fremdschlüssel direkt mit der ersten Schicht verbunden ist. Sie dient zur Verlinkung verschiedener Attribute mit ihren jeweiligen Eltern-Tabellen, speichert zusätzlich aber auch grundlegende Informationen über die Attribute ab. Die dritte Schicht beherbergt die Werte, und verbindet diese mit

ihren zugehörigen Attributen. In dieser Schicht sind Informationen zu der Natur der Werte, aber auch zum Inhalt abgespeichert. Im Folgenden sollen diese drei Schichten mit ihren jeweiligen Tabellen genauer beleuchtet werden.

5.1.1 1. Domänenspezifische Tabellen

„Newport_Project“ bildet das übergeordnete Forschungsprojekt und ihre zugehörigen Daten ab, wobei „Formulation“ nur ein Forschungsobjekt beschreibt, welches an ein Projekt geknüpft sein kann, aber nicht unbedingt muss:

Tabelle 2: Newport_Project

Spalte	Datentyp	Schlüssel?	Beschreibung
ProjectID	Object Identifier (oid)	Primärschlüssel	Primärer Identifier für den Eintrag
AttributeID	Object Identifier (oid)	Fremdschlüssel	Verweis auf zugewiesene Attribute für das jeweilige Projekt

Quelle: Eigene Darstellung

Tabelle 3: Formulation

Spalte	Datentyp	Schlüssel?	Beschreibung
FormulationID	Object Identifier (oid)	Primärschlüssel	Primärer Identifier für den Eintrag
AttributeID	Object Identifier (oid)	Fremdschlüssel	Verweis auf zugewiesene Attribute für das jeweilige Projekt
ProjectID	Object Identifier (oid)	Fremdschlüssel	Verweis auf ein gegebenenfalls zugewiesenes Newport-Projekt

Quelle: Eigene Darstellung

Tabelle 4: Newport_Segments

Spalte	Datentyp	Schlüssel?	Beschreibung
SegmentID	Object Identifier (oid)	Primärschlüssel	Primärer Identifier für den Eintrag
AttributeID	Object Identifier (oid)	Fremdschlüssel	Verweis auf zugewiesene Attribute für das jeweilige Segment
ProjectID	Object Identifier (oid)	Fremdschlüssel	Verweis auf das zugehörige Newport-Projekt

Quelle: Eigene Darstellung

Tabelle 5: Formulation_Segments

Spalte	Datentyp	Schlüssel?	Beschreibung
SegmentID	Object Identifier (oid)	Primärschlüssel	Primärer Identifier für den Eintrag
Formulation	Object Identifier (oid)	Fremdschlüssel	Verweis auf zugewiesene Attribute für das jeweilige Segment
ProjectID	Object Identifier (oid)	Fremdschlüssel	Verweis auf das zugehörige Newport-Projekt

Quelle: Eigene Darstellung

5.1.2 2. Attributebene

Tabelle 6: Attribute

Spalte	Datentyp	Schlüssel?	Beschreibung
ReferenceType	String (oid)	/	Automatisch gesetzte wörtliche Referenz auf den Owner des Attributs
ReferenceID	Object Identifier (oid)	Fremdschlüssel	Direkter Verweis auf den Owner des Attributs
AttributeID	Object Identifier (oid)	Primärschlüssel	Verweis auf das zugehörige Attribut
AttributeTitle	String	/	Titel des Attributs
SpecID	Object Identifier (oid)	Fremdschlüssel	Verweis auf die zugehörige Spezifikation

Quelle: Eigene Darstellung

5.1.3 3. Werteebene und Spezifikation

Tabelle 7: Value

Spalte	Datentyp	Schlüssel?	Beschreibung
AttributeID	Object Identifier (oid)	Fremdschlüssel	Verweis auf das zugehörige Attribut
ValueID	Object Identifier (oid)	Primärschlüssel	Primärer Identifier für den Eintrag
Description	String	/	Name des Werts
Value	String	/	Wert

Quelle: Eigene Darstellung

Tabelle 8: Specification

Spalte	Datentyp	Schlüssel?	Beschreibung
SpecID	Object Identifier (oid)	Primärschlüssel	Primärer Identifier für den Eintrag
Unit	String	/	Einheit

Quelle: Eigene Darstellung

5.2 Herausforderungen

Im Folgenden sollen die Herausforderungen, die die Anforderungen an das Projekt posieren, und mögliche Lösungsansätze für diese diskutiert werden.

5.2.1 Datenkonsistenz

Aufgrund der hohen Flexibilität der einzutragenen Daten muss die Datenbank modular aufgebaut sein. Um die Datenkonsistenz zu garantieren, muss die API (Direkte Manipulation ist in der Architektur nicht vorgesehen) sicherstellen, dass keine inkorrekten Daten gespeichert werden. Dafür müssen alle API-Requests noch vor Absendung auf Validität geprüft werden. Schlägt die Prüfung an, soll der Nutzer über den Fehler informiert werden. Da die Datenbank modular aufgebaut ist, muss die Erweitbarkeit und Performanz sichergestellt werden.

5.2.2 Referentielle Integrität

Die referentielle Integrität wird durch sogenannte „Constraints“ schon im Datenbank-Management-System (DBMS) sichergestellt. Dadurch, dass Foreign Keys als solche deklariert werden, überprüft das DBMS bei Erstellung eines neuen Eintrags mit einem Foreign Key, ob der referenzierte Eintrag auch tatsächlich existiert. Ist das nicht der Fall, wird die Erstellung des Eintrags verhindert.

5.2.3 Erweiterbarkeit und Performanz

Um die Erweiterbarkeit zu garantieren, speichert die Datenbank auch Informationen, die im aktuellen Funktionsumfang noch nicht zwingend Erforderlich sind, jedoch bei eventuell auftretenden Erweiterungen notwendig werden können. Ein Beispiel dafür ist die Tabelle „Specification“. Sie speichert genauere Informationen über die Eigenschaften der Werte wie der Einheit ab. Das ist noch nicht erforderlich, da alle vorhersehbaren Daten Numerisch sind. Sobald sich das aber ändert kann die Erweiterung ablaufen, ohne die Datenbank-Struktur zu verändern. Das ist wichtig, da für eine solche Veränderung das gesamte Backend bearbeitet werden muss. Es ist effizienter, die möglichen Veränderungen sofort einzuplanen. Dabei darf die Performanz aber nicht vernachlässigt werden. Durch die vielen Sicherheitsmechanismen, hinter welchen die Daten auf AWS gelagert werden, wird die Response-Time ohnehin verlängert, der restliche Prozess muss sich daran also anpassen. Der Nutzer soll jederzeit über den Fortschritt ausstehender Anfragen informiert werden, die Anwendung muss, auch während einer laufenden Anfrage, weiter bedienbar sein und alle Prozesse rund um den Datenabruf sollten möglichst effizient gestaltet sein. Ein Beispiel für eine optimierende Planung in der Architektur ist die Spalte „ReferenceType“. Durch diese Spalte, die automatisch gesetzt wird, müssen die großen Tabellen von Attribut und Attribut-Owner nicht miteinander verbunden werden, um sie zuzuordnen, wodurch (bei größeren Datenmengen in den Tabellen) die Response Time deutlich verbessert wird. Trotz dieser Optimierungen darf aber die Architektur nicht so komplex werden, dass die Wartbarkeit darunter leidet.

5.2.4 Wartbarkeit und Benutzerfreundlichkeit

Die Gesamtarchitektur muss stets, trotz aller Herausforderungen, simpel genug sein, um mit möglichst geringem zusätzlichen Arbeitsaufwand gepflegt werden zu können. Dementsprechend muss die Gesamtheit der Architektur bis ins Detail dokumentiert und alle Entscheidungen festgehalten werden. Neben den Entwicklern, die für die Wartung zuständig sind, müssen aber auch die Nutzer in der Lage sein, die Anwendung zu verstehen und effektiv anzuwenden. Deshalb muss das User Interface so selbsterlklärend wie möglich sein, und alle weiteren Informationen in einer User-Dokumentation festgehalten werden, auf welche klar und eindeutig verwiesen wird.

6 Datenmodellierung

Im Sinne der Modularität basiert die Datenmodellierung auf dem Entity-Value-Attribut-Konzept (EAV). Dieses Konzept ermöglicht die Erweiterung des starren relationalen Schema um eine variable Anzahl benutzerdefinierter Attribute, ohne dabei eine Schema-Veränderung zu erfordern. Dadurch sind die dynamischen Attribute von den Domänenobjekten (Projekte und Formulationen) getrennt. Im Folgenden soll der Aufbau und die Funktionsweise des Datenmodells genauer erläutert werden.

6.1 ER-Modell und Tabellenübersicht

Das relationale Schema gliedert sich in 3 Hauptblöcke: Domänentabellen, Attributdefinition und der Werteebene.

6.1.1 Domänentabellen

„Newport_Project“ verbindet die Datenbank über den Primärschlüssel „ProjectID“ mit der Newport-Datenbank aus dem CropScience Warehouse (CSW). Das ermöglicht indirekten Zugriff auf externe Projektdaten. „Newport_Segments“ beinhaltet sogenannte Segmente[9] für die jeweiligen Newport-Projekte, und (sofern gegeben) deren Attribute. „Formulation“ und „Formulation_Segments“ fungieren entsprechend für zu speichernde Formulationen.

6.1.2 Attributdefinition

„Attribute“ enthält alle potentiell verwendbaren, dynamischen Felder. Jede Zeile verfügt über eine eindeutige „AttributeID“, einen entsprechenden „AttributeTitle“, und sowohl eine direkte („ReferenceType“), als auch eine indirekte Referenz(„ReferenceID“) auf den Attribut-Owner. Mit der „SpecID“ wird zusätzlich auf eine Tabelle verwiesen, in der genauere Informationen über das Attribut (bspw. Einheit) hinterlegt werden können.

[9] Segmente sind in der Enwticklung einer Formulation beispielsweise verschiedene Länder, in denen das Produkt lizensiert werden soll

6.1.3 Werteebene

„Value“ speichert die benutzerdefinierten Werte, mit denen das Attribut angelegt wurde. Wesentliche Spalten sind „ValueID“, der Primärschlüssel, „AttributeID“, die Referenz auf das zugehörige Attribut, „Description“ für eine mögliche genauere Beschreibung und „Value“, worin der eigentliche Wert gespeichert wird.

6.2 Beziehungen und Referentialität

Ein Domänenobjekt kann über die AttributeID mit beliebig vielen Attributen verbunden werden. Ein Attribut kann widerum nur einem Domänenobjekt zugewiesen werden. Die referentielle Integrität wird durch die Fremdschlüssel-Paarungen sichergestellt, wonach kein Attribut ohne Verweis auf ein Domänenobjekt erstellt werden kann. Die API ist hingegen dafür zuständig, dass ein Attribut nicht auf mehrere verschiedene Domänenobjekte verweist, indem es benutzerdefiniertes Setzen der AttributeID verhindert.

6.3 Datenkonsistenz und Validierung

Das EAV-Modell sieht vor, dass die Datenintegrität durch die mit der Datenbank verbundene API sichergestellt wird, indem eingegebene Werte stets auf Validität geprüft werden. Folgende Prüfungen sind für die API vorgesehen:

6.3.1 Datentypprüfung

Jedes Attribut hat in der Specification einen hinterlegten Datentyp. Sollte der vom Benutzer angegebene Datentyp nicht in der Menge unterstützter Datentypen vorhanden sein, soll die Erstellung des Attributs verhindert werden und eine entsprechende Fehlermeldung ausgegeben.

6.3.2 Pflichtfelder und Standardwerte

Um eine reibungslose Behandlung fehlerhafter Nutzerangaben sicherzustellen, soll schon das Front-End Pflichtfelder als solche markieren, und das Abschicken der Form verhindern, bis diese ausgefüllt sind. Das Setzen der Schlüssel übernimmt jedoch das Backend, weshalb diese, obwohl sie Pflichtfelder sind, nicht vom Nutzer gesetzt werden müssen.

6.3.3 Transaktionen

Das Anlegen eines neuen Attributs und das direkte Zuweisen eines ersten Werts sollen in einer Transaktion gebündelt sein, um zu verhindern, dass Attribute ohen zugehörige Werte existieren.

6.4 Beispielhafte Speicherung

Angenommen, ein Nutzer legt für „Projekt A“ ein neues Attribut „Versuchsdauer“ (Einheit Integer) an und vergibt den Wert „3“, dann sähen die Abläufe und Datenbankeinträge folgendermaßen aus:

Tabelle 9: Attributdefinition

AttributeID	AttributeTitle	ReferenceType	SpecID
42	Versuchsdauer	Newport_Project	2

Tabelle 10: Specification (Einheitenzuordnung)

SpecID	Unit
2	Integer

Tabelle 11: Speicherung eines Attribut-Wert-Paares

ValueID	AttributeID	Description	Value
101	42	null	3

Durch diese Trennung bleiben das feste Schema in „Newport_Project“ und die dynamischen Erweiterungen klar voneinander getrennt, und trotzdem werden alle zusätzlichen relevanten Informationen abgespeichert.

Mit diesem Datenmodell können beliebig viele neue Attribute hinzugefügt werden, ohne das Grundschema der Domänentabelle anzupassen.

7 Bakend-Implementierung

Im Backend übernimmt eine mit Node.js implementierte API die Geschäftslogik. Da die Daten in AWS hinter einer Firewall liegen, sitzt die API in einer EC2-Instanz, die eine Schnittstelle zwischen der gesicherten AWS-Landschaft und externen Apps bildet. Zustäzlich wird API Gateway, ein AWS-Serice verwendet, um den automatisierten Zugriff auf die API zu ermöglichen. Gespeichert sind die Daten in einer Aurora PostgreSQL Datenbank.

7.1 Datenbank

Zur Implementierung der Datenbank auf der EC2-Instanz muss zuerst eine Verbindung mit derlokalen Datenbankmanagement-System aufgebaut werden. Dafür wird die AWS-CLI verwendet.[10] Mit ihr wird dann[11] ein Tunnel zwischen dem lokalen Port 2222[12] und dem TCP-Port 22 der EC2-Instanz geöffnet: Dieser Tunnel ist zwingend erforderlich, da

Listing 1: SSH-Tunnel mit AWS-CLI

```
aws --profile {Profile-ID} ec2-instance-connect open-tunnel --instance-id {Ins
```

aufgrund von Sicherheitsrichtlinien Bayer's die EC2-Instanz keine öffentliche IP haben darf.
In PgAdmin kann nun eine Verbindung zu der Datenbank hergestellt werden. Dafür werden folgende Informationen benötigt:

1. Host name/Adresse: Die URL der Datenbank auf AWS-Ebene (name.id.server.rds.amazonaws.c
2. Port: 5432 (Standard Postgres-Port)
3. Maintenaince Database: Name der Datenbank auf AWS
4. UserName: Name des Nutzers, mit dem auf die Datenbank zugegriffen werden soll
5. Parameter „SSL Mode“: „prefer“
6. Use SSH Tunneling: „enabled“
7. Tunnel Host: localhost (da der SSH-Tunnel auf dem localhost aufgesetzt ist)
8. Tunnel Port: 2222 (entspricht –local-port in der CLI)

[10] https://aws.amazon.com/cli/
[11] Nach Authentifizierung mit aws login –{user}
[12] Der Port ist frei wählbar, solange er nicht reserviert ist (bspw. 22 ist nicht wählbar, da belegt durch TCP)

9. Authentication: „Identity File“
10. Identity File: Hier das .pem-File hinterlegen[13]

Mit diesen Einstellungen kann der Server gespeichert werden, und ein Zugriff auf die Datenbank ist möglich. In PgAdmin kann nun wie üblich das geplante Schema umgesetzt werden. Nun müssen die Daten in React abrufbar gemacht werden.

7.2 API

Für die API muss zuerst eine Infrastruktur in AWS errichtet werden, die eine sichere Verbindung zwischen AWS-Externen Clients und den AWS-Internen Daten garantieren kann. Diese Infrastruktur sieht folgendermaßen aus: (Hier bild) An erster Stelle steht die Virtual Private Cloud (VPC). Auf ihr liegt die gesamte Infrastruktur. Inbound und Outbound traffic aller IP-Adressen sind vollständig blockiert, um die Sicherheit der Daten zu gewährleisten. Auf dieser VPC liegt die Datenbank, auf welche Zugriff durch eine EC2-Instanz ermöglicht wird. Die Datenbank ist eine Aurora Postgres Datenbank in Standardausführung[14]. Die EC2-Instanz entspricht ebenfalls der Standardausführung, und ist so eingerichtet, dass Inbound-traffic auf TCP-Ebene ausgehend von AWS-Internen IP-Adressen möglich ist. Zusätzlich ist die EC2-Instanz mit einem Network Load Balancer (NLB) ausgestattet, wodurch andere AWS-Programme direkt auf Elemente innerhalb der VPC zugreifen können. Dieser Zugriff ist durch eine Target Group möglich, über den ein NLB standardmäßig verfügt, und welcher in diesem Fall direkt auf das VPC zeigt. In einem NodeJS-Programm, welches direkt auf der EC2-Instanz liegt, wird eine Proxy errichtet, mit der eine Verbindung nach außen hergestellt wird: In diesem Code-Snippet wird die Proxy auf den Localhost gerichtet, in der Produktivumgebung zeigt die Proxy auf die URL der Umgebung. Die über die Proxy weitergeleiteten Requests werden von API Gateway verarbeitet, auf welchem die oben formulierten Methoden umgesetzt sind. Jede Methode entspricht einer Lambda-Funktion, über welche die Interaktion mit der Datenbank ermöglicht wird: Zuerst wird in Form der Kontextvariable „pool“ der Gesamtkontext (alle Informationen zu) der Datenbank gespeichert. Mit diesen Informationen wird dann eine Query auf der Datenbank ausgeführt, und das Ergebnis zurückgesendet. Die Lambda-Funktionen sind in API Gateway einer eigenen URL zugeordnet, die über

[13] Key-Files können im AWS-Dashboard unter EC2 erstellt werden
[14] Standardausführung festgelegt durch den Unternehmensinternen Softwarekatalog

die Proxy auch außerhalb von AWS bei gegebener Authentifizierung abrufbar ist. Diese wird durch Cognito abgewickelt.

7.3 Authentifizierung mit Cognito

In Cognito liegt, speziell für die Authentifizierung von Nutzern für dieses Projekt, ein User-Pool. Dieser hat eine eigene Domain, in der hinterlegte Nutzer ihre Credentials angeben können. Werden die Credentials bestätigt, stellt Cognito ein Auth-Token zur Verfügung, mit welchem dann der Zugriff auf die API möglich ist. Im Frontend wird mit einem Login-Button ein Link zu der Cognito-Auth-Seite hergestellt, der den User nach erfolgreichem Login automatisch zurücklenkt.

Listing 2: EC2-Proxy in NodeJS

```
    // Load .env at startup
require('dotenv').config();

const express = require('express');
const morgan = require('morgan');
const { Pool } = require('pg');

// Sanitize and trim environment variables
const dbUser = process.env.DATABASE_USER?.trim();
const dbPass = process.env.DATABASE_PASSWORD?.trim();
const dbHost = process.env.DATABASE_HOST?.trim();
const dbPort = Number(process.env.DATABASE_PORT);
const dbName = process.env.DATABASE_NAME?.trim();

console.log('Starting DB proxy service');
console.log('CWD:', process.cwd());
console.log('Database config:', { host: dbHost, port: dbPort, user: dbUser, databa

// Set up Express
const app = express();

// 1. Morgan for HTTP logging
app.use(morgan(':method :url :status :res[content-length] - :response-time ms'));

// 2. JSON body parsing
app.use(express.json());

// 3. Sanity dump for POST bodies
app.use((req, res, next) => {
if (['POST','PUT','PATCH'].includes(req.method)) console.log('> BODY:', req.body);
next();
});

// 4. Postgres pool using sanitized env
const pool = new Pool({
host: dbHost,
port: dbPort,
user: dbUser,
password: dbPass,
database: dbName,
ssl: { rejectUnauthorized: false }
});

// Async wrapper helper
defaultWrapAsync = fn => (req, res, next) => fn(req, res, next).catch(next);

// 5. Health endpoint
defaultWrapAsync(async (req, res) => {
await pool.query('SELECT 1');
res.sendStatus(200);
});
app.get('/health', defaultWrapAsync(async (req, res) => res.sendStatus(200)));

// 6. Query endpoint
app.post('/query', defaultWrapAsync(async (req, res) => {
const { text, params } = req.body;
const { rows } = await pool.query(text, params);
res.json(rows);
}));

// 7. 404 catch-all
app.use((req, res) => res.sendStatus(404));

// 8. Error handler
```

Listing 3: Lambda-Funktion für die API

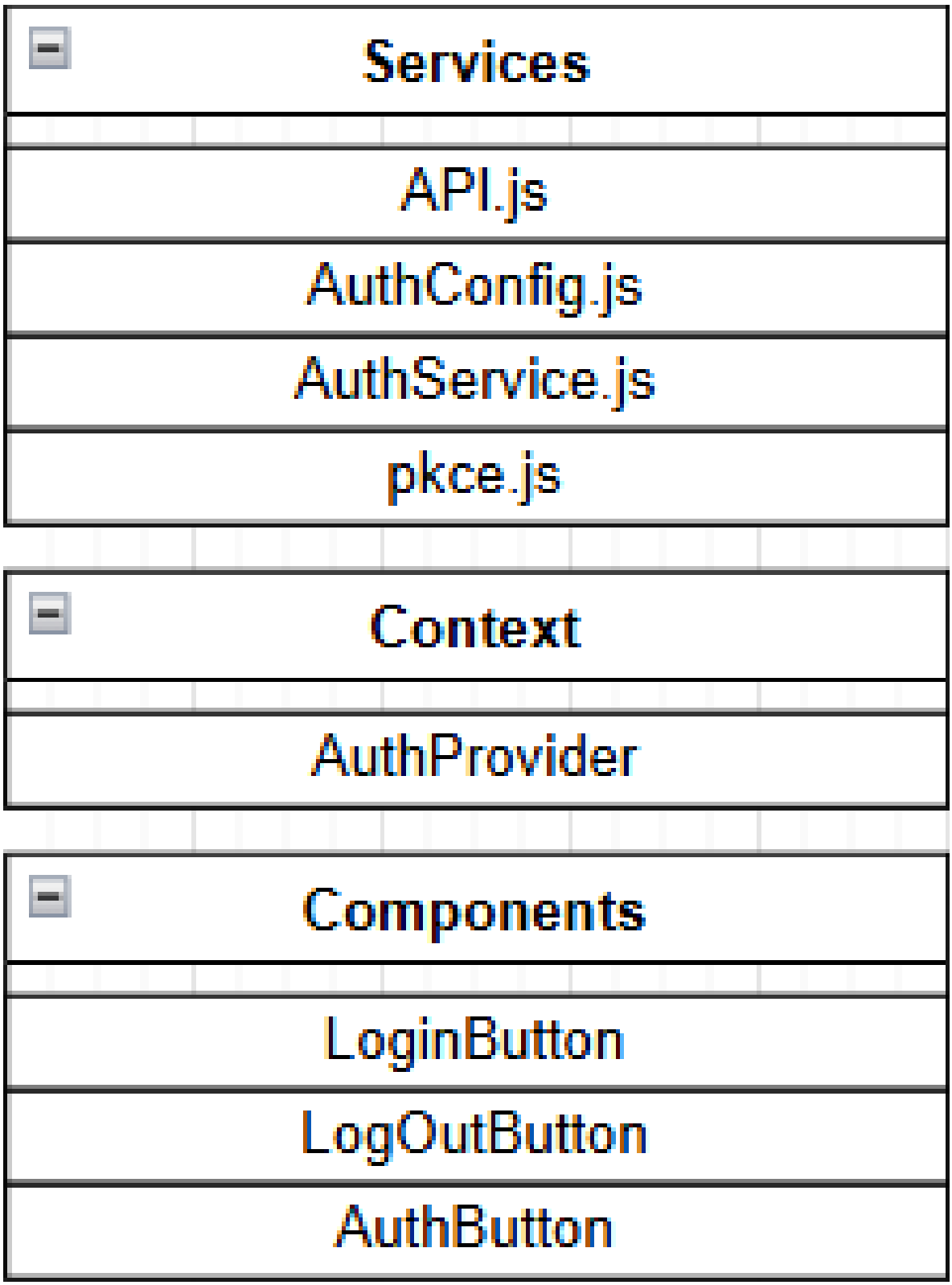
```
    import { Pool } from 'pg';

// Create a pool as a singleton so Lambda can reuse TCP connections
const pool = new Pool({
  host:     process.env.DB_HOST,
  database: process.env.DB_NAME,
  user:     process.env.DB_USER,
  password: process.env.DB_PASSWORD,
  port:     process.env.DB_PORT,
  // If you need SSL, uncomment and adjust:
  // ssl: { rejectUnauthorized: false }
});

export const handler = async (event) => {
  const projectId = event.pathParameters?.projectId;
  if (!projectId) {
    return { statusCode: 400, body: 'Missing projectId path parameter' };
  }

  let client;
  try {
    client = await pool.connect();

    const result = await client.query(
      `SELECT "ProjectID", "AttributeID"
         FROM public."Newport_Project"
        WHERE "ProjectID" = $1`,
      [projectId]
    );

    if (result.rows.length === 0) {
      return { statusCode: 404, body: 'Project not found' };
    }

    return {
      statusCode: 200,
      headers: { 'Content-Type': 'application/json',
      'Access-Control-Allow-Origin': 'http://localhost:3000',
      'Access-Control-Allow-Credentials': true,
      // if you need cookies
      // add any other headers your client uses:
      'Access-Control-Allow-Headers': 'Authorization,Content-Type',},
      body: JSON.stringify(result.rows[0])
    };

  } catch (err) {
    console.error('DB error', err);
    return {
      statusCode: 500,
      body: 'Internal server error'
    };

  } finally {
    client?.release();
  }
};
```

8 Frontend-Implementierung

Das Frontend der Anwendung ist in drei wesentliche logische Abschnitte eingeteilt. Der erste Teil ist die Authorisierung, welcher für Abfragen von Credentials und der Speicherung dieser zuständig ist. Der zweite Teil verwendet die Credentials dann um auf die API zuzugreifen, und benötigte Daten zu extrahieren. Diese Daten werden dann im dritten Teil, dem User Interface, verwendet.

8.1 Authorisierung

Im Sinne der Erweiterbarkeit und Wartbarkeit wurde folgende Ordnerstruktur gewählt:



Der Login-Prozess wird in drei semantische Kategorien aufgeteilt. An erster Stelle

stehen die Komponenten, die dem User die Interaktion mit der Authorisierungs-Logik ermöglichen.

8.1.1 Components

Obwohl theoretisch auch eine einzelne Komponente für den Login-Prozess ausreichen würde, wurde der Login/Logout-Button im Sinne der Übersichtlichkeit getrittelt. Der Login- sowie Logout-Button sind sind in der Logik bis auf die ausgeführte Methode identisch:

Listing 4: JS-Code for the LogIn-Button

```
// components/LoginButton.js
import React from 'react';
import { useAuth } from '../context/AuthContext';
import { Button } from '@element/react-components';

export default function LoginButton() {
    const { login } = useAuth();

    return <Button onClick={login} label="Log In"/>
}
```

Der Login-Button, welcher aus der Unternehmens-internen React-Bibliothek entnommen wird, ruft bei Interaktion die `login()`-Methode aus dem Authentifizierungs-Kontext auf, welcher im nächsten Abschnitt beschrieben wird.
Der gleiche Prozess findet beim Logout-Button statt, nur dass hier die `logout()`-Methode aufgerufen wird.

Listing 5: JS-Code for the LogOut-Button

```
// components/LogoutButton.js
import React from 'react';
import { useAuth } from '../context/AuthContext';
import { Button } from '@element/react-components';

export default function LogoutButton() {
    const { logout } = useAuth();

    return <Button onClick={logout} label="Log Out"/>
}
```

Diese beiden Komponenten werden dann im AuthButton kombiniert, wobei der Auth-Status entscheidet, welcher Button angezeigt wird:

Listing 6: JS-Code for the AuthButton

```
// components/AuthButton.js
import React from 'react';
import { useAuth } from '../context/AuthContext';
import LoginButton from './LoginButton';
import LogoutButton from './LogoutButton';

export default function AuthButton() {
    const { isAuthenticated } = useAuth();

    return isAuthenticated ? <LogoutButton /> : <LoginButton />;
}
```

Für die Entscheidung, welcher Button angezeigt wird, wird zuerst über die `useAuth()`-Hook[15] der Authentifizierungs-Kontext abgerufen. Der daraus resultierende Boolean-Wert `isAuthenticated` gibt an, ob der User eingeloggt ist oder nicht. Mit diesem Boolean-Wert wird dann entschieden, ob der Login- oder Logout-Button angezeigt wird. Das geschieht in diesem Fall mithilfe eines ternären Operators, der den Wert von `isAuthenticated` überprüft und abhängig vom Wert den entsprechenden Button zurückgibt.[16]

8.1.2 Context

Der Authentifizierungs-Kontext ist ein zentraler Bestandteil der Authorisierungs-Logik. Er stellt die Methoden `login()` und `logout()` zur Verfügung, ist aber zusätzlich auch für die Verarbeitung des Callbacks von Cognito zuständig. Zuerst werden für den Kontexst die benötigten Hooks importiert und ein Context-Objekt erstellt:

[15] In JavaScript, speziell in React, ist eine Hook eine Funktion, mit der ein Zugriff auf React-Features wie State oder Lifecycle-Methoden in Funktionskomponenten möglich gemacht wird

[16] `https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Operators/Conditional_operator`

Listing 7: Import und Kontext

```
import React, { createContext, useState,
useEffect, useContext } from 'react';
import { useNavigate, useLocation } from 'react-router-dom';
import {buildAuthUrl, generateChallenge, generateVerifier,
exchangeCodeForTokens} from '../service/authService';
import authConfig from '../services/authConfig';
import {generateVerifier, generateChallenge} from '../service/pkce';

const AuthContext = createContext();
```

Daraufhin werden für den Kontext relevante Variablen definiert, die den User, den Authentifizierungsstatus und die Tokens enthalten:

Listing 8: Variablen für den Authentifizierungs-Kontext

```
const [user, setUser] = useState(null);
const [isAuthenticated, setIsAuthenticated] = useState(false);
const [tokens, setTokens] = useState(null);
const navigate = useNavigate();
const location = useLocation();
```

Die `login()`-Methode generiert einen zufälligen State und einen PKCE-Verifier, speichert diese im Session Storage und leitet den User zur Authentifizierungs-URL weiter:

Listing 9: Login-Methode

```
async function login() {
    const state = crypto.randomUUID();
    const verifier = generateVerifier();
    const challenge = await generateChallenge(verifier);

    sessionStorage.setItem('oauth_state', state);
    sessionStorage.setItem('pkce_verifier', verifier);

    const url = buildAuthUrl({state, code_challenge: challenge});

    window.location.href = url;
}
```

Die `logout()`-Methode löscht den Session Storage und leitet den User zur Logout-URL weiter:

Listing 10: Logout-Methode

```
function logout() {
    sessionStorage.clear();
    const {logoutEndpoint, clientId, logoutUri} =authConfig;
    window.location.href = `${logoutEndpoint}?client_id=${clientId}&logout_uri=
}
```

Die `handleCallback()`-Methode wird aufgerufen, wenn der User nach der Authentifizierung zurück zur Anwendung geleitet wird. Das wird durch die `useEffect()`-Hook realisiert, die prüft, ob der User auf der Callback-Route ist und ob ein Code in der URL vorhanden ist.

Listing 11: Callback-Handling

```
useEffect(() => {
    if (location.pathname === '/callback' && location.search.includes('code=')
        handleCallback();
    }
}, [location, handleCallback]);
```

Die `handleCallback()`-Methode extrahiert den Code und den State aus der URL, vergleicht den State mit dem im Session Storage gespeicherten Wert und tauscht den Code gegen Tokens aus. Falls der Austausch erfolgreich ist, werden die Tokens im Zustand gespeichert und der User wird zur Dashboard-Seite weitergeleitet:

Listing 12: Callback-Handling

```
async function handleCallback() {
    const params = new URLSearchParams(location.search);
    const code = params.get('code');
    const state = params.get('state');
    const saved = sessionStorage.getItem('oauth_state');

    if(!code || !state || state !== saved) {
        return navigate('/', {replace: true});
    }

    try{
        const verifier = sessionStorage.getItem('pkce_verifier');
        const tokenSet = await exchangeCodeForTokens(code, verifier);
        setTokens(tokenSet);

        const [, payload] = tokenSet.id_token.split('.');
        const userInfo = JSON.parse(atob(payload));
        setIsAuthenticated(true);

        sessionStorage.removeItem('pkce_verifier');
        sessionStorage.removeItem('oauth_state');

        navigate('/dashboard', {replace: true});
    } catch (err) {
        console.error('Error during authentication:', err);
        navigate('/', {replace: true});
    }
}
```

Die `AuthProvider`-Komponente stellt den Authentifizierungs-Kontext für die gesamte Anwendung bereit:

Listing 13: AuthProvider-Komponente

```
    return (
        <AuthContext.Provider
        value={{ user, isAuthenticated, tokens, login, logout }}>
            {children}
        </AuthContext.Provider>
    );
}
export function useAuth() {
    return useContext(AuthContext);
}
```

Die `useAuth()`-Hook ermöglicht den Zugriff auf den Authentifizierungs-Kontext in anderen Komponenten der Anwendung.

8.1.3 Service

Der Service-Ordner enthält unterstützende Funktion für die Authorisierung, wie die Generierung des PKCE-Verifiers und -Challenges, den Austausch des Codes gegen Tokens und die Estellung der Authentifizierungs-URL. Zuerst muss dafür die Konfiguration definiert werden, mit der gearbeitet wird.

8.1.4 AuthConfig

Die `authConfig.js`-Datei enthält die Konfiguration für die Authentifizierung, einschließlich der Endpunkte, Client-ID und Redirect-URI. Zusätzlich wird auch die Basis-URL der API definiert, um später API-Anfragen zu ermöglichen:

Listing 14: AuthConfig

```
const domain = process.env.REACT_APP_COGNITO_DOMAIN;
const clientId = process.env.REACT_APP_COGNITO_CLIENT_ID;
const redirectUri = process.env.REACT_APP_COGNITO_REDIRECT_URI;
const logoutUri = process.env.REACT_APP_COGNITO_LOGOUT_URI;
const apiBaseUrl = process.env.REACT_APP_API_BASE_URL;
export const authConfig = {
    domain,
    clientId,
    redirectUri,
    logoutUri,
    apiBaseUrl: apiBaseUrl,
    authEndpoint: `https://${domain}/oauth2/authorize`,
    tokenEndpoint: `https://${domain}/oauth2/token`,
    logoutEndpoint: `https://${domain}/logout`,
    responseType: 'code',
    scope: 'openid profile email',
};
```

Mit dieser Konfiguration wird nun gearbeitet, um alle weiteren benötigten Daten zu generieren.

8.1.5 AuthService

Der AuthService enthält drei Methoden, die für die Authorisierung benötigt werden:

- `buildAuthUrl()`: Diese Methode generiert die Authentifizierungs-URL, die den User zur Cognito-Anmeldeseite weiterleitet.

- `exchangeCodeForTokens()`: Diese Methode tauscht den erhaltenen Code gegen Tokens aus, die für die Authentifizierung und Autorisierung verwendet werden.
- `refreshTokens()`: Diese Methode aktualisiert die Tokens, wenn sie abgelaufen sind.

Die `buildAuthUrl()`-Methode erstellt die Authentifizierungs-URL, indem sie die Konfiguration und die PKCE-Challenge verwendet:

Listing 15: Build-Auth Methode

```
export function buildAuthUrl({state, code_challenge}) {
    const {
        authorizeEndpoint,
        clientId,
        redirectUri,
        responseType,
        scope
    } = authConfig;
    const params = new URLSearchParams({
        client_id: clientId,
        redirect_uri: redirectUri,
        response_type: responseType,
        scope,
        state,
        code_challenge_method: 'S256',
        code_challenge
    });
    return '${authorizeEndpoint}?{params}';
}
```

Die `exchangeCodeForTokens()`-Methode tauscht bei Rückruf von der Cognito-Authentifizierung den mitgegebenen Code für ein gültiges Auth-Token. Dieses kann dann verwendet werden, um API-Abfragen durchzuführen:

Listing 16: ExchangeCodeForToken Methode

```
export async function exchangeCodeForToken(code, code_verifier){
    const {tokenEndpoint, clientId, redirectUri} = authConfig;

    const params = new URLSearchParams({
        grant_type: 'authorization_code',
        client_id: clientId,
        code,
        redirect_uri: redirectUri,
        code_verifier
    });

    const resp = await fetch(tokenEndpoint, {
        method: 'POST',
        headers: {'Content-Type': 'application/x-www-form-urlencoded' },
        body: params.toString()
    });

    const text = await resp.text();

    if(!resp.ok) throw new Error('Token Exchange failed: $(text)')
    return JSON.parse(text);
}
```

Dafür werden zuerst die nötigen Konfigurations-Daten geladen und die Parameter für die URL-Suche definiert. Mit diesen Daten wird dann eine Anfrage an den TokenEndpoint gesendet und die Antwort als das Token zurückgegeben, sollten keine Fehler auftreten.

8.1.6 PKCE

PKCE(Proof Key for Code Exchange) ist eine Erweiterung des OAuth 2.0-Protokolls, welches zusätzliche Sicherheit für Clients verspricht, die nicht in der Lage sind, ihre Client-Geheimnisse sicher zu speichern. Innerhalb dieser Anwendung wird PKCE verwendet, um den Authentifizierungsprozess sicherer zu gestalten. Dies geschieht über zwei Methoden, `generateVerifier()` und `generateChallenge()`, die jeweils den Verifier und die Challenge generieren.

Die `generateVerifier()`-Methode generiert einen zufälligen Verifier, der als Basis für die Challenge dient. Das geschieht, indem ein Array von 32 zufälligen Bytes generiert wird, welches dann in einen hexadezimalen String umgewandelt wird:

Listing 17: PKCE-Verifier-Generierung

```
export function generateVerifier() {
    const array = new Uint8Array(32);
    crypto.getRandomValues(array);
    return Array.from(array, b => ('0'+ b.toString(16)).slice(-2)).join('');
}
```

Die `generateChallenge()`-Methode nimmt den Verifier als Eingabe und generiert die Challenge, indem der Verifier in einen SHA-256-Hash umgewandelt wird. Das Ergebnis wird dann in einen Base64-URL-kodierten String umgewandelt:

Listing 18: PKCE-Challenge-Generierung

```
export async function generateChallenge(verifier) {
    const encoder = new TextEncoder();
    const data = encoder.encode(verifier);
    const hash = await crypto.subtle.digest('SHA-256', data);
    return btoa(String.fromCharCode(...new Uint8Array(hash)))
        .replace(/\+/g, '-').replace(/\//g, '_').replace(/=+$/, '');
}
```

8.1.7 API

Der API-Service ist die Hook `useApi()`, welche für die Kommunikation mit der Backend-API zuständig ist. Sie Kapselt die Methode `callAPI()` ab, welche den Zugriff auf die Konfigurierte API ermöglicht:

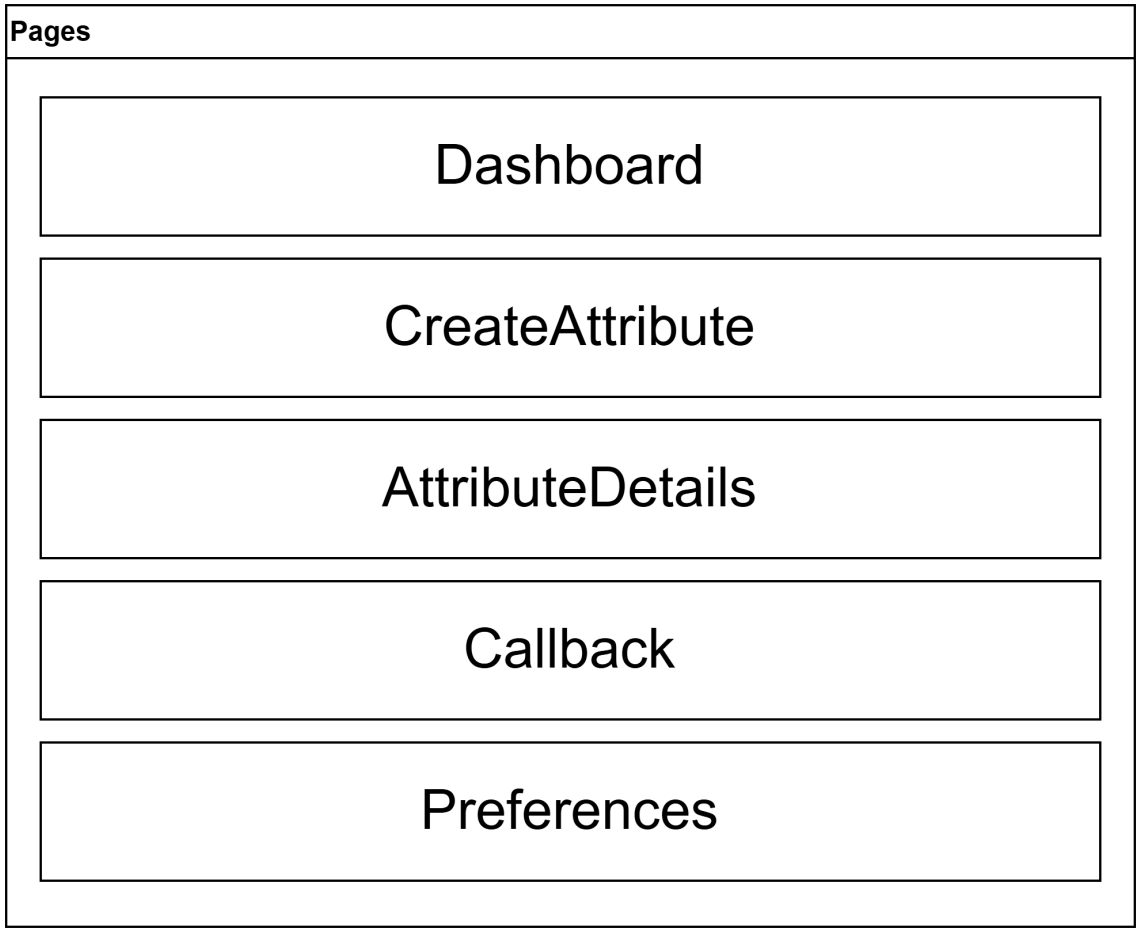
Listing 19: PKCE-Challenge-Generierung

```
async function callApi(path, options = {}){
    const url = '${authConfig.apiBaseUrl}${path}';
    const resp = await fetch(url, {
        ...options,
        headers: {
            'Content-Type': 'application/json',
            Authorization: 'Bearer ${tokens.access_token}',
            ...options, headers
        }
    });
    if (!resp.ok) throw
    new Error('API error ${resp.status}: ${await resp.text()}');
    return resp.json();
}
```

Die Daten, die aus der `callApi()`-Methode zurückgegeben werden, können dann in den Komponenten verwendet werden, um die Daten anzuzeigen oder zu verarbeiten.

8.2 User Interface

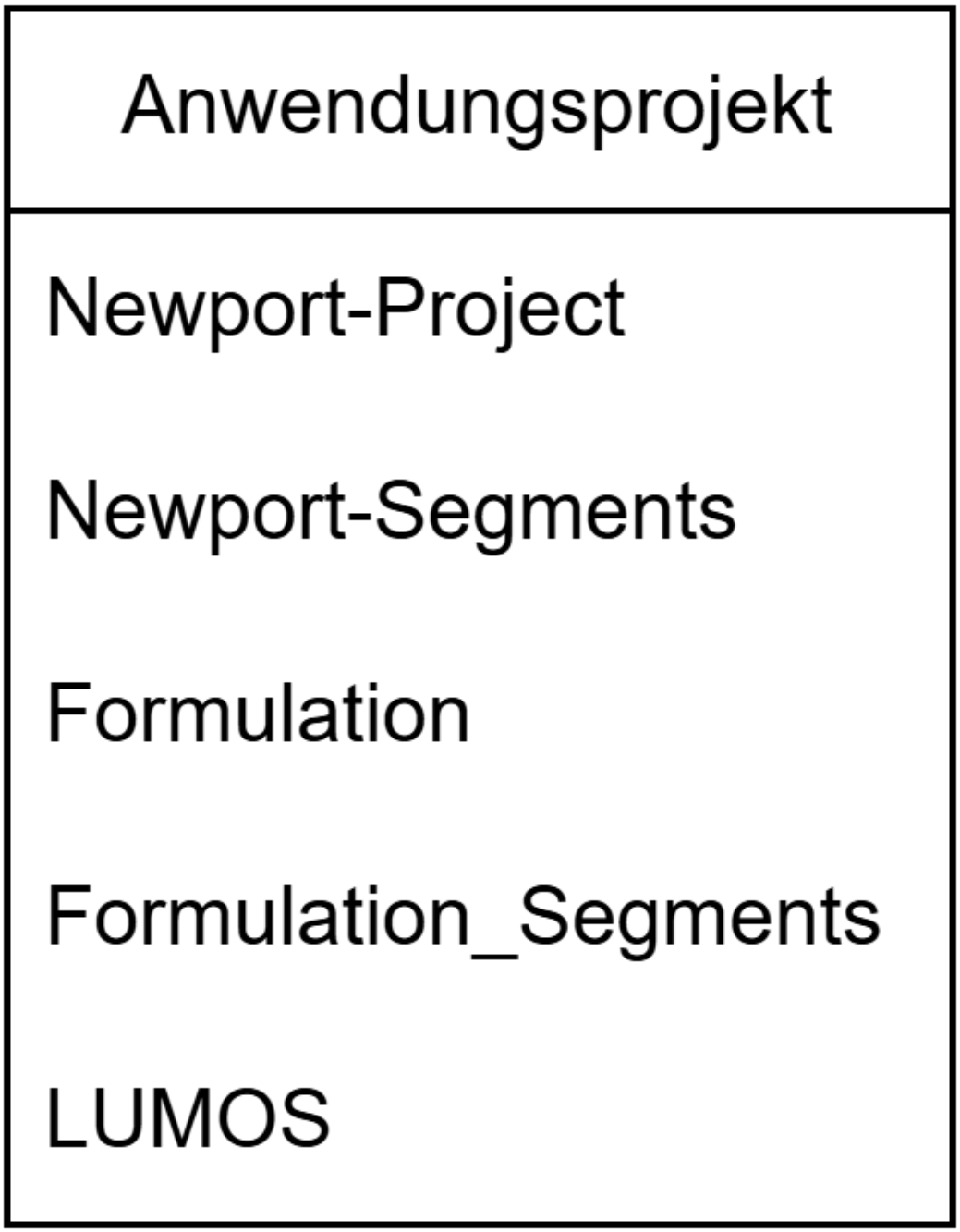
Das User Interface der Anwendung ist in mehrere Komponenten unterteilt, die jeweils für verschiedene Teile der Anwendung zuständig sind:



Den Kern der Anwendung bildet die `Dashboard`-Komponente, welche die Hauptansicht der Anwendung beinhaltet. Von hier aus werden die verscheidenen Unterseiten aufgerufen (mit Ausnahme der Callback-Seite, die nur für die Authorisierung zuständig ist).

8.3 Dashboard

Das Dashboard teilt sich in drei Sektionen auf, mit denen der User seine Attribut-Wahl schrittweise konkretisieren kann. Die erste Sektion ist die Projekt-Auswahl, welche in Form einer Navigationsleiste am oberen Rand der Seite dargestellt wird. Hier ist es wichtig, zwischen einem Projekt im Rahmen dieser Anwendung, und einem Projekt, wie es in der Newport_Projects-Tabelle abgebildet ist, zu unterscheiden. Ein Projekt im Rahmen dieser Anwendung beinhaltet Daten aus allen Datenbanken des CSW, stellt also übergeordnet alle Komponenten einer Wirkstoff-Enwticklung dar. Ein Projekt in der Newport_Projects-Tabelle hingegen beschränkt sich auf die Attribute des Newport-Eintrags, der für den Wirkstoff angelegt wurde. Die folgende Abbildung stellt diese Unterscheidung dar:



Die zweite Sektion ist die Tabellen-Auswahl. Der User hat hier die Möglichkeit, zu entscheiden, welche der Tabellen des Anwendungsprojekts er um Attribute erweitern möchte. Die dritte Sektion stellt die Attribute dar, die der Tabelle und dem Anwen-

dungsprojekt zugeordnet sind. Hier kann der User Attribute auswählen, um diese zu bearbeiten, betrachten oder exportieren. Zusätzlich kann der User hier auch neue Attribute anlegen, die dann in dieser Ansicht angezeigt werden. Um ein neues Attribut anzulegen, wird der Nutzer auf eine neue Seite weitergeleitet, auf der alle Daten für das neue Attribut eingegeben werden können.

8.4 Attribut-Kreation

Die Attribut-Kreation ist in mehrere Schritte unterteilt, die der User durchlaufen muss, um ein neues Attribut zu erstellen. Auf der ersten Seite muss der User grundlegende Informationen zum Attribut angeben, worauf dann die weiteren Schritte angepasst werden. Unter anderem muss der User hier den Name, die Beschreibung und den Typ des Attributs angeben. Dazu kommt auch die Angabe, ob das Attribut aus einem oder mehreren Werten bestehen soll. Diese Angabe ist wichtig, da sie die weiteren Schritte beeinflusst.

Listing 20: Attribut-Kreation

```
<div>
    <label>Name:</label>
    <input type="text" value={name}
    onChange={(e) => setName(e.target.value)} />
    <label>Beschreibung:</label>
    <input type="text" value={description}
    onChange={(e) => setDescription(e.target.value)} />
    <label>Typ:</label>
    <select value={type} onChange={(e) => setType(e.target.value)}>
        <option value="string">String</option>
        <option value="number">Number</option>
        <option value="boolean">Boolean</option>
        <option value="date">Date</option>
    </select>
</div>
```

Im zweiten Schritt muss der User dann den Wert populieren. Ob hier ein einzelner Wert oder mehrere Werte eingegeben werden müssen, hängt von der Angabe im ersten Schritt ab. Hier wird der User aufgefordert, den Wert für das Attribut einzugeben. Je nach Typ des Attributs wird hier ein entsprechendes Eingabefeld angezeigt:

Listing 21: Attribut-Kreation

```
<div>
    <label>Wert:</label>
    {type === 'string' && <input type="text" value={value} onChange={(e) => se
    {type === 'number' && <input type="number" value={value} onChange={(e) =>
    {type === 'boolean' && (
        <select value={value} onChange={(e) => setValue(e.target.value)}>
            <option value="true">True</option>
            <option value="false">False</option>
        </select>
    )}
    {type === 'date' && <input type="date" value={value} onChange={(e) => setV
</div>
```

Zuletzt wird dem User eine Zusammenfassung der Eingaben angezeigt, die er dann bestätigen kann.

Listing 22: Attribut-Kreation

```
<div>
    <h3>Zusammenfassung</h3>
    <p>Name: {name}</p>
    <p>Beschreibung: {description}</p>
    <p>Typ: {type}</p>
    <p>Wert: {value}</p>
    <button onClick={handleSubmit}>Attribut erstellen</button>
</div>
```

Mit Bestätigung des Attributs wird dieses automatisch der Tabelle des Anwendungsprojekts zugeordnet, das zum Zeitpunkt der Erstellung aktiv ist, und dann in der Übersicht aufgeführt.Will der Nutzer nun auf die Werte dieses Attributs zugreifen, kann er dies durch Klicken auf die Karte des jeweiligen Attributs tun. Dadurch öffnet sich eine neue Ansicht, die Details über das Attribut, unter anderem auch die Werte, anzeigt.

8.5 Attribut-Details

Die Attribut-Ansicht ist in vier Abschnitte unterteilt. Der erste Abschnitt zeigt die Details des Attributs an, wie Name, Beschreibung und Typ. Der zweite Abschnitt zeigt die Werte des Attributs an, die der User im Rahmen der Attribut-Kreation eingegeben

hat. Der dritte Abschnitt ermöglicht es dem User, die Werte des Attributs zu bearbeiten, ergo weitere Werte hinzuzufügen, oder bestehende Werte zu ändern oder zu löschen. Im vierten Abschnitt kann der User die Werte des Attributs exportieren. Der Export erfolgt noch automatisch als CSV-Datei, die dann heruntergeladen werden kann. Eine Erweiterung auf andere Formate ist in Zukunft denkbar, jedoch erst bei entsprechendem Nutzer-Feedback.

Listing 23: Attribut-Details

```
<div>
    <h2>{attribute.name}</h2>
    <p>{attribute.description}</p>
    <p>Typ: {attribute.type}</p>
    <h3>Werte</h3>
    <ul>
        {attribute.values.map((value, index) => (
            <li key={index}>{value}</li>
        ))}
    </ul>
    <button onClick={handleEdit}>Werte bearbeiten</button>
    <button onClick={handleExport}>Werte exportieren</button>
</div>
```

Die `handleEdit()`-Methode leitet den User zur Attribut-Kreation-Seite weiter, um die Werte des Attributs zu bearbeiten:

Listing 24: Attribut-Details

```
function handleEdit() {
    navigate(`/attribute/${attribute.id}/edit`);
}
```

Die `handleExport()`-Methode exportiert die Werte des Attributs als CSV-Datei:

Listing 25: Attribut-Details

```
function handleExport() {
    const csvContent = 'data:text/csv;charset=utf-8,' +
    attribute.values.join('\n');
    const encodedUri = encodeURI(csvContent);
    const link = document.createElement('a');
    link.setAttribute('href', encodedUri);
    link.setAttribute('download', `${attribute.name}.csv`);
    document.body.appendChild(link);
    link.click();
}
```

Die CSV-Datei wird dann automatisch heruntergeladen, wenn der User auf den Export-Button klickt. Dies ermöglicht die Verwendung dieser Attribut-Daten in anderen Anwendungen wie PowerBI, um Dashboards oder weitere Auswertungen zu ermöglichen. Die letzte Komponente des Frontends ist die `Preferences`-Komponente, in welcher der User wichtige Einstellungen zur Anwendung bearbeiten kann.

8.6 Preferences

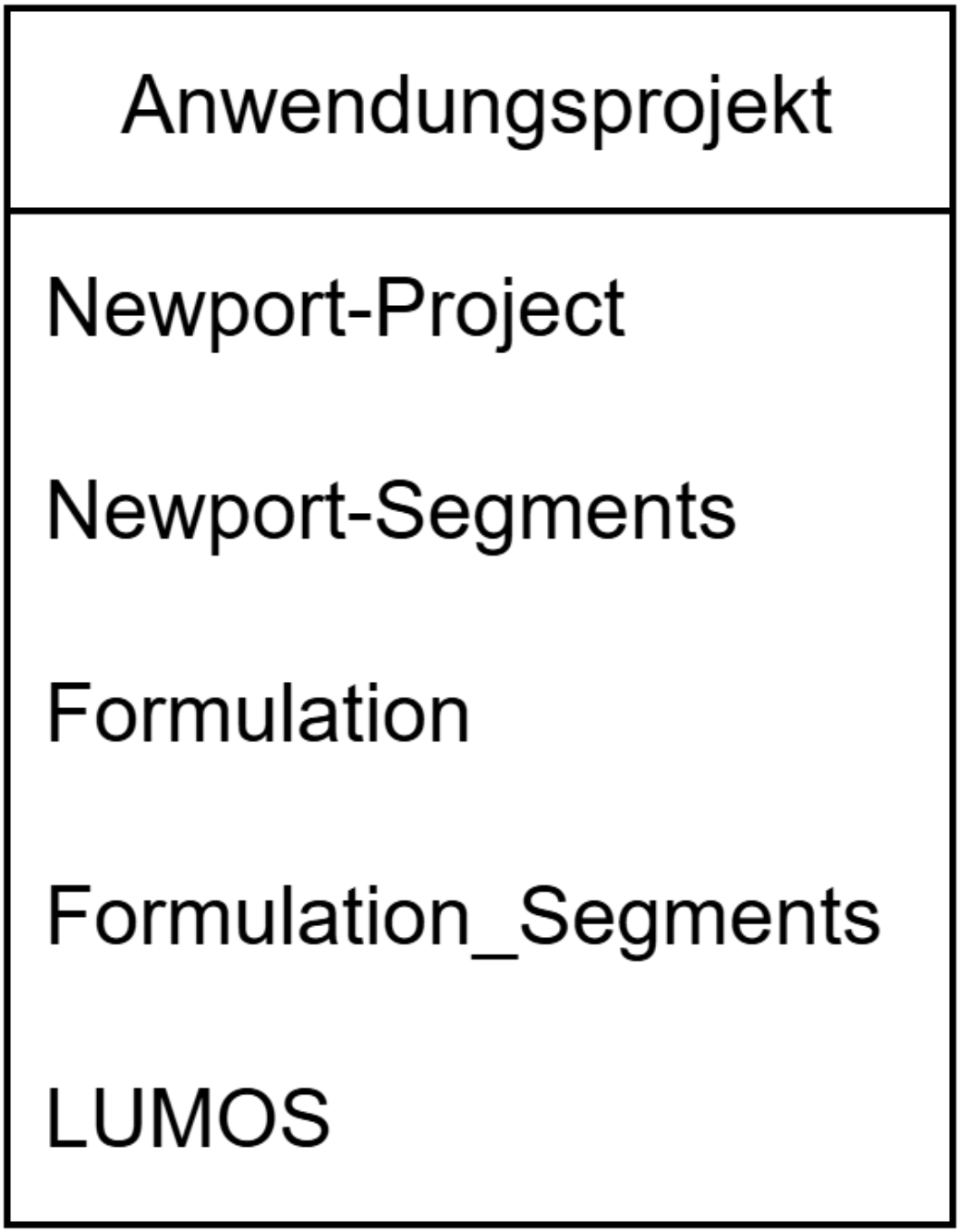
Die wichtigste Einstellung ist die Auswahl der Anwendungssprache. Da die Anwendung unter anderem in Lateinamerika und Asien eingesetzt werden soll, sind nativ Englisch, Spanisch und Portugiesisch unterstützt. Die Anwendung ist jedoch so aufgebaut, dass weitere Sprachen auch von Nutzern hinzugefügt werden können, indem Sprach-Pakete hochgeladen werden. Diese Sprach-Pakete sind JSON-Dateien, die ein Mapping für alle Inhalte der Anwendung auf die jeweilige Sprache enthalten. Hier ein (stark verkürztes) Beispiel für ein solches Sprach-Paket:

Listing 26: Beispiel für ein Sprach-Paket

```
{
    "en": {
        "login": "Login",
        "logout": "Logout",
        "dashboard": "Dashboard",
        "attribute": "Attribute"
    },
    "es": {
        "login": "Iniciar sesion",
        "logout": "Cerrar sesion",
        "dashboard": "Tablero",
        "attribute": "Atributo"
    },
    "pt": {
        "login": "Entrar",
        "logout": "Sair",
        "dashboard": "Painel",
        "attribute": "Atributo"
    }
}
```

Weitere Einstellungen sind momentan nicht vorgesehen, können aber bei Bedarf in Zukunft hinzugefügt werden.

Das resultierende Frontend sieht wie folgt aus:


Anwendungsprojekt
Newport-Project
Newport-Segments
Formulation
Formulation_Segments
LUMOS

9 Evaluierung

Im Folgenden soll die Anwendung auf Basis der zuvor definierten Ziele evaluiert werden. Dabei soll zuerst die Einhaltung der funktionalen, und daraufhin die der nicht-funktionalen Ziele bewertet werden.[17]

9.1 Funktionale Zielerreichung

Die funktionale Zielerreichung ist anhand der Erfüllung der Must-Have-Anforderungen zu bewerten. Diese sind in der folgenden Tabelle zusammengefasst:

Tabelle 12: Funktionale Zielerreichung

Anforderung	**Beschreibung**	**Erfüllt**
Anlegen neuer dynamischer Attribute	Nutzer*innen können neue Attribute anlegen, die einem Projektelement zugewiesen werden können.	Ja
Zuweisung von Attributen zu konkreten Einträgen	Bereits definierte Attribute können spezifischen Datenbankeinträgen zugeordnet und mit Werten befüllt werden.	Ja
Anzeige und Bearbeitung vorhandener Attribut-Werte	Alle zugewiesenen Attribute mitsamt ihren Werten für ein Projektelement werden angezeigt und sind editierbar.	Ja
Löschung von Attribut-Zuweisungen	Bestehende Attribut-Wert-Paare können entfernt werden, ohne das globale Attribut zu löschen.	Ja
Benutzerführung und Eingabeunterstützung	Die Oberfläche bietet verständliche Beschriftungen, Platzhaltertexte und Tooltips zur Unterstützung der Nutzer.	Ja

[17] Ich arbeite momentan an einer ordentlichen wissenschaftlichen Evaluierung mit KPIs, das hier ist nur eine erste grobe Einschätzung.

Von einem funktionalen Standpunkt sind die Ziele vollständig erreicht. Alle definierten Must-Have-Anforderungen sind implementiert und funktionieren wie vorgesehen.

9.2 Nicht-funktionale Zielerreichung

Die nicht-funktionale Zielerreichung ist anhand der Response-Time und der Zukunftstauglichkeit der Anwendung zu bewerten. Diese sind in der folgenden Tabelle zusammengefasst:

Tabelle 13: Nicht-funktionale Zielerreichung

Anforderung	**Beschreibung**	**Erfüllt**
Performance	Ladezeit für die Anzeige eines Projektelements inklusive dynamischer Felder liegt unter 2000 ms.	Ja
Skalierbarkeit	Die Lösung ist so ausgelegt, dass sie mit wachsender Datenmenge und Nutzerzahl ohne grundlegende Umstrukturierung betrieben werden kann.	Ja
Datenintegrität und Validierung	Alle Eingaben werden auf Plausibilität und Formatkonformität geprüft, um konsistente Daten zu gewährleisten.	Ja
Wartbarkeit	Der Quellcode ist modular strukturiert und dokumentiert, um zukünftige Weiterentwicklungen zu erleichtern.	Ja

Die nicht-funktionalen Ziele sind ebenfalls vollständig erreicht. Die Anwendung reagiert schnell und ist so aufgebaut, dass sie auch bei wachsender Nutzerzahl und Datenmenge performant bleibt. Die Datenintegrität wird durch Validierungen sichergestellt, und der Quellcode ist modular und gut dokumentiert.

10 Fazit

Im Rahmen dieser Bachelor-Arbeit wurde, basierend auf den definierten Anforderungen und Zielen, ein flexibles Framework aufgebaut, welches in Zukunft eine Vielzahl verschiedener Anwendungen auf Basis des unterstützten Datenstamms ermöglicht. Für die speziell angeforderte Anwendung konnte ein MVP erstellt werden, der in den kommenden Monaten verbessert und erweitert werden kann. Die Implementierung der dynamischen Attribute ermöglicht es, dass Nutzer*innen ihre Projektelemente flexibel anpassen können, ohne dass dafür eine neue Datenbankstruktur entworfen werden muss. In Zukunft wird das Framework ermöglichen, das Bayer-Portfolio um viele weitere Funktionalitäten zu erweitern, mit denen die Produktivität der Division erheblich gesteigert werden kann. Insgesamt leistet das Ergebnis der Arbeit einen praktischen Beitrag zur Selbstständigkeit von Fachabteilungen bei der Datenverarbeitung und legt das Fundament für zukünftige Fortschritte in der Softwareentwicklung bei Bayer.

Anhang

Anhangsverzeichnis

Anhang 1 Gesprächsnotizen

Anhang 1.1 Gespräch mit Werner Müller

Gespräch mit Werner Müller am 01.01.2013 zum Thema XXX:

- Über das gute Wetter gesprochen
- Die Regenwahrscheinlichkeit liegt immer bei ca. 3%
- Das Unternehmen ist total super
- Hier könnte eine wichtige Gesprächsnotiz stehen

Quellenverzeichnis

Ehrenwörtliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Bachelorthesis selbständig angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Langenfeld, 10.06.2025

Thomas Benjamin Hopf