

CESC

DIPLOMARBEIT

verfasst im Rahmen der

Reife- und Diplomprüfung

an der

Höheren Abteilung für Informatik

Eingereicht von:

Elias Mahr
Leopold Mistelberger
Timon Schmalzer

Betreuer:

Thomas Stütz

Projektpartner:

Herbsthofer

Leonding, 4. April 2025

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Die Arbeit wurde bisher in gleicher oder ähnlicher Weise keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Die vorliegende Diplomarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Leonding, 4. April 2025

Elias Mahr & Leopold Mistelberger

Abstract

Brief summary of our amazing work. In English. This is the only time we have to include a picture within the text. The picture should somehow represent your thesis. This is untypical for scientific work but required by the powers that are.



Zusammenfassung

Zusammenfassung unserer genialen Arbeit. Auf Deutsch. Das ist das einzige Mal, dass eine Grafik in den Textfluss eingebunden wird. Die gewählte Grafik soll irgendwie eure Arbeit repräsentieren. Das ist ungewöhnlich für eine wissenschaftliche Arbeit aber eine Anforderung der Obrigkeit. *Bitte auf keinen Fall mit der Zusammenfassung verwechseln, die den Abschluss der Arbeit bildet!*



Inhaltsverzeichnis

1	Einleitung	1
1.1	Ausgangslage	1
1.2	Ist-Zustand	1
1.3	Problem	1
1.4	Aufgabenstellung	1
2	Umfeldanalyse	2
3	Technologien	3
3.1	Mqtt	3
3.2	Keycloak	3
3.3	Reverse Proxy	4
4	Umsetzung	5
4.1	Keycloak	5
4.2	Reverse Proxy	7
5	Zusammenfassung	9
	Literaturverzeichnis	V
	Abbildungsverzeichnis	VI
	Tabellenverzeichnis	VII
	Quellcodeverzeichnis	VIII
	Anhang	IX

1 Einleitung

1.1 Ausgangslage

Die Firma Herbsthofer plant, liefert, montiert und wartet HKLS-Anlagen und Reinräume für Industrie, Gesundheitswesen und Forschung. Das Unternehmen nutzt 3D-Planung und digitale Baustellenlogistik zur Kosten- und Qualitätskontrolle. Nationale und internationale Projekte werden vom Hauptsitz Linz aus umgesetzt.

1.2 Ist-Zustand

Das Unternehmen betreibt zahlreiche Baustellen im In- und Ausland. Für die Dauer der Projekte werden auf diesen Baustellen Containeranlagen genutzt, die als Büro-, Aufenthalts- und Lagerräume dienen. Diese Container werden rund um die Uhr beheizt, um einen durchgehenden Betrieb und geeignete Arbeitsbedingungen für das Personal zu gewährleisten.

1.3 Problem

Ein Baustellencontainer ohne Überwachung produziert unnötige Energiekosten. Zudem fehlt eine Kontrolle über den Zustand des Containers. Häufig wird in einem Container eingebrochen, welche unbemerkt bleiben, und der Täter nicht identifiziert werden kann.

1.4 Aufgabenstellung

Ziel dieser Diplomarbeit ist die Entwicklung des Systems CESC zur Überwachung und Steuerung eines Baustellencontainers. Das System soll Temperatur, Luftfeuchtigkeit, Türstatus und Anwesenheit erfassen, visualisieren und bei kritischen Ereignissen Benachrichtigungen senden. CESC soll dazu beitragen, Energiekosten zu senken und Einbrüche frühzeitig zu erkennen.

2 Umfeldanalyse

Citing [1] properly.

Was ist eine GUID? Eine GUID kollidiert nicht gerne.

Kabellose Technologien sind in abgelegenen Gebieten wichtig [2].

3 Technologien

3.1 Mqtt

3.2 Keycloak

Keycloak ist ein Open Source System für Identität und Zugriff, das die sichere Anmeldung und die Rechteverwaltung für unsere Anwendungen übernimmt. Die Anwendungen schicken die Anmeldung an Keycloak und müssen das Speichern und das Prüfen von Benutzerkonten nicht mehr selbst erledigen. So kann die Anwendung sich auf das Wesentliche konzentrieren, während Keycloak die Anmeldung und die Rechte im Hintergrund mit Sicherheitsstandard für Unternehmen regelt.

3.2.1 Grundidee und Zweck

Die Firma Herbsthofer legt sehr großen Wert auf Sicherheit. Die externe Bedienung von Heizung, Kühlung und Beleuchtung kann, wenn es ausgenutzt wird zu erheblichen Schäden führen.

- **Mitarbeiterschutz:** Bei voll eingeschalteter Kühlung an kalten Wintertagen kann es zu Gesundheitlichen Schäden in Form von verkühlungen bei Arbeitern/Arbeiterinnen führen, die auch mit einem Ausfall für ein paar Tage enden können und so der Firma Geld kosten.
- **Brandgefahr:** Nicht zu vergessen ist auch die erhöhte Brandgefahr. Unkontrollierte Heizbetriebe auf einer zu hohen Temperaturstufe kann im Schlimmsten Fall zu Bränden führen und so erheblichen Schaden anrichten und Personenschaden mit sich führen.
- **Kosten:** Strom wird immer Teurer. Bei durchgehender Nutzung auch an Tagen an denen niemand im Container ist, ist erstens der Schaden an der Umwelt durch extreme Ressourcen Verschwendung zu Beachten. Jedoch auch die immensen, unnötigen Kosten die, die Firma bei Ihrer Stromrechnung erwarten.

3.3 Reverse Proxy

Ein Reverse Proxy steht zwischen dem Webserver und dem Internet. Im Grunde fungiert es wie ein Türsteher für den Server. Anfragen werden von außen entgegen genommen und zum richtigen Dienst weitergeleitet (Frontend, Backend, Keycloak,...). Durch dies werden die echten Adressen verschleiert.

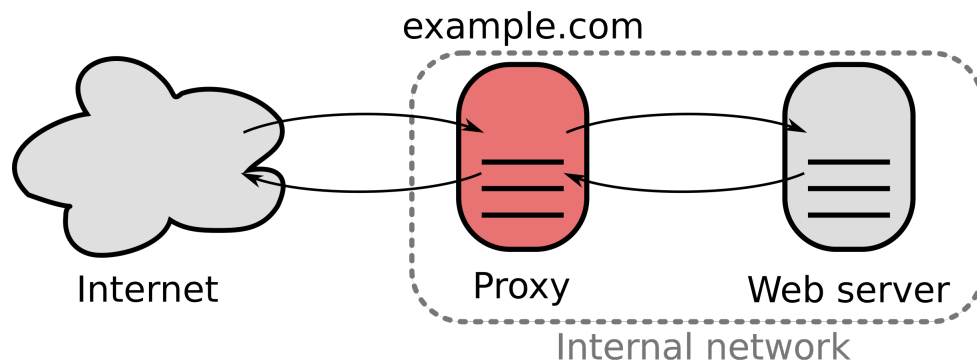


Abbildung 1: Reverse Proxy (Quelle: https://commons.wikimedia.org/wiki/File:Reverse_proxy_h2g2bob.svg, Lizenz: CC0)

3.3.1 Nutzen in der Diplomarbeit

Hauptsächlich gibt es drei Hauptgründe weshalb wir ein Reversproxy einbauen wollten/mussten.

- Keycloaks https Redirects: Keycloak verwendet moderne Standards wie OpenID Connect. Diese Standards setzen auch eine HTTPs Redirect URL voraus. Https setzt im Gegensatz zu http die nötigen Sicherheitsstandards um zum Beispiel Man in the Middle Angriffe zu verhindern.
- Port Chaos: Mit vielen verschiedenen Ports wie 80 für das Frontend, 8080 für Keycloak und 5000 für das Backend wäre alles sehr unübersichtlich. Der User müsste sich 3 URLs merken und im Docker Netzwerk würde es ständig Konflikte geben.
- Sicherheit: Umso mehr Ports öffentlich zugänglich sind umso mehr Angriffsfläche gibt es für eine potenzielle Bedrohung. Ports wie 5000 für das Backend sind von außen gar nicht erreichbar so bleiben die internen Dienste unsichtbar. Auch wenn die Webapplikation nur durch das Intranet erreicht werden kann ist eine zusätzliche Sicherheitsstufe nie ein Fehler.

4 Umsetzung

4.1 Keycloak

4.1.1 Einbindung ins Frontend

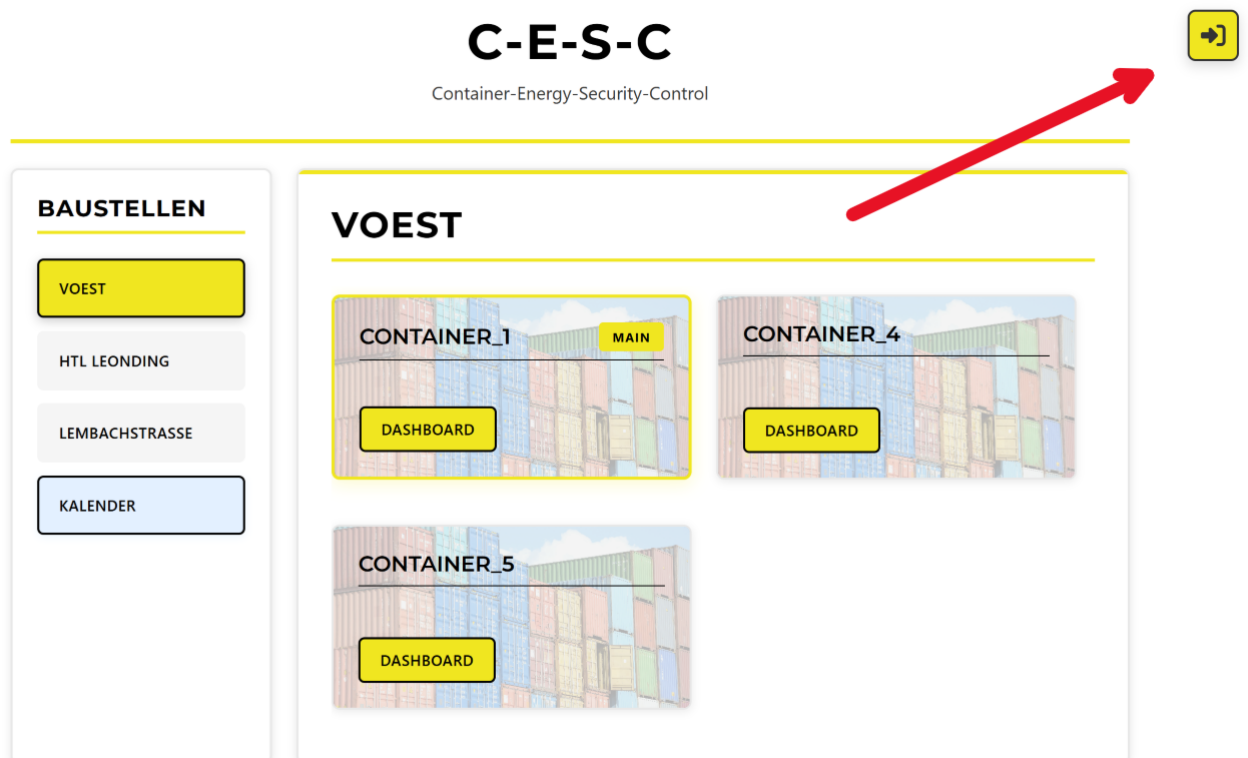


Abbildung 2: Button im Frontend

Um die Webapp möglichst unkompliziert und Benutzerfreundlich zu halten ist der Button wie im Screenshot rechts oben in der Ecke platziert. Unabhängig vom Scroll-Zustand oder der aktuell ausgewählten Page bleibt er auch immer dort, um sich sofort und schnell anmelden zu können.



Abbildung 3: Login- und Logout-Buttons

Das Icon stammt aus der Font Awesome Bibliothek:

```
<i class="fas fa-sign-in-alt"></i>
```

Bei Klick darauf wird man weitergeleitet zum Pfad:

```
https://192.168.20.202/auth/realms/cesc/protocol/openid-connect
```

/auth?client_id=cesc-frontend&redirect_uri=https... Hier kommt dann die Standard Keycloak Login Page. Nach erfolgreicher anmeldung bekommt der User seinen Token, wir automatisch wieder umgeleitet zur vorher besuchten Seite und es werden alle funktionen der Webseite freigeschalten.

4.1.2 das Realm

Ein Realm in Keycloak ist ein isolierter Sicherheitsbereich. Er umfasst Benutzer, Rollen, Clients und Policies für eine bestimmte Anwendung. Wir haben ein Realm namens "cesc" erstellt. Es definiert die gesamte Identitätsinfrastruktur für die Weboberfläche.

Realm Einstellungen

Listing 1: Keycloak Realm Konfiguration

```
1 {  
2   "realm": "cesc",  
3   "enabled": true,  
4   "sslRequired": "external",  
5   "bruteForceProtected": true,  
6   "loginWithEmailAllowed": true  
7 }
```

Rollen**Benutzer****Clients**

4.2 Reverse Proxy

Nginx ist als eigener Docker Container mit nginx.conf implimentiert. Nur der Port 443 ist öffentlich mit Let's Encrypt-Zertifikaten. Die Ports werden Pfadbasiert weitergeleitet:

- http://Keycloak:8080 → location /auth

Listing 2: Nginx Konfiguration /auth

```

1      location /auth {
2          proxy_pass http://keycloak:8080;
3          proxy_set_header Host $host;
4          proxy_set_header X-Real-IP $remote_addr;
5          proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
6          proxy_set_header X-Forwarded-Proto https;
7          proxy_set_header X-Forwarded-Host $host;
8          proxy_set_header X-Forwarded-Port 443;
9          proxy_buffer_size 128k;
10         proxy_buffers 4 256k;
11         proxy_busy_buffers_size 256k;
12     }
```

- http://frontend:80 → location /

Listing 3: Nginx Konfiguration /

```

1      location / {
2          proxy_pass http://frontend:80;
3      }
```

- http://backend:5000 → location /api

Listing 4: Nginx Konfiguration /api

```

1      location /api {
2          proxy_pass http://backend:5000;
3      }
```

Siehe tolle Daten in Tab. 1.

Siehe und staune in Abb. ??.

Dann betrachte den Code in Listing ??.

	Regular Customers	Random Customers
Age	20-40	>60
Education	university	high school

Tabelle 1: Ein paar tabellarische Daten

5 Zusammenfassung

Aufzählungen:

- Itemize Level 1
 - Itemize Level 2
 - Itemize Level 3 (vermeiden)
- 1. Enumerate Level 1
 - a. Enumerate Level 2
 - i. Enumerate Level 3 (vermeiden)

Desc Level 1

Desc Level 2 (vermeiden)

Desc Level 3 (vermeiden)

Literaturverzeichnis

- [1] P. Rechenberg, G. Pomberger *et al.*, *Informatik Handbuch*, 4. Aufl. München – Wien: Hanser Verlag, 2006.
- [2] Association for Progressive Communications, „Wireless technology is irreplaceable for providing access in remote and scarcely populated regions,” 2006, letzter Zugriff am 23.05.2021. Online verfügbar: <http://www.apc.org/en/news/strategic/world/wireless-technology-irreplaceable-providing-access>

Abbildungsverzeichnis

1	Reverse Proxy (Quelle: https://commons.wikimedia.org/wiki/File:Reverse_proxy_h2g2bob.svg , Lizenz: CC0)	4
2	Button im Frontend	5
3	Login- und Logout-Buttons	6

Tabellenverzeichnis

1	Ein paar tabellarische Daten	8
---	--	---

Quellcodeverzeichnis

1	Keycloak Realm Konfiguration	6
2	Nginx Konfiguration /auth	7
3	Nginx Konfiguration /	7
4	Nginx Konfiguration /api	7

Anhang