



**AKADEMIA GÓRNICZO-HUTNICZA IM. STANISŁAWA STASZICA W KRAKOWIE**  
**Wydział Fizyki i Informatyki Stosowanej**

KATEDRA INFORMATYKI STOSOWANEJ I FIZYKI KOMPUTEROWEJ

## Praca dyplomowa

*System do akwizycji danych z rozproszonych systemów  
pomiarowych*  
*System for data acquisition from distributed measurement  
systems*

Autor:  
Kierunek studiów:  
Opiekun pracy:

*Mateusz Barnacki*  
Informatyka Stosowana  
dr inż. Antoni Dydejczyk

Kraków, 2023r.

## **Spis treści**

1. Wstęp
2. Przegląd wzorców architektury aplikacji
3. Elementy charakterystyczne dla architektury mikrousługowej
4. Zapewnienie jakości w projekcie IT
5. Architektura aplikacji
6. Technologie wykorzystane w projekcie
7. Dokumentacja komponentów
8. Podsumowanie

## **1. Wstęp**

## **2. Przegląd wzorców architektury aplikacji**

### **3. Elementy charakterystyczne dla architektury mikrousługowej**

#### **4. Zapewnienie jakości w projekcie IT**

## **5. Architektura aplikacji**

## **6. Technologie wykorzystane w projekcie**



## 7. Dokumentacja komponentów

### 7.1. Wdrożenie aplikacji na serwer wydziału

Jednym z problemów jakie należało rozwiązać w trakcie projektowania aplikacji było znalezienie sposobu na względnie szybkie zbudowanie i uruchomienie systemu na dowolnym środowisku. Istotnymi elementami przy wyborze odpowiedniego narzędzia było uwzględnienie popularności wykorzystania danej technologii przez środowisko programistów oraz przejrzyste napisana dokumentacja. Ponadto ze względów formalnych narzędzie musi być darmowe.

Uwzględniając wyżej wymienione kryteria autor pracy podjął decyzję o wykorzystaniu technologii konteneryzacji przy użyciu narzędzia Docker. Każdy kontener zawiera w sobie wszystkie potrzebne zależności do zbudowania oraz uruchomienia danego komponentu aplikacji. Kontenery są tworzone na podstawie obrazów, które w terminologii Dockera oznaczają niezmiennie szablony definiujące reguły budowania kontenerów. Obrazy są definiowane za pomocą instrukcji zawartych w specjalnych plikach o nazwie Dockerfile.

W przypadku zastosowania architektury mikrousługowej uruchomienie programu wymaga stworzenia większej ilości kontenerów. Narzędziem dedykowanym do zarządzania rozbudowaną infrastrukturą aplikacji jest Docker Compose, który umożliwia zbudowanie i uruchomienie programu przy użyciu jednej komendy. Reguły budowania projektu są umieszczone w pliku o nazwie *docker-compose.yml*. W ramach budowania wielokontenerowej aplikacji można ustalić m.in. kolejność budowania oraz uruchamiania kontenerów, lokalizację plików Dockerfile na podstawie których budowane są kontenery, lokalizację pliku zawierającego kopię zapasową dla baz danych.

Ważnym aspektem związanym z wykorzystaniem technologii konteneryzacji jest oddzielenie kontenera od środowiska zewnętrznego. Aplikacja działa w taki sam sposób na dowolnym systemie operacyjnym lub maszynie wirtualnej. Wobec tego można przetestować program na lokalnej maszynie nie wpływając na działanie systemu na środowisku produkcyjnym. W przypadku naprawy błędu wystarczy zreprodukować dane wejściowe, które spowodowały błąd i wprowadzić konieczne poprawki.

W celu uruchomienia aplikacji wymagana jest instalacja na docelowym urządzeniu systemu kontroli wersji Git oraz wyżej opisanego narzędzia Docker. System kontroli wersji Git służy do stworzenia lokalnej kopii zdalnego repozytorium. Jeżeli aplikacja jest uruchamiana na systemie operacyjnym Windows należy zainstalować dodatek o nazwie Git Bash. Uzasadnienie wykorzystania konsoli Git Bash nastąpi w kolejnej sekcji. Narzędzie Docker umożliwia automatyczne zbudowania oraz uruchomienia aplikacji.

W momencie pisania niniejszej pracy kod źródłowy programu jest umieszczony na platformie GitHub. W celu zabezpieczenia wrażliwych informacji dotyczących sposobu budowania API-Key oraz JWT repozytorium zostało oznaczone jako prywatne. Wydział udostępnił maszynę wirtualną wykorzystującą system operacyjny Rocky Linux. Maszyna znajduje się pod adresem *172.20.40.211*. W celu uruchomienia systemu zainstalowałem wszystkie potrzebne aplikacje wymienione powyżej. Działanie aplikacji można sprawdzić tylko i wyłącznie będąc zalogowanym do sieci wydziału. Strona logowania do systemu znajduje się pod adresem <http://172.20.40.211:3000>.

## 7.2 Pierwsze uruchomienie systemu

Poniższa instrukcja przedstawia wykorzystanie komend w dowolnym wierszu poleceń. Część niżej wymienionych operacji może zostać zastąpiona poprzez wykorzystanie narzędzi posiadających graficzny interfejs użytkownika takich jak IntelliJ IDEA lub Docker Desktop.

Pierwszym krokiem wymagany do uruchomienia systemu na dowolnej maszynie jest utworzenie lokalnej kopii repozytorium za pomocą komendy `git clone`. Aplikacja do wygenerowania JWT wykorzystuje parę asymetrycznych kluczy służących do kodowania oraz dekodowania żetonów. W związku z tym do prawidłowego działania mechanizmu autoryzacji wymagane jest utworzenie klucza publicznego oraz klucza prywatnego. W tym celu trzeba przenieść się do lokalizacji `master-thesis/auth-service/src/main/resources`. Następnie administrator musi utworzyć nowy katalog o nazwie `certs`. W katalogu `certs` należy wykonać poniższą sekwencję komend.

```
1 openssl genrsa -out keypair.pem 2048
2 openssl rsa -in keypair.pem -pubout -out public.pem
3 openssl pkcs8 -topk8 -inform PEM -outform PEM -nocrypt -in keypair.pem -out private.pem
```

Rysunek 1 Utworzenie klucza publicznego oraz klucza prywatnego

Biblioteka OpenSSL jest dostępna na systemach operacyjnych MacOS oraz Linux. W przypadku systemu operacyjnego Windows rekomendowane jest zainstalowanie konsoli Git Bash, która jest dodatkiem przy instalacji systemu kontroli wersji Git i zawiera wbudowaną wersję biblioteki OpenSSL. Pierwsza linia przedstawionego powyżej skryptu generuje klucz prywatny za pomocą algorytmu RSA o rozmiarze 2048 bitów, a następnie zapisuje go do pliku `keypair.pem`. Druga instrukcja procesuje wygenerowany klucz prywatny i generuje na jego podstawie klucz publiczny zapisując go do pliku `public.pem`. Ostatnia komenda tworzy klucz prywatny na podstawie danych z pliku `keypair.pem` w formacie PKCS8 i zapisuje go do pliku `private.pem`. Opcja `-nocrypt` została użyta ze względu na implementacje obsługi JWT we frameworku Spring Boot Security. Po utworzeniu plików `public.pem` oraz `private.pem` można usunąć plik `keypair.pem` oraz skopiować cały katalog do folderu `master-thesis/api-gateway/src/main/resources`.

Kolejnym krokiem jest wykorzystanie narzędzia Docker Compose. W tym celu należy przejść do folderu `master-thesis/` i wykonać poniższą komendę.

```
1 docker compose up -d
```

Rysunek 2 Zbudowanie oraz uruchomienie aplikacji

Przedstawiona komenda umożliwia wygenerowanie obrazów Dockera. Następnie na podstawie obrazów tworzone są kontenery zawierające poszczególne komponenty aplikacji. Opcja `-d` umożliwia wyłączenie śledzenia logów aplikacji po zakończeniu procesu budowania kontenerów.

Aplikacja po pierwszym uruchomieniu zawiera puste bazy danych. Dane logowania dla utworzonych użytkowników znajdują się w pliku `docker-compose.yml`. Utworzenie schematu

bazy danych wymaga wykorzystania narzędzia konsolowego *psql*. Poniższa komenda umożliwi uruchomienie wiersza poleceń PostgreSQL.

```
1 | docker exec -it master-thesis-postgres-1 psql -U postgres
```

*Rysunek 3 Uruchomienie wiersza poleceń dla użytkownika postgres*

Po wykonaniu powyższego polecenia można stworzyć nową bazę danych *auth*. Następnie należy przejść do nowoutworzonej bazy za pomocą następującej komendy.

```
1 | docker exec -it master-thesis-postgres-1 psql -U postgres -W auth
```

*Rysunek 4 Uruchomienie wiersza poleceń dla bazy danych auth*

Do utworzenia schematu bazy relacyjnej należy wykorzystać skrypt, który zawiera polecenia tworzące tabele oraz polecenia wstawiające podstawowe encje. Skrypt znajduje się w pliku *master-thesis/auth-service/src/main/resources/db-scripts/init\_db.sql*.

Ostatnim elementem koniecznym do rozpoczęcia korzystania z aplikacji jest utworzenie pierwszego konta użytkownika o uprawnieniach administratora. Użytkownik ma przypisaną rolę administratora, ponieważ jest to jedyna rola, która daje uprawnienie do stworzenia nowego konta z poziomu klienta aplikacji. Serwis służący do autoryzacji podczas tworzenia nowego konta koduje hasło za pomocą funkcji haszującej o nazwie *bcrypt*. W konsekwencji nie można dodać nowego użytkownika z poziomu bazy danych, ponieważ podczas operacji logowania niezakodowane hasło znajdujące się w bazie będzie się różniło od hasła przetworzonego przez serwer aplikacji. Jedynym sposobem dodania nowego utworzenia z poziomu wiersza poleceń jest wykorzystanie biblioteki *cURL*.

```
1 | curl -d
2 | '{ "username": "Admin",
3 |   "email": "admin@agh.edu.pl",
4 |   "description": "Admin user",
5 |   "password": "admin",
6 |   "roles": ["ADMIN"],
7 |   "projects": [] }'
8 | -H "Content-Type: application/json"
9 | -X POST http://localhost:8080/users
```

*Rysunek 5 Utworzenie konta użytkownika przy użyciu biblioteki cURL*

Powyższe polecenie wysyła żądanie HTTP typu POST. Do wysłanego żądania dołączony jest obiekt JSON (JavaScript Object Notation). W ciele obiektu JSON znajdują się dane potrzebne do stworzenia nowego konta. Alternatywnym sposobem wysłania powyższego zapytania jest wykorzystanie narzędzia o nazwie Postman. Postman udostępnia graficzny interfejs użytkownika, który znacząco ułatwia zmiany parametrów wykonywanych zapytań.

Po utworzeniu konta użytkownika można zalogować się do systemu działającego pod adresem <http://172.20.40.211:3000>.

### **7.3 Wdrażanie zmian w systemie**

## **8. Podsumowanie**

## **Bibliografia**