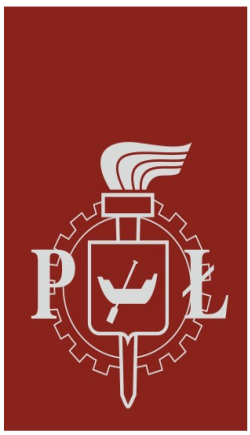


Politechnika Łódzka

Systemy przetwarzania w chmurze

Dokumentacja projektowa

‘Data Room’

Zespół:

→ ***Dawid Wolszczak*** ***224542***
→ ***Michał Markiewicz*** ***224507***

1. Wprowadzenie

- **Cel projektu**

  Celem napisanego przez nas oprogramowania jest udostępnienie użytkownikom prywatnym jak i podmiotom gospodarczych usługi pozwalającej na bezpieczne przechowywanie dokumentów na serwerach chmurowych oraz zarządzaniem dostępu do nich.
- **Odbiorca oprogramowania**

  Docelowymi odbiorcami naszego oprogramowania są podmioty gospodarcze, które pragną skorzystać z usługi składowania danych (w tym danych wrażliwych) na zewnętrznych serwerach oraz przy tym posiadać całkowitą kontrolę nad dostępem do tych danych. Nasza usługa będzie głównie przeznaczona do tych podmiotów, które w swych szeregach posiadają pracowników ‘starszej daty’, którzy niekoniecznie potrafią z płynnością obsługiwać komputer. Dzięki naszemu prostemu interfejsowi nie będą konieczne żadne szkolenia w zakresie korzystania z naszego oprogramowania.
- **Zasada działania**

  Użytkownik (dalej nazywany administratorem) tworzy główny katalog (wirtualny budynek), którego podkatalogi reprezentują wirtualne działy bądź piętra. W katalogach-dzieciach administrator bądź osoba przez niego upoważniona może tworzyć kolejną warstwę podkatalogów reprezentującą wirtualne pokoje, w których to właśnie składowane są dane.

  Tym co wyróżnia nasze rozwiązanie od innych typu ‘cloud storage’ jest system autoryzacji generujący jednorazowe tokeny użytkowników przy każdym logowaniu, które umożliwiają pokonywanie barier (drzwi budynku, drzwi do działów, drzwi do pokoi, działania na plikach). System ten niweluje możliwość zdobycia przez osoby trzecie działających kluczy, ponieważ przy każdym wylogowaniu czy zamknięciu przeglądarki sesja użytkownika jest zamykana a co az tym idzie te wygenerowane tokeny przestają działać. Naturalnym jest, że istnieje możliwość uzyskania danych autoryzacji danego użytkownika przez jego nieuwagę, dlatego nasz system będzie zakładał również dodatkową autoryzację kodu SMS na podany przez użytkownika numer telefonu.

Co więcej generowane tokeny możemy rozróżnić na dwie kategorie: pokonywania wcześniej wspomnianych barier oraz tokeny zezwalające na operację na plikach

Nad całym systemem autoryzacji piecze trzyma grupa administratorów danego budynku. Mogą oni zabierać bądź przyznawać poszczególne klucze.

Opisując powyższe na przykładzie: załóżmy, że mamy użytkownika, który po zalogowaniu do aplikacji otrzymał cztery tokeny:

- klucz wejścia do budynku firmy ‘BubbleCore’
- klucz wejścia do działu ‘marketing’ firmy ‘BubbleCore’
- klucz-wartownik poziomu pełnego pokoju ‘207’ w dziale ‘marketing’ firmy ‘BubbleCore’
- klucz-wartownik poziomu zerowego pokoju ‘208’ w dziale ‘marketing’ firmy ‘BubbleCore’

Oto przykładowe działania jakie ten użytkownik <u>może</u> wykonać:

- Wejść do budynku ‘BubbleCore’;
- Wejść do działu ‘marketing’ w budynku firmy ‘BubbleCore’;
- Wejść do pokoju ‘207’ i ‘208’ w tym dziale;
- Nadpisać, pobrać, usunąć lub dodać dowolny plik w pokoju ‘207’
- Pobrać plik w pokoju ‘208’
    - opcjonalnie: jeżeli istnieje jakiś pokój w dziale ‘marketing’, który nie wymaga autoryzacji, może do niego wejść i pobrać z niego każdy plik;
    - opcjonalnie: jeżeli istnieje dział w budynku ‘BubbleCore’, który nie wymaga autoryzacji, może do niego wejść oraz pobrać każde dane z każdego pokoju;

Oto przykładowe działania jakich ten użytkownik <u>nie może</u> wykonać:

- Wejść do działu ‘logistyka’;
- Nadpisać pliku w pokoju ‘208’;
- Wejść do pokoju ‘209’;
- W dziale ‘dla wszystkich’ nie wymagającego autoryzacji nadpisać, dodać czy usunąć jakiegokolwiek pliku;

2. Prezentacja chmury i dostawcy chmury

- Typ chmury: publiczna
- Dostawca chmury: Google Cloud
- Usługi:
    - App Engine – hosting aplikacji serwerowej
    - Firebase Auth – usługa zarządzania systemem logowania
    - Cloud SQL – (PostgreSQL) baza danych systemu, zawiera informacje takie jak:
        - dane użytkowników
        - uprawnienia użytkowników
        - uprawnienia administratorów
        - informacje o budynkach
    - Cloud Storage – miejsce przechowywania budynków i dokumentów w nich zawartych
    - Cloud SQL Admin/IAM – API wykorzystywane przez aplikację serwerową w celu wykonywania operacji na bazie danych Cloud SQL
    -

3. Prezentacja techniczna systemu informatycznego

- Aplikacja kliencka - frontend

  Aplikacja kliencka wykonana została w technologii JavaScript przy wykorzystaniu frameworka Vue.js

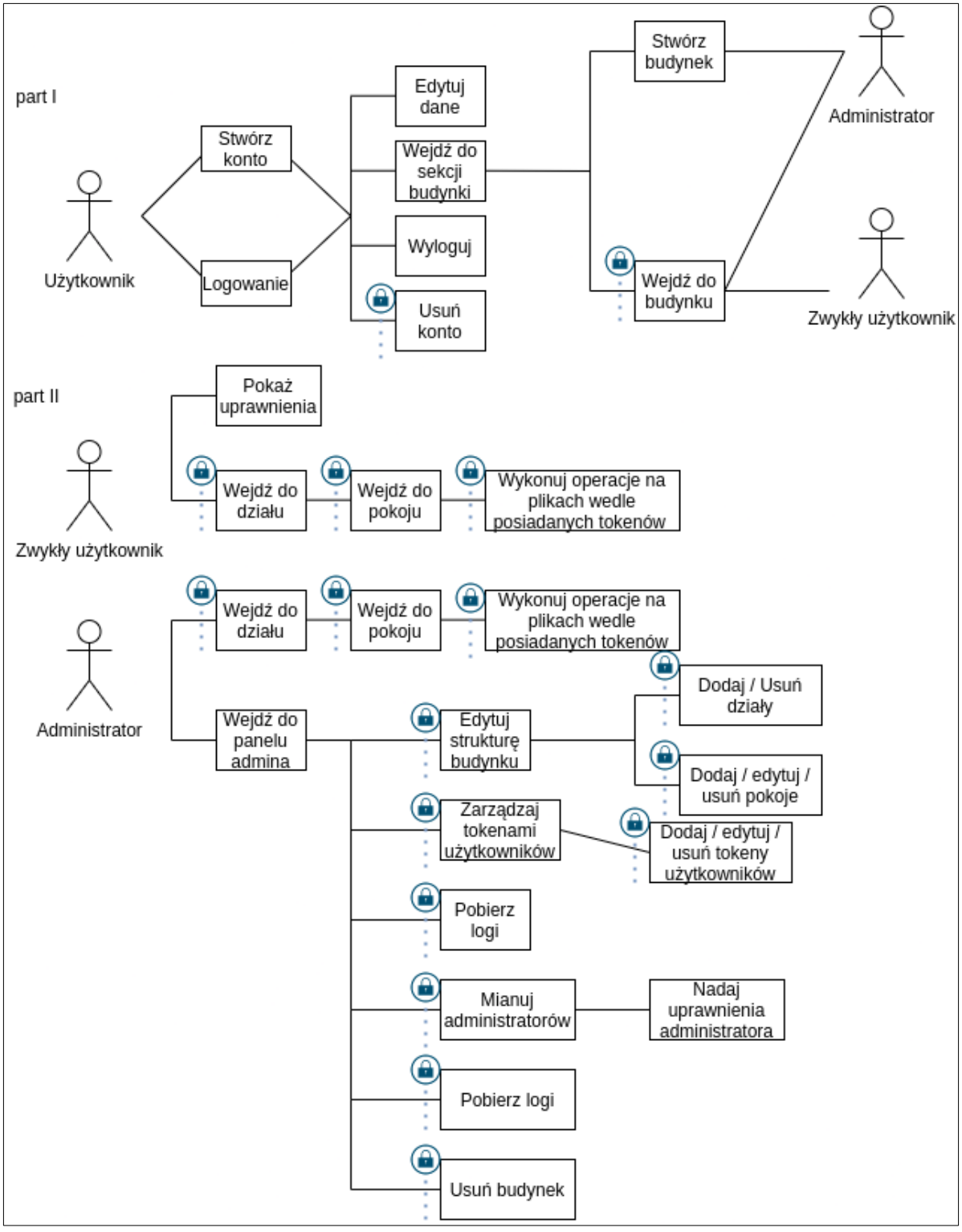
  - Wymagania funkcjonalne:
    - ✔ Do korzystania z aplikacji niezbędne jest połączenie z internetem
    - ✔ Użytkownik może zarejestrować się w systemie
    - ✔ W celu korzystania z systemu użytkownik musi przejść proces autoryzacji – logowanie (w tym kod SMS)
    - ✔ Użytkownik może stworzyć swój wirtualny budynek
    - ✔ Użytkownik może zmienić swoje dane profilowe
    - ✔ Użytkownik-administrator swojego budynku ma pełną kontrolę nad systemem autoryzacji
    - ✔ Użytkownik w celu pobrania lub edycji plików musi przejść przez szereg barier bezpieczeństwa przy użyciu tokenów generowanych podczas logowania przez aplikację serwerową
    - ✔ Po wylogowaniu się użytkownika jego aktualne tokeny wygasają
    - ✔ Użytkownik nie może mieć dostępu do danych, do których nie posiada autoryzacji
    - ✔ Użytkownik-administrator może mianować innych użytkowników administratorami systemu bądź poszczególnych działów
    - ✔ Aplikacja posiada prosty i płynny interfejs

- Aplikacja serwera – backend

  Aplikacja serwerowa wykonana została w technologii Python przy wykorzystaniu frameworka Flask

  - Wymagania funkcjonalne:
    - ✔ Zapisywanie logów działań użytkowników w poszczególnych budynkach
    - ✔ Generowanie i przypisywanie jednorazowych tokenów użytkownikom podczas procesu logowania
    - ✔ Szyfrowanie i deszyfrowanie danych
    - ✔ Niezawodność – pełna kontrola błędów

- Diagram przypadków użycia



Ikona ‘lock’ jest równoznaczne z autoryzacją dostępu wykonania danej operacji.

Administrator to szeroko pojęta rola. Administratorzy mają swoje uprawnienia nadane przez superadministratora. Administrator może przypisać równoznaczną jemu samemu rolę innemu użytkownikowi.

4. Aspekty bezpieczeństwa

- autoryzacja loginem i hasłem
- autoryzacja kodem SMS
- każda operacja w aplikacji wymaga posiadania przez użytkownika tokenu przyznającego możliwość jej wykonania
- wykorzystywanie protokołu HTTPS podczas wymiany danych na linii klient-serwer
- operacje kryptograficzne przy uploadzie, downloadzie plików z budynku