WOJSKOWA AKADEMIA TECHNICZNA

Projekt zespołowy

Temat projektu:

System wspomagający zarządzanie plikami w chmurze prywatnej

Zajęcia prowadził:	mgr inż. Kamil Małysz
Projekt wykonali:	Karol Jampolski
	Mateusz Jarzębski
	Rafał Kępczyński
	Kamil Kiryło
Grupa:	WCY18IJ5S1

Spis treści

1. Obieg danych w przedsiębiorstwie wczoraj i dziś ... 4
   1.1. Przedsiębiorstwo wczoraj ... 4
   1.2. Faza przejściowa ... 4
   1.3. Przedsiębiorstwo dziś ... 5
2. Istniejące systemy zarządzania plikami w chmurze ... 6
   2.1. Dropbox ... 6
   2.2. OneDrive for Business ... 8
   2.3. Google Drive ... 10
   2.4. Filegator ... 11
3. Specyfikacja wymagań ... 12
   3.1. Wymagania funkcjonalne ... 12
   3.2. Wymagania niefunkcjonalne ... 13
      3.2.1. Wymagania użytkowe ... 14
      3.2.2. Wymagania wydajnościowe ... 14
      3.2.3. Wymagania procesu tworzenia ... 14
      3.2.4. Wymagania bezpieczeństwa ... 15
4. Projekt systemu ... 15
   4.1. Model przypadków użycia ... 15
   4.2. Scenariusze przypadków użycia ... 16
   4.3. Macierz związku pomiędzy wymaganiami a przypadkami użycia ... 18
   4.4. Szczegółowy opis przypadków użycia ... 18
   4.5. Diagram klas ... 23
   4.6. Diagram wdrożeniowy ... 24
5. Identyfikacja ryzyka ... 25
   5.1. Ryzyka związane z przedmiotem projektu ... 25
   5.2. Ryzyka projektowe ... 25
6. Opis wykorzystanych technologii ... 28
7. Raport testowy ... 28
   7.1. Zakres testów ... 28
   7.2. Wykonane testy ... 28
      7.2.1. Przypadek użycia: Uwierzytelnianie użytkownika ... 29
      7.2.2. Przypadek użycia: Autoryzacja ... 29
      7.2.3. Przypadek użycia: Wyświetlanie plików ... 29
      7.2.4. Przypadek użycia: Udostępnianie plików innym użytkownikom ... 30

7.2.5. Przypadek użycia: Wyświetlanie plików tekstowych 30
7.2.6. Przypadek użycia: Wyświetlanie zdjęć 30
7.2.7. Przypadek użycia: Wyświetlanie metadanych 31
7.3. Podsumowanie działań testowych 31
8. Wdrożenie systemu 31

1. Obieg danych w przedsiębiorstwie wczoraj i dziś

Przedsiębiorstwa, zarówno w przeszłości, jak i te działające współcześnie, przetwarzają wiele danych. Nieustannie, posiadanie ich stanowi pewien rodzaj kapitału. Sposób ich przetwarzania wraz z upływem czasu zmieniał się. Wszystko zaczęło się od przechowywania danych w formie papierowej, z czasem ten rodzaj utrwalenia informacji zmieniał swoją formę na cyfrową. Z uwagi na kluczową rolę danych, niezbędnym staje się opracowanie dobrych praktyk podczas pracy z wykorzystaniem danych, a także potrzebny jest system zarządzania danymi.

1.1. Przedsiębiorstwo wczoraj

Przez termin *przedsiębiorstwo wczoraj* uznaje się przedsiębiorstwo gromadzące dane w sposób ręczny, to jest dane były zapisywane bądź drukowane na papierze. Taki sposób utrwalania danych generuje duże koszty przechowywania takich danych, nie są one odporne na przypadkowe zniszczenia, takie jak zalanie, ale także na nieprzewidziane sytuacje, na przykład pożar. W przytoczonych sytuacjach dane zapisane w tradycyjny sposób stają się nieodzyskiwalne. Można oczywiście przechowywać dane w przynajmniej kilku kopiach, ale zajmują one wtedy odpowiednio więcej miejsca. Dodatkowo nad dokumentami w formie papierowej ciężko jest współpracować, dzielić się nimi. Podczas pracy powstaje wiele wersji danego dokumentu i ciężko jest zawsze mieć tę najnowszą wersję. W ten sposób powstają wykluczające się, sprzeczne dokumenty, dane, których ujednolicenie zajmuje znaczną ilość czasu.

1.2. Faza przejściowa

Wraz z rozpowszechnianiem się urządzeń komputerowych będących w stanie przetwarzać w efektywny i oszczędny sposób, przedsiębiorstwa zmieniały i ciągle zmieniają swoje podejście do przechowywania danych. Komputery okazują się być bardzo dobrymi urządzeniami przechowywującymi dane. Dane były i nadal są przechowywane na dyskach wewnętrznych w komputerach personalnych pojedynczych użytkowników, a co gorsze, również na dyskach zewnętrznych. Komputery te, zazwyczaj mobilne, oraz dyski były często przenoszone, były zabierane w liczne podróże służbowe, prezentacje u Klientów. W takich sytuacjach bardzo prosto wyobrazić sobie kradzież tych nośników danych, albo nawet zgubienie tych urządzeń. Dane stają się łatwym łupem na przykład konkurencji, która może je bardzo sprawnie wykorzystać. Taki rodzaj nośników danych bardzo łatwo uszkodzić, zwłaszcza jeżeli są to dyski twarde, których budowa opiera się na obracających się talerzach, z których dane są odczytywane za pomocą głowicy. Wystarczy, że w trakcie

pracy dysku urządzenie lub sam dysk zewnętrzny dozna wstrząsów bądź upadku, wtedy dane mogą być bezpowrotnie uszkodzone. Kolejną wadą przechowywania danych w sposób zdecentralizowany jest to, że najczęściej nie stosowane są kopie zapasowe, co skutkuje nieodwracalną utratą danych. Innym problemem związanym z takim sposobem przechowywania danych jest brak synchronizacji wersji dokumentów. Problem ten pojawia się w sytuacji, gdy kilku pracowników równolegle pracuje nad tym samym dokumentem, nanosi poprawki, zmiany czy też dodaje i usuwa fragmenty. Zmiany nakładają się na siebie, tworząc później konflikty pomiędzy wersjami i trudno jest scalić dokument do spójnej wersji. Proces ujednolicania wersji może wymagać wiele czasu i wysiłków. Kolejny problem wynikający z równoległej pracy nad dokumentami to utrudniona wspólna prace nad dokumentami – po każdej zmianie pracownicy muszą przesyłać sobie różnymi metodami, na przykład korzystając z poczty elektronicznej, kolejne wersje dokumentu. Jest to dość uciążliwe oraz przede wszystkim zabiera czas. Również dzielenie się dokumentami z Klientami wymaga wysłania wiadomości przy użyciu poczty elektronicznej. Każda, nawet drobna zmiana wiąże się w ten sposób z kolejną wiadomością do Klienta.

1.3. Przedsiębiorstwo dziś

Współczesne przedsiębiorstwo nie może sobie pozwolić na brak dostępności dokumentów. Wszystkie opisane wyżej problemy nie mogą dotyczyć efektywnie działającej firmy, w której utrata dostępu do danych może skutkować w ogromnych problemach i kosztach. Jednym ze stosowanych dzisiaj podejść jest przechowywanie danych, dokumentów w jednym miejscu. Tym miejscem jest serwer umieszczony w serwerowni, czyli pomieszczeniu mającym określone wymagania. Są nimi redundantne zasilanie, sieć, zachowanie odpowiedniej temperatury. Oprócz tego już same serwery są przystosowane do ciągłej, nieprzerwanej pracy. Są budowane w taki sposób, aby każdy krytyczny moduł posiadał redundancję i mógł być wymieniany bez potrzeby wyłączania całego serwera, ang. *hot swap*. Przykładami takich komponentów są karty sieciowe, zasilacze, a nawet wentylatory. Dane przechowywane i przetwarzane w serwerach umieszczone są na specjalnie przystosowanych dyskach, mogących pracować nieprzerwanie. Często też tworzone są macierze dyskowe, które służą do łączenia kilku fizycznych dysków w jeden wirtualny widziany w systemie. Taka konfiguracja dysków pozwala na odzyskanie wszystkich danych z dysku wirtualnego w przypadku awarii jednego z nich. Dużo łatwiej również wykonywać kopię zapasową danych będących w jednym miejscu i przechowywać ją na zapasowych serwerach, dyskach, a nawet

w chmurze. Również ryzyko fizycznej kradzieży danych jest zminimalizowane – dane są przechowywane w siedzibie firmy, w serwerowni, do której dostęp jest ograniczony nawet dla pracowników danego przedsiębiorstwa. Scentralizowanie miejsca przechowywania danych ułatwia pracę na jednej, zawsze aktualnej wersji dokumentu. Wystarczy, że pracownik po ukończeniu bieżącej pracy nad dokumentem prześle go na serwer, a kolejny współpracownik będzie mógł zacząć pracę na najnowszej wersji. Przechowując dane na serwerze jesteśmy w stanie również odizolować je od zewnętrznej sieci Internet – minimalizując ryzyko zdalnej kradzieży danych. Wraz ze wzrostem rozmiaru przechowywanych danych jesteśmy w stanie w łatwy i stosunkowo tani sposób rozszerzyć pojemność w serwerze. Jeżeli firma dysponuje serwerem innym niż NAS, to jest możliwość wykorzystania go również do innych celów takich jak wirtualizacja.

2. Istniejące systemy zarządzania plikami w chmurze

Wraz z rosnącą popularnością przechowywania plików w chmurze prywatnej powstało wiele rozwiązań umożliwiających przechowywanie danych oraz zarządzanie nimi w łatwy i bezpieczny sposób.

2.1. Dropbox

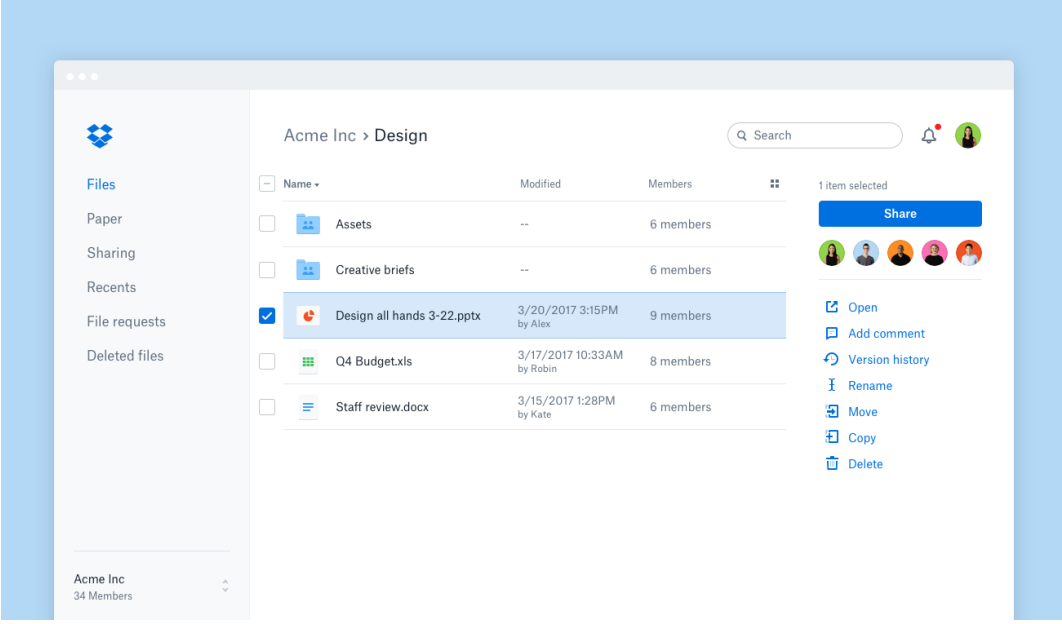
Dropbox to usługa oferowana przez przedsiębiorstwo o tej samej nazwie przechowywania danych Klienta (zarówno klient prywatny jak i przedsiębiorstwo) na serwerach tej firmy. Dla przedsiębiorstw została przygotowana rozszerzona oferta usług w postaci produktu o nazwie Dropbox Business.

Usługa ta, poza miejscem przechowywania plików udostępnia przestrzeń do współpracy nad różnymi plikami. Z jednego miejsca można tworzyć, edytować i udostępniać zawartość opartą o rozwiązania różnych dostawców usług, na przykład aplikacji biurowych Google jak i Microsoft. Oprócz tego, w jednym miejscu można przechowywać i zarządzać plikami z chmur firm trzecich, dzięki czemu nie ma potrzeby przełączania się na platformy innych dostawców, aby znaleźć poszukiwany plik czy dokument. System Dropbox Business można wykorzystywać z użyciem dowolnego urządzenia – komputera, smartfonu, tabletu czy po prostu przeglądarki internetowej.

System integruje się również z najpopularniejszymi aplikacjami do komunikacji, takimi jak Slack czy Zoom, dzięki czemu jest możliwość zaplanowania spotkania bądź wysłania wiadomości prosto z poziomu jednego systemu.

Dropbox kładzie duży nacisk na bezpieczeństwo przechowywanych i udostępnianych na zewnątrz plików. Oferuje w tym zakresie funkcję Dropbox Transfer, która umożliwia ustawienie haseł do udostępnianych plików, dat ich wygaśnięcia.

Interfejs użytkownika jest prosty w obsłudze, nie trzeba zagłębiać się w podstrony aby skorzystać z podstawowych funkcjonalności i operacji na plikach. Podstawowy widok z perspektywy użytkownika końcowego został przedstawiony na Rysunku nr 1.



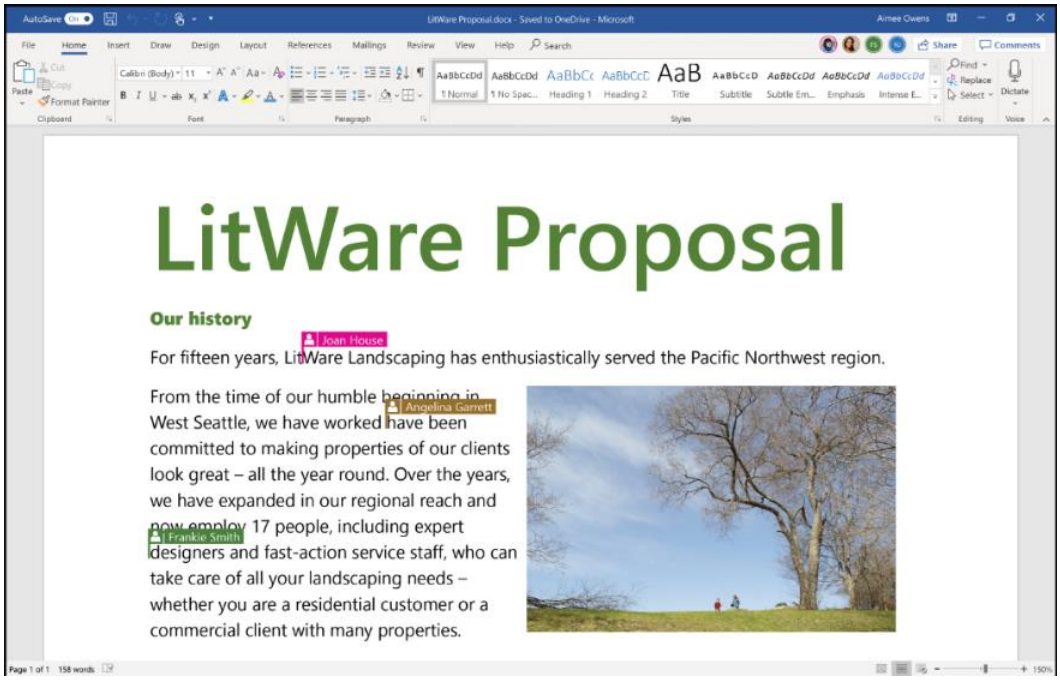
Rysunek 1 Główny widok systemu Dropbox

Na rysunku nr 1 zostały zaprezentowane podstawowe funkcjonalności oferowane przez Dropbox. Menu pionowe z lewej strony ekranu służy do nawigacji pomiędzy dostępnymi narzędziami w ramach systemu, między innymi Kosz, Ostatnio używane pliki, Udostępnianie i inne. W centralnej części panelu użytkownika znajdziemy listę folderów i plików umieszczonych w chmurze wraz z ich nazwami, datą modyfikacji. Zaznaczając kontrolkę typu checkbox po lewej stronie wiersza reprezentującego plik lub folder, po prawej stronie panelu uaktywniają się przyciski odpowiedzialne za akcje związane z zaznaczonymi plikami i/lub folderami. Akcje te umożliwiają udostępnienie pliku, wylistowanie użytkowników, którym plik został już udostępniony, a także najbardziej podstawowe operacje na plikach, takie jak: otwarcie pliku, zmiana nazwy, przeniesienie, skopiowanie, usunięcie. Dodatkowymi funkcjonalnościami są: dodanie komentarza czy historia wersji. Funkcje te są przydatne przy pracy zespołowej nad danym plikiem. W górnej części paneli znajduje się nawigacja pomiędzy katalogami, okno wyszukiwarki, powiadomienia, czy dostęp do profilu użytkownika.

2.2. OneDrive for Business

Usługa OneDrive for Business oferowana jest przez firmę Microsoft. Udostępnia magazyn w chmurze i możliwość udostępniania plików. Istnieje możliwość współpracy nad plikami w ramach usługi. Z uwagi na fakt, że Microsoft jest również wydawcą aplikacji biurowych z rodziny Microsoft Office, OneDrive został zintegrowany z nimi. Nawet z poziomu przeglądarki można wyświetlać i edytować dokumenty.

Dostęp do systemu jest możliwy z dowolnego miejsca, podobnie jak w przypadku Dropbox, czyli komputer, smartfon, tablet i przeglądarka internetowa bez konieczności instalacji jakiejkolwiek aplikacji na urządzeniu. Bardzo przydatną, zwłaszcza w przypadku pracy zespołowej, funkcjonalnością jest możliwość współpracy w czasie rzeczywistym – zmiany wprowadzane przez innych dokumentów są widoczne dla wszystkich współedytujących niemalże w tym samym momencie. Miejsca położenia ich kursorów są zaznaczane kolorami wraz z imieniem i nazwiskiem osoby edytującej. Przykładowy widok edytowanego dokumentu przedstawia Rysunek nr 2.

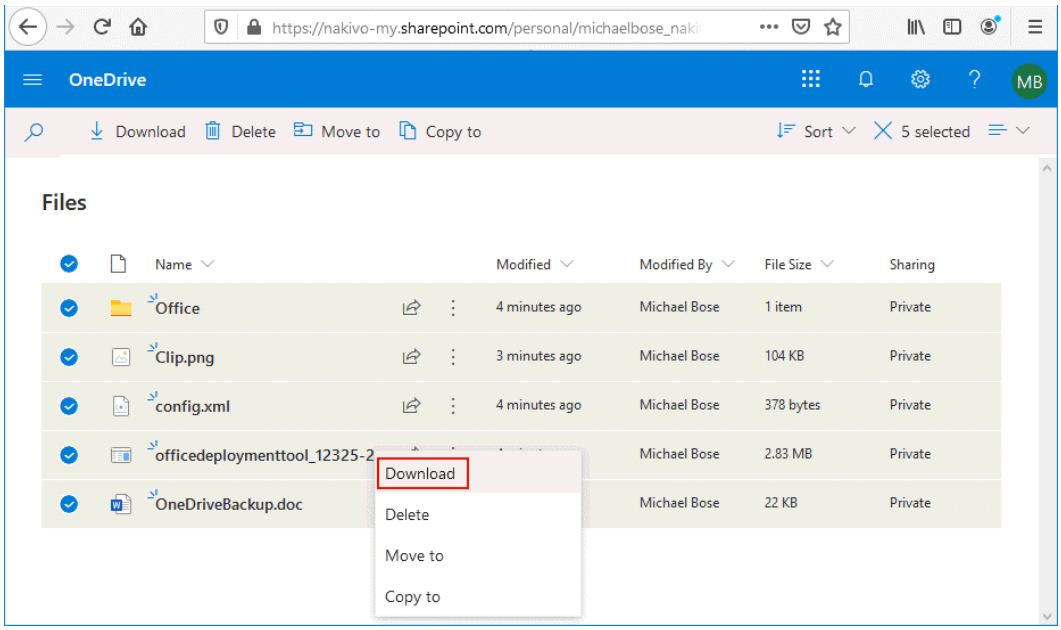


Rysunek 2 Widok edytowanego przez kilka osób dokumentu

Mechanizm udostępniania plików działa w podobny sposób jak w Dropbox, udostępnia możliwość ustawienia hasła, daty wygasania elementu, uprawnień do udostępnianego pliku.

OneDrive jest preinstalowany wraz z systemem operacyjnym Windows i umożliwia automatyczne tworzenie kopii zapasowych plików przechowywanych lokalnie na komputerze.

Na Rysunku nr 3 przedstawiono wygląd interfejsu użytkownika usługi OneDrive for Business.



Rysunek 3 Interfejs użytkownika usługi OneDrive

Rysunek nr 3 przedstawia wygląd aplikacji internetowej OneDrive. W centralnej części widoku znajduje się listing folderów i plików przesłanych do chmury. Operacje na nich możemy wykonać poprzez zaznaczenie kontrolki typu checkbox w wierszu odpowiadającym danemu pliku. Operacje na plikach można wykonać na dwa sposoby: poprzez wywołanie prawym przyciskiem menu kontekstowego bądź wykorzystując pasek narzędziowy w górnej części okna. W obu przypadkach użytkownik ma do dyspozycji funkcję pobrania pliku na dysk lokalny komputera, usunięcia pliku, przeniesienia bądź skopiowania pliku. Opcja udostępniania dostępna jest po kliknięciu na charakterystyczną ikonę bezpośrednio po kolumnie zawierającej nazwę pliku.

Dostęp do innych usług udostępnianych przez firmę Microsoft jest możliwy przy wykorzystaniu górnego paska nawigacyjnego. Również przy jego wykorzystaniu istnieje możliwość odczytu powiadomień, przejście do profilu użytkownika, dostęp do ustawień.

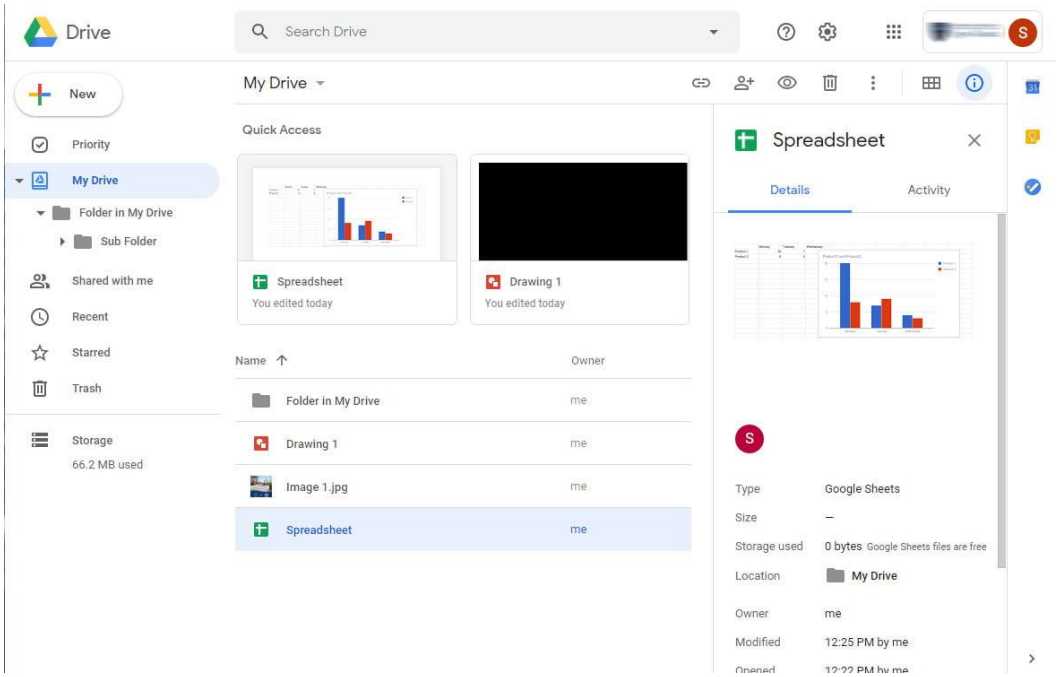
Istnieje również możliwość wyszukiwania plików przy użyciu ikony wyszukiwania.

2.3. Google Drive

Google Drive dla firm jest oferowany przez firmę Google wyłącznie w pakiecie wraz z innymi usługami firmy Google. Z uwagi na taki model sprzedaży, każdy produkt i integracja między nimi, a Google Drive jest eksponowana. Kupując pakiet Google Workspace, oprócz przestrzeni dyskowej uzyskujemy firmową pocztę elektroniczną, możliwość przeprowadzania spotkań wideo, możliwość współpracy nad dokumentami z wykorzystaniem aplikacji biurowych Google, własny komunikator od Google.

Tak jak dla wcześniej opisywanych usług innych firm, Google Drive oferuje dostęp z dowolnego urządzenia będącego w zasięgu sieci Internet.

Rysunek nr 4 przedstawia główny widok interfejsu użytkownika usługi Google Drive.



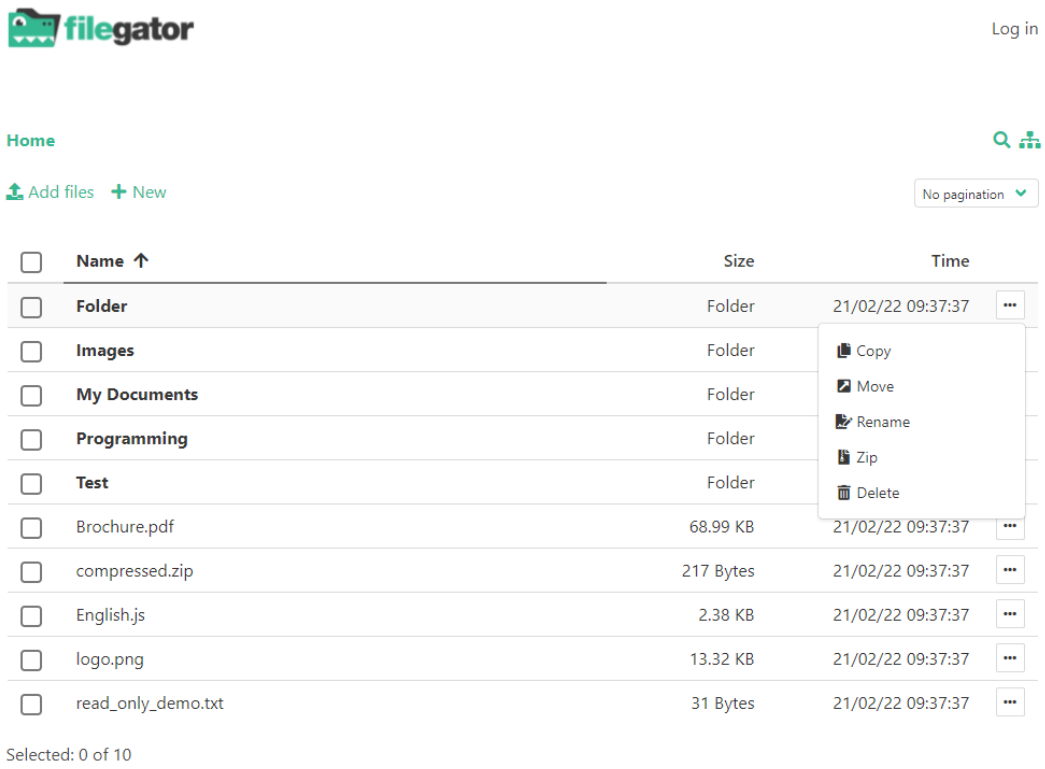
Rysunek 4 Główny interfejs użytkownika Google Drive

Górny pasek nawigacyjny zawiera pole wyszukiwania plików, a także dostęp do ustawień i profilu użytkownika. Lewa strona interfejsu zawiera odnośniki do katalogu głównego dysku, plików udostępnionych, ostatnio używanych czy kosza. W centralnej części ponownie znajduje się listing folderów i plików w bieżącym katalogu. Dostęp do typowych operacji na plikach możliwy jest poprzez wywołanie menu kontekstowego na wierszu odpowiadającemu pliku a także na pasku narzędziowym w górnej części okna. Istnieje możliwość wyświetlenia szczegółów praz podglądu wybranego pliku poprzez kliknięcie na ikonę informacji.

2.4. Filegator

Filegator jest darmowym, otwarto-źródłowym rozwiązaniem umożliwiającym przechowywanie i zarządzanie plikami i folderami. Od zaprezentowanych wcześniej alternatywnych rozwiązań różni się tym, że uruchamiamy go we własnej infrastrukturze. Oferuje on mniejszą liczbę funkcji, ale podstawowe założenie przechowywania plików zostało spełnione.

Po wejściu na stronę internetową aplikacji użytkownik kierowany jest na ekran uwierzytelnienia. Po tej czynności przechodzi na ekran główny aplikacji zaprezentowany na Rysunku nr 5.



Rysunek 5 Interfejs główny użytkownika

Centralną część okna zajmuje listing plików i folderów. Foldery zostały wyróżnione pogrubioną czcionką. Każdy wiersz reprezentujący plik lub folder składa się z checkbox'a, nazwy pliku/folderu, rozmiaru pliku lub określenia *folder*, czas ostatniej modyfikacji, a także menu podręczne zawierające podstawowe akcje na plikach. Dostępne operacje to kopiowanie, przenoszenie, zmiana nazwy, usunięcie bądź spakowanie pliku(ów). Określone typy plików mogą być otwarte bezpośrednio w przeglądarce, na przykład obrazki, dokumenty pdf, kody źródłowe, dokumenty txt. W górnej części aplikacji znajdują się opcje dodawania plików, utworzenia nowego pliku bezpośrednio w chmurze, a także funkcję wyszukiwania, nawigacji po folderach oraz ustawień paginacji.

3. Specyfikacja wymagań

Rozdział ten zawiera specyfikację wymagań funkcjonalnych oraz niefunkcjonalnych. Wymagania funkcjonalne określają jakie możliwości system ma oferować, natomiast wymagania niefunkcjonalne określają co musi spełnić system, aby był przyjemny i wygodny w użyciu dla użytkownika końcowego. Niezwykle ważne jest też to aby system spełniał normy bezpieczeństwa, działał odpowiednia na różnych urządzeniach, oraz był ukończony w przewidzianym dla niego czasie.

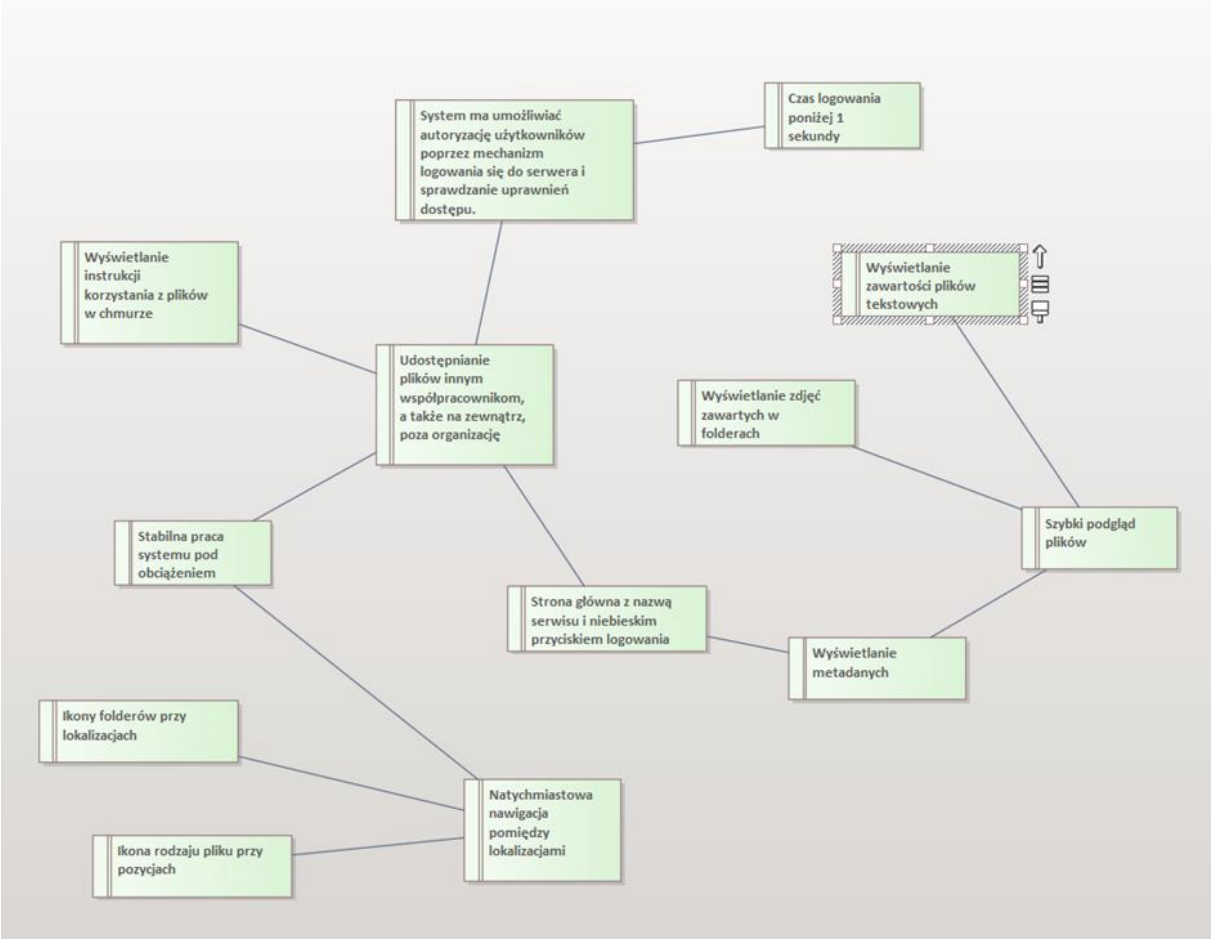
3.1. Wymagania funkcjonalne

Wymagania funkcjonalne mające zostać spełnione przez system przedstawione zostały w tabeli nr 1.

Tabela nr 1. – Zestawienie wymagań funkcjonalnych

L. p.	Wymaganie funkcjonalne
1.	System ma umożliwiać autoryzację użytkowników poprzez mechanizm logowania się do serwera i sprawdzanie uprawnień dostępu.
2.	Wyświetlanie zawartości plików tekstowych
3.	Wyświetlanie zdjęć zawartych w folderach
4.	Udostępnianie plików innym współpracownikom, a także na zewnątrz, poza organizację
5.	Wyświetlanie metadanych
6.	Wyświetlanie instrukcji korzystania z plików w chmurze
7.	Strona główna z nazwą serwisu i niebieskim przyciskiem logowania
8.	Ikony folderów przy lokalizacjach
9.	Ikona rodzaju pliku przy pozycjach

Próbę ich zestawienia i pokazania zależności między nimi przedstawia rysunek nr 6.



Rysunek 6 Diagram wymagań i powiązań między nimi

3.2. Wymagania niefunkcjonalne

Wymagania niefunkcjonalne bywają niekiedy bardziej istotne od wymagań funkcjonalnych. Niespełnienie ich może doprowadzić do tego że system stanie się bezużyteczny dla użytkownika końcowego. Wymagania te wynikają z potrzeb użytkownika, ograniczeń budżetowych, strategii firmy, konieczności współpracy z innymi systemami, czynników zewnętrznych takich jak np. przepisy o bezpieczeństwie, ochronie prywatności dlatego szczególnie ważne jest aby system brał pod uwagę to aby ich implementacja była zgodna z początkowymi założeniami.

Przedstawione w kolejnych podrozdziałach wymagania obejmują dziedziny takie jak: użytkowa, wydajnościowa, bezpieczeństwa oraz procesu tworzenia.

3.2.1. Wymagania użytkowe

- Główna strona systemu musi posiadać nazwę serwisu oraz niebieski przycisk logowania.
- Muszą być wyświetlane ikony folderów przy lokalizacjach.
- Musi być wyświetlana ikona rodzaju pliku przy pozycjach.
- System musi umożliwiać wyświetlanie w trybie ciemnym.
- Tekst musi być czytelny.
- Podstrony serwisu muszą być łatwo widoczne na różnych ekranach urządzeń.
- Strony nie mogą zawierać zbędnych informacji.
- Ikony funkcyjne muszą być łatwo rozpoznawalne.
- Logo serwisu musi być umieszczone w łatwo widocznym miejscu.
- Logo serwisu musi być rozpoznawalne i minimalistyczne.
- Poszczególne pozycje na liście muszą być łatwo odróżnialne.
- Pola tekstowe muszą być responsywne.
- System musi być możliwy do obsługi przez osoby z najczęstszymi typami daltonizmu

3.2.2. Wymagania wydajnościowe

- Czas logowania do systemu nie może przekraczać 1 sekundy.
- Nawigacja pomiędzy lokalizacjami musi być natychmiastowa.
- Praca systemu pod obciążeniem musi być stabilna.
- System musi umożliwiać szybki podgląd plików umieszczonych na serwerze.
- System musi być możliwy do uruchomienia na wielu rodzajach urządzeń.
- System musi być dostępny przez minimum 99% czasu

3.2.3. Wymagania procesu tworzenia

- System musi zostać wykonany w początkowo ustalonym dla niego czasie. Poszczególne fazy systemu muszą zostać sprawozdane przed terminami ich oddania.

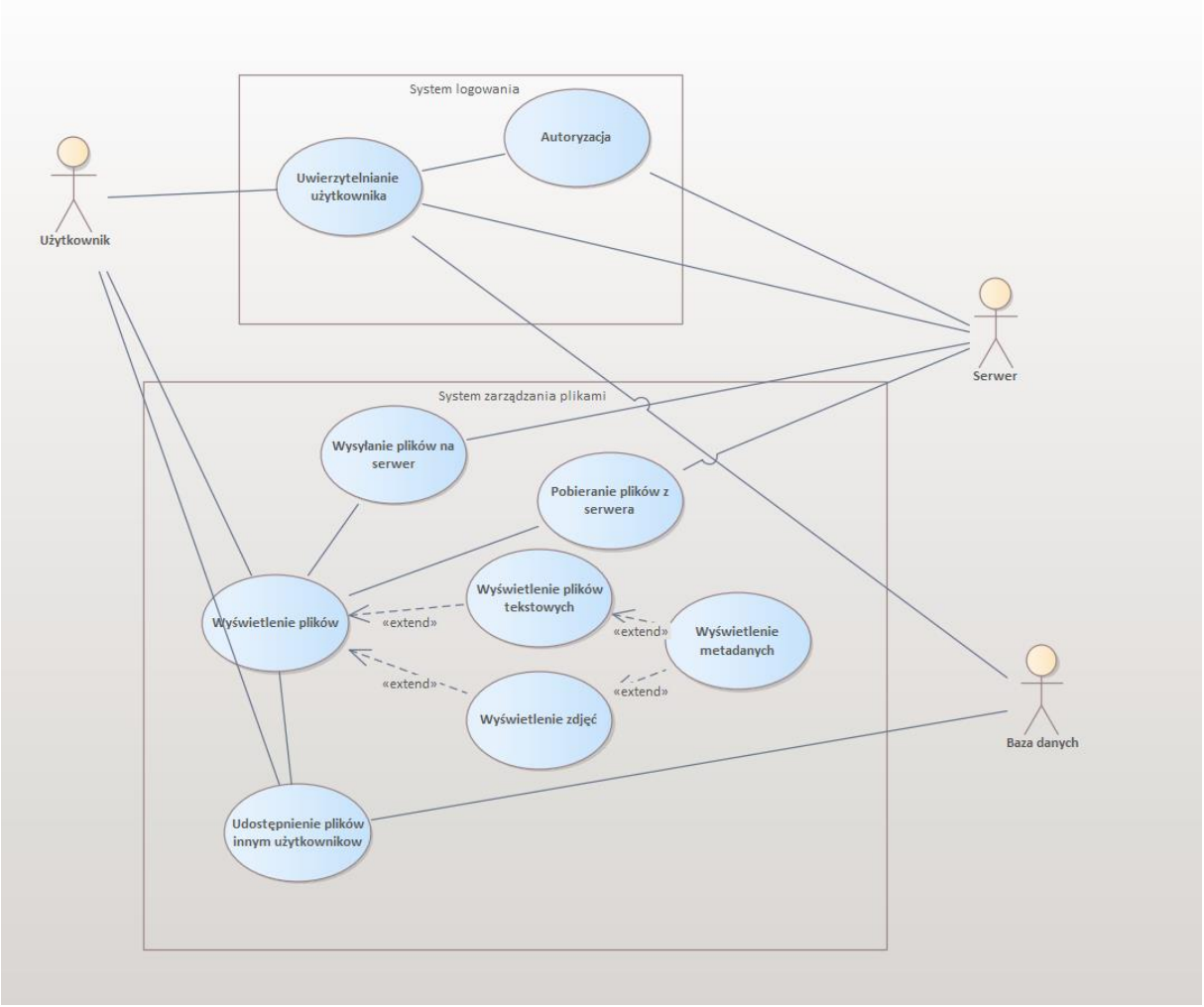
3.2.4. Wymagania bezpieczeństwa

- Hasła muszą być szyfrowane
- Podczas wprowadzania hasła, tekst musi być niewidoczny, zapisany w postaci gwiazdek (*)
- Dane o użytkownikach muszą być przechowywane w bezpiecznym miejscu

4. Projekt systemu

Projekt systemu informatycznego może składać się z różnych elementów. Podczas pracy projektowej, wyróżniono kilka rodzajów diagramów projektowych niezbędnych do całościowego opisu tworzonego systemu.

4.1. Model przypadków użycia



4.2. Scenariusze przypadków użycia

UseCase : Uwierzytelnianie użytkownika

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Użytkownik wchodzi na stronę
2	System uruchamia widok logowania
3	Użytkownik wprowadza dane uwierzytelniające
4	System sprawdza dane uwierzytelniające z bazą danych

UseCase : Autoryzacja

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Na podstawie uwierzytelnionego użytkownika sprawdzane są jego prawa dostępu do danych.
2	Użytkownikowi przydzielane są odpowiednie prawa dostępu do danych

UseCase : Wyświetlenie plików

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Użytkownik uruchamia stronę aplikacji
2	System wyświetla pliki do których użytkownik ma dostęp

UseCase : Udostępnienie plików innym użytkownikow

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Użytkownik wyraża chęć udostępnienia plików poza organizacje
2	System oznacza plik jako ogólnie dostępny

UseCase : Wyświetlenie plików tekstowych

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	System przeszukuje zawartość swoich katalogów
2	Widok wyświetla wszystkie znalezione pliki tekstowe

UseCase : Wyświetlenie zdjęć

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	System przeszukuje swoje katalogi w poszukiwaniu wszystkich plików ze zdjęciami
2	Widok wyświetla informacje o wszystkich znalezionych zdjęciach.

UseCase : Wyświetlenie metadanych

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Pliki są badane w poszukiwaniu zawartych w nich metadanych.
2	Metadane są wyświetlane obok każdego pliku.

4.3. Macierz związku pomiędzy wymaganiami a przypadkami użycia

Source \ Target	Use Cases::Autoryzacja	Use Cases::Udostępnienie plików innym użytkownikow	Use Cases::Uwierzytelnianie użytkownika	Use Cases::Wyświetlenie metadanych	Use Cases::Wyświetlenie plików	Use Cases::Wyświetlenie plików tekstowych	Use Cases::Wyświetlenie zdjęć
Requirement Diagram::Czas logowania poniżej 1 sekundy	←		←				
Requirement Diagram::Ikona rodzaju pliku przy pozycjach		←					
Requirement Diagram::Ikony folderów przy lokalizacjach		←			←	←	←
Requirement Diagram::Natychmiastowa nawigacja pomiędzy lokalizacjami					←		
Requirement Diagram::Stabilna praca systemu pod obciążeniem					←		
Requirement Diagram::Strona główna z nazwą serwisu i niebieskim przyciskiem logowania					←		
Requirement Diagram::System ma umożliwiać autoryzację użytkowników poprzez mechanizm logowania się do serwera i sprawdzanie uprawnień dostępu.	←						
Requirement Diagram::Szybki podgląd plików						←	←
Requirement Diagram::Udostępnianie plików innym współpracownikom, a także na zewnątrz, poza organizację		←					
Requirement Diagram::Wyświetlanie instrukcji korzystania z plików w chmurze					←		
Requirement Diagram::Wyświetlanie metadanych				←			
Requirement Diagram::Wyświetlanie zawartości plików tekstowych						←	
Requirement Diagram::Wyświetlanie zdjęć zawartych w folderach							←

4.4. Szczegółowy opis przypadków użycia

1. Nazwa przypadku użycia: Uwierzytelnianie użytkownika

1.1. Krótki opis przypadku użycia

System sprawdza to czy użytkownik jest tym za kogo się podaje. W celu ustalenia dalszej jego autoryzacji do dostępu do plików.

2. Przepływ zdarzeń

2.1. Typowy przepływ

Użytkownik wchodzi na stronę. System uruchamia widok logowania. Użytkownik wprowadza dane uwierzytelniające. System sprawdza dane uwierzytelniające z bazą danych. Użytkownik ma dostęp do plików.

2.2. Alternatywny przepływ

Użytkownik wchodzi na stronę. System uruchamia widok logowania. Użytkownik wprowadza dane uwierzytelniające. System sprawdza dane uwierzytelniające z bazą danych. Użytkownik jest odrzucony i nie ma dostępu do plików.

3. Specjalne wymagania

Posiadana jest baza danych użytkowników posiadających prawa dostępu do plików.

4. Warunki wstępne

Użytkownik musi znać swoje dane logowania.

5. Warunki końcowe

Tylko uwierzytelnieni użytkownicy mogą mieć dostęp do plików.

6. Extension Points

Brak

1. Nazwa przypadku użycia: Autoryzacja

1.1. Krótki opis przypadku użycia

System sprawdza to do jakich plików dany użytkownik ma dostęp.

2. Przepływ zdarzeń

2.1. Typowy przepływ

Dane uwierzytelnionego użytkownika są konfrontowane z prawami dostępu do poszczególnych danych. Przydzielane są odpowiednie prawa do dostępu do plików.

2.2. Alternatywny przepływ

Dane uwierzytelnionego użytkownika są konfrontowane z prawami dostępu do poszczególnych danych. Brak przydzielenia praw dostępu do plików.

3. Specjalne wymagania

System wie jakie prawa dostępu są wymagane do wyświetlenia danego pliku.

4. Warunki wstępne

System potrafi blokować dostęp do niektórych plików.

5. Warunki końcowe

Przydzielone są prawa dostępu odpowiednie dla danego użytkownika.

6. Extension Points

Brak

1. Nazwa przypadku użycia: Udostępnienie plików innym użytkownikom

1.1. Krótki opis przypadku użycia

Użytkownik może podzielić się swoimi plikami z wybranymi innymi użytkownikami

2. Przepływ zdarzeń

2.1. Typowy przepływ

Użytkownik klika na ikonę pliku lub plików, którymi chce się podzielić, następnie wybiera z menu pozycje „udostępnij”. Pojawia się okno, w którym użytkownik wpisuje dane użytkowników którym chce udostępnić pliki. Na końcu użytkownik zatwierdza operację klikając przycisk „potwierdź”.

3. Specjalne wymagania

Znajomość danych innych użytkowników.

4. Warunki wstępne

Użytkownik musi być zalogowany.

5. Warunki końcowe

Wybrani użytkownicy są w stanie przejrzeć udostępnione pliki.

6. Extension Points

Brak

1. Nazwa przypadku użycia: wyświetlenie metadanych

1.1. Krótki opis przypadku użycia

Użytkownik wyświetla metadane dostępnego dla niego pliku.

2. Przepływ zdarzeń

2.1. Typowy przepływ

Użytkownik widzi w oknie aplikacji rekord przedstawiający dowolny plik. Po jego kliknięciu wyświetla się zawartość tego pliku wraz z dołączonymi do niego metadanymi.

3. Specjalne wymagania

Użytkownik musi mieć połączenie z Internetem.

4. Warunki wstępne

Użytkownik musi być zalogowany

Użytkownik musi być w folderze aplikacji zawierającym plik

Wybrany plik musi posiadać metadane

5. Warunki końcowe

System wyświetla plik, który użytkownik wybrał wraz z metadanymi tego pliku

6. Extension Points

brak

1. Nazwa przypadku użycia: wyświetlenie plików

1.1. Krótki opis przypadku użycia

Użytkownik wyświetla pliki dostępne dla niego

2. Przepływ zdarzeń

2.1. Typowy przepływ

Użytkownik w oknie widzi foldery, w których znajdują się jego pliki, oraz pozostałe pliki. Po kliknięciu na dowolny folder jest w stanie zobaczyć jego zawartość.

3. Specjalne wymagania

Użytkownik musi mieć połączenie z Internetem.

4. Warunki wstępne

Użytkownik musi być zalogowany.

5. Warunki końcowe

System wyświetla folder który użytkownik wybrał

6. Extension Points

- Wyświetlenie plików tekstowych
- Wyświetlenie zdjęć

1. Nazwa przypadku użycia: wyświetlenie plików tekstowych

1.1. Krótki opis przypadku użycia

Użytkownik wyświetla dostępne dla niego pliki tekstowe.

2. Przepływ zdarzeń

2.1. Typowy przepływ

Użytkownik widzi w oknie aplikacji rekord przedstawiający plik tekstowy. Po jego kliknięciu wyświetla się zawartość tego pliku w postaci tekstu.

3. Specjalne wymagania

Użytkownik musi mieć połączenie z Internetem.

4. Warunki wstępne

Użytkownik musi być zalogowany

Użytkownik musi mieć dostęp do pliku tekstowego

Użytkownik musi być w folderze aplikacji zawierającym plik tekstowy

5. Warunki końcowe

System wyświetla plik tekstowy który użytkownik wybrał

6. Extension Points

- Wyświetlenie metadanych

1. Nazwa przypadku użycia: wyświetlenie zdjęć

1.1. Krótki opis przypadku użycia

Użytkownik wyświetla dostępne dla niego zdjęcia.

2. Przepływ zdarzeń

2.1. Typowy przepływ

Użytkownik widzi w oknie aplikacji rekord przedstawiający zdjęcie. Po jego kliknięciu wyświetla się zawartość tego pliku, w postaci obrazu.

3. Specjalne wymagania

Użytkownik musi mieć połączenie z Internetem.

4. Warunki wstępne

Użytkownik musi być zalogowany

Użytkownik musi mieć dostęp do zdjęcia

Użytkownik musi być w folderze aplikacji zawierającym zdjęcie

5. Warunki końcowe

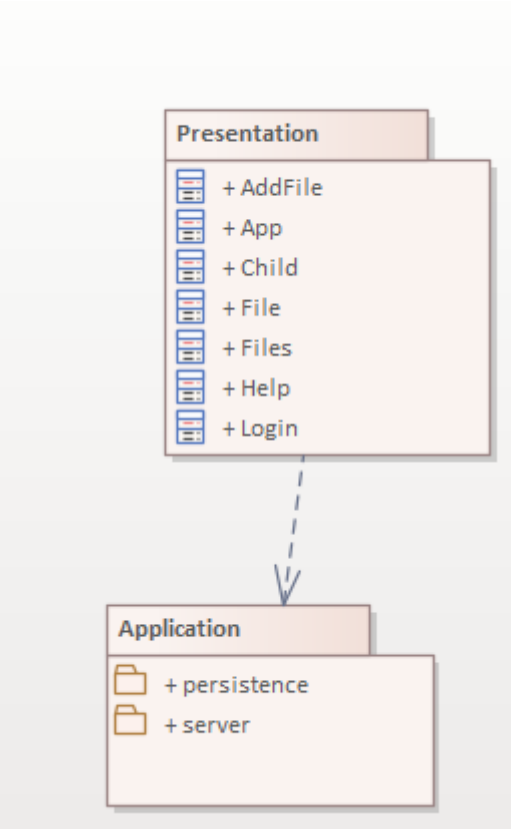
System wyświetla zdjęcie, które użytkownik wybrał

6. Extension Points

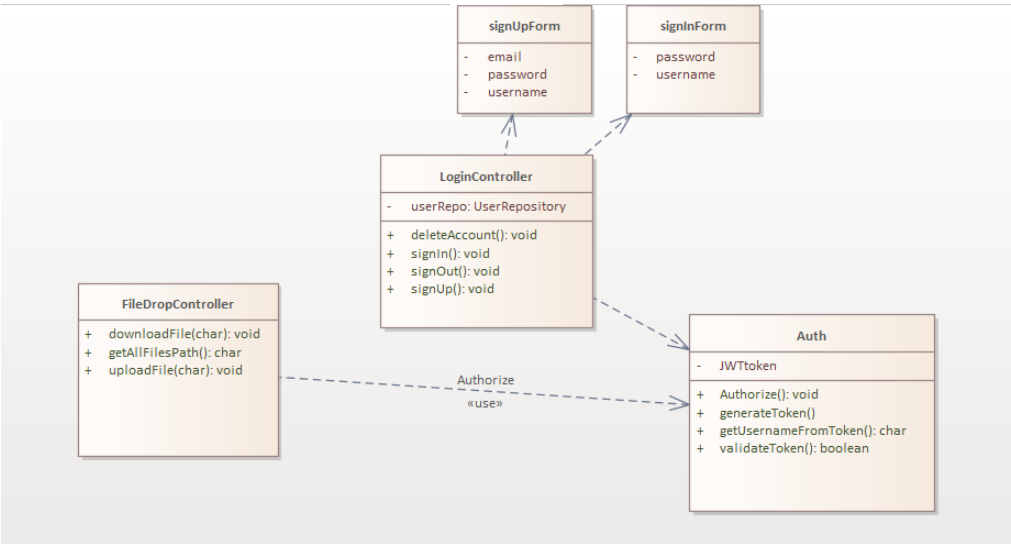
- Wyświetlenie metadanych

4.5. Diagram klas

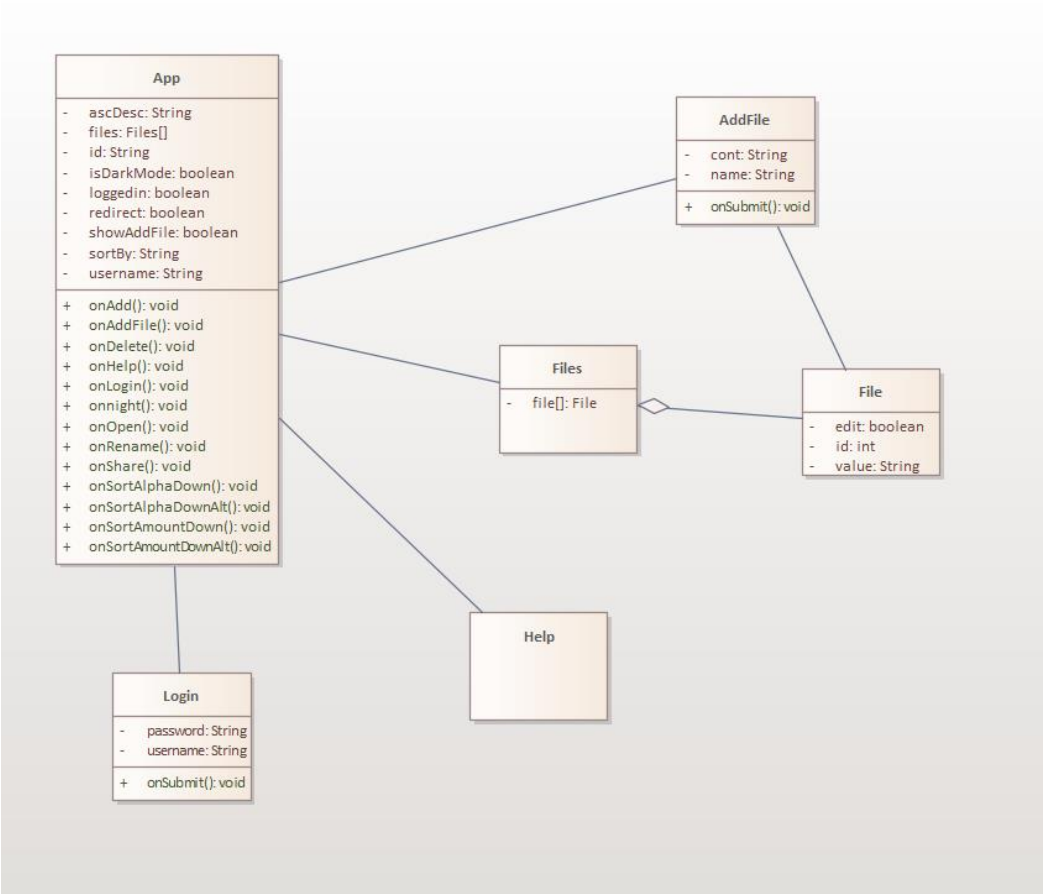
Ogólny widok:



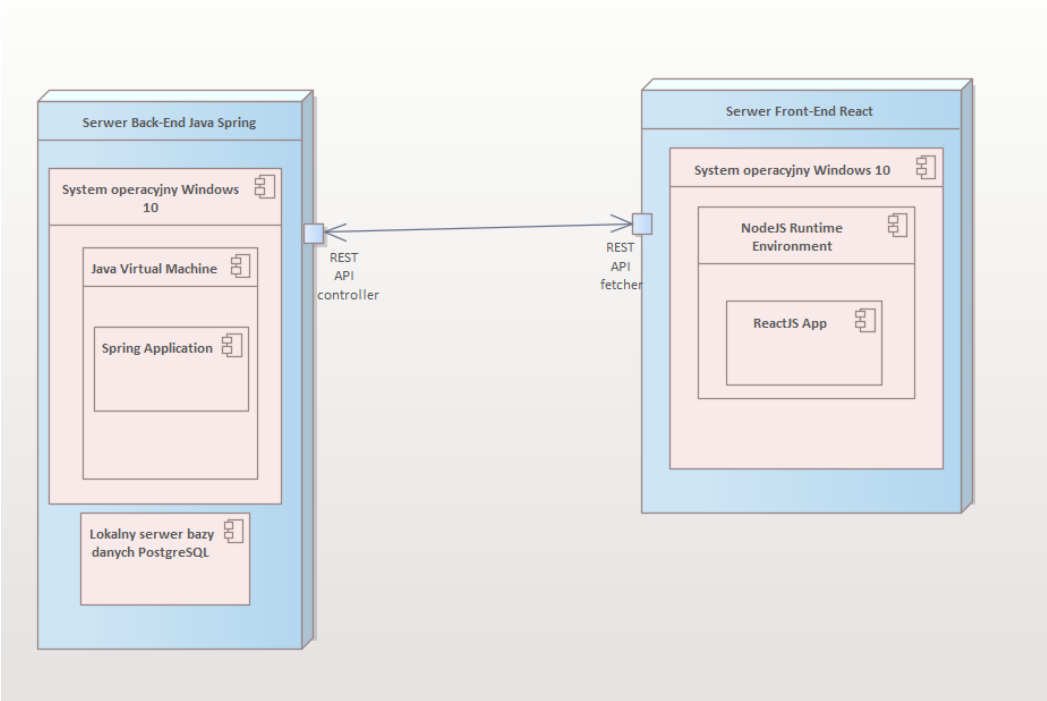
Część aplikacyjna:



Część prezentacyjna:



4.6. Diagram wdrożeniowy



5. Identyfikacja ryzyka

5.1. Ryzyka związane z przedmiotem projektu

Zasoby wrażliwe:

- Serwer
- Hasła
- Dane użytkowników
- Pliki

Zagrożenia:

Nazwa zasobu	Zagrożenie	Ocena poziomu zagrożenia
Serwer	Włamanie	Średnie
Hasła	Wyciek	Wysokie
Dane użytkowników	Wyciek	Wysokie
Pliki	Nieautoryzowany dostęp	Średnie

Redukcja poziomu ryzyka:

Nazwa zasobu	Zabezpieczenie	Ocena poziomu zagrożenia	Ocena poziomu zagrożenia po zabezpieczeniu
Serwer	Brak dostępu do sieci Internet	Średnie	Niskie
Hasła	Szyfrowanie	Wysokie	Niskie
Dane użytkowników	Certyfikacja SSL	Wysokie	Niskie
Pliki	Obowiązkowa autoryzacja	Średnie	Niskie

5.2. Ryzyka projektowe

Legenda:

- P – prawdopodobieństwo wystąpienia ryzyka
- K – konsekwencje wystąpienia ryzyka

Oba te wskaźniki w opracowaniu przyjmują wartości w skali 1 – 5.

1. Brak pełnej znajomości wykorzystywanych narzędzi:

P = 4

K = 5

P * K = 20

Działania zapobiegające ryzyku:

- zapoznanie się ze specjalistyczną literaturą
- wzięcie udziału w szkoleniach on-line
- przepracowanie materiałów dostępnych w Internecie

Czynniki wczesnego wykrycia realizacji ryzyka:

- Przestój w pracach projektowych
- Niezadowolenie członków zespołu
- Wskazywanie na braki wykorzystywanych narzędzi

2. Konieczność rozdzielenia uwagi na wiele innych zadań i projektów:

P = 5

K = 4

P * K = 20

Działania zapobiegające ryzyku:

- Organizacja czasu pracy w ciągu tygodnia, sztywne trzymanie się terminów
- Łączenie, w miarę możliwości, efektów pracy powiązanych zadań
- Ustalenie priorytetów

Czynniki wczesnego wykrycia realizacji ryzyka:

- Przestój w pracach nad projektem
- Brak komunikacji pomiędzy członkami zespołu

3. Opóźnienia w dostarczaniu kolejnych etapów projektu, w tym efektu końcowego

P = 3

K = 5

P * K = 15

Działania zapobiegające ryzyku:

- Trzymanie się terminów realizacji prac
- Zorientowanie zespołu na efekty
- Sprawna komunikacja

Czynniki wczesnego wykrycia realizacji ryzyka:

- Brak dostarczenia efektów pracy w wyznaczonym terminie
- Brak istotnych postępów w pracy
- Brak komunikacji pomiędzy członkami zespołu

4. Zakończenie wsparcia producenta/społeczności wybranych narzędzi projektowych:

P = 2

K = 5

P * K = 10

Działania zapobiegające ryzyku:

- Użycie oprogramowania w najnowszej dostępnej wersji
- Śledzenie komunikatów twórców oprogramowania dotyczących zakończenia wsparcia

Czynniki wczesnego wykrycia realizacji ryzyka:

- Ukazanie się komunikatu o planowanym zakończeniu wsparcia
- Brak aktualizacji narzędzia przez dłuższy czas

5. Awaria fizycznego sprzętu członków zespołu

P = 2

K = 4

P * K = 8

Działania zapobiegające ryzyku:

- Używanie sprawnego sprzętu komputerowego
- Unikanie pracy w miejscach niesprzyjających pracy sprzętu komputerowego

Czynniki wczesnego wykrycia realizacji ryzyka:

- Niestabilna praca sprzętu, np. restarty, blue screen’y
- Zawieszanie się systemu operacyjnego

6. Utrata danych z fizycznego nośnika

P = 2

K = 5

P * K = 10

Działania zapobiegające ryzyku:

- Przechowywanie plików projektowych w zdalnych repozytoriach, np. GitHub
- Unikanie wykorzystywania przenośnych nośników danych

Czynniki wczesnego wykrywania ryzyka:

- Czasowa utrata dostępu do danych
- Komunikaty o błędzie odczytu danych w systemie operacyjnym
- Głośna lub nierówna praca nośnika danych

6. Opis wykorzystanych technologii

Do stworzenia front-endu została wykorzystana biblioteka React bazująca na środowisku uruchomieniowym Node.js. Back-end został wykonany przy pomocy frameworka Spring. System zarządzania relacyjnymi bazami danych zależnie od sposobu dystrybucji PostgreSQL/MySQL.

Front-end zachowuje zasady Single-Page Application wykorzystując mechanizm Routera, dzięki czemu nie trzeba przeładowywać całej strony przy każdej zmianie lokalizacji. Do wykonywania zapytań do serwera wykorzystano komendy fetch oraz axios które działają asynchronicznie. Większość komponentów jest zbudowanych na podstawie indywidualnych parametrów w pliku css.

Back-end wykorzystuje architekturę wielowarstwową z oddzielnymi klasami dla controllerów, serwisów, repozytoriów, data-transfer-objectów itd. Logowanie wykorzystuje mechanizm autoryzacji z wykorzystaniem tokenów JWT. Aplikacja wystawia interfejs REST API który wykorzystuje zapytania CRUD do tworzenia, odczytu, aktualizacji i usuwania danych z bazy.

7. Raport testowy

7.1. Zakres testów

Zakres testów obejmuje przeprowadzenie kontroli działania podstawowych funkcjonalności systemu, oraz jego odporności na błędy.

7.2. Wykonane testy

Testy wykonywane były sekwencyjnie na komputerze z systemem Windows 10. Wszelkie odstępstwa od norm zostały umieszczone w komentarzu do danego przypadku użycia.

7.2.1. Przypadek użycia: Uwierzytelnianie użytkownika

UseCase : Uwierzytelnianie użytkownika

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Użytkownik wchodzi na stronę
2	System uruchamia widok logowania
3	Użytkownik wprowadza dane uwierzytelniające
4	System sprawdza dane uwierzytelniające z bazą danych

Test przeprowadzony zgodnie z sekwencją. Wynik testu zgodny z oczekiwaniami, brak odstępstw od normy. Jedynym odstępstwem jest brak sprawdzania wartości wprowadzanych przez użytkownika.

7.2.2. Przypadek użycia: Autoryzacja

UseCase : Autoryzacja

*Use Case Diagram | Scenarios

Type: Basic Path

Scenario: Basic Path

Step	Action
1	Na podstawie uwierzytelnionego użytkownika sprawdzane są jego prawa dostępu do danych.
2	Użytkownikowi przydzielane są odpowiednie prawa dostępu do danych

System poprawnie przydziela autoryzacje użytkownikowi do zawartości do której ma dostęp.

7.2.3. Przypadek użycia: Wyświetlanie plików

UseCase : Wyświetlenie plików

*Use Case Diagram | Scenarios

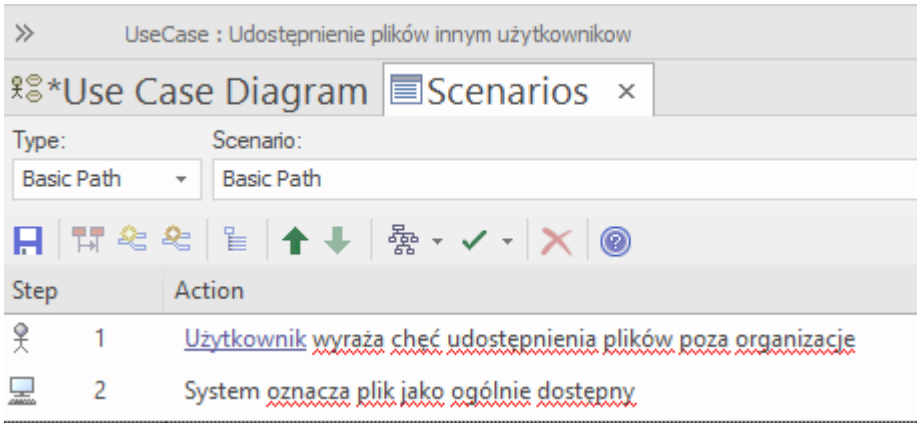
Type: Basic Path

Scenario: Basic Path

Step	Action
1	Użytkownik uruchamia stronę aplikacji
2	System wyświetla pliki do których użytkownik ma dostęp

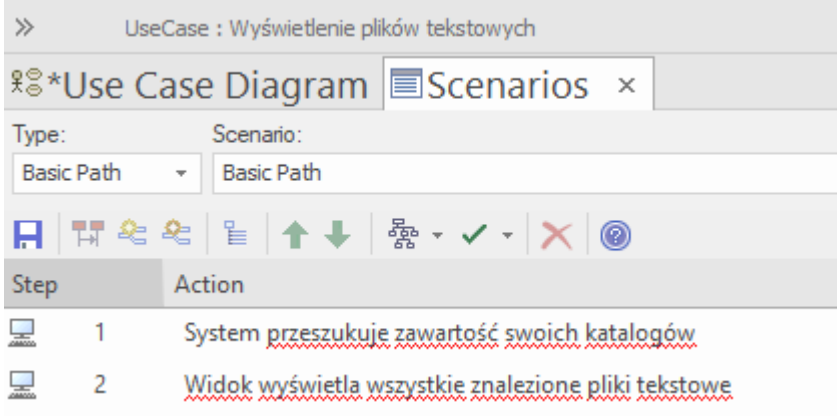
System poprawnie przydziela widok odpowiednich plików dla użytkownika.

7.2.4. Przypadek użycia: Udostępnianie plików innym użytkownikom



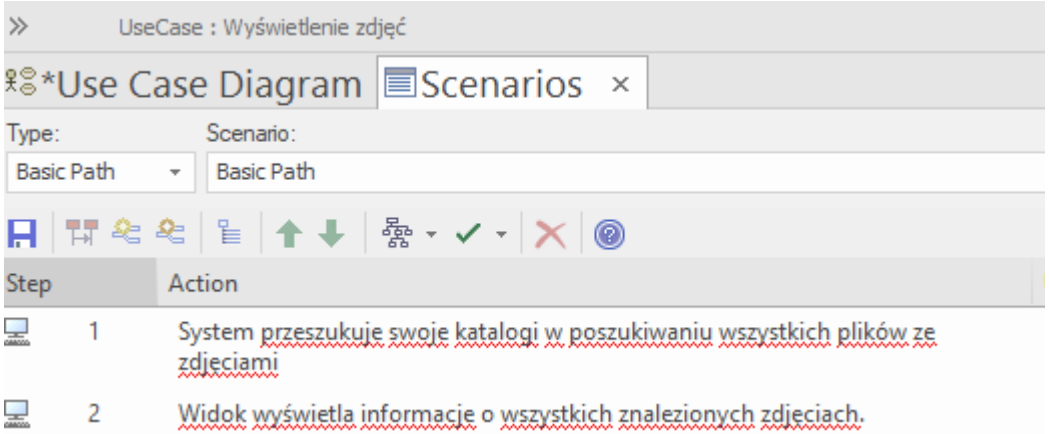
Udostępnianie zostało zrealizowane poprzez wybranie konkretnego użytkownika któremu udostępniany jest plik i ta funkcjonalność wykonuje się poprawnie.

7.2.5. Przypadek użycia: Wyświetlanie plików tekstowych



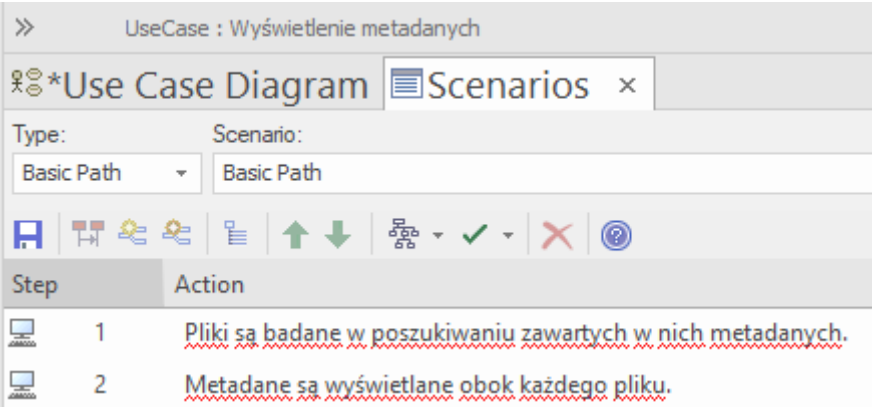
Pliki tekstowe wyświetlają się poprawnie

7.2.6. Przypadek użycia: Wyświetlanie zdjęć



Pliki ze zdjęciami wyświetlają się poprawnie. Jedynym odstępstwem jest brak sprawdzania poprawności rozmiaru zdjęcia.

7.2.7. Przypadek użycia: Wyświetlanie metadanych



Rozmiar plików wyświetla się poprawnie.

7.3. Podsumowanie działań testowych

Testy przeprowadzono z wynikiem pozytywnym. Głównymi obszarami które mogłyby zostać poprawione to sprawdzanie wartości wprowadzanych przez użytkownika.

8. Wdrożenie systemu

Po satysfakcjonującym przebiegu testów, system jest gotowy do wdrożenia. W tym celu podjęto szereg kroków, które w efekcie końcowym przyczyniły się do opublikowania systemu w Internecie, tak, aby był dostępny z dowolnego urządzenia i miejsca na świecie pod warunkiem dostępu do Internetu.

- Pobranie plików źródłowych z repozytorium (backend oraz frontend)
- Kompilacja i wygenerowanie artefaktów
- Uruchomienie serwerów backend oraz frontend na określonych wcześniej portach
- Otwarcie portów z poziomu firewalla
- Konfiguracja wirtualnych serwerów Apache2 wraz z certyfikatami Let's Encrypt oraz mechanizmem reverse proxy
- Rejestracja domeny chmurazwaty.ml
- Ustawienie serwera DNS tak, aby nazwa domenowa była rozwiązywana na adres IP serwera

Po wykonaniu wyżej wskazanych kroków, system jest dostępny z poziomu sieci Internet, pod adresem https://chmurazwaty.ml/.