**AKADEMIA NAUK STOSOWANYCH**

**W NOWYM SĄCZU**

**WYDZIAŁ NAUK INŻYNIERYJNYCH**

**PRACA DYPLOMOWA**

**APLIKACJA WEBOWA PRZECHOWUJĄCA PLIKI Z DOSTĘPEM CHRONIONYM**

Spis treści

[Wstęp 4](#_Toc186834085)

[1. ZAGROŻENIA W CHMURZE 5](#_Toc186834086)

[2. ISTNIEJĄCE ROZWIĄZANIA 7](#_Toc186834087)

[2.1. PODSUMOWANIE ISTNIEJĄCYCH ROZWIĄZAŃ 8](#_Toc186834088)

[3. CEL I ZAKRES PRACY 9](#_Toc186834089)

[4. PROJEKT 10](#_Toc186834090)

[4.1. WYMAGANIA FUNKCJONALNE 10](#_Toc186834091)

[4.2. WYMAGANIA NIEFUNKCJONALNE 12](#_Toc186834092)

[4.3. TECHNOLOGIE 12](#_Toc186834093)

[4.4. DIAGRAMY 16](#_Toc186834094)

[4.4.1. DIAGRAM PRZYPADKÓW UŻYCIA 16](#_Toc186834095)

[4.4.2. DIAGRAM ERD 18](#_Toc186834096)

[4.4.3. DIAGRAMY AKTYWNOŚCI 21](#_Toc186834097)

[4.5. SCENARIUSZE UŻYCIA 25](#_Toc186834098)

[5. IMPLEMENTACJA 31](#_Toc186834099)

[5.1. SYSTEM LOGOWANIA I REJESTRACJI 31](#_Toc186834100)

[5.2. SYSTEM ZARZĄDZANIA PLIKAMI 34](#_Toc186834101)

[5.3. SYSTEM ZNAJOMYCH 38](#_Toc186834102)

[5.4. SYSTEM MAGAZYNÓW 43](#_Toc186834103)

[5.7. SYSTEM POWIADOMIEŃ I WIADOMOŚCI 52](#_Toc186834104)

[6. PODSUMOWANIE 55](#_Toc186834105)

[7. BIBLIOGRAFIA 56](#_Toc186834106)

[SPIS TABEL 59](#_Toc186834107)

[SPIS RYSUNKÓW 60](#_Toc186834108)

[ZAŁĄCZNIKI 61](#_Toc186834109)

# Wstęp

Rozwój technologii oraz powszechna dostępność internetu przyczyniły się do tego,   
że przechowywanie plików w chmurze stało się integralnym elementem współczesnego życia. Systemy chmurowe umożliwiają wygodny dostęp do danych z dowolnego miejsca oraz ich synchronizację pomiędzy różnymi urządzeniami. Popularność tych rozwiązań wynika z ich uniwersalności, elastyczności i możliwości integracji z nowoczesnymi narzędziami oraz procesami. Dzięki chmurze użytkownicy mogą efektywniej organizować swoją pracę, optymalizując jednocześnie wykorzystanie zasobów technologicznych. Chociaż systemy chmurowe oferują liczne zalety, takie jak dostępność, skalowalność czy wysoki poziom bezpieczeństwa, wiążą się również z istotnymi wyzwaniami. Kluczowe kwestie dotyczą ochrony danych i prywatności użytkowników, które stają się coraz bardziej palącym problemem w obliczu rosnącego zagrożenia cyberatakami. Przykłady takich zagrożeń obejmują ataki ransomware, przejęcia danych uwierzytelniających oraz wycieki informacji wynikające   
z błędów konfiguracji systemów. Te wyzwania podkreślają znaczenie zaawansowanych mechanizmów ochrony, takich jak szyfrowanie danych, kontrola dostępu czy wielopoziomowe uwierzytelnianie. Wraz z upowszechnieniem przechowywania danych w chmurze, zarówno przez użytkowników indywidualnych, jak i przedsiębiorstwa, wzrosły potrzeby w zakresie bezpiecznych i funkcjonalnych rozwiązań umożliwiających zarządzanie plikami. Projektowanie aplikacji spełniających te wymagania stanowi kluczowe wyzwanie współczesnej inżynierii oprogramowania. Celem takich narzędzi jest zapewnienie intuicyjnej obsługi przy jednoczesnym zachowaniu wysokich standardów ochrony informacji. Niniejsza praca koncentruje się na problematyce tworzenia aplikacji internetowej, która odpowiada   
na te potrzeby, oferując użytkownikom większe bezpieczeństwo i prywatność   
w przechowywaniu oraz udostępnianiu danych. (Scroll - Chmura internetowa 2021) (AppsOnHMS 2022) (TeleTropiciel 2022)

# 1. ZAGROŻENIA W CHMURZE

Przechowywanie danych w chmurze to jedna z kluczowych funkcji technologii chmurowych, oferująca użytkownikom możliwość przechowywania i udostępniania danych   
za pośrednictwem platform internetowych. Systemy te charakteryzują się elastycznością, wysoką dostępnością oraz niskimi kosztami użytkowania, dzięki czemu są powszechnie wykorzystywane zarówno przez użytkowników indywidualnych, jak i przedsiębiorstwa różnej wielkości. W zależności od potrzeb, przechowywanie danych w chmurze może przyjmować różne formy, w tym chmurę publiczną, prywatną, hybrydową, osobistą i społecznościową.   
Pod względem technologicznym, systemy przechowywania danych w chmurze opierają się   
na trzech głównych modelach: pamięci blokowej, plikowej oraz obiektowej. Pamięć blokowa, stosowana głównie w środowiskach wymagających wysokiej wydajności, umożliwia szybki dostęp do danych w bazach danych i aplikacjach transakcyjnych. Pamięć plikowa, zintegrowana z technologią NAS, oferuje elastyczne zarządzanie danymi w strukturze plików, co sprawia, że jest intuicyjna dla użytkowników końcowych. Pamięć obiektowa, zoptymalizowana pod kątem przechowywania dużych zbiorów niestrukturalnych danych, takich jak multimedia, wyróżnia się wysoką skalowalnością i efektywnością w obsłudze różnorodnych zastosowań. Rozwój technologii przechowywania w chmurze pozwala   
na przezwyciężenie ograniczeń tradycyjnych metod, takich jak wysokie koszty konserwacji sprzętu czy brak elastyczności w zarządzaniu zasobami. Dzięki swojej wszechstronności   
i efektywności, systemy te stają się integralnym elementem współczesnych rozwiązań technologicznych, wspierając zarówno użytkowników indywidualnych, jak i organizacje   
w zarządzaniu danymi na coraz większą skalę. (Yang, Xiong, Ren 2020) (Odun-Ayo 2017)

Zagrożenia związane z przechowywaniem danych w chmurze obejmują zarówno aspekty technologiczne, jak i organizacyjne. Jednym z kluczowych problemów jest podatność   
na cyberataki, w tym kradzież danych czy ataki typu ransomware. Chociaż wiele firm stosuje zaawansowane technologie szyfrowania danych, nie eliminuje to ryzyka złamania zabezpieczeń przez atakujących wykorzystujących np. ataki brute-force lub phishing w celu zdobycia danych logowania. Kolejnym zagrożeniem jest brak pełnej kontroli   
nad przechowywanymi danymi. Współpracując z zewnętrznymi dostawcami chmury, użytkownicy muszą polegać na ich procedurach bezpieczeństwa, które nie zawsze spełniają najwyższe standardy. Ponadto dane mogą być przechowywane w różnych jurysdykcjach,   
co rodzi ryzyko związane z przepisami prawnymi i dostępem organów państwowych   
do informacji. Niezawodność połączenia internetowego stanowi dodatkowy problem.   
W sytuacji awarii infrastruktury sieciowej użytkownicy mogą utracić dostęp do swoich danych. Brak odpowiednich mechanizmów tworzenia kopii zapasowych przez niektórych dostawców zwiększa ryzyko ich nieodwracalnej utraty. Kwestia prywatności pozostaje jednym   
z największych wyzwań. Wiele platform gromadzi metadane użytkowników, które mogą   
być wykorzystywane do analizy lub sprzedaży stronom trzecim. Taka praktyka rodzi obawy   
o nadmierne gromadzenie informacji i potencjalne naruszenia prywatności. Rozwiązania minimalizujące te zagrożenia obejmują włączenie uwierzytelniania dwuskładnikowego, szyfrowanie danych przed ich przesłaniem do chmury, regularne monitorowanie bezpieczeństwa kont oraz wybór dostawców oferujących jasne polityki prywatności   
i bezpieczeństwa. Ważne jest również systematyczne edukowanie użytkowników na temat cyberbezpieczeństwa, aby unikali ryzykownych zachowań, takich jak otwieranie podejrzanych wiadomości e-mail czy korzystanie z niezabezpieczonych sieci publicznych. (Steinberg 2023) (Schneier 2017) (Huang i in, 2014) (360money 2024)(Bitdefender 2025)

# 2. ISTNIEJĄCE ROZWIĄZANIA

Obecnie dostępnych jest wiele usług umożliwiających przechowywanie plików   
w chmurze. Ze względu na swoją dostępność, funkcjonalność i wygodę, platformy te są szeroko wykorzystywane zarówno w codziennym życiu, jak i w środowisku zawodowym. Mimo licznych zalet, usługi te napotykają na istotne ograniczenia oraz wyzwania, które mogą wpływać na poziom zaufania użytkowników do tych rozwiązań.

**Dysk Google** – usługa stworzona przez Google, umożliwiająca przechowywanie, synchronizację i udostępnianie plików. Uruchomiona 24 kwietnia 2012 roku, pozwala użytkownikom przechowywać pliki na serwerach Google, synchronizować je na różnych urządzeniach oraz udostępniać innym. Dysk Google obejmuje pakiet biurowy (Dokumenty, Arkusze i Prezentacje Google), który umożliwia wspólną edycję dokumentów, arkuszy kalkulacyjnych, prezentacji, rysunków, formularzy i innych plików. Wszystkie pliki utworzone w pakiecie biurowym są automatycznie zapisywane na Dysku Google. (Wikipedia – Dysk Google 2024) ( Scroll - Dysk Google 2021)

**Dropbox** - usługa oferowana przez firmę Dropbox, Inc., umożliwiająca przechowywanie danych na zdalnych serwerach. Dostęp do plików jest możliwy za pośrednictwem przeglądarki internetowej lub dedykowanej aplikacji instalowanej na komputerze. W wersji darmowej użytkownik otrzymuje 2 GB przestrzeni dyskowej, z opcją zwiększenia jej za dodatkową opłatą. Istnieje również możliwość bezpłatnego powiększenia dostępnej przestrzeni poprzez skorzystanie z ofert promocyjnych, takich jak zapraszanie nowych użytkowników   
(do maksymalnie 16 GB) czy instalacja oficjalnej aplikacji. (Wikipedia - Dropbox 2024) (CodziennyEkspert 2023)

**Microsoft One Drive** - OneDrive oferuje użytkownikom 5 GB darmowej przestrzeni dyskowej z możliwością rozszerzenia pojemności do 100 GB. Subskrybenci usługi Microsoft 365 mają dodatkowo dostęp do 1 TB miejsca na swoje pliki. Pojedyncze pliki mogą mieć rozmiar do 100 GB. Usługa jest oficjalnie kompatybilna z przeglądarkami Internet Explorer oraz Mozilla Firefox, choć możliwe jest korzystanie z niej także w innych przeglądarkach. Warto jednak zauważyć, że funkcja przeciągania plików wymaga instalacji kontrolki ActiveX, co ogranicza jej działanie do Internet Explorera 6+ oraz Mozilla Firefox 1.5+.  
(Wikipedia - OneDrive 2024) (Komputer Świat 2022)

## 2.1. PODSUMOWANIE ISTNIEJĄCYCH ROZWIĄZAŃ

Usługi takie jak Google Drive i OneDrive charakteryzują się konkurencyjną ceną, co czyni je popularnym wyborem wśród użytkowników. Niemniej jednak ich wykorzystanie wiąże   
się z pewnymi kompromisami, które mogą budzić wątpliwości. Niskie koszty często oznaczają ograniczoną kontrolę użytkownika nad przechowywanymi danymi oraz utratę prywatności. Firmy takie jak Google i Microsoft mają dostęp do plików użytkowników oraz rutynowo   
je analizują w celu wykrywania potencjalnych zagrożeń. Działania te, choć uzasadniane troską o bezpieczeństwo, wzbudzają obawy o naruszanie prywatności. Stabilność działania tych usług również pozostawia czasem wiele do życzenia. Zgłaszano przypadki znikania plików, nawet   
w przypadku użytkowników korzystających z kont premium, co negatywnie wpływa   
na zaufanie do tych platform. Brak gwarancji bezpieczeństwa i dostępności danych jest istotnym mankamentem. Dropbox Inc. stosuje inną strategię, która również może być przedmiotem krytyki. Darmowy plan tej usługi oferuje jedynie 2 GB przestrzeni dyskowej,   
co w porównaniu z konkurencyjnymi rozwiązaniami jest niewielką wartością. Dodatkowo, liczba urządzeń, które mogą korzystać z jednego konta, jest ograniczona do dwóch,   
co zmniejsza funkcjonalność. Plany płatne są stosunkowo drogie, zaczynając od około   
900zł rocznie za 2 TB przestrzeni. Brak elastycznych opcji pośrednich między darmowym planem a kosztownymi subskrypcjami premium ogranicza dostępność tej usługi dla szerokiego grona użytkowników. Dodatkowo, Dropbox został skrytykowany za brak przejrzystości   
w zakresie polityki prywatności. Firma dzieli się danymi telemetrycznymi z partnerami biznesowymi, co rodzi pytania o ochronę danych użytkowników. Ponadto zgłaszano przypadki ponownego pojawiania się plików, które miały być trwale usunięte z serwerów, co może   
być postrzegane jako naruszenie zaufania użytkowników. Rosnące zapotrzebowanie   
na alternatywne rozwiązania, które łączą konkurencyjną cenę, funkcjonalność i bezpieczeństwo danych, wskazuje na potrzebę poszukiwania bardziej zrównoważonych modeli usług chmurowych. (Fotc 2022) (Futurebeat 2023) (Youtube - Mateusz Chrobok 2024)

# 3. CEL I ZAKRES PRACY

Temat pracy dyplomowej skupia się on na zaprojektowaniu oraz implementacji internetowej aplikacji do przechowywania danych, która w odpowie na współczesne potrzeby użytkowników w zakresie bezpieczeństwa, prywatności i zarządzania plikami w środowisku online. Głównym celem aplikacji jest stworzenie narzędzia, które nie tylko zapewni użytkownikom możliwość przechowywania plików, i jednocześnie ułatwi współpracę   
i interakcję z innymi użytkownikami. Projektowana aplikacja powinna być przystosowana   
do funkcjonowania jako prywatny magazyn internetowy, który stawia na ochronę prywatności użytkownika. System będzie w pełni szyfrować dane, eliminując ryzyko nieautoryzowanego dostępu. Wykorzystanie algorytmów szyfrowania zapewni bezpieczeństwo przechowywanych informacji, dając użytkownikom pewność, że ich dane są chronione przed zagrożeniami zewnętrznymi. Kolejnym kluczowym aspektem aplikacji jest wsparcie współpracy między użytkownikami. Aplikacja powinna umożliwiać tworzenie dedykowanych przestrzeni współdzielonych, nazywanych magazynami, w których użytkownicy będą mogli gromadzić, organizować i wspólnie edytować pliki. System kontroli wersji plików pozwoli na jednoczesną pracę kilku osób nad jednym dokumentem, a w razie wystąpienia konfliktów umożliwi   
ich rozwiązanie poprzez porównanie różnic między wersjami i wybór najbardziej odpowiedniej. Projektowana aplikacja powinna również odpowiadać na potrzeby związane   
z zarządzaniem plikami w sposób przyjazny użytkownikowi. Użytkownicy powinni mieć możliwość łatwego przesyłania, pobierania, zmieniania nazw oraz usuwania plików. Szczególny nacisk należy położyć na przejrzysty interfejs, który pozwoli na intuicyjne korzystanie z dostępnych funkcji, takich jak zarządzanie znajomymi, wysyłanie wiadomości oraz przeglądanie udostępnionych zasobów. Ważnym celem aplikacji jest również zapewnienie użytkownikom możliwości edycji wybranych typów plików bez konieczności ich pobierania. Dzięki integracji z odpowiednimi narzędziami użytkownicy będą mogli edytować pliki tekstowe i dokumenty Worda bezpośrednio w przeglądarce, co zwiększy wygodę i efektywność korzystania z systemu. Podsumowując, celem projektu jest stworzenie aplikacji, która stanie się alternatywą dla istniejących rozwiązań, takich jak Google Drive czy Dropbox, oferując przy tym większe bezpieczeństwo i prywatność. Projektowana aplikacja ma na celu zbudowanie zaufania użytkowników poprzez wdrożenie zaawansowanych funkcji zarządzania plikami, wysokiego poziomu ochrony danych oraz łatwego udostępniania i współpracy w ramach środowiska cyfrowego.

# 4. PROJEKT

## 4.1. WYMAGANIA FUNKCJONALNE

**System rejestracji** - Aplikacja powinna umożliwiać rejestrację użytkowników, którzy podają adres e-mail, hasło oraz imię i nazwisko. Hasła należy bezpiecznie przechowywać, stosując haszowanie. Logowanie powinno odbywać się przy użyciu e-maila i hasła,   
a dla dodatkowego bezpieczeństwa warto dodać dwuetapowe uwierzytelnianie (2FA), które wykorzysta aplikacje typu Google Authentyicator. Autoryzacja użytkowników powinna   
być oparta na tokenach JWT (JSON Web Token), które przechowują zaszyfrowane dane użytkownika, takie jak identyfikator. Po zalogowaniu generowany jest unikalny token, który można przechowywać w przeglądarce (np. w plikach cookies) i używać do autoryzacji żądań do serwera.

**Zarządzanie plikami –** System zarządzania plikami powinien umożliwiać użytkownikom przesyłanie plików, które będą przechowywane w indywidualnym obszarze. Podczas przesyłania należy zapisywać metadane, takie jak nazwa pliku, data, typ i identyfikator właściciela, w bazie danych, co ułatwi zarządzanie i wyszukiwanie zasobów. Każdy użytkownik powinien mieć dostęp do widoku z listą swoich plików, z możliwością przeglądania szczegółów oraz wykonywania operacji, takich jak pobieranie, zmiana nazwy, usuwanie lub udostępnianie. Zmiana nazwy powinna być odnotowywana w bazie danych   
i systemie plików, aby zachować spójność danych. Usuwanie plików powinno działać poprzez zmianę ich statusu w bazie danych na „soft delete”. Udostępnianie plików powinno umożliwiać wybór odbiorców z listy znajomych oraz określenie poziomu dostępu (np. odczyt, edycja). Udostępnione pliki powinny być widoczne w dedykowanej sekcji aplikacji zarówno   
dla właściciela, jak i odbiorców.

**Szyfrowanie danych** - Projektowany system powinien zapewniać pełne bezpieczeństwo   
i prywatność danych użytkowników, dlatego kluczowym elementem funkcjonalności aplikacji musi być implementacja szyfrowania danych. Wszystkie pliki przechowywane   
w aplikacji powinny być szyfrowane na serwerze. Proces ten ma na celu ochronę zawartości plików przed nieautoryzowanym dostępem, nawet w przypadku naruszenia bezpieczeństwa serwera. Szyfrowanie powinno być realizowane za pomocą nowoczesnych i uznanych algorytmów kryptograficznych, takich jak AES (Advanced Encryption Standard). AES,   
ze względu na swoją wyższą wydajność i odporność na ataki, powinien być preferowanym algorytmem. System powinien umożliwiać szyfrowanie plików za pomocą kluczy kryptograficznych generowanych indywidualnie dla każdego użytkownika lub magazynu plików.

**Edycja plików Word i TXT** - Aplikacja powinna wspierać przeglądanie i edycję plików tekstowych, takich jak .txt oraz dokumentów .docx (Word). Dzięki integracji   
z odpowiednimi narzędziami do konwersji i edycji plików użytkownicy mogliby modyfikować dokumenty bez konieczności pobierania ich na urządzenie lokalne, a zmiany mogłyby być zapisywane bezpośrednio w systemie.

**System znajomych -** System znajomych w aplikacji powinien oferować użytkownikom łatwe narzędzia do zarządzania relacjami i komunikacji. Użytkownicy powinni móc wyszukiwać innych za pomocą wyszukiwarki (np. po adresie e-mail) i wysyłać zaproszenia   
do znajomych. Akceptacja dodaje osobę do listy znajomych widocznej w aplikacji. Lista znajomych powinna umożliwiać przeglądanie podstawowych informacji, takich jak imię   
i nazwisko, oraz szybkie usuwanie znajomych. System powinien wspierać udostępnianie plików i zasobów – właściciel wybiera osobę z listy znajomych, a udostępnione zasoby   
są widoczne w dedykowanej sekcji. Aplikacja powinna mieć wbudowany system wiadomości do prywatnej komunikacji między znajomymi oraz zapewniać powiadomienia o nowych zaproszeniach i wiadomościach.

**System magazynów** – System magazynów w aplikacji powinien umożliwiać zarządzanie plikami w dedykowanych zbiorach, które można współdzielić z innymi użytkownikami. Użytkownicy powinni mieć możliwość tworzenia magazynów z nazwami ułatwiającymi identyfikację i organizację plików. Aplikacja powinna wspierać udostępnianie magazynów innym użytkownikom, pozwalając właścicielowi na zarządzanie dostępem, w tym dodawanie   
i usuwanie osób. Kluczową funkcją powinna być kontrola wersji plików, która wspiera współpracę wielu osób nad jednym plikiem. System powinien automatycznie wykrywać konflikty wersji i umożliwiać ich rozwiązanie przez porównanie różnic i wybór odpowiedniej wersji.

## 4.2. WYMAGANIA NIEFUNKCJONALNE

**Interfejs** **-** Aplikacja powinna być zaprojektowana w taki sposób, aby interfejs użytkownika był prosty, przejrzysty i intuicyjny, umożliwiając użytkownikom szybki dostęp do wszystkich kluczowych funkcji w maksymalnie pięciu kliknięciach. Oznacza   
to, że użytkownik, korzystając z aplikacji, nie powinien być zmuszony do wykonywania zbędnych czynności lub przechodzenia przez skomplikowane struktury menu, aby osiągnąć zamierzony cel. Interfejs powinien być responsywny, dostosowany do różnych rozdzielczości ekranów. Dzięki temu użytkownicy będą mogli łatwo korzystać z aplikacji niezależnie   
od miejsca i urządzenia, z którego korzystają. Kluczowe funkcje, takie jak przesyłanie plików, zarządzanie magazynami, udostępnianie zasobów czy komunikacja ze znajomymi, powinny być widoczne i dostępne z poziomu głównego ekranu lub intuicyjnych ikon nawigacyjnych.

**Dostępność** - System powinien być zaprojektowany w sposób zapewniający pełną kompatybilność z wszystkimi popularnymi przeglądarkami internetowymi, takimi jak Google Chrome, Mozilla Firefox, Microsoft Edge oraz Safari, w ich najnowszych stabilnych wersjach. Zapewnienie zgodności z szeroką gamą przeglądarek jest kluczowe, aby użytkownicy mieli dostęp do aplikacji niezależnie od preferowanego środowiska pracy. Dzięki temu aplikacja może dotrzeć do szerszego grona odbiorców i zagwarantować spójne doświadczenie użytkownika bez względu na wybór przeglądarki. Tokeny autoryzacyjne JWT powinny być ważne maksymalnie przez 60 minut od ostatniego żądania użytkownika.

**Spójność** - W projektowanej aplikacji proces usuwania plików przez użytkowników powinien opierać się na mechanizmie „soft delete”. Zamiast natychmiastowego, fizycznego usuwania plików z bazy danych lub systemu plików, system powinien jedynie zmieniać status danego pliku w bazie danych. Dzięki temu aplikacja zapewni dodatkowy poziom bezpieczeństwa oraz pozwoli użytkownikom na ewentualne przywrócenie plików   
w przyszłości, minimalizując ryzyko przypadkowej utraty danych.

## 4.3. TECHNOLOGIE

**JavaScript** - to język programowania wysokiego poziomu używany głównie w tworzeniu dynamicznych stron internetowych. Początkowo zaprojektowany jako język skryptowy   
do przeglądarek, dziś jest jednym z najpopularniejszych języków wykorzystywanych nie tylko po stronie klienta, ale również po stronie serwera (dzięki Node.js). JavaScript pozwala   
na tworzenie interaktywnych aplikacji internetowych, manipulowanie strukturą HTML i CSS w czasie rzeczywistym oraz integrację z backendem aplikacji. Język wspiera różne paradygmaty programowania, w tym programowanie obiektowe i funkcjonalne.   
(Wikipedia - JavaScript 2024) (Justgeekit - node.js 2021)

**Node.js -** to środowisko uruchomieniowe JavaScript, które umożliwia wykonywanie kodu JavaScript po stronie serwera. Dzięki Node.js programiści mogą tworzyć aplikacje serwerowe w JavaScript, co pozwala na pełne wykorzystanie tego języka zarówno   
po stronie klienta, jak i serwera. Node.js jest oparty na silniku V8 Google, co sprawia,   
że jest bardzo wydajny. Obsługuje asynchroniczne operacje wejścia/wyjścia, co czyni   
go idealnym do obsługi dużych obciążeń i jednoczesnych żądań. Node.js wspiera moduły,   
co pozwala na łatwe zarządzanie i organizowanie kodu. (Justgeekit - node.js 2021)   
(Wikipedia - node.js 2024)

**Express.js -** to minimalistyczny framework dla Node.js, który umożliwia tworzenie aplikacji sieciowych i API w szybki i przejrzysty sposób. Zapewnia elastyczność i prostotę, umożliwiając programistom łatwe tworzenie aplikacji sieciowych dzięki gotowym funkcjom, takim jak routowanie, obsługa żądań HTTP i middleware. Express pozwala   
na rozwój zarówno prostych aplikacji, jak i złożonych aplikacji typu SPA i mikroserwisów, dzięki czemu jest popularny wśród programistów Node.js. (Aviary 2023)   
( Wikipedia - express.js 2024)

**JWT (JSON Web Token) -** to otwarty standard (RFC 7519) używany do bezpiecznego przekazywania informacji między stronami jako obiekt JSON. JWT jest szeroko stosowany   
do uwierzytelniania w aplikacjach internetowych, gdzie po pomyślnym zalogowaniu użytkownik otrzymuje token, który jest następnie wysyłany w każdym kolejnym żądaniu jako dowód autentyczności. Tokeny są bezpieczne, ponieważ są podpisane kryptograficznie, dzięki czemu nie można ich łatwo podrobić, co sprawia, że są one często wykorzystywane   
do tworzenia bezpiecznych sesji w aplikacjach sieciowych. (Wikipedia - JWT 2024) (devszczepaniak 2023)

**MySQL** - to dobrze znany system zarządzania relacyjnymi bazami danych (RDBMS), który wykorzystuje Structured Query Language (SQL) do manipulowania danymi. Został zaprojektowany przez szwedzką firmę MySQL AB w 1995 roku, a jego rozwój jest obecnie kontynuowany przez Oracle Corporation, która przejęła firmę w 2010 roku. MySQL jest znany ze swojej wydajności, niezawodności i łatwości użytkowania. MySQL jest dostępny na licencji GNU General Public License, co oznacza, że użytkownicy mogą go swobodnie pobierać, używać i modyfikować bez ponoszenia kosztów licencyjnych. Dostępna jest również komercyjna edycja MySQL, która zapewnia dodatkowe funkcje i wsparcie, idealne dla firm poszukujących zaawansowanych rozwiązań i bezpieczeństwa operacyjnego. System obsługuje różne typy tabel, które wykorzystują różne silniki pamięci masowej, takie jak InnoDB, który zapewnia obsługę transakcji, oraz MyISAM, znany z wydajnego indeksowania danych. MySQL oferuje również funkcje replikacji, które są kluczowe dla ciągłości biznesowej   
i skalowalności systemu, a także partycjonowanie tabel, które ułatwia zarządzanie dużymi zbiorami danych. (Wikipedia - mysql 2024)( Oracle 2024)

**Algorytm AES -** (Advanced Encryption Standard) to zaawansowany standard szyfrowania symetrycznego, opracowany w 1998 roku przez belgijskich kryptografów Joan Daemen   
i Vincent Rijmen, znany również jako algorytm "Rijndael". Został zaakceptowany przez amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) w 2001 roku jako standard szyfrowania i obecnie jest używany na całym świecie do ochrony danych. AES działa   
na zasadzie kluczy symetrycznych, co oznacza, że ten sam klucz służy zarówno do szyfrowania, jak i deszyfrowania danych. Algorytm operuje na blokach danych o długości 128 bitów   
i obsługuje klucze o długości 128, 192 lub 256 bitów. Struktura algorytmu opiera się na wielu rundach, w których wykonywane są operacje takie jak zamiana bajtów według tablicy S-box, przesuwanie wierszy w macierzy danych, mieszanie kolumn macierzy oraz dodawanie klucza rundy za pomocą operacji XOR. Dzięki swojej odporności na ataki kryptograficzne AES zapewnia wysoki poziom bezpieczeństwa, co czyni go jednym z najczęściej stosowanych algorytmów szyfrowania w aplikacjach internetowych, bankowości i przechowywaniu danych. (Wikipedia - AES 2024) (Webporadnik 2025)

**Google Authentyicator-** to aplikacja mobilna służąca do generowania jednorazowych kodów, które są używane w celu uwierzytelniania dwuskładnikowego (2FA, Two-Factor Authentication). Ta metoda uwierzytelniania zwiększa bezpieczeństwo, wymagając   
od użytkownika nie tylko podania hasła, ale także wprowadzenia jednorazowego kodu generowanego przez aplikację. Google Authenticator opiera swoje działanie na protokole TOTP (Time-Based One-Time Password) lub HOTP (HMAC-Based One-Time Password), które wykorzystują klucz tajny oraz aktualny czas systemowy do generowania kodów. Klucz tajny jest wprowadzany przez użytkownika poprzez skanowanie kodu QR lub ręczne wpisanie ciągu znaków w aplikacji. Na podstawie tego klucza i aktualnego czasu aplikacja generuje unikalne kody, które są ważne przez krótki czas, najczęściej około 30 sekund. Google Authenticator jest szeroko stosowany w różnych serwisach, takich jak Google, GitHub   
czy Dropbox, zapewniając skuteczny i prosty sposób ochrony kont użytkowników przed nieautoryzowanym dostępem. Dzięki swojej prostocie i efektywności aplikacja stała się jednym z najpopularniejszych rozwiązań wspierających bezpieczeństwo w sieci. (Wikipedia - Google Authentyicator 2024) (Nano.komputronik 2023)

**MySQL Workbench -** to narzędzie graficzne do zarządzania bazami danych MySQL. Zapewnia użytkownikom interfejs do tworzenia, edytowania, zarządzania i przeglądania struktury baz danych, a także pozwala na pisanie i wykonywanie zapytań SQL. Workbench jest narzędziem wszechstronnym, umożliwiającym tworzenie kopii zapasowych, importowanie danych i administrowanie serwerem. Jest szczególnie przydatny dla programistów   
i administratorów baz danych, którzy mogą w prosty sposób wizualizować struktury baz danych oraz optymalizować ich wydajność. (Wikipedia - MySQL Workbench 2024)   
(Boringowl 2024)

**Git -** to rozproszony system kontroli wersji zaprojektowany w celu umożliwienia programistom efektywnego zarządzania zmianami w kodzie źródłowym podczas pracy   
nad projektami. Stworzony przez Linusa Torvaldsa w 2005 roku, Git pozwala   
na przechowywanie historii zmian lokalnie, umożliwiając szybką pracę nad kodem nawet   
w trybie offline. Jego główną cechą jest to, że każdy, kto pobierze kopię repozytorium, otrzymuje pełną historię zmian, co oznacza, że każde repozytorium może służyć jako pełna kopia zapasowa. Git jest niezwykle elastyczny w zarządzaniu wieloma gałęziami kodu, umożliwiając eksperymentowanie, rozwój funkcji i naprawianie błędów niezależnie   
od głównej linii kodu. (Wikipedia - Git 202)

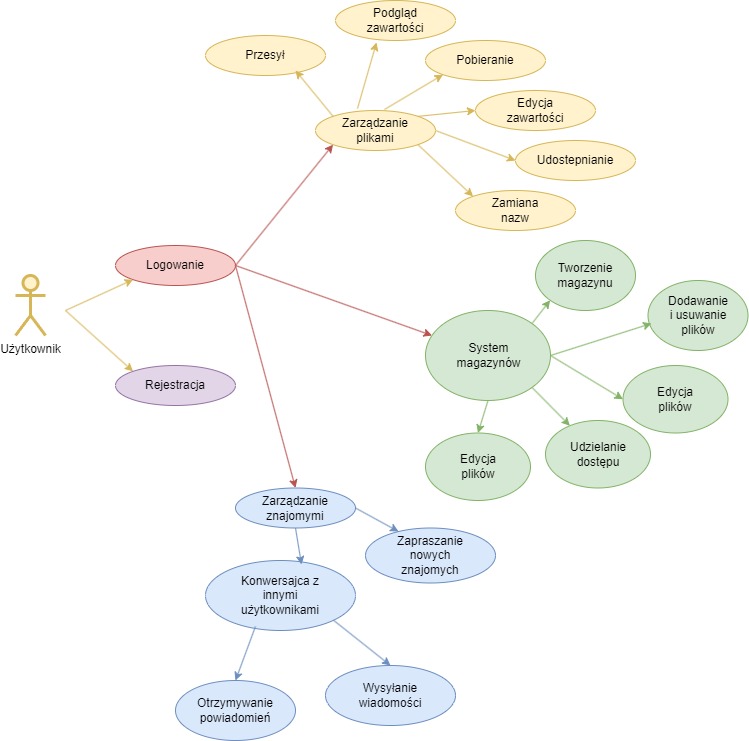
**GitHub -** to internetowa platforma hostingowa wykorzystująca Git do zarządzania projektami oprogramowania. Uruchomiony w 2008 roku przez Toma Prestona-Wernera, Chrisa Wanstratha i PJ Hyetta, GitHub pozwala programistom i firmom przechowywać, zarządzać   
i kontrolować ich projekty kodu źródłowego. Jest to również społeczność,   
w ramach której deweloperzy mogą współpracować nad projektami, udostępniając kod, pracując nad poprawkami i opracowując nowe funkcje. GitHub oferuje różne funkcje, takie   
jak śledzenie zgłoszeń, pull requesty, zarządzanie projektami i wiki dla każdego repozytorium. (Wikipedia - Git 2024) (git-scm 2024)

**Draw.io -** to narzędzie do tworzenia diagramów online, które oferuje szeroki zakres możliwości wizualizacji danych i procesów. Jest to aplikacja internetowa, która umożliwia użytkownikom łatwe tworzenie diagramów, takich jak diagramy przepływu pracy,   
schematy blokowe, organigramy, diagramy sieciowe, mapy myśli i wiele innych.   
(Wikipedia - diagrams.net 2024)

## 4.4. DIAGRAMY

### 4.4.1. DIAGRAM PRZYPADKÓW UŻYCIA

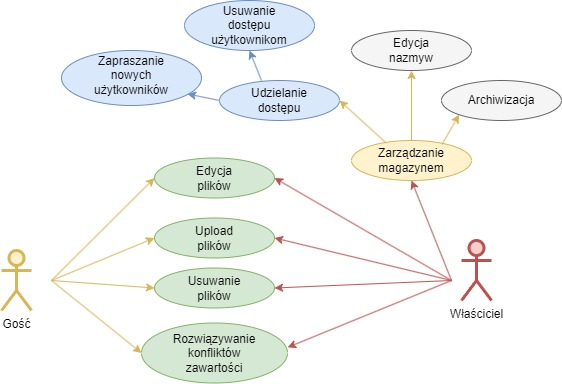
Rysunek 1 przedstawia kluczowe funkcjonalności, które powinna oferować projektowana aplikacja webowa, oraz relacje pomiędzy użytkownikiem a poszczególnymi modułami systemu. Centralnym elementem tego diagramu jest logowanie, które będzie stanowić punkt wyjścia do korzystania z pozostałych funkcji aplikacji. Proces ten powinien zapewnić użytkownikowi bezpieczny dostęp do systemu po wcześniejszej rejestracji, podczas której użytkownik będzie miał możliwość utworzenia konta. Rejestracja będzie niezbędnym krokiem, aby zidentyfikować użytkownika i przypisać mu dostęp do zasobów aplikacji. Po zalogowaniu użytkownik powinien zyskać dostęp do modułu zarządzania plikami, który będzie podstawowym obszarem funkcjonalnym aplikacji. W ramach tego modułu użytkownik będzie mógł przesyłać pliki do systemu, pobierać je na swoje urządzenie oraz przeglądać   
ich zawartość. Aplikacja powinna również umożliwić edytowanie plików tekstowych, zmianę ich nazw oraz udostępnianie plików innym użytkownikom. Kolejnym modułem będzie system magazynów, który umożliwi organizację plików. System magazynów powinien oferować funkcje dodawania oraz usuwania plików, a także edycji ich zawartości. Ważnym elementem tej funkcjonalności będzie zarządzanie dostępem do magazynów. Właściciel magazynu będzie mógł udzielać dostępu innym użytkownikom. Ważną częścią projektowanego systemu będzie również moduł zarządzania znajomymi, który będzie wspierał nawiązywanie relacji między użytkownikami aplikacji. Użytkownicy powinni mieć możliwość wyszukiwania innych osób w systemie, zapraszania ich do listy znajomych oraz zarządzania swoimi kontaktami. System powinien pozwalać na prowadzenie konwersacji z innymi użytkownikami, co będzie istotnym elementem komunikacji w kontekście współdzielenia plików i magazynów. Funkcjonalność   
ta ułatwi nawiązywanie współpracy i usprawni komunikację pomiędzy użytkownikami systemu.



Rysunek 1. Diagram przypadków użycia – użytkownik

[źródło: Opracowanie własne]

Rysunek 2 przedstawia funkcjonalności związane z systemem magazynów oraz role użytkowników, którzy mogą z niego korzystać. W systemie wyróżniono dwie główne   
role: Właściciela magazynu oraz Gościa, z których każda posiada określone uprawnienia   
i zakres działań. Właściciel magazynu otrzyma pełną kontrolę nad zarządzaniem magazynem   
i jego zawartością. Podstawową funkcjonalnością dostępną dla właściciela będzie zarządzanie magazynem, które obejmuje takie operacje jak edycja nazwy magazynu oraz archiwizacja,   
co pozwali na porządkowanie i długoterminowe przechowywanie plików. Dodatkowo właściciel powinien mieć możliwość udzielania dostępu innym użytkownikom oraz usuwania dostępu w razie potrzeby, co da mu pełną kontrolę nad tym, kto może korzystać z magazynu. Po udzieleniu dostępu, użytkownicy posiadający rolę Gościa zyskują uprawnienia do pracy   
z plikami w magazynie. Goście mogą wykonywać operacje takie jak edycja plików, upload plików (przesyłanie nowych plików do magazynu) oraz usuwanie plików. Kluczową funkcjonalnością będzie także rozwiązywanie konfliktów zawartości, które może wystąpić   
w sytuacji, gdy kilka osób jednocześnie pracuje nad tym samym plikiem. Mechanizm   
ten umożliwi porównywanie różnic w wersjach plików i wybór odpowiedniej zawartości,   
co zapewni spójność danych. Obie role użytkowników – Właściciel i Gość – otrzymają dostęp do operacji związanych z plikami, jednak to Właściciel posiada nadrzędne uprawnienia   
do zarządzania dostępem, edycji magazynu oraz jego konfiguracji.

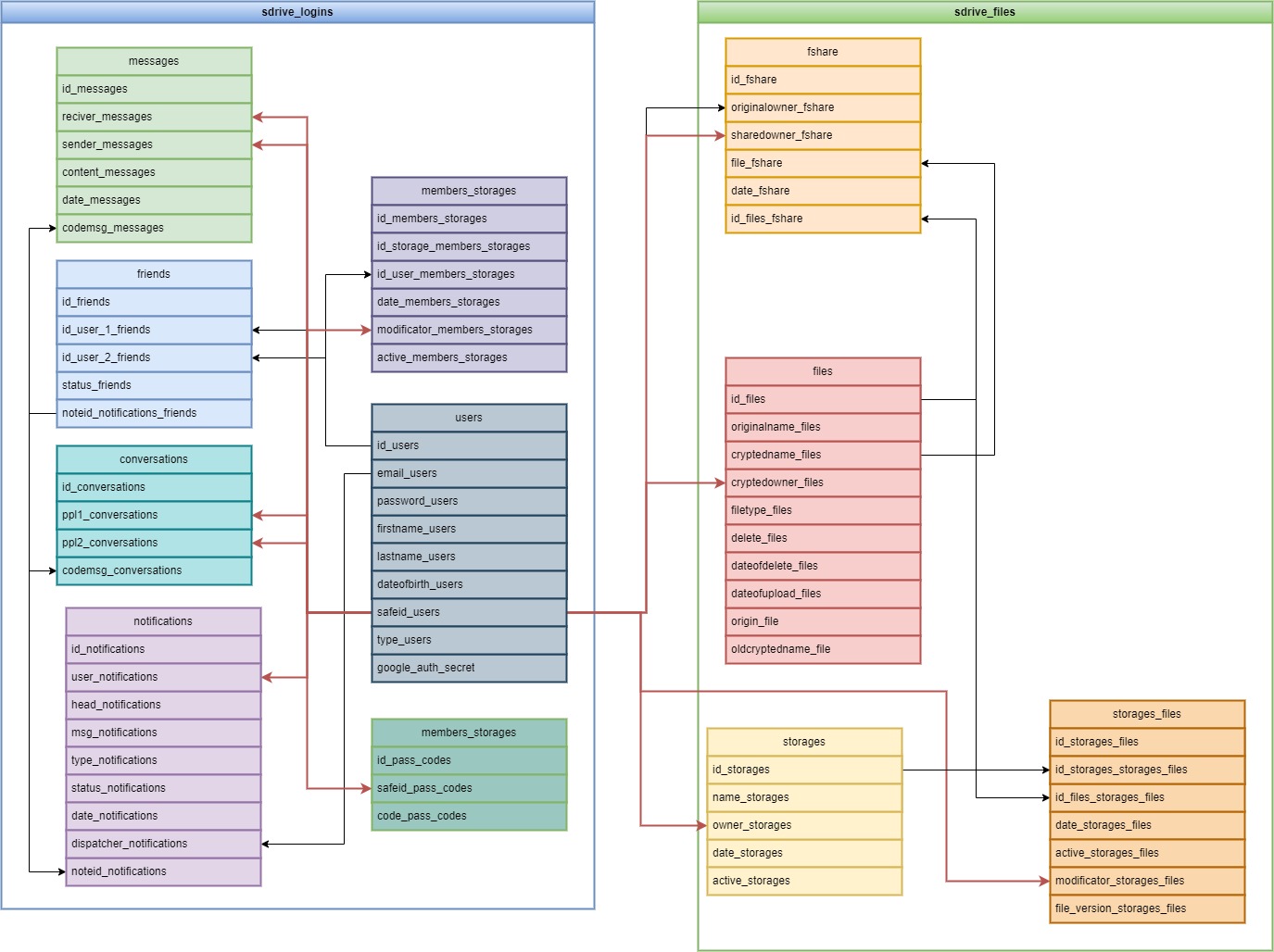


Rysunek 2. Diagram przypadków użycia – magazyny

[źródło: Opracowanie własne]

### 4.4.2. DIAGRAM ERD

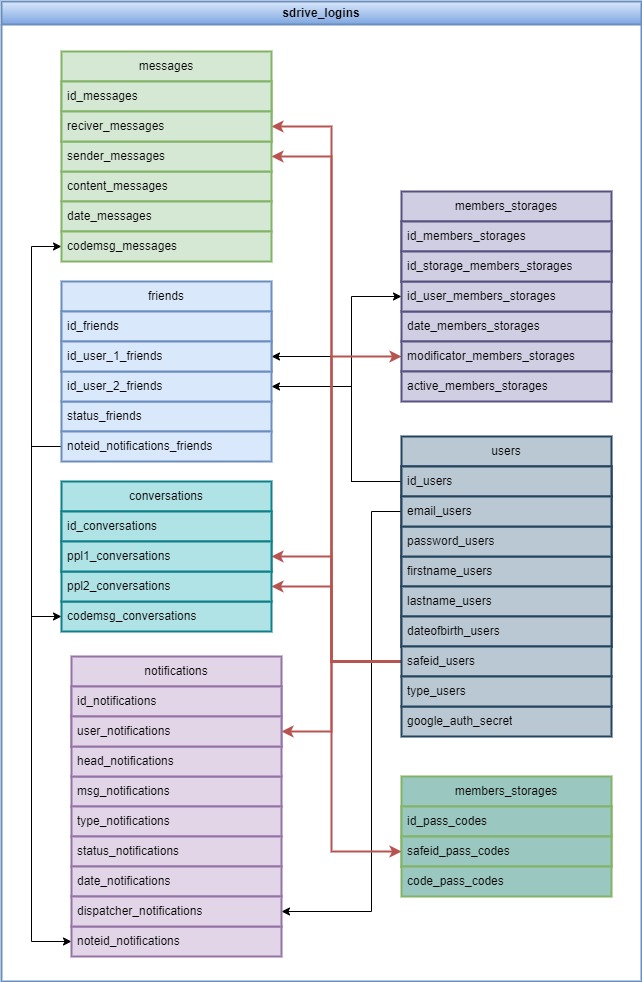
Rysunek 3 ilustruje diagram ERD (Entity-Relationship Diagram), który przedstawia   
pełną strukturę baz danych projektu sDrive. Projekt ten korzysta z dwóch oddzielnych   
baz danych: sdrive\_logins oraz sdrive\_files.



Rysunek 3. Diagram ERD

[źródło: Opracowanie własne]

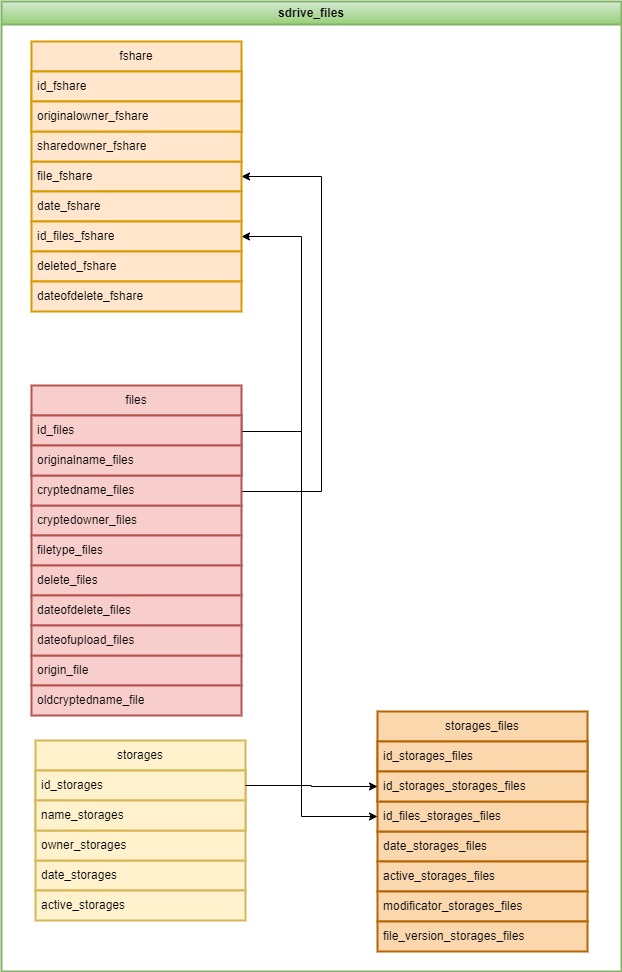
Rysunek 4 przedstawia diagram ERD bazy danych **sdrive\_logins** systemu **sDrive**, składający się z siedmiu tabel odpowiedzialnych za przechowywanie danych użytkowników oraz obsługę kluczowych funkcji systemu. Baza zarządza informacjami uwierzytelniającymi, relacjami znajomych, wiadomościami, powiadomieniami, konwersacjami oraz członkami magazynów. Tabele przechowują takie dane jak adresy e-mail, zaszyfrowane hasła, treści wiadomości, statusy relacji, a także klucze zabezpieczające. Struktura bazy jest zaprojektowana z myślą o bezpieczeństwie i efektywności zarządzania danymi w systemie.



Rysunek 4. Diagram ERD - sdrive\_logins

[źródło: Opracowanie własne]

Rysunek 5 przedstawia diagram ERD bazy danych sdrive\_files systemu sDrive, który odpowiada za zarządzanie plikami oraz ich powiązaniami z magazynami i udostępnieniami. Struktura bazy składa się z tabel przechowujących informacje o plikach, takich jak oryginalne i szyfrowane nazwy, typy, daty przesłania oraz status usunięcia. Tabele zarządzają również relacjami między plikami a magazynami, wspierając wersjonowanie oraz kontrolę dostępu. System umożliwia udostępnianie plików pomiędzy użytkownikami, przechowując szczegóły dotyczące właścicieli, statusów plików oraz ich historii. Baza została zaprojektowana z myślą o bezpieczeństwie i elastyczności w zarządzaniu danymi przechowywanymi w systemie.

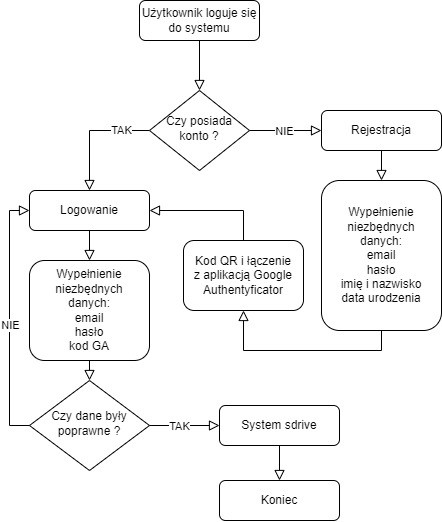


Rysunek 5. Diagram ERD - sdrive\_files

[źródło: Opracowanie własne]

### 4.4.3. DIAGRAMY AKTYWNOŚCI

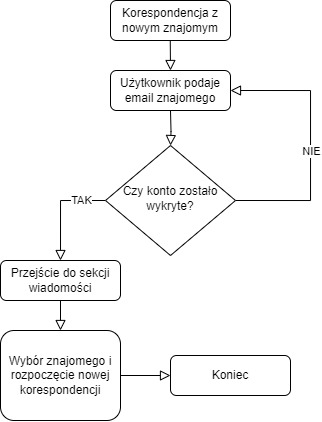
Rysunek 6 przedstawia proces logowania użytkownika do systemu, który rozpoczyna   
się od próby uzyskania dostępu przez użytkownika. Pierwszym krokiem jest weryfikacja,   
czy użytkownik posiada już konto w systemie. W przypadku odpowiedzi twierdzącej, użytkownik przechodzi do etapu logowania, gdzie wprowadza niezbędne dane, takie jak adres e-mail oraz hasło. Jeżeli podane dane są poprawne, użytkownik uzyskuje dostęp do systemu sdrive, co kończy proces logowania. Jeśli dane okażą się niepoprawne, system ponownie kieruje użytkownika do etapu logowania, umożliwiając ponowne wprowadzenie informacji.   
W sytuacji, gdy użytkownik nie posiada konta, przechodzi on przez proces rejestracji, który polega na wypełnieniu formularza rejestracyjnego wymagającego podania takich informacji   
jak adres e-mail, hasło, imię, nazwisko oraz data urodzenia. Po zakończeniu rejestracji użytkownik może przystąpić do logowania, aby uzyskać dostęp do systemu.



Rysunek 6. Diagram aktywności – logowanie

[źródło: Opracowanie własne]

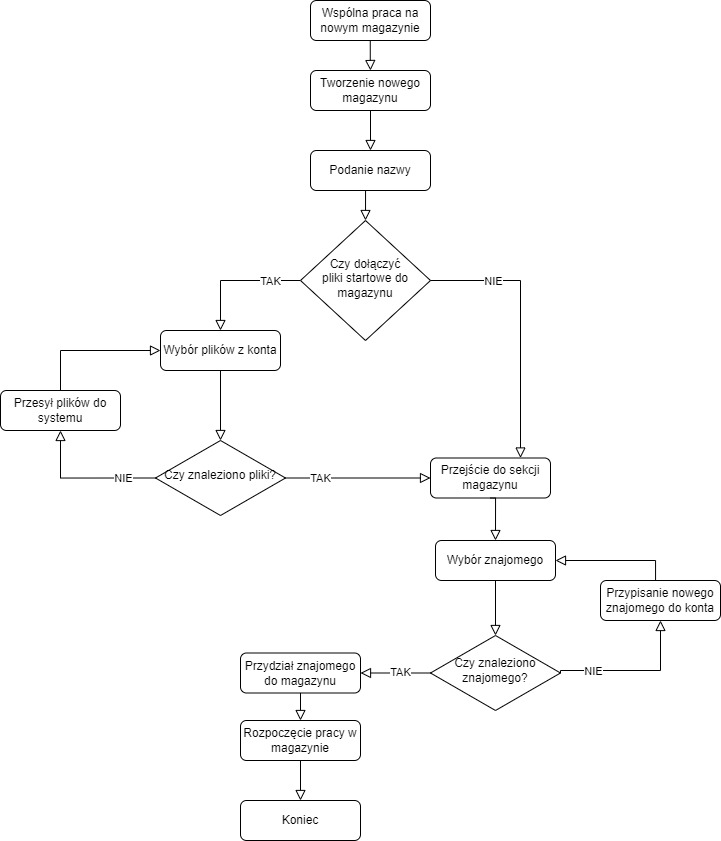
Rysunek 7 przedstawia proces nawiązania korespondencji z nowym znajomym   
w systemie. Całość rozpoczyna się od podania przez użytkownika adresu e-mail znajomego. System weryfikuje, czy konto odpowiadające podanemu e-mailowi istnieje. W przypadku,   
gdy konto zostanie wykryte, użytkownik przechodzi do sekcji wiadomości, gdzie może wybrać znajomego z listy i rozpocząć nową korespondencję. Jeśli system nie znajdzie konta odpowiadającego podanemu adresowi e-mail, proces zostaje przerwany, a użytkownik   
ma możliwość ponownego podania danych znajomego.



Rysunek 7. Diagramy aktywności - wysłanie wiadomości do nowego znajomego

[źródło: Opracowanie własne]

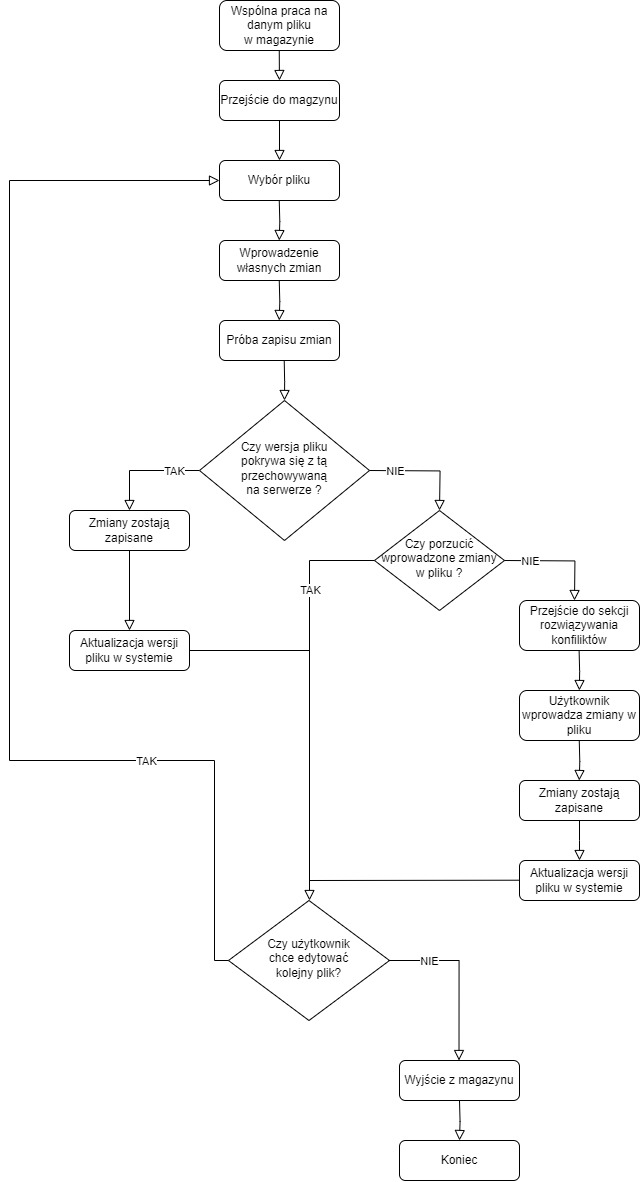
Rysunek 8 przedstawia proces tworzenia nowego magazynu w kontekście współpracy   
z innymi użytkownikami. Całość rozpoczyna się od podania nazwy nowego magazynu. Następnie użytkownik decyduje, czy chce dołączyć pliki startowe do magazynu.   
Jeśli odpowiedź jest twierdząca, system przechodzi do etapu wyboru plików z konta użytkownika, po czym następuje ich przesył do systemu. W przypadku braku plików użytkownik ma możliwość ponownej próby wyboru. Jeśli użytkownik rezygnuje z dodania plików, system przechodzi do sekcji magazynu, gdzie można przypisać znajomego   
do współpracy. W dalszym etapie użytkownik wybiera znajomego. System weryfikuje,   
czy dany znajomy został znaleziony w bazie danych. Jeśli znajomy istnieje, zostaje   
on przypisany do magazynu, co umożliwia rozpoczęcie wspólnej pracy. W przeciwnym wypadku użytkownik może przypisać nowego znajomego do swojego konta. Proces kończy się, gdy znajomy zostanie przydzielony, a praca w magazynie może się rozpocząć. Diagram   
w sposób przejrzysty ukazuje zarówno proces organizacji zasobów, jak i integrację funkcji współpracy między użytkownikami systemu.



Rysunek 8. Diagramy aktywności - praca na nowym magazynie

[źródło: Opracowanie własne]

Rysunek 9 przedstawia proces wspólnej pracy nad plikiem w magazynie, względniający zarówno edycję, jak i rozwiązywanie potencjalnych konfliktów. Proces rozpoczyna   
się od przejścia użytkownika do magazynu, gdzie dokonuje on wyboru pliku i wprowadza własne zmiany. W momencie próby zapisu system sprawdza, czy wersja pliku pokrywa   
się z aktualną wersją na serwerze. Jeśli wersje są zgodne, zmiany zostają zapisane, a system dokonuje aktualizacji wersji pliku. W przypadku wykrycia niezgodności użytkownik podejmuje decyzję, czy porzucić wprowadzone zmiany. Jeśli decyduje się na ich odrzucenie, wraca do wcześniejszego etapu. Jeśli natomiast wybierze kontynuację pracy, system przenosi go do sekcji rozwiązywania konfliktów. Tam użytkownik może wprowadzić odpowiednie modyfikacje, które następnie zostają zapisane i zaktualizowane w systemie. Po zakończeniu operacji użytkownik ma możliwość wyboru kolejnego pliku do edycji. Jeśli zdecyduje   
się na kontynuację, proces powtarza się od etapu wyboru pliku. W przeciwnym przypadku użytkownik wychodzi z magazynu, kończąc pracę.



Rysunek 9. Diagramy aktywności - praca na wspólnym pliku w magazynie

[źródło: Opracowanie własne]

## 4.5. SCENARIUSZE UŻYCIA

Scenariusze użycia aplikacji sDrive przedstawione w tabelach 1-10 ilustrują kluczowe funkcjonalności systemu oraz typowe interakcje użytkowników z aplikacją. Opisane przypadki użycia obejmują zarówno podstawowe operacje, takie jak rejestracja, logowanie   
czy przesyłanie plików, jak i bardziej zaawansowane funkcje, takie jak współdzielenie zasobów, edycja plików w magazynach czy zarządzanie znajomymi. Każdy scenariusz został szczegółowo opisany, uwzględniając warunki początkowe, przebieg główny, alternatywne ścieżki oraz końcowe rezultaty. Scenariusze te odzwierciedlają projektowane możliwości systemu, stanowiąc jednocześnie podstawę dla przyszłych działań testowych oraz rozwoju funkcjonalności aplikacji.

Tabela 1   
Scenariusz użycia - logowanie do systemu

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Logowanie do systemu |
| Nr. Scenariusza | 01 |
| Aktorzy | Użytkownik, system |
| Warunek początkowy | Użytkownik posiada konto w systemie sdrive. |
| Przebieg główny | Użytkownik podaje email i hasło. |
| Alternatywny przebieg | Hasło lub email zostaje odrzucone, podjęcie ponownej próby. |
| Wynik | Użytkownik zostaje zalogowany do systemu sdrive. |

[źródło: Opracowanie własne]

Tabela 2  
Scenariusz użycia - rejestracja w systemie sdrive

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Rejestracja w systemie sdrive |
| Nr. Scenariusza | 02 |
| Aktorzy | Użytkownik, system |
| Warunek początkowy | Brak --- |
| Przebieg główny | Użytkownik przechodzi do sekcji rejestracji, podaje email, imię i nazwisko oraz datę urodzenia. |
| Alternatywny przebieg | Wprowadzono błędne dane, należy ponowić próbę rejestracji. |
| Wynik | Użytkownik tworzy konto w systemie sdrive. |

[źródło: Opracowanie własne]

Tabela 3   
Scenariusz użycia - przesył plików do systemu sdrive

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Przesył plików do systemu sdrive |
| Nr. Scenariusza | 003 |
| Aktorzy | Użytkownik, system |
| Warunek początkowy | Użytkownik ma konto w systemie i jest zalogowany. |
| Przebieg główny | Użytkownik w sekcji przesyłu plików wybiera plik z komputera i wysyła  go do swojego konta. |
| Alternatywny przebieg | Nie udało się przesłać pliku, podjęcie ponownej próby. |
| Wynik | Udało się użytkownikowi przesłać plik z komputera do systemu. |

[źródło: Opracowanie własne]

Tabela 4   
Scenariusz użycia - udostępnianie plików w systemie

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Udostępnianie plików w systemie |
| Nr. Scenariusza | 04 |
| Aktorzy | Użytkownik 1, użytkownik 2, system |
| Warunek początkowy | Użytkownicy 1 i 2 mają konto w systemie i są znajomymi,  użytkownik 1 musi być zalogowany. |
| Przebieg główny | Użytkownik 1 z listy swoich plików lub udostępnianych mu plików  wybiera plik i opcję „udostępnij”, następnie z listy znajomych wybiera  użytkownika 2 i klika przycisk udostepnij. |
| Alternatywny przebieg | Nie udało się udostępnić pliku, podjęcie ponownej próby. |
| Wynik | Użytkownik 1 udostępnia plik użytkownikowi 2 |

[źródło: Opracowanie własne]

Tabela 5   
Scenariusz użycia - zapraszanie nowych znajomych

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Zapraszanie nowych znajomych |
| Nr. Scenariusza | 05 |
| Aktorzy | Użytkownik 1, użytkownik 2, system |
| Warunek początkowy | Użytkownicy 1 i 2 mają konto w systemie, użytkownik 1 musi być zalogowany. |
| Przebieg główny | Użytkownik 1 w sekcji znajomych wpisuje email użytkownika 2, wyświetla się okno ze szczegółowymi danymi użytkownika 2, użytkownik 1 wybiera opcję „zaproś do znajomych”. |
| Alternatywny przebieg | Nie udało się zaprosić użytkownika 2 do znajomych (najprawdopodobniej podano zły adres email), podjęcie ponownej próby. |
| Wynik | Użytkownik 2 i użytkownik 1 zostają znajomymi. |

[źródło: Opracowanie własne]

Tabela 6   
Scenariusz użycia - konwersacja ze znajomym

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Konwersacja ze znajomym |
| Nr. Scenariusza | 06 |
| Aktorzy | Użytkownik 1, użytkownik 2, system |
| Warunek początkowy | Użytkownicy 1 i 2 mają konto w systemie i są znajomymi,  użytkownik 1 musi być zalogowany. |
| Przebieg główny | Użytkownik 1 po zalogowaniu przechodzi do sekcji wiadomości, wybiera opcję rozpoczęcia nowej konwersacji, wybiera z listy znajomych użytkownika 2, wpisuje treść wiadomości i wybiera opcję „wyślij wiadomość”. |
| Alternatywny przebieg | Nie udało się przesłać wiadomości, podjęcie ponownej próby. |
| Wynik | Użytkownik 2 i użytkownik 1 wymieniają między sobą korespondencję. |

[źródło: Opracowanie własne]

Tabela 7   
Scenariusz użycia - tworzenie magazynu

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Tworzenie magazynu |
| Nr. Scenariusza | 07 |
| Aktorzy | Użytkownik 1, system |
| Warunek początkowy | Użytkownicy ma konto w systemie, użytkownik 1 musi być zalogowany, użytkownik 1 musi mieć przesłany przynajmniej jeden plik do systemu sdrive. |
| Przebieg główny | Użytkownik 1 po zalogowaniu wybiera opcję „utwórz” w sekcji magazynów, podaje nazwę magazynu, wybiera pliki które mają być załączone do danego magazynu i na koniec klika „Stwórz magazyn”. |
| Alternatywny przebieg | Nie udało się stworzenie magazynu, podjęcie ponownej próby. |
| Wynik | Użytkownik 1 tworzy magazyn |

[źródło: Opracowanie własne]

Tabela 8   
Scenariusz użycia - edycja pliku w magazynie

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Edycja pliku w magazynie |
| Nr. Scenariusza | 08 |
| Aktorzy | Użytkownik 1, użytkownik 2, system |
| Warunek początkowy | Użytkownicy 1 i 2 mają konto w systemie i są znajomymi,  użytkownik 1 musi być zalogowany, użytkownik 1 musi być przypisany przynajmniej do jednego magazynu. |
| Przebieg główny | Użytkownik 1 przechodzi do sekcji magazynów, wybiera konkretny magazyn, w magazynie wybiera plik, dokonuje zmian, zapisuje zmiany. |
| Alternatywny przebieg | Wykryto rozbieżność wersji pliku podczas zapisu (najprawdopodobniej użytkownik 2 dokonał zmian i zapisał je w pliku zanim użytkownik 1 zdołał zapisać swoje), użytkowink wybiera opcję rozwiązania konfliktu, przechodzi do sekcji konfliktów, dokonuje odpowiednich zmian w pliku i go zapisuje. |
| Wynik | Użytkownik 1 edytuje plik w magazynie |

[źródło: Opracowanie własne]

Tabela 9   
Scenariusz użycia - przypisanie znajomego do magazynu

|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Przypisanie znajomego do magazynu |
| Nr. Scenariusza | 09 |
| Aktorzy | Użytkownik 1, użytkownik 2, system |
| Warunek początkowy | Użytkownicy 1 i 2 mają konto w systemie i są znajomymi,  użytkownik 1 musi być zalogowany, użytkownik 1 musi być właścicielem przynajmniej jednego magazynu. |
| Przebieg główny | Użytkownik 1 po zalogowaniu przechodzi do swojego magazynu, wybiera opcję udostępniania, z listy znajomych wybiera użytkownika 2 i klika opcję „Udostępnij” |
| Alternatywny przebieg | Nie udało się udostępnić dostępu do magazynu, podjęcie ponownej próby. |
| Wynik | Użytkownik 1 udziela dostępu do swojego magazynu |

[źródło: Opracowanie własne]

Tabela 10   
Scenariusz użycia - przypisywanie nowych plików do magazynu

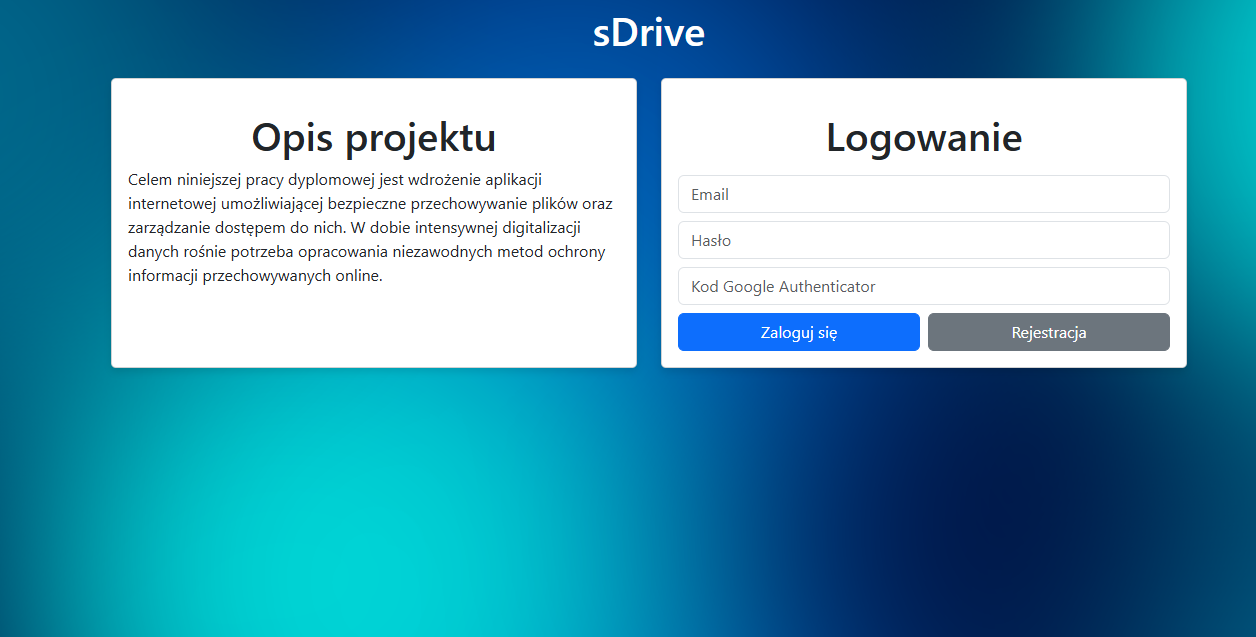
|  |  |
| --- | --- |
| Element | Opis |
| Nazwa scenariusza | Przypisywanie nowych plików do magazynu |
| Nr. Scenariusza | 10 |
| Aktorzy | Użytkownik 1, użytkownik 2, system |
| Warunek początkowy | Użytkownicy 1 ma konto w systemie, użytkownik 1 musi być zalogowany, użytkownik 1 musi być przypisany przynajmniej do jednego magazynu. |
| Przebieg główny | Użytkownik 1 po zalogowaniu się przechodzi do magazynu, wybiera opcję dodania pliku, z listy wybiera plik i klika opcję „Dodaj do magazynu”. |
| Alternatywny przebieg | Nie udało się dodać pliku do magazynu, podjęcie ponownej próby. |
| Wynik | Użytkownik 1 dodaje plik do magazynu. |

[źródło: Opracowanie własne]

# 5. IMPLEMENTACJA

## 5.1. SYSTEM LOGOWANIA I REJESTRACJI

System logowania i rejestracji w aplikacji sDrive został zaimplementowany   
z wykorzystaniem mechanizmów umożliwiających bezpieczną autoryzację użytkowników. Rejestracja polega na wypełnieniu formularza, w którym użytkownik podaje wymagane dane, takie jak adres e-mail i hasło. Po przesłaniu formularza generowany jest kod QR, który służy do integracji z aplikacją Google Authenticator, co wprowadza dwuskładnikowe uwierzytelnianie (2FA). Logowanie odbywa się poprzez wprowadzenie adresu e-mail, hasła oraz jednorazowego kodu generowanego przez Google Authenticator. Dane przesyłane   
do serwera są szyfrowane, a hasła zapisywane są w bazie danych w postaci zahaszowanej przy użyciu algorytmu bcrypt. Weryfikacja kodu QR i jednorazowego hasła odbywa się w czasie rzeczywistym, co zapewnia dodatkowy poziom zabezpieczeń. Na rysunkach   
10–12 przedstawiono poszczególne elementy systemu, w tym widok formularza rejestracji, ekranu logowania oraz integracji kodu QR z Google Authenticator. Funkcjonalność ta została wdrożona w celu zapewnienia zarówno wysokiego poziomu bezpieczeństwa, jak i płynności działania systemu, umożliwiając użytkownikom bezpieczny dostęp do ich kont.



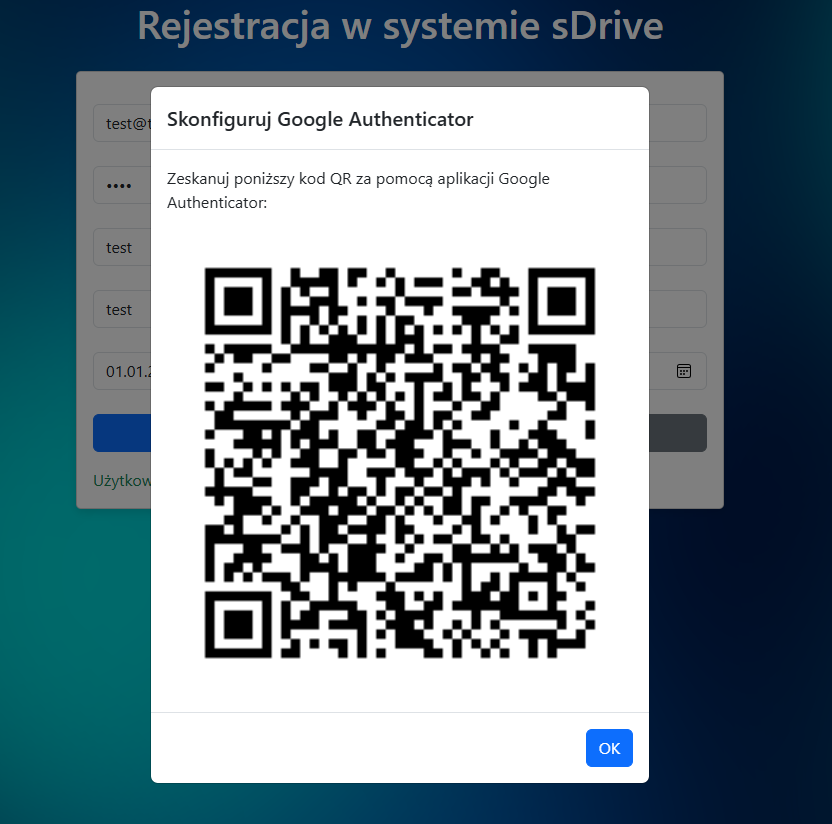
Rysunek 10. System logowania i rejestracji - ekran logowania

[źródło: Opracowanie własne]



Rysunek 11. System logowania i rejestracji - ekran rejestracji

[źródło: Opracowanie własne]



Rysunek 12. System logowania i rejestracji - kod qr

[źródło: Opracowanie własne]

Listing 1 przedstawia funkcję odpowiedzialną za obsługę logowania użytkownika   
w aplikacji webowej. Funkcja asynchroniczna login przyjmuje żądanie z danymi logowania   
(e-mail i hasło) przesyłanymi przez użytkownika i weryfikuje je w bazie danych. Najpierw sprawdza, czy dane zostały podane, a następnie wykonuje zapytanie SQL, aby pobrać odpowiadający użytkownika rekord z bazy danych. W przypadku poprawnych danych funkcja porównuje hasło z zahaszowanym hasłem w bazie za pomocą biblioteki bcryptjs. Jeśli logowanie się powiedzie, generowany jest token JWT z identyfikatorem użytkownika, który zostaje zapisany w ciasteczku z ustawionymi parametrami, takimi jak czas wygaśnięcia   
i dostępność jedynie po stronie serwera (httpOnly). Ostatecznie funkcja zwraca odpowiedź   
o sukcesie wraz z informacją o przekierowaniu na stronę domową, a w przypadku błędnych danych zwracany jest odpowiedni komunikat o błędzie.

1. const login = async (req, res) => {
2. const { email, password, totp } = req.body;
3. console.log("Odebrane dane logowania:", req.body);
4. if (!email || !password || !totp) {
5. return res.json({ status: "error", error: "Podaj swój email, hasło i kod Google Authenticator" });
6. } else {
7. dbLogins.query('SELECT email\_users, password\_users, safeid\_users, id\_users, google\_auth\_secret FROM users WHERE email\_users = ?', [email], async (err, result) => {
8. if (err) throw err;
9. if (!result[0] || !await bcryptjs.compare(password, result[0].password\_users)) {
10. return res.json({ status: "error", error: "Niepoprawne hasło lub email" });
11. } else {
12. const safeId = result[0].safeid\_users;
13. const googleAuthSecret = result[0].google\_auth\_secret;
14. if (!googleAuthSecret) {
15. return res.json({ status: "error", error: "Brak skonfigurowanego Google Authenticator dla tego konta" });
16. }
17. const verified = speakeasy.totp.verify({
18. secret: googleAuthSecret,
19. encoding: "base32",
20. token: totp
21. });
22. if (!verified) {
23. return res.json({ status: "error", error: "Niepoprawny kod Google Authenticator" });
24. }
25. dbLogins.query('SELECT code\_pass\_codes FROM pass\_codes WHERE safeid\_pass\_codes = ?', [safeId], async (err, keyResult) => {
26. if (err) throw err;
27. if (keyResult.length > 0) {
28. const key = Buffer.from(keyResult[0].code\_pass\_codes, "hex");
29. const userFolder = path.join(\_\_dirname, "..", "data", "users", safeId);
30. const sharesFolder = path.join(\_\_dirname, "..", "data", "shares", safeId);
31. decryptDirectory(userFolder, key);
32. decryptDirectory(sharesFolder, key);
33. }
34. const token = jwt.sign({ id: result[0].id\_users }, process.env.JWT\_SECRET, {
35. expiresIn: process.env.JWT\_EXPIRES
36. });
37. const cookieOptions = {
38. expires: new Date(Date.now() + process.env.COOKIE\_EXPIRES \* 24 \* 60 \* 60 \* 1000),
39. httpOnly: true
40. };
41. res.cookie("userRegistered", token, cookieOptions);
42. console.log("Ciasteczko ustawione: ", token);
43. return res.json({ status: "success", redirect: "/home" });
44. });

Listing 1. System logowania i rejestracji **–** logowanie

[źródło: Opracowanie własne]

Listing 2 przedstawia rejestrację nowego użytkownika w systemie. Najpierw sprawdzane jest, czy wszystkie wymagane pola zostały wypełnione (e-mail, hasło, imię, nazwisko, data urodzenia), a następnie system weryfikuje, czy podany adres e-mail już istnieje w bazie danych. Jeśli e-mail nie występuje, hasło użytkownika jest hashowane za pomocą biblioteki bcrypt,   
co zwiększa bezpieczeństwo przechowywanych danych. Dodatkowo generowany jest unikalny identyfikator safeId, który jest sprawdzany pod kątem unikalności za pomocą pętli,   
aby upewnić się, że nie występuje on już w systemie. W końcu nowy użytkownik zostaje zapisany do bazy danych z odpowiednimi danymi, a jego typ konta domyślnie ustawiany jest na „Normal”. Funkcja zwraca komunikat o sukcesie rejestracji lub odpowiedni błąd, jeśli wystąpią nieprawidłowości, takie jak duplikacja e-maila lub błąd serwera.

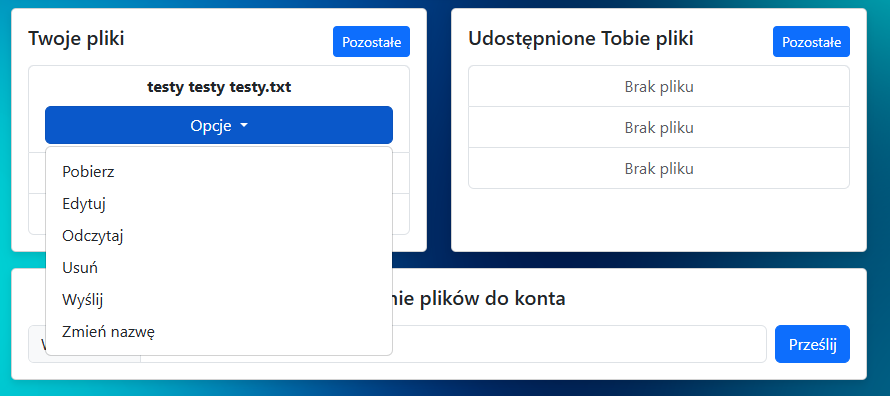
1. const register = async (req, res) => {
2. const { email, password: Npassword, firstName, lastName, birthDate } = req.body;
3. if (!email || !Npassword || !firstName || !lastName || !birthDate) {
4. return res.json({ status: "error", error: "Proszę wypełnić wszystkie pola" });
5. } else {
6. dbLogins.query('SELECT email\_users FROM users WHERE email\_users = ?', [email], async (err, result) => {
7. if (err) throw err;
8. if (result[0]) {
9. return res.json({ status: "error", error: "Email już jest w systemie" });
10. } else {
11. const password = await bcrypt.hash(Npassword, 8);
12. let safeId;
13. let unique = false;
14. while (!unique) {
15. safeId = generateSafeId();
16. unique = await isSafeIdUnique(safeId);}
17. const { secret, qrCodeDataUrl } = await generateGoogleAuthSecret(safeId);
18. dbLogins.query('INSERT INTO users SET ?', {
19. email\_users: email,
20. password\_users: password,
21. firstname\_users: firstName,
22. lastname\_users: lastName,
23. dateofbirth\_users: birthDate,
24. safeid\_users: safeId,
25. type\_users: "Normal",
26. google\_auth\_secret: secret.base32
27. }, (error, results) => {
28. if (error) throw error;
29. return res.json({
30. status: "success",
31. success: "Użytkownik został zarejestrowany",
32. qrCode: qrCodeDataUrl

Listing 2**.** System logowania i rejestracji – rejestracja

[źródło: Opracowanie własne]

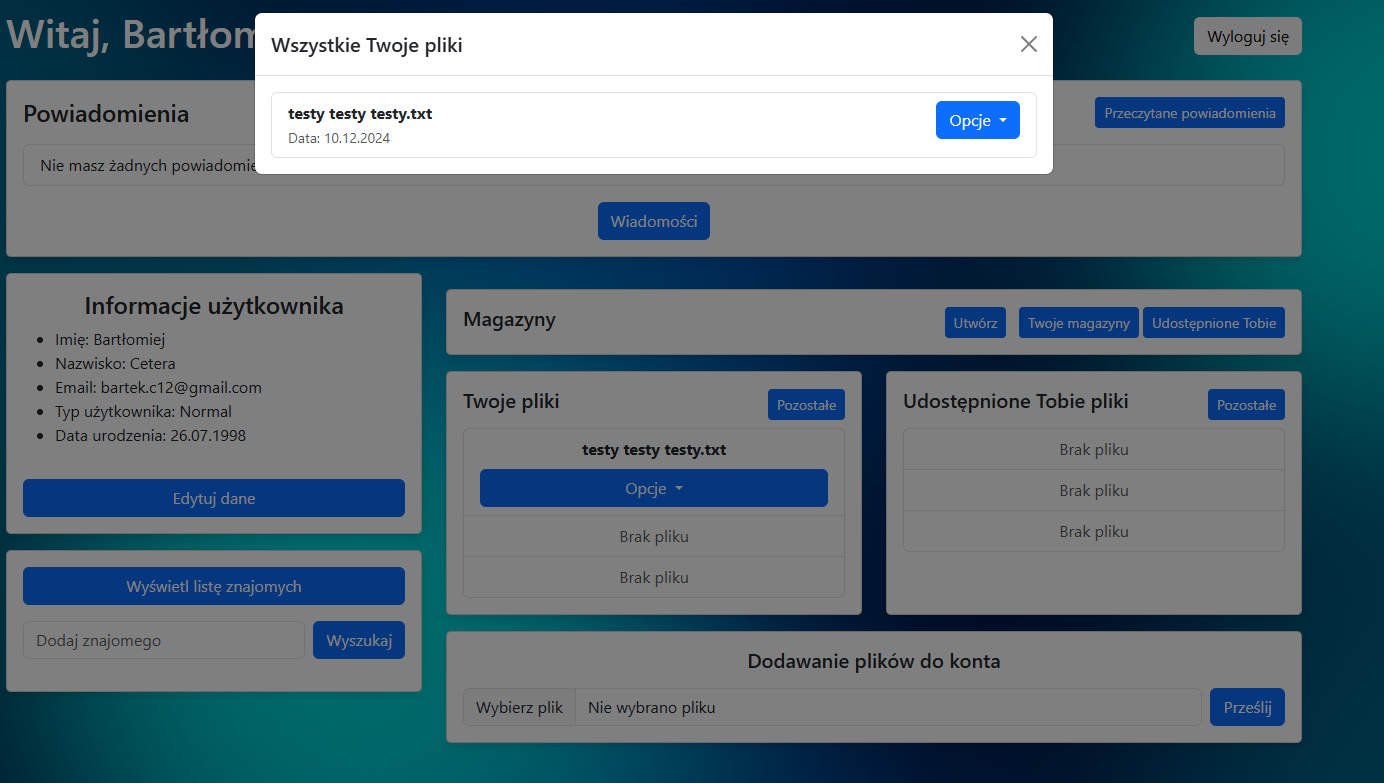
## 5.2. SYSTEM ZARZĄDZANIA PLIKAMI

System zarządzania plikami w aplikacji sDrive został zaimplementowany w sposób umożliwiający użytkownikom wykonywanie operacji na przechowywanych danych. Użytkownicy mają możliwość przesyłania plików na swoje konta, pobierania ich, przeglądania zawartości, edytowania, usuwania oraz zmieniania nazw. Dodatkowo system pozwala   
na udostępnianie plików znajomym przypisanym do konta, a także zarządzanie plikami udostępnionymi przez innych użytkowników. Edycja plików jest możliwa bezpośrednio   
w systemie, co eliminuje potrzebę ponownego przesyłania zmodyfikowanych danych. Funkcja usuwania plików została zrealizowana z użyciem mechanizmu "soft delete", który umożliwia odzyskanie przypadkowo usuniętych plików w określonym czasie. Na rysunkach   
13–15 przedstawiono zaimplementowane kluczowe elementy systemu zarządzania plikami, takie jak interfejs sekcji plików, widok szczegółowy dla zarządzania plikami oraz ekran edycji.



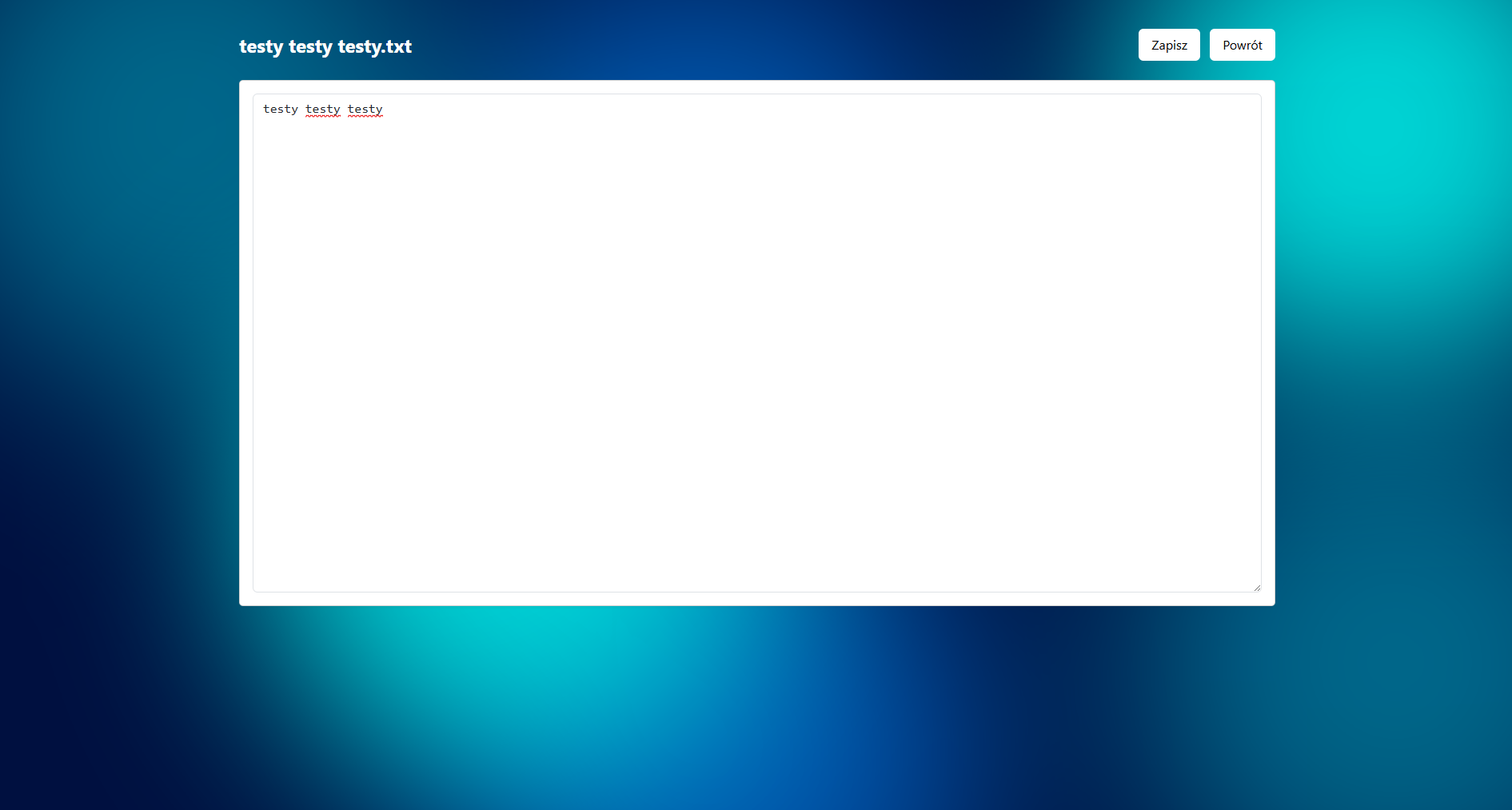
Rysunek 13. System zarządzania plikami - sekcja plików

[źródło: Opracowanie własne]



Rysunek 14. System zarządzania plikami - sekcja wszystkich plików

[źródło: Opracowanie własne]



Rysunek 15. System zarządzania plikami - edycja pliku

[źródło: Opracowanie własne]

Listing 3 przedstawia funkcję showUserFileContent, odpowiadającą za wyświetlanie zawartości pliku użytkownika na podstawie jego unikalnego identyfikatora safeId oraz nazwy pliku przesłanej w parametrach żądania. Najpierw wykonuje zapytanie do bazy danych,   
aby sprawdzić, czy plik o podanej zaszyfrowanej nazwie (cryptedname\_files) należy   
do użytkownika. Jeśli plik istnieje, funkcja pobiera jego oryginalną nazwę, określa rozszerzenie pliku oraz buduje ścieżkę do pliku w katalogu użytkownika. Następnie sprawdza, czy plik fizycznie istnieje na serwerze, i jeśli tak, wywołuje funkcję handleFileRead, która odpowiednio odczytuje plik i przesyła jego zawartość do klienta. W przypadku braku pliku w systemie plików lub bazie danych funkcja zwraca odpowiedź o błędzie z kodem 404. Funkcja zawiera także obsługę błędów serwera oraz informuje użytkownika o problemach z dostępem do pliku lub jego brakiem.

1. const showUserFileContent = (req, res) => {
2. const safeId = req.user.safeid\_users;
3. const filename = req.params.filename;
4. dbFiles.query(
5. 'SELECT originalname\_files, cryptedname\_files, filetype\_files FROM files WHERE cryptedname\_files = ? AND cryptedowner\_files = ?',
6. [filename, safeId],
7. (err, result) => {
8. if (err) {
9. console.error('Błąd podczas pobierania pliku z bazy danych:', err);
10. return res.status(500).json({ status: 'error', error: 'Błąd pobierania pliku z bazy danych' });}
11. if (result.length > 0) {
12. const originalName = result[0].originalname\_files;
13. const fileExtension = path.extname(originalName).toLowerCase();
14. const userDir = path.join(\_\_dirname, '..', 'data', 'users', safeId);
15. const filePath = path.join(userDir, filename);
16. if (fs.existsSync(filePath)) {
17. handleFileRead(filePath, fileExtension, originalName, res);
18. } else {
19. res.status(404).send("Plik nie istnieje");}
20. } else {
21. res.status(404).send("Plik nie istnieje w bazie danych");

Listing 3. System zarządzania plikami - wyświetlanie plików użytkownika

[źródło: Opracowanie własne]

Listing 4 przedstawia funkcję getFileContent, która jest odpowiedzialna za pobieranie zawartości pliku użytkownika z serwera na podstawie jego unikalnego identyfikatora safeId oraz nazwy pliku przekazanej jako parametr żądania. Na początku generowana jest ścieżka   
do katalogu użytkownika oraz docelowego pliku, po czym system sprawdza, czy plik istnieje na serwerze. Jeśli plik ma rozszerzenie .docx, jego zawartość jest odczytywana przy użyciu biblioteki mammoth, która przekształca dokument Worda na tekst w formacie surowym.   
Dla plików o innych rozszerzeniach funkcja korzysta z metody fs.readFile do odczytania zawartości pliku jako tekstu w formacie UTF-8. W przypadku powodzenia zawartość pliku zostaje przesłana do klienta w formacie JSON z odpowiednim statusem. Jeśli plik nie istnieje lub wystąpią błędy podczas odczytu, system zwraca komunikaty błędów odpowiednio z kodami 404 lub 500, informując o problemie z dostępem lub odczytem pliku.

1. const getFileContent = (req, res) => {
2. const safeId = req.user.safeid\_users;
3. const filename = req.params.filename;
4. const userDir = path.join(\_\_dirname, '..', 'data', 'users', safeId);
5. const filePath = path.join(userDir, filename);
6. console.log(`Próbuję pobrać zawartość pliku: ${filePath}`);
7. if (fs.existsSync(filePath)) {
8. const fileExtension = path.extname(filename).toLowerCase();
9. if (fileExtension === '.docx') {
10. const mammoth = require('mammoth');
11. mammoth.extractRawText({ path: filePath })
12. .then(result => {
13. res.json({ status: 'success', content: result.value });
14. })
15. .catch(err => {
16. console.error('Błąd podczas odczytu pliku .docx:', err);
17. res.status(500).json({ status: 'error', error: 'Błąd odczytu pliku .docx' });
18. });
19. } else {
20. fs.readFile(filePath, 'utf8', (err, data) => {
21. if (err) {
22. console.error('Błąd odczytu pliku:', err);
23. return res.status(500).json({ status: 'error', error: 'Błąd odczytu pliku' });
24. }
25. res.json({ status: 'success', content: data });
26. });
27. }
28. } else {
29. console.error('Plik nie istnieje:', filePath);
30. res.status(404).json({ status: 'error', error: 'Plik nie istnieje' });
31. }
32. };

Listing 4. System zarządzania plikami - wyświetlanie zawartości pliku

[źródło: Opracowanie własne]

Listing 5 przedstawia funkcję renameFile, która odpowiada za zmianę nazwy pliku należącego do konkretnego użytkownika. Proces rozpoczyna się od walidacji nowej nazwy pliku, aby upewnić się, że jest ona poprawnym, niepustym ciągiem znaków. Następnie funkcja wykonuje zapytanie do bazy danych w celu sprawdzenia, czy plik o podanym identyfikatorze (cryptedname\_files) istnieje i należy do użytkownika na podstawie jego unikalnego identyfikatora safeId. Jeżeli plik zostanie odnaleziony, system aktualizuje jego oryginalną nazwę (originalname\_files) w bazie danych, pozostawiając zaszyfrowaną nazwę pliku   
bez zmian. Po pomyślnym zakończeniu operacji funkcja zwraca odpowiedź potwierdzającą zmianę nazwy pliku. W przypadku wystąpienia błędów, takich jak brak pliku, brak dostępu lub problem z serwerem, funkcja zwraca odpowiedni komunikat błędu z właściwym kodem HTTP.

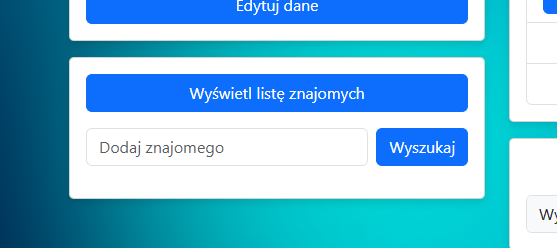
1. const renameFile = (req, res) => {
2. const safeId = req.user.safeid\_users;
3. const { fileId } = req.params;
4. const { newFileName } = req.body;
5. if (!newFileName || typeof newFileName !== 'string' || !newFileName.trim()) {
6. return res.status(400).json({ status: 'error', error: 'Nazwa pliku nie może być pusta.' });
7. }
8. dbFiles.query(
9. 'SELECT originalname\_files, cryptedname\_files FROM files WHERE cryptedname\_files = ? AND cryptedowner\_files = ?',
10. [fileId, safeId],
11. (err, results) => {
12. if (err) {
13. console.error('Błąd podczas wyszukiwania pliku:', err);
14. return res.status(500).json({ status: 'error', error: 'Błąd serwera.' });
15. }
16. if (results.length === 0) {
17. return res.status(404).json({ status: 'error', error: 'Plik nie istnieje lub brak dostępu.' });
18. }
19. const currentOriginalName = results[0].originalname\_files;
20. const cryptedName = results[0].cryptedname\_files;
21. const userDir = path.join(\_\_dirname, '..', 'data', 'users', safeId);
22. const oldFilePath = path.join(userDir, cryptedName);
23. const newFilePath = path.join(userDir, cryptedName);
24. dbFiles.query(
25. 'UPDATE files SET originalname\_files = ? WHERE cryptedname\_files = ? AND cryptedowner\_files = ?',
26. [newFileName, fileId, safeId],
27. (err) => {
28. if (err) {
29. console.error('Błąd podczas aktualizacji nazwy pliku:', err);
30. return res.status(500).json({ status: 'error', error: 'Błąd serwera podczas zmiany nazwy pliku.' });
31. }
32. console.log(`Zmieniono nazwę pliku z "${currentOriginalName}" na "${newFileName}"`);
33. res.json({ status: 'success', message: 'Nazwa pliku została pomyślnie zmieniona.' });

Listing **5.** System zarządzania plikami - zmiana nazwy pliku

[źródło: Opracowanie własne]

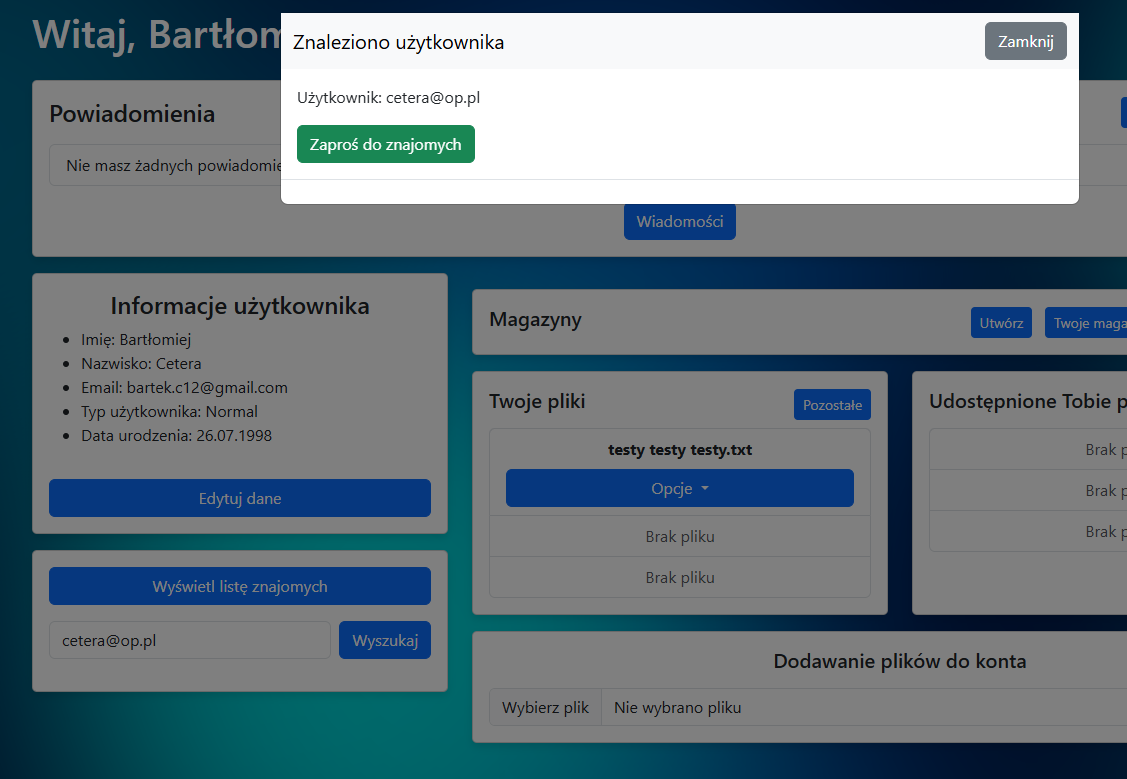
## 5.3. SYSTEM ZNAJOMYCH

System znajomych w aplikacji sDrive został zaimplementowany w sposób umożliwiający użytkownikom nawiązywanie i zarządzanie relacjami z innymi osobami w ramach aplikacji. Funkcjonalność obejmuje możliwość wyszukiwania użytkowników na podstawie ich adresu   
e-mail oraz wysyłania zaproszeń do znajomych. Po zaakceptowaniu zaproszenia użytkownik uzyskuje dostęp do szeregu dodatkowych opcji, takich jak udostępnianie plików, wysyłanie wiadomości czy przypisywanie znajomych do wspólnych magazynów. Wdrożony system umożliwia również zarządzanie listą kontaktów, co pozwala użytkownikom na szybki dostęp do podstawowych informacji o znajomych oraz efektywne współdzielenie zasobów w obrębie aplikacji. Mechanizmy te wspierają współpracę i komunikację między użytkownikami, zapewniając jednocześnie intuicyjność obsługi i spójność danych. Rysunki 16–17 ilustrują implementację systemu znajomych, w tym interfejsy odpowiedzialne za wyszukiwanie użytkowników, wysyłanie zaproszeń oraz zarządzanie kontaktami.



Rysunek 16. System znajomych - sekcja znajomych

[źródło: Opracowanie własne]



Rysunek 17. System znajomych - wyszukiwanie nowych znajomych

[źródło: Opracowanie własne]

Listing 6 przedstawia funkcję inviteFriend, która jest odpowiedzialna za zapraszanie nowego znajomego w systemie oraz wysyłanie powiadomienia o zaproszeniu. Proces rozpoczyna się od pobrania identyfikatora oraz e-maila użytkownika zapraszającego, a także identyfikatora użytkownika, który ma zostać zaproszony. Funkcja sprawdza, czy użytkownicy nie są już znajomymi za pomocą funkcji areUsersAlreadyFriends. Jeśli relacja nie istnieje, wykonywane jest zapytanie do bazy danych w celu znalezienia unikalnego identyfikatora (safeid\_users) oraz e-maila zapraszanego użytkownika. Następnie generowany jest unikalny kod identyfikujący zaproszenie (noteId) przy użyciu funkcji bcrypt i pętli sprawdzającej unikalność kodu. Po wygenerowaniu kodu zaproszenie zostaje zapisane w tabeli friends   
z odpowiednim statusem ("NotActive"), co oznacza oczekiwanie na akceptację. Równocześnie tworzona jest wiadomość zawierająca szczegóły zaproszenia, która zostaje zapisana w tabeli notifications jako powiadomienie typu friend\_request. W przypadku powodzenia funkcja zwraca komunikat o sukcesie, informując, że znajomy został zaproszony i powiadomienie zostało wysłane. W razie wystąpienia błędów na którymkolwiek etapie (wyszukiwania użytkownika, zapisu zaproszenia lub powiadomienia), funkcja zwraca odpowiedni komunikat błędu w formacie JSON.

1. const inviteFriend = async (req, res) => {
2. const inviterId = req.user.id\_users;
3. const inviterEmail = req.user.email\_users;
4. const { friendId } = req.body;
5. const alreadyFriends = await areUsersAlreadyFriends(inviterId, friendId);
6. if (alreadyFriends) {
7. return res.json({ status: 'error', error: 'Użytkownicy są już znajomymi.' });
8. }
9. dbLogins.query('SELECT safeid\_users, email\_users FROM users WHERE id\_users = ?', [friendId], async (err, result) => {
10. if (err) {
11. return res.json({ status: 'error', error: 'Błąd wyszukiwania użytkownika' });
12. }
13. if (result.length === 0) {
14. return res.json({ status: 'error', error: 'Nie znaleziono zapraszanego użytkownika' });
15. }
16. const recipientSafeId = result[0].safeid\_users;
17. const recipientEmail = result[0].email\_users;
18. let noteId;
19. let unique = false;
20. while (!unique) {
21. noteId = await bcrypt.hash(Date.now().toString(), 10);
22. unique = await isNoteIdUnique(noteId);
23. }

Listing 6. System znajomych - zapraszanie nowych znajomych 1/2

[źródło: Opracowanie własne]

1. dbLogins.query(
2. 'INSERT INTO friends (id\_user\_1\_friends, id\_user\_2\_friends, status\_friends, noteid\_notifications\_friends) VALUES (?, ?, "NotActive", ?)',
3. [inviterId, friendId, noteId],
4. (err, result) => {
5. if (err) {
6. return res.json({ status: 'error', error: 'Błąd zaproszenia znajomego' });}
7. const message = `Użytkownik ${req.user.firstname\_users} ${req.user.lastname\_users} (${inviterEmail}) wysłał ci zaproszenie do znajomych.`;
8. dbLogins.query(
9. 'INSERT INTO notifications (user\_notifications, head\_notifications, msg\_notifications, type\_notifications, status\_notifications, date\_notifications, dispatcher\_notifications, noteid\_notifications) VALUES (?, "Zaproszenie do znajomych", ?, "friend\_request", "unread", CURDATE(), ?, ?)',
10. [recipientSafeId, message, inviterEmail, noteId],
11. (err, result) => {
12. if (err) {
13. return res.json({ status: 'error', error: 'Błąd wysyłania powiadomienia' });}
14. res.json({ status: 'success', success: 'Znajomy został zaproszony, a powiadomienie wysłane.' });

Listing 6. System znajomych - zapraszanie nowych znajomych 2/2

[źródło: Opracowanie własne]

Listing 7 przedstawia funkcję respondToFriendRequest, która odpowiada za obsługę odpowiedzi na zaproszenie do znajomych, umożliwiając użytkownikowi jego zaakceptowanie lub odrzucenie. Proces rozpoczyna się od walidacji parametru action, który musi przyjmować wartość „accept” lub „deny”. Na podstawie tej akcji system ustala nowy status relacji („Active” dla akceptacji, „Denied” dla odrzucenia) i sprawdza w bazie danych, czy istnieje zaproszenie odpowiadające przesłanemu identyfikatorowi noteId. Jeśli zaproszenie zostanie znalezione, jego status jest aktualizowany w tabeli friends, a odpowiadające mu powiadomienie w tabeli notifications zostaje oznaczone jako „read”. W przypadku akceptacji system dodatkowo pobiera dane użytkownika zapraszającego (safeid\_users) i generuje powiadomienie informujące go, że jego zaproszenie zostało zaakceptowane. Powiadomienie to zawiera szczegóły akcji i jest zapisywane w tabeli notifications z odpowiednim statusem („unread”). Ostatecznie funkcja zwraca komunikat o sukcesie, informując, czy zaproszenie zostało zaakceptowane, czy odrzucone. W razie wystąpienia błędów na dowolnym etapie, takich   
jak problem z bazą danych lub brak zaproszenia, funkcja zwraca odpowiedni komunikat błędu.

1. const respondToFriendRequest = (req, res) => {
2. const { noteId, action } = req.body;
3. let newStatus = action === 'accept' ? 'Active' : 'Denied';
4. if (!['accept', 'deny'].includes(action)) {
5. return res.json({ status: 'error', error: 'Nieprawidłowa akcja' });
6. }
7. dbLogins.query(
8. 'SELECT \* FROM friends WHERE noteid\_notifications\_friends = ?',
9. [noteId],
10. (err, result) => {
11. if (err) {
12. return res.json({ status: 'error', error: 'Błąd podczas szukania zaproszenia' });
13. }
14. if (result.length === 0) {
15. return res.json({ status: 'error', error: 'Nie znaleziono zaproszenia' });
16. }
17. const friendEntryId = result[0].id\_friends;
18. const inviterId = result[0].id\_user\_1\_friends;
19. const accepterId = result[0].id\_user\_2\_friends;
20. dbLogins.query(
21. 'UPDATE friends SET status\_friends = ? WHERE id\_friends = ?',
22. [newStatus, friendEntryId],
23. (err) => {
24. if (err) {
25. return res.json({ status: 'error', error: 'Błąd aktualizacji statusu' });
26. }
27. dbLogins.query(
28. 'UPDATE notifications SET status\_notifications = "read" WHERE noteid\_notifications = ?',
29. [noteId],
30. (err) => {
31. if (err) {
32. return res.json({ status: 'error', error: 'Błąd aktualizacji statusu powiadomienia' });
33. }
34. if (action === 'accept') {
35. dbLogins.query(
36. 'SELECT safeid\_users, email\_users FROM users WHERE id\_users = ?',
37. [inviterId],
38. (err, inviterResult) => {
39. if (err || inviterResult.length === 0) {
40. return res.json({ status: 'error', error: 'Błąd pobierania danych zapraszającego' });
41. }
42. const inviterSafeId = inviterResult[0].safeid\_users;
43. const accepterEmail = req.user.email\_users;
44. const message = `Użytkownik o mailu ${accepterEmail} zaakceptował twoje zaproszenie do znajomych.`;
45. dbLogins.query(
46. 'INSERT INTO notifications (user\_notifications, head\_notifications, msg\_notifications, type\_notifications,

Listing 7. System znajomych - zapraszanie nowych znajomych 1/2

[źródło: Opracowanie własne]

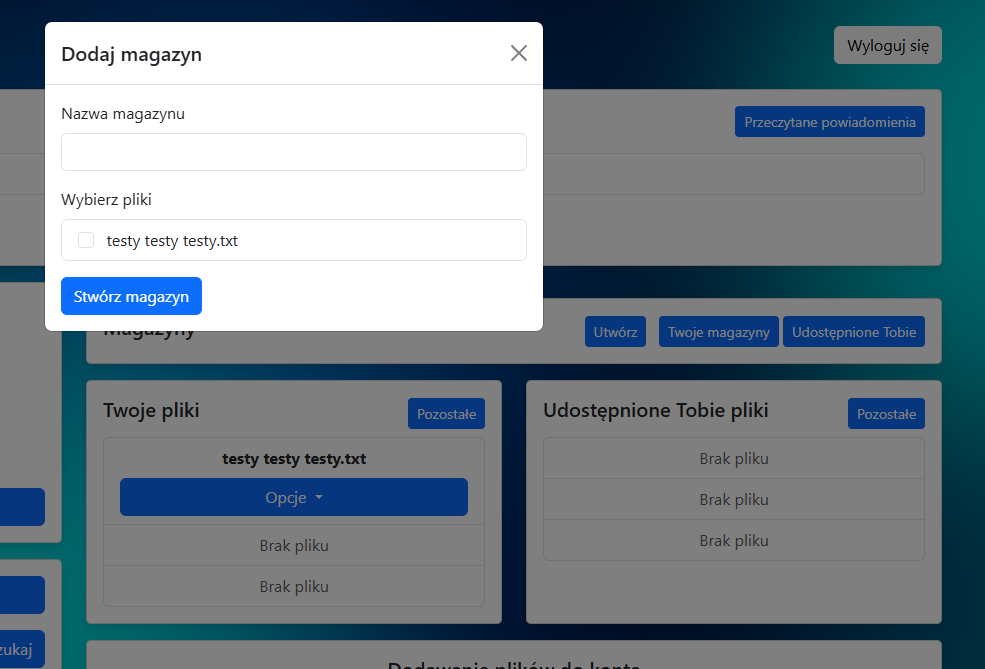
1. status\_notifications, date\_notifications, dispatcher\_notifications) VALUES (?, "Nowy znajomy", ?, "friend\_response", "unread", CURDATE(), ?)',
2. [inviterSafeId, message, accepterEmail],
3. (err) => {
4. if (err) {
5. return res.json({ status: 'error', error: 'Błąd podczas dodawania powiadomienia' });
6. }
7. return res.json({ status: 'success', success: 'Zaproszenie zaakceptowane i powiadomienie wysłane.' });
8. }
9. );
10. }
11. );
12. } else {
13. return res.json({ status: 'success', success: 'Zaproszenie zostało odrzucone.' });

Listing 7. System znajomych - zapraszanie nowych znajomych 2/2

[źródło: Opracowanie własne]

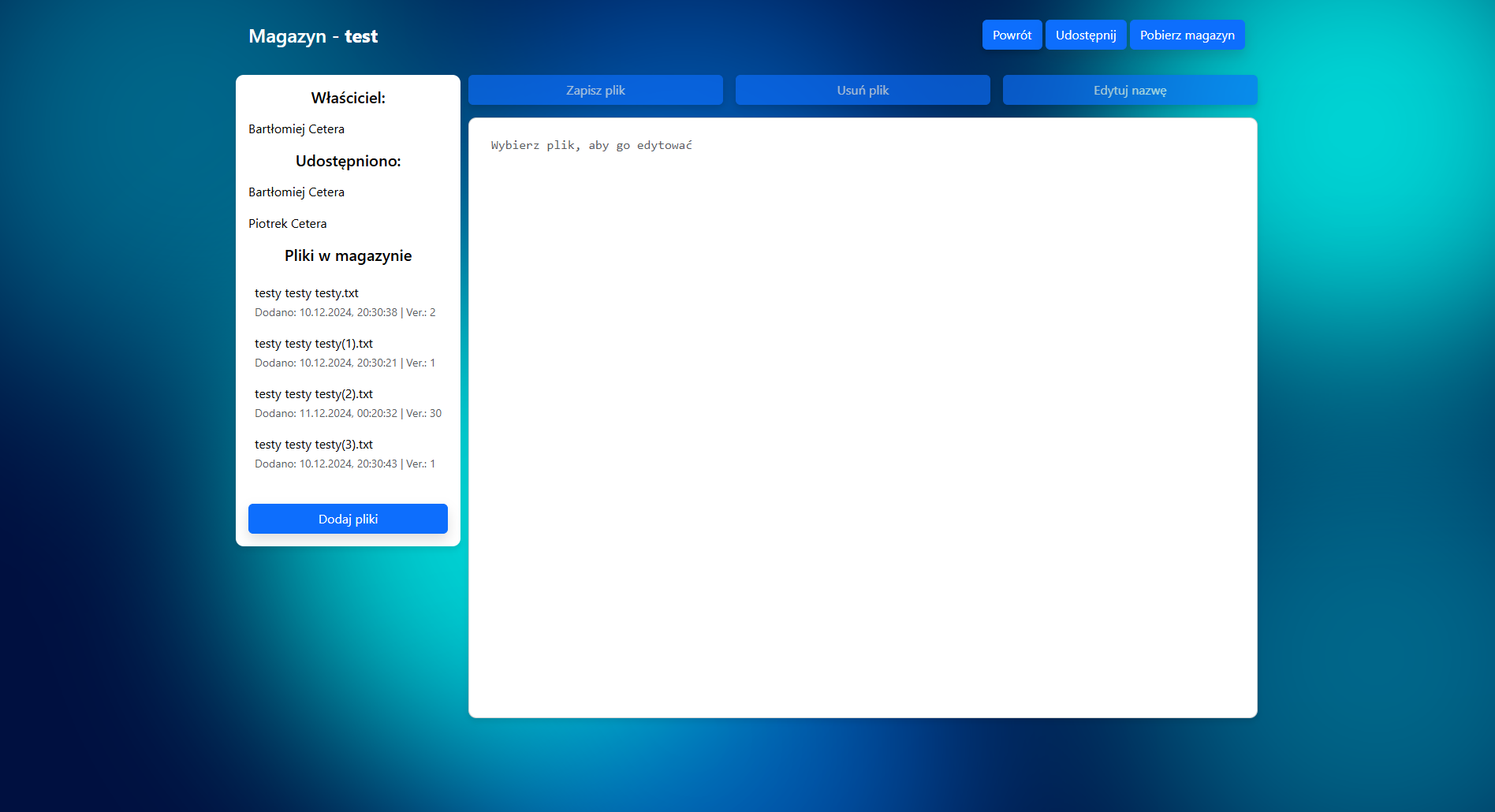
## 5.4. SYSTEM MAGAZYNÓW

System magazynów w aplikacji sDrive został zaimplementowany jako przestrzeń dedykowana do przechowywania plików oraz wspólnej pracy użytkowników. Umożliwia tworzenie nowych magazynów oraz zarządzanie nimi, w tym usuwanie, zmianę nazwy czy przypisywanie innych użytkowników do współpracy. W ramach magazynu można dodawać pliki, edytować je oraz korzystać z mechanizmu kontroli wersji, który zapewnia spójność danych. W przypadku wystąpienia konfliktu wersji użytkownik ma możliwość jego rozwiązania poprzez dedykowaną stronę, gdzie wyświetlane są szczegóły problemu. Dodatkowo magazyny mogą być pobierane w całości w formie archiwum ZIP. Rysunki 18–20 wizualizują implementację kluczowych funkcjonalności systemu magazynów, takich jak tworzenie przestrzeni przechowywania, zarządzanie zawartością, rozwiązywanie konfliktów wersji oraz wspólna praca użytkowników.



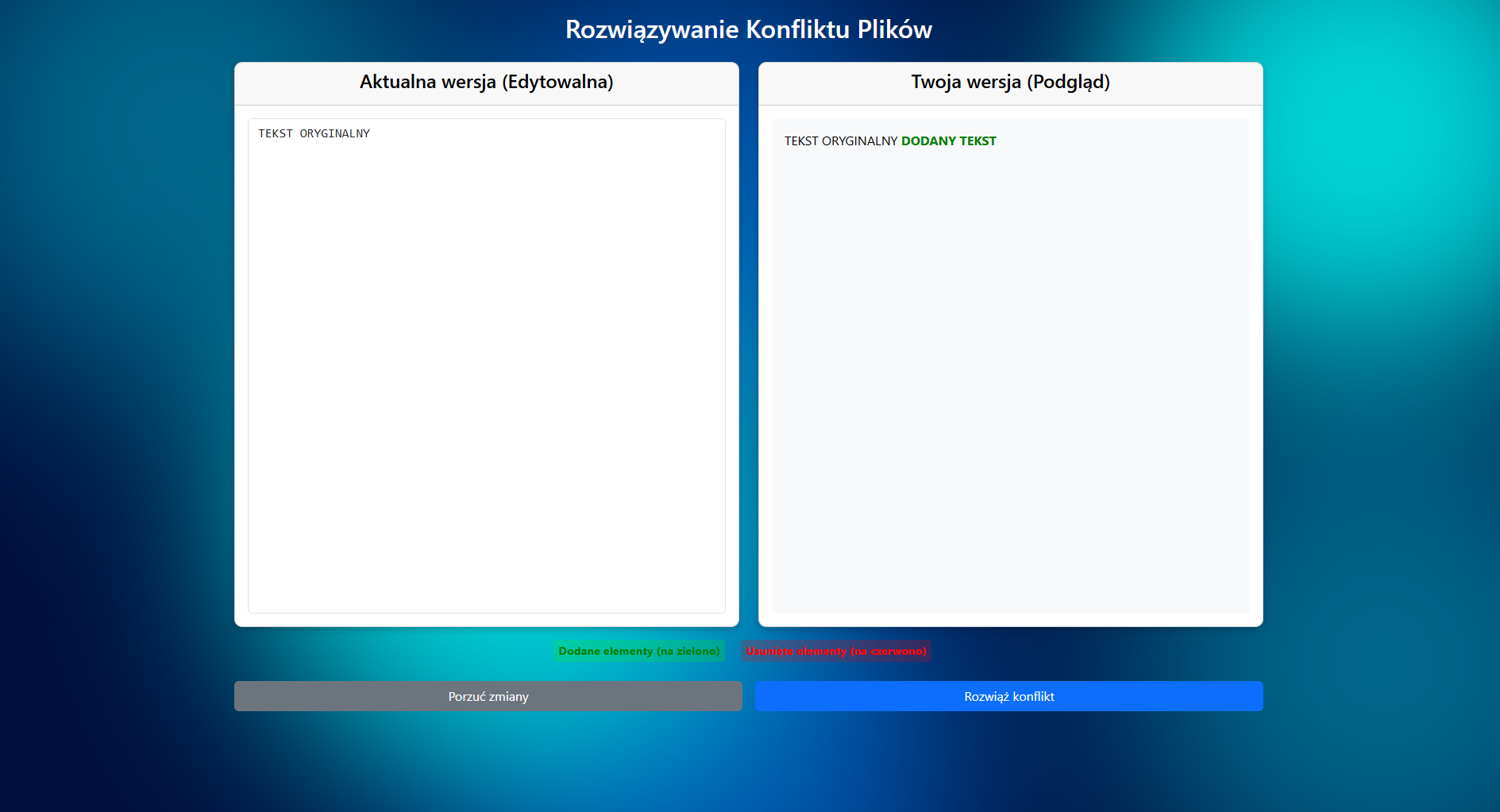
Rysunek 18. System magazynów - tworzenie magazynu

[źródło: Opracowanie własne]



Rysunek 19. System magazynów – magazyn

[źródło: Opracowanie własne]



Rysunek 20. System magazynów - rozwiązywanie konfliktu w magazynie

[źródło: Opracowanie własne]

Listing 08 przedstawia funkcję saveResolvedFileContent, która zapisuje rozwiązaną zawartość pliku i aktualizuje jego wersję w systemie magazynów. Funkcja pobiera dane, takie jak zaszyfrowana nazwa pliku, identyfikator magazynu, identyfikator użytkownika i nową zawartość pliku, po czym weryfikuje ich obecność oraz istnienie ścieżki zapisu na serwerze. Następnie sprawdza w bazie danych, czy plik istnieje, i pobiera jego bieżącą wersję. Jeśli plik istnieje, jego zawartość jest nadpisywana, a wersja zwiększana o jeden. Aktualizacja wersji   
i daty modyfikacji zapisywana jest w bazie danych. W przypadku sukcesu funkcja zwraca komunikat z potwierdzeniem i nową wersją pliku. W razie błędów, takich jak brak danych, problem z bazą lub zapisem pliku, funkcja zwraca odpowiednie komunikaty błędów,   
a logowanie szczegółów wspiera debugowanie procesu.

1. const saveResolvedFileContent = (req, res) => {
2. const cryptedName = req.params.fileId;
3. const storageId = req.query.storageId;
4. const safeId = req.user.safeid\_users;
5. const { content } = req.body;
6. console.log('DEBUG: Rozpoczęcie zapisu rozwiązanej zawartości pliku.');
7. console.log(`DEBUG: fileId: ${cryptedName}`);
8. console.log(`DEBUG: storageId: ${storageId}`);
9. console.log(`DEBUG: safeId: ${safeId}`);
10. console.log(`DEBUG: Długość zawartości: ${content ? content.length : 'brak zawartości'}`);
11. if (!cryptedName || !storageId || !content) {
12. console.error('DEBUG: Brak wymaganych danych');
13. return res.status(400).json({ status: 'error', error: 'Brak wymaganych danych' });
14. }
15. const filePath = path.join(\_\_dirname, '..', 'data', 'storages', safeId, storageId, cryptedName);
16. console.log(`DEBUG: Ścieżka do pliku: ${filePath}`);
17. const dirPath = path.dirname(filePath);
18. if (!fs.existsSync(dirPath)) {
19. console.error(`DEBUG: Katalog nie istnieje: ${dirPath}`);
20. return res.status(500).json({ status: 'error', error: 'Ścieżka do zapisu pliku nie istnieje.' });
21. }
22. dbFiles.query(
23. `SELECT f.id\_files, sf.file\_version\_storages\_files
24. FROM storages\_files sf
25. JOIN files f ON sf.id\_files = f.id\_files
26. WHERE f.cryptedname\_files = ? AND sf.id\_storages = ?`,
27. [cryptedName, storageId],
28. (err, results) => {
29. if (err) {
30. console.error(`DEBUG: Błąd podczas pobierania pliku: ${err.message}`);
31. return res.status(500).json({ status: 'error', error: 'Błąd podczas wyszukiwania pliku.' });
32. }
33. if (results.length === 0) {
34. console.error('DEBUG: Plik nie został znaleziony.');
35. return res.status(404).json({ status: 'error', error: 'Plik nie został znaleziony.' });
36. }
37. const fileId = results[0].id\_files;
38. const currentVersion = results[0].file\_version\_storages\_files || 1;
39. const newVersion = currentVersion + 1;
40. fs.writeFile(filePath, content, 'utf8', (err) => {
41. if (err) {
42. console.error(`DEBUG: Błąd zapisu pliku: ${err.message}`);
43. return res.status(500).json({ status: 'error', error: 'Błąd podczas zapisywania pliku.' });
44. }
45. console.log(`DEBUG: Plik zapisany pomyślnie: ${filePath}`);
46. dbFiles.query(
47. `UPDATE storages\_files
48. SET file\_version\_storages\_files = ?, date\_storages\_file = NOW()
49. WHERE id\_storages = ? AND id\_files = ?`,
50. [newVersion, storageId, fileId],
51. (updateErr) => {
52. if (updateErr) {
53. console.error(`DEBUG: Błąd podczas aktualizacji wersji pliku: ${updateErr.message}`);
54. return res.status(500).json({ status: 'error', error: 'Błąd podczas aktualizacji wersji pliku.' });
55. }
56. console.log(`DEBUG: Wersja pliku zaktualizowana do Ver. ${newVersion}`);
57. res.json({ status: 'success', message: `Plik zapisany pomyślnie. Aktualna wersja: Ver. ${newVersion}` });

Listing 8. System magazynów - rozwiązywanie konfliktu plikow

[źródło: Opracowanie własne]

Listing 9 przedstawia funkcję saveConflictedFile, która obsługuje sytuacje konfliktu plików w systemie, tworząc oddzielne kopie aktualnej wersji pliku oraz zmian wprowadzonych przez użytkownika. Na początku pobierane są wymagane dane, takie jak zaszyfrowana nazwa pliku (cryptedName), identyfikator magazynu (storageId), identyfikator użytkownika (safeId) oraz treść zmian. Funkcja weryfikuje, czy wszystkie niezbędne dane zostały przesłane,   
a następnie określa ścieżkę do oryginalnego pliku na serwerze oraz do katalogu tymczasowego, w którym będą przechowywane pliki konfliktowe. Jeśli katalog tymczasowy nie istnieje, zostaje on utworzony. Następnie funkcja sprawdza, czy oryginalny plik znajduje   
się na serwerze. Jeśli plik istnieje, jego kopia zostaje zapisana w katalogu tymczasowym. Równocześnie zmiany wprowadzone przez użytkownika są zapisywane jako osobny plik w tym samym katalogu, z dopiskiem \_tmp w nazwie. Na koniec funkcja zwraca komunikat   
o powodzeniu wraz ze ścieżkami do obu plików konfliktowych. W przypadku błędów, takich jak problem z dostępem do pliku lub operacjami na systemie plików, funkcja zwraca odpowiedni komunikat o błędzie i loguje szczegóły do debugowania.

1. const saveConflictedFile = (req, res) => {
2. const cryptedName = req.query.fileId;
3. const storageId = req.query.storageId;
4. const safeId = req.user.safeid\_users;
5. const { content } = req.body;
6. console.log('DEBUG: Rozpoczęcie obsługi konfliktu pliku.');
7. console.log(`DEBUG: fileId: ${cryptedName}`);
8. console.log(`DEBUG: storageId: ${storageId}`);
9. console.log(`DEBUG: safeId: ${safeId}`);
10. console.log(`DEBUG: Długość zawartości: ${content ? content.length : 'brak zawartości'}`);
11. if (!cryptedName || !storageId || !content) {
12. console.error('DEBUG: Brak wymaganych danych');
13. return res.status(400).json({ status: 'error', error: 'Brak wymaganych danych' });
14. }
15. const filePath = path.join(\_\_dirname, '..', 'data', 'storages', safeId, storageId, cryptedName);
16. const tempDir = path.join(\_\_dirname, '..', 'data', 'temp');
17. if (!fs.existsSync(tempDir)) {
18. fs.mkdirSync(tempDir);
19. }
20. const tempFilePath = path.join(tempDir, cryptedName);
21. const tempFilePathTmp = path.join(
22. tempDir,
23. `${path.basename(cryptedName, path.extname(cryptedName))}\_tmp${path.extname(cryptedName)}`
24. );
25. try {
26. if (fs.existsSync(filePath)) {
27. fs.copyFileSync(filePath, tempFilePath);
28. console.log(`DEBUG: Utworzono kopię pliku z serwera: ${tempFilePath}`);
29. } else {
30. console.warn(`DEBUG: Plik z serwera nie istnieje: ${filePath}`);
31. }
32. fs.writeFileSync(tempFilePathTmp, content, 'utf8');
33. console.log(`DEBUG: Utworzono kopię zmian użytkownika: ${tempFilePathTmp}`);
34. res.json({
35. status: 'success',
36. message: 'Pliki konfliktowe zostały utworzone.',
37. tempFilePath,
38. tempFilePathTmp,
39. });
40. } catch (err) {
41. console.error('DEBUG: Błąd podczas obsługi konfliktu pliku:', err);
42. res.status(500).json({ status: 'error', error: 'Wystąpił błąd podczas obsługi konfliktu pliku.' });

Listing 9. System magazynów - obsługa konfliktu w magazynie

[źródło: Opracowanie własne]

Listing 10 przedstawia funkcję addFilesToStorage, która odpowiada za dodawanie wybranych plików użytkownika do określonego magazynu danych. Na początku pobierane   
są informacje o identyfikatorze magazynu (storageId), identyfikatorze użytkownika (safeId) oraz liście wybranych plików (selectedFiles). Funkcja sprawdza, czy wszystkie wymagane dane zostały przekazane i czy magazyn istnieje na serwerze. Następnie wykonuje zapytanie   
do bazy danych, aby zweryfikować, czy pliki należą do użytkownika i nie zostały usunięte.   
Dla każdego pliku funkcja sprawdza unikalność nazwy w obrębie magazynu, a w przypadku konfliktu modyfikuje nazwę pliku, dodając odpowiedni sufiks. Pliki są następnie kopiowane do katalogu magazynuz nadaniem nowej zaszyfrowanej nazwy, a informacje o plikach   
są zapisywane w bazie danych w tabelach files i storages\_files. Funkcja zapewnia obsługę błędów na każdym etapie procesu, takich jak problemy z dostępem do plików czy konflikty nazw, a w przypadku powodzenia zwraca komunikat potwierdzający dodanie plików   
do magazynu. Dzięki szczegółowemu logowaniu debugowania administratorzy mogą łatwo monitorować i rozwiązywać ewentualne problemy.

1. const addFilesToStorage = async (req, res) => {
2. const { storageId } = req.params;
3. const safeId = req.user.safeid\_users;
4. const { selectedFiles } = req.body;
5. console.log(`DEBUG: Rozpoczęcie dodawania plików do magazynu. storageId: ${storageId}, safeId: ${safeId}`);
6. console.log(`DEBUG: Wybrane pliki: ${selectedFiles.join(', ')}`);
7. if (!selectedFiles || !Array.isArray(selectedFiles) || selectedFiles.length === 0) {
8. return res.status(400).json({ status: 'error', error: 'Brak wybranych plików do dodania.' });
9. }
10. const storagePath = path.join(\_\_dirname, '..', 'data', 'storages', safeId, storageId);
11. if (!fs.existsSync(storagePath)) {
12. return res.status(404).json({ status: 'error', error: 'Magazyn nie istnieje.' });
13. }
14. try {
15. const files = await new Promise((resolve, reject) => {
16. dbFiles.query(
17. 'SELECT \* FROM files WHERE originalname\_files IN (?) AND cryptedowner\_files = ? AND delete\_files = 0',
18. [selectedFiles, safeId],
19. (err, results) => {
20. if (err) {
21. return reject(err);
22. }
23. resolve(results);
24. }
25. );
26. });

Listing 10. System magazynów - dodawanie pliku do magazynu 1/3

[źródło: Opracowanie własne]

1. const currentDate = new Date();
2. const storageFilesValues = [];
3. for (const file of files) {
4. const sourcePath = path.join(\_\_dirname, '..', 'data', 'users', safeId, file.cryptedname\_files);
5. let newOriginalName = file.originalname\_files;
6. const fileExtension = path.extname(file.originalname\_files);
7. const fileBaseName = path.basename(file.originalname\_files, fileExtension);
8. let suffix = 0;
9. let isOriginalNameUnique = false;
10. while (!isOriginalNameUnique) {
11. const conflictingFiles = await new Promise((resolve, reject) => {
12. dbFiles.query(
13. `SELECT f.originalname\_files
14. FROM storages\_files sf
15. JOIN files f ON sf.id\_files = f.id\_files
16. WHERE sf.id\_storages = ? AND f.originalname\_files = ? AND sf.active\_storages\_files = 1`,
17. [storageId, newOriginalName],
18. (err, results) => {
19. if (err) {
20. return reject(err);
21. }
22. resolve(results);  });});
23. if (conflictingFiles.length > 0) {
24. suffix++;
25. newOriginalName = `${fileBaseName}(${suffix})${fileExtension}`;
26. } else {
27. isOriginalNameUnique = true;
28. }
29. }
30. if (fs.existsSync(sourcePath)) {
31. const newCryptedName = `${crypto.randomBytes(16).toString('hex')}${fileExtension}`;
32. const destPath = path.join(storagePath, newCryptedName);
33. fs.copyFileSync(sourcePath, destPath);
34. console.log(`DEBUG: Skopiowano plik: ${file.cryptedname\_files} -> ${destPath}`);
35. const newFileId = await new Promise((resolve, reject) => {
36. dbFiles.query(
37. `INSERT INTO files (originalname\_files, cryptedname\_files, cryptedowner\_files, filetype\_files, delete\_files, dateofupload\_files, origin\_file, oldcryptedname\_file)
38. VALUES (?, ?, ?, ?, 0, ?, ?, ?)`,
39. [ newOriginalName,
40. newCryptedName,
41. safeId,
42. file.filetype\_files,
43. currentDate,
44. 'storage',
45. file.cryptedname\_files, ],
46. (err, result) => {
47. if (err) {
48. return reject(err);
49. }
50. resolve(result.insertId);}); });
51. storageFilesValues.push([
52. storageId,
53. newFileId,
54. currentDate,
55. 1,
56. safeId,
57. 1,
58. ]);

Listing 10. System magazynów - dodawanie pliku do magazynu 2/3

[źródło: Opracowanie własne]

1. } else {
2. console.warn(`DEBUG: Plik nie istnieje: ${sourcePath}`);
3. }
4. }
5. if (storageFilesValues.length > 0) {
6. await new Promise((resolve, reject) => {
7. dbFiles.query(
8. 'INSERT INTO storages\_files (id\_storages, id\_files, date\_storages\_file, active\_storages\_files, modificator\_storages\_files, file\_version\_storages\_files) VALUES ?',
9. [storageFilesValues],
10. (err) => {
11. if (err) {
12. return reject(err);
13. }
14. resolve();
15. }
16. );
17. });
18. }
19. console.log('DEBUG: Pliki zostały pomyślnie dodane do magazynu.');
20. res.json({ status: 'success', message: 'Pliki zostały dodane do magazynu.' });
21. } catch (err) {
22. console.error(`DEBUG: Błąd podczas dodawania plików do magazynu: ${err.message}`);
23. res.status(500).json({ status: 'error', error: 'Błąd podczas dodawania plików do magazynu.' });
24. }

Listing 10. System magazynów - dodawanie pliku do magazynu 3/3

[źródło: Opracowanie własne]

Listing 11 przedstawia funkcję saveFileStorageContent, która zajmuje się zapisywaniem zawartości pliku w magazynie danych i aktualizacją jego wersji. Na początku pobierane   
są kluczowe dane, takie jak zaszyfrowana nazwa pliku (cryptedName), identyfikator magazynu (storageId), identyfikator użytkownika (safeId) oraz nowa zawartość pliku i jego aktualna wersja. Funkcja sprawdza, czy wszystkie wymagane dane zostały przekazane, a także weryfikuje, czy ścieżka do magazynu istnieje na serwerze. Następnie system wykonuje zapytania do bazy danych, aby zweryfikować, czy plik istnieje w tabelach files i storages\_files. Po uzyskaniu informacji o wersji pliku zapisanej w bazie danych (dbVersion), następuje porównanie z wersją przesłaną w żądaniu (currentVersion). Jeśli wersje się różnią, funkcja zgłasza konflikt wersji i odrzuca żądanie z odpowiednim komunikatem błędu. W przypadku zgodności wersji zawartość pliku zostaje zapisana na serwerze, a wersja pliku w tabeli storages\_files jest zwiększana o jeden. Po pomyślnym zakończeniu operacji funkcja zwraca odpowiedź potwierdzającą zapis pliku oraz aktualną wersję. Jeśli w dowolnym etapie wystąpią błędy, takie jak problem z dostępem do pliku, zapisaniem zawartości czy aktualizacją wersji, funkcja zwraca odpowiedni komunikat błędu z kodem statusu. Debugowanie funkcji jest wspierane przez szczegółowe logowanie, co ułatwia rozwiązywanie potencjalnych problemów.

1. const saveFileStorageContent = (req, res) => {
2. const cryptedName = req.params.fileId; // cryptedname\_files
3. const storageId = req.query.storageId;
4. const safeId = req.user.safeid\_users;
5. const { content, currentVersion } = req.body; // Pobieramy wersję z przekazanych danych
6. console.log('DEBUG: Rozpoczęcie zapisu pliku do magazynu.');
7. console.log(`DEBUG: fileId: ${cryptedName}`);
8. console.log(`DEBUG: storageId: ${storageId}`);
9. console.log(`DEBUG: safeId: ${safeId}`);
10. console.log(`DEBUG: Aktualna wersja: ${currentVersion}`);
11. console.log(`DEBUG: Długość zawartości: ${content ? content.length : 'brak zawartości'}`);
12. if (!cryptedName || !storageId || !content) {
13. console.error('DEBUG: Błąd - Brak wymaganych danych');
14. return res.status(400).json({ status: 'error', error: 'Brak wymaganych danych' });
15. }
16. const filePath = path.join(\_\_dirname, '..', 'data', 'storages', safeId, storageId, cryptedName);
17. console.log(`DEBUG: Ścieżka do pliku: ${filePath}`);
18. const dirPath = path.dirname(filePath);
19. if (!fs.existsSync(dirPath)) {
20. console.error(`DEBUG: Katalog nie istnieje: ${dirPath}`);
21. return res.status(500).json({ status: 'error', error: 'Ścieżka do zapisu pliku nie istnieje.' });
22. }
23. // Znajdź `id\_files` na podstawie `cryptedname\_files`
24. dbFiles.query(
25. `SELECT id\_files FROM files WHERE cryptedname\_files = ?`,
26. [cryptedName],
27. (err, fileResults) => {
28. if (err) {
29. console.error(`DEBUG: Błąd podczas pobierania id\_files: ${err.message}`);
30. return res.status(500).json({ status: 'error', error: 'Błąd podczas wyszukiwania pliku.' });
31. }
32. if (fileResults.length === 0) {
33. console.error('DEBUG: Plik nie został znaleziony w tabeli `files`.');
34. return res.status(404).json({ status: 'error', error: 'Plik nie został znaleziony.' });
35. }
36. const fileId = fileResults[0].id\_files;
37. console.log(`DEBUG: Znaleziono id\_files: ${fileId}`);
38. // Pobierz wersję pliku z tabeli `storages\_files`
39. dbFiles.query(
40. `SELECT file\_version\_storages\_files
41. FROM storages\_files
42. WHERE id\_storages = ? AND id\_files = ? AND active\_storages\_files = 1`,
43. [storageId, fileId],
44. (err, results) => {
45. if (err) {
46. console.error(`DEBUG: Błąd podczas pobierania wersji pliku: ${err.message}`);
47. return res.status(500).json({ status: 'error', error: 'Błąd podczas pobierania wersji pliku.' });
48. }
49. if (results.length === 0) {
50. console.error('DEBUG: Plik nie został znaleziony w tabeli `storages\_files`.');
51. return res.status(404).json({ status: 'error', error: 'Plik nie został znaleziony w magazynie.' });
52. }

Listing 11**.** System magazynów - zapis zawartości pliku w magazynie 1/2

[źródło: Opracowanie własne]

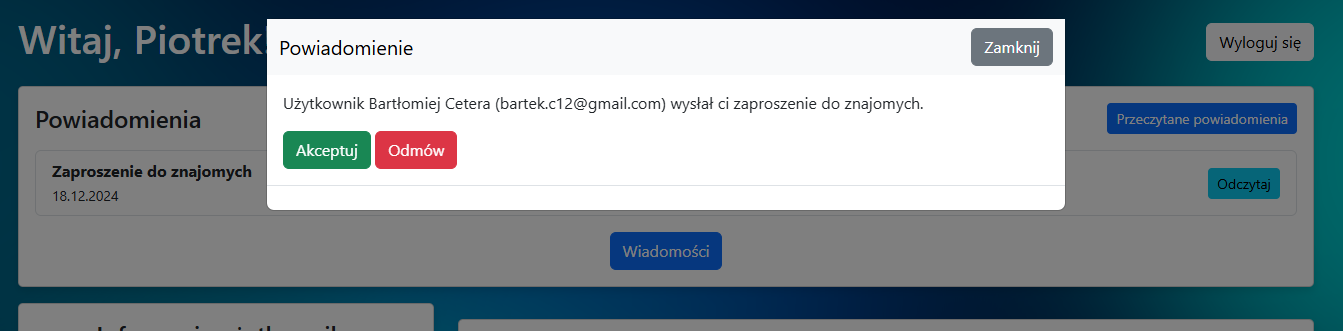
1. const dbVersion = results[0].file\_version\_storages\_files || 1; // Domyślnie 1, jeśli brak wersji
2. console.log(`DEBUG: Wersja pliku w bazie danych: Ver. ${dbVersion}`);
3. // Porównanie wersji
4. if (dbVersion !== currentVersion) {
5. console.error(
6. `DEBUG: Konflikt wersji pliku. Wersja w bazie: ${dbVersion}, przesłana wersja: ${currentVersion}`
7. );
8. return res.status(409).json({
9. status: 'error',
10. error: `Konflikt wersji pliku. Oczekiwana wersja: Ver. ${dbVersion}`,
11. });
12. }
13. // Zapisanie pliku na dysku
14. fs.writeFile(filePath, content, 'utf8', (err) => {
15. if (err) {
16. console.error(`DEBUG: Błąd zapisu pliku: ${err.message}`);
17. return res.status(500).json({ status: 'error', error: 'Błąd podczas zapisywania pliku.' });
18. }
19. console.log(`DEBUG: Plik zapisany pomyślnie: ${filePath}`);
20. // Zwiększenie wersji pliku
21. const newVersion = dbVersion + 1;
22. dbFiles.query(
23. `UPDATE storages\_files
24. SET file\_version\_storages\_files = ?, date\_storages\_file = NOW()
25. WHERE id\_storages = ? AND id\_files = ?`,
26. [newVersion, storageId, fileId],
27. (updateErr) => {
28. if (updateErr) {
29. console.error(`DEBUG: Błąd podczas aktualizacji wersji pliku: ${updateErr.message}`);
30. return res.status(500).json({ status: 'error', error: 'Błąd podczas aktualizacji wersji pliku.' });
31. }
32. console.log(`DEBUG: Wersja pliku zaktualizowana do Ver. ${newVersion}`);
33. res.json({ status: 'success', message: `Plik został zapisany pomyślnie. Aktualna wersja: Ver. ${newVersion}` });

Listing 11**.** System magazynów - zapis zawartości pliku w magazynie 2/2

[źródło: Opracowanie własne]

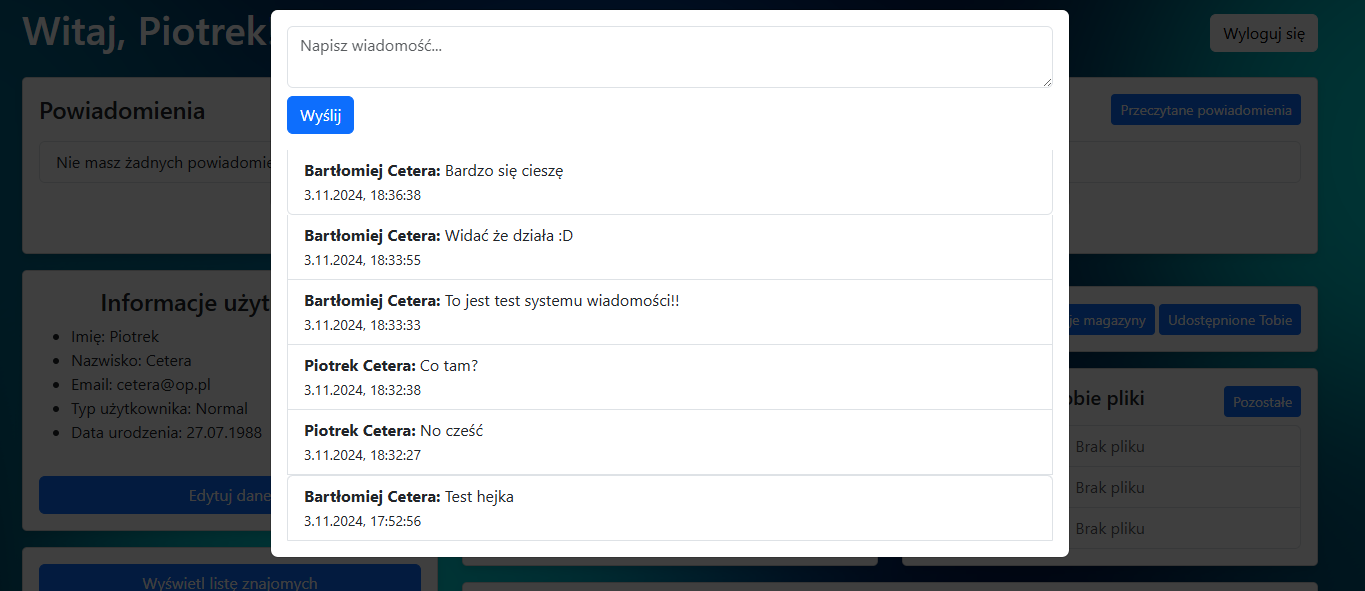
## 5.7. SYSTEM POWIADOMIEŃ I WIADOMOŚCI

System powiadomień i wiadomości w aplikacji sDrive został zaimplementowany jako element wspierający interakcje między użytkownikami oraz informowanie o istotnych zdarzeniach w systemie. W sekcji powiadomień użytkownik otrzymuje automatyczne komunikaty o zdarzeniach, takich jak nowe wiadomości, akceptacje zaproszeń od znajomych, udostępnienia plików czy aktualizacje w magazynach. Powiadomienia te są prezentowane w uporządkowanej formie, a użytkownik ma możliwość przeglądania zarówno nowych,   
jak i wcześniej odczytanych komunikatów. Dodatkowo w ramach tej sekcji dostępny jest moduł wiadomości, który umożliwia użytkownikom przesyłanie i odbieranie wiadomości. Każda konwersacja zawiera pełną histori. Rysunki 21 i 22 ilustrują implementację systemu powiadomień i wiadomości, przedstawiając kluczowe funkcjonalności, takie jak zarządzanie powiadomieniami oraz przesyłanie wiadomości między użytkownikami.



Rysunek 21. System powiadomień i wiadomości - podgląd powiadomienia

[źródło: Opracowanie własne]



Rysunek 22. System powiadomień i wiadomości – konwersacja

[źródło: Opracowanie własne]

Listing 12 przedstawia fragment kodu, który zawiera trzy funkcje obsługujące powiadomienia w systemie. Pierwsza z nich, getNotification, umożliwia pobranie szczegółowych informacji o konkretnym powiadomieniu na podstawie jego identyfikatora (notificationId). Wykonywane jest zapytanie do bazy danych, aby uzyskać dane takie jak tytuł, treść, nadawca, identyfikator notyfikacji oraz typ powiadomienia. Jeśli powiadomienie istnieje, zwracane są jego szczegóły w odpowiedzi JSON. W przeciwnym wypadku funkcja zwraca komunikat o błędzie. Druga funkcja, markNotificationAsRead, służy do oznaczania konkretnego powiadomienia jako przeczytane. Na podstawie identyfikatora powiadomienia (notificationId) wykonywane jest zapytanie aktualizujące w bazie danych pole status\_notifications, zmieniając jego wartość na „read”. W przypadku powodzenia funkcja zwraca komunikat o sukcesie, a w razie błędów zwraca odpowiedni komunikat o błędzie. Trzecia funkcja, getReadNotifications, pozwala na pobranie listy wszystkich przeczytanych powiadomień dla danego użytkownika. Na podstawie identyfikatora użytkownika (safeId) system wyszukuje w bazie danych powiadomienia oznaczone jako „read” i zwraca ich listę   
w odpowiedzi JSON, zawierając szczegóły takie jak tytuł, treść i data. W razie błędów funkcja zwraca komunikat o błędzie z kodem statusu 500. Kod ten umożliwia zarządzanie powiadomieniami w sposób przejrzysty i efektywny, a dzięki zastosowaniu odpowiednich zapytań SQL zapewnia spójność danych w systemie.

1. const getNotification = (req, res) => {
2. const notificationId = req.params.id;
3. dbLogins.query(
4. 'SELECT head\_notifications, msg\_notifications, dispatcher\_notifications, noteid\_notifications, type\_notifications FROM notifications WHERE id\_notifications = ?',
5. [notificationId],
6. (err, result) => {
7. if (err) {
8. return res.json({ status: 'error', error: 'Błąd pobierania powiadomienia' });
9. }
10. if (result.length === 0) {
11. return res.json({ status: 'error', error: 'Powiadomienie nie istnieje' });
12. }
13. res.json({ status: 'success', notification: result[0] });
14. });};
15. // Nowa funkcja do aktualizacji statusu powiadomienia na "read"
16. const markNotificationAsRead = (req, res) => {
17. const notificationId = req.params.id;
18. dbLogins.query(
19. 'UPDATE notifications SET status\_notifications = "read" WHERE id\_notifications = ?',
20. [notificationId],
21. (err, result) => {
22. if (err) {
23. return res.json({ status: 'error', error: 'Błąd podczas oznaczania powiadomienia jako przeczytane' });}
24. return res.json({ status: 'success', success: 'Powiadomienie zostało oznaczone jako przeczytane' });
25. });};
26. const getReadNotifications = (req, res) => {
27. const safeId = req.user.safeid\_users;
28. dbLogins.query(
29. 'SELECT id\_notifications, head\_notifications, msg\_notifications, date\_notifications FROM notifications WHERE user\_notifications = ? AND status\_notifications = "read"',
30. [safeId],
31. (err, results) => {
32. if (err) {
33. console.error("Błąd podczas pobierania przeczytanych powiadomień:", err);
34. return res.status(500).json({ status: "error", error: "Błąd podczas pobierania przeczytanych powiadomień" });}
35. res.json({ status: "success", notifications: results });

Listing 12. System powiadomień i wiadomości **–** powiadomienia

[źródło: Opracowanie własne]

# 6. PODSUMOWANIE

W ramach pracy inżynierskiej zrealizowano projekt aplikacji webowej, który pozwolił osiągnąć wszystkie cele wyznaczone w sekcji "Cel i zakres". Zrealizowana aplikacja spełnia funkcjonalne i technologiczne założenia, stanowiąc bezpieczne i nowoczesne narzędzie   
do przechowywania i zarządzania danymi, jednocześnie ułatwiając współpracę pomiędzy użytkownikami. Jednym z najważniejszych osiągnięć projektu było wdrożenie zaawansowanego szyfrowania danych, które zapewnia pełną ochronę informacji nawet   
w sytuacji potencjalnego naruszenia serwera. Kolejnym kluczowym aspektem była integracja funkcji współdzielenia zasobów, w tym przestrzeni magazynów, umożliwiających wspólne zarządzanie plikami, co w połączeniu z systemem kontroli wersji stanowi odpowiedź   
na rosnące zapotrzebowanie na efektywne narzędzia współpracy. Uzupełnieniem tych funkcjonalności było stworzenie modułu zarządzania znajomymi oraz systemu powiadomień, które wspierają interakcje między użytkownikami i pozwalają na budowanie cyfrowych społeczności wokół aplikacji. Pomimo osiągnięcia wszystkich założonych celów, projekt wyznaczył również obszary, które mogą posłużyć do przyszłego rozwoju aplikacji w celu stworzenia produktu gotowego na wprowadzenie na rynek. Jednym z takich aspektów jest dalsze ulepszenie interfejsu użytkownika poprzez zastosowanie nowoczesnego frameworka   
do tworzenia bardziej responsywnego i intuicyjnego UI, co poprawiłoby komfort użytkowania na różnych urządzeniach. Kolejnym kierunkiem rozwoju jest rozbudowa systemu powiadomień, który mógłby zostać wzbogacony o bardziej zaawansowane opcje, takie jak spersonalizowane alerty, integracja z kalendarzem czy możliwość konfiguracji preferencji użytkownika. Rozszerzenie funkcji edycji plików bezpośrednio w przeglądarce również stanowi istotny potencjał rozwojowy. Wreszcie, stworzenie dedykowanego komponentu mobilnego jest kluczowym krokiem w kierunku pełnego dostosowania systemu   
do współczesnych potrzeb użytkowników. Podsumowując, realizacja projektu była nie tylko potwierdzeniem możliwości osiągnięcia wszystkich założonych celów, ale także stanowiła solidny fundament dla dalszego rozwoju aplikacji. Zrealizowany system łączy w sobie zaawansowane rozwiązania technologiczne z dbałością o potrzeby użytkowników,   
a wyznaczone kierunki rozwoju umożliwiają dalsze doskonalenie aplikacji, tak aby stała   
się ona produktem w pełni gotowym na konkurencję z istniejącymi rozwiązaniami na rynku, jednocześnie oferując unikalne korzyści związane z bezpieczeństwem, prywatnością   
i współpracą w środowisku cyfrowym.

# 7. BIBLIOGRAFIA

Strony internetowe

* Scroll - Chmura internetowa 2021: https://scroll.morele.net/poradniki/chmura-internetowa-co-to-jest-jak-dziala-i-jak-jej-uzywac-przechowywanie-danych-w-chmurze-poradnik/, Data odczytu: 05.11.2024
* AppsOnHMS 2022: https://appsonhms.com/pl/articles/362/przechowywanie-danych-w-chmurze-jak-to-dziala/, Data odczytu: 05.11.2024
* TeleTropiciel 2022: https://teletropiciel.pl/chmura-co-to/, Data odczytu: 07.11.2024
* 360money 2024: https://www.360money.pl/czy-trzymanie-plikow-w-chmurze-jest-bezpieczne/, Data odczytu: 07.11.2024
* Bitdefender 2025: https://bitdefender.pl/bezpieczne-korzystanie-z-chmury/, Data odczytu: 03.01.2025
* Wikipedia – Dysk Google 2024: https://pl.wikipedia.org/wiki/Dysk\_Google, Data odczytu: 08.11.2024
* Scroll - Dysk Google 2021: https://scroll.morele.net/poradniki/dysk-google-jak-dziala-i-czy-warto-z-niego-korzystac-najlepsze-funkcje-google-drive/, Data odczytu: 08.11.2024
* CodziennyEkspert 2023: https://codziennyekspert.pl/co-to-jest-dropbox-i-do-czego-sluzy/, Data odczytu: 11.11.2024
* Wikipedia - Dropbox 2024: https://pl.wikipedia.org/wiki/Dropbox, Data odczytu: 11.11.2024
* Komputer Świat 2022: https://www.komputerswiat.pl/poradniki/jak-to-dziala/microsoft-onedrive-co-to-jest-i-jak-na-nim-pracowac/9vg56n9, Data odczytu: 11.11.2024
* Wikipedia - OneDrive 2024: https://pl.wikipedia.org/wiki/OneDrive, Data odczytu: 20.11.2024
* Fotc 2022: https://fotc.com/pl/blog/microsoft-onedrive-vs-google-drive/, Data odczytu: 20.11.2024
* Futurebeat 2023: https://futurebeat.pl/newsroom/pliki-z-dysku-google-znikaja-na-niektorych-komputerach-z-windowse/z7277a6, Data odczytu: 20.11.2024
* Youtube - Mateusz Chrobok 2024: https://www.youtube.com/@MateuszChrobok - Mateusz Chrobok, Data odczytu: 20.11.2024
* Wikipedia - JavaScript 2024: https://pl.wikipedia.org/wiki/JavaScript, Data odczytu: 22.11.2024
* Justgeekit - JavaScript 2021: https://justjoin.it/blog/wszystko-co-musicie-wiedziec-o-javascript-co-to-dla-kogo-i-ile-zarobimy, Data odczytu: 22.11.2024
* Justgeekit - node.js 2021: https://justjoin.it/blog/pierwsze-kroki-w-node-js, Data odczytu: 22.11.2024
* Wikipedia - node.js 2024: https://pl.wikipedia.org/wiki/Node.js, Data odczytu: 22.11.2024
* Aviary 2023: https://aviary.pl/express-js/, Data odczytu: 22.11.2024
* Wikipedia - express.js 2024: https://en.wikipedia.org/wiki/Expressjs, Data odczytu: 22.11.2024
* Wikipedia - JWT 2024: https://pl.wikipedia.org/wiki/JSON\_Web\_Token, Data odczytu: 22.11.2024
* devszczepaniak 2023: https://devszczepaniak.pl/json-web-token/, Data odczytu: 22.11.2024
* Wikipedia - mysql 2024: https://pl.wikipedia.org/wiki/MySQL, Data odczytu: 22.11.2024
* Oracle 2024: https://www.oracle.com/pl/mysql/what-is-mysql/, Data odczytu: 22.11.2024
* Wikipedia - AES 2024: https://pl.wikipedia.org/wiki/Advanced\_Encryption\_Standard, Data odczytu: 22.11.2024
* Webporadnik 2025: https://webporadnik.pl/algorytm-szyfrowania-aes-advanced-encryption-standard/, Data odczytu: 22.11.2024
* Wikipedia - Google Authentyicator 2024: https://pl.wikipedia.org/wiki/Google\_Authenticator, Data odczytu: 22.11.2024
* Nano.komputronik 2023: https://nano.komputronik.pl/n/co-to-jest-google-authenticator-jak-dziala/, Data odczytu: 22.11.2024
* Wikipedia - MySQL Workbench 2024: https://pl.wikipedia.org/wiki/MySQL\_Workbench, Data odczytu: 16.12.2024
* Boringowl 2024: https://boringowl.io/blog/mysql-workbench-co-to-jest-i-jakie-sa-jego-glowne-funkcje, Data odczytu: 22.11.2024
* Wikipedia - Git 2024: https://pl.wikipedia.org/wiki/Git\_(oprogramowanie), Data odczytu: 22.11.2024
* git-scm 2024: https://git-scm.com/book/pl/v2/Pierwsze-kroki-Podstawy-Git, Data odczytu: 22.11.2024
* Wikipedia - diagrams.net 2024: https://en.wikipedia.org/wiki/Diagrams.net, Data odczytu: 22.11.2024

Książki

* Steinberg J, Werner G, (2023) Cyberbezpieczeństwo dla bystrzaków Wydanie II, Helion
* Schneier B, Zatorska J, (2017) Dane i Goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem, Helion

Artykuły

* [Yang](https://ieeexplore.ieee.org/author/37089922253) P, [Xiong](https://ieeexplore.ieee.org/author/37271732200) N, [Ren](https://ieeexplore.ieee.org/author/37088418175) J, (2022) Data Security and Privacy Protection for Cloud Storage: A Survey, https://ieeexplore.ieee.org/abstract/document/9142202
* Odun-Ayo I, Ajayi O, Akanle B, Ahuja R, (2017) An Overview of Data Storage in Cloud Computing, https://ieeexplore.ieee.org/abstract/document/8520306
* [Huang](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Chun-Ting%20Huang&eventCode=SE-AU) C, [Huang](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Lei%20Huang&eventCode=SE-AU) L, [Qin](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Zhongyuan%20Qin&eventCode=SE-AU) Z, [Yuan](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Hang%20Yuan&eventCode=SE-AU) H, [Zhou](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Lan%20Zhou&eventCode=SE-AU) L, [Varadharajan](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=Vijay%20Varadharajan&eventCode=SE-AU) V, [Jay Kuo](https://www.cambridge.org/core/search?filters%5BauthorTerms%5D=C.-C.%20Jay%20Kuo&eventCode=SE-AU) C, (2014) Survey on securing data storage in the cloud, https://www.cambridge.org/core/journals/apsipa-transactions-on-signal-and-information-processing/article/survey-on-securing-data-storage-in-the-cloud/D3E3ED530F4E026E695E32BD71DDBD0D

# SPIS TABEL

[Tabela 1 Scenariusz użycia - logowanie do systemu 26](#_Toc186834110)

[Tabela 2 Scenariusz użycia - rejestracja w systemie sdrive 26](#_Toc186834111)

[Tabela 3 Scenariusz użycia - przesył plików do systemu sdrive 27](#_Toc186834112)

[Tabela 4 Scenariusz użycia - udostępnianie plików w systemie 27](#_Toc186834113)

[Tabela 5 Scenariusz użycia - zapraszanie nowych znajomych 28](#_Toc186834114)

[Tabela 6 Scenariusz użycia - konwersacja ze znajomym 28](#_Toc186834115)

[Tabela 7 Scenariusz użycia - tworzenie magazynu 29](#_Toc186834116)

[Tabela 8 Scenariusz użycia - edycja pliku w magazynie 29](#_Toc186834117)

[Tabela 9 Scenariusz użycia - przypisanie znajomego do magazynu 30](#_Toc186834118)

[Tabela 10 Scenariusz użycia - przypisywanie nowych plików do magazynu 30](#_Toc186834119)

# SPIS RYSUNKÓW

[Rysunek 1. Diagram przypadków użycia – użytkownik 17](#_Toc186834120)

[Rysunek 2. Diagram przypadków użycia – magazyny 18](#_Toc186834121)

[Rysunek 3. Diagram ERD 19](#_Toc186834122)

[Rysunek 4. Diagram ERD - sdrive\_logins 20](#_Toc186834123)

[Rysunek 5. Diagram ERD - sdrive\_files 21](#_Toc186834124)

[Rysunek 6. Diagram aktywności – logowanie 22](#_Toc186834125)

[Rysunek 7. Diagramy aktywności - wysłanie wiadomości do nowego znajomego 23](#_Toc186834126)

[Rysunek 8. Diagramy aktywności - praca na nowym magazynie 24](#_Toc186834127)

[Rysunek 9. Diagramy aktywności - praca na wspólnym pliku w magazynie 25](#_Toc186834128)

[Rysunek 10. System logowania i rejestracji - ekran logowania 31](#_Toc186834129)

[Rysunek 11. System logowania i rejestracji - ekran rejestracji 32](#_Toc186834130)

[Rysunek 12. System logowania i rejestracji - kod qr 32](#_Toc186834131)

[Rysunek 13. System zarządzania plikami - sekcja plików 35](#_Toc186834132)

[Rysunek 14. System zarządzania plikami - sekcja wszystkich plików 35](#_Toc186834133)

[Rysunek 15. System zarządzania plikami - edycja pliku 35](#_Toc186834134)

[Rysunek 16. System znajomych - sekcja znajomych 39](#_Toc186834135)

[Rysunek 17. System znajomych - wyszukiwanie nowych znajomych 39](#_Toc186834136)

[Rysunek 18. System magazynów - tworzenie magazynu 43](#_Toc186834137)

[Rysunek 19. System magazynów – magazyn 44](#_Toc186834138)

[Rysunek 20. System magazynów - rozwiązywanie konfliktu w magazynie 44](#_Toc186834139)

[Rysunek 21. System powiadomień i wiadomości - podgląd powiadomienia 53](#_Toc186834140)

[Rysunek 22. System powiadomień i wiadomości – konwersacja 53](#_Toc186834141)

# ZAŁĄCZNIKI

* Aplikacja
* Instrukcja instalacyjna
* Wniosek o temat pracy dyplomowej