Uniwersytet Zielonogórski
Wydział Informatyki, Elektrotechniki i Automatyki

Platforma .NET – Projekt
Prowadzący: dr inż. Marek Sawerwain

Tytuł raportu/sprawozdania

Wykonał: Damian Radecki, Grupa dziekańska: 33-INF-SSI-SP
Projekt realizowano razem z:
Damian Kurkiewicz

Data oddanie projektu: DD mmmm YYYY

Ocena: .....

Spis treści

Spis listingów

Motto:
Pisanie raportu przywilejem każdego studenta.

1 Wprowadzenie

1.1 Aplikacje czasu rzeczywistego

Aplikacje działające na żywo oferują wiele korzyści, które są sporym ułatwieniem dla użytkowników podczas używania takiej aplikacji. Czynności wykonywane bez odświeżania strony nie tylko skracają czas wykonywania czynności czy obsługiwania samej witryny to jeszcze znacznie ułatwiają komunikację, unikają blokowania strony i tworzą bardziej intuicyjny interface. Takie aplikacje internetowe staja się normą w dzisiejszych czasach. Każde przeładowanie strony jest nie komfortowe i stwarza pewnego rodzaju niebezpieczeństwo wykradnięcia danych. Serwisy internetowe obsługujące komunikację real-time z klientem są lepiej zabezpieczone i działają wydajnościowo lepiej. Powstawało wiele technologii do wsparcia komunikacji na żywo, które działają zarówno po stronie witryny i serwera. Są to między innymi *WebSocket, SignalR, RabbitMQ czy Apache Kafka*. Wszystkie z nich są dziś globalnie używane do wsparcia przekazu informacji.

1.2 Opis działania

Projekt chatu na żywo jest aplikacją, która wspiera komunikację między użytkownikami, aby ich konwersacje nie działały w stylu w jakim działa klasyczny serwer e-mail. Założenie projektu są takie, aby użytkownicy bez przeładowania strony mogli wymieniać miedzy sobą wiadomości. Dodatkowo wszelkie powiadomienia przychodzą również bez zbędnego odświeżania witryny. Sprawia to, że witryna jest bardziej intuicyjna, łatwiejsza i szybsza w obsłudze. Taka architektura aplikacji jest przyjazna użytkownikowi, od którego będzie wymagana minimalny wysiłek w trakcie używania strony. Celem takiej aplikacji jest też maksymalne bezpieczeństwo wspierane przez bearen token i autoryzację użytkowników z zachowaniem szyfrowania danych poufnych. Architektura zapewnia, że nie będziemy otrzymywać wiadomości od niezaakceptowanych użytkowników lecz daje możliwość uczestnictwa w czatach posiadających osoby nieznajome poprzez mechanizm grup. W grupach każdy użytkownik może zaprosić swoich znajomych co może spowodować komunikację między nieznajomymi w danym czacie.

1.3 Grupa docelowa

Grupą docelową są wszyscy użytkownicy którzy cenią sobie bezpieczeństwo i wygodę. Chcą szybko skomunikować się ze swoimi przyjaciółmi bądź grupą docelową bez żadnych opóźnień czy niepotrzebnych przeładować strony. Są pewni tego, że ich dane są przechowywane w bezpiecznym miejscu i nikt nie wkradnie się na ich konto. Mogą to być zarówno firmy, które chcą komunikować się między sobą i ewentualnie z klientami poprzez utworzenie chatu dla grupy użytkowników jak i dla szkół, uniwersytetów, grup pracowników, przyjaciół czy kolegów.

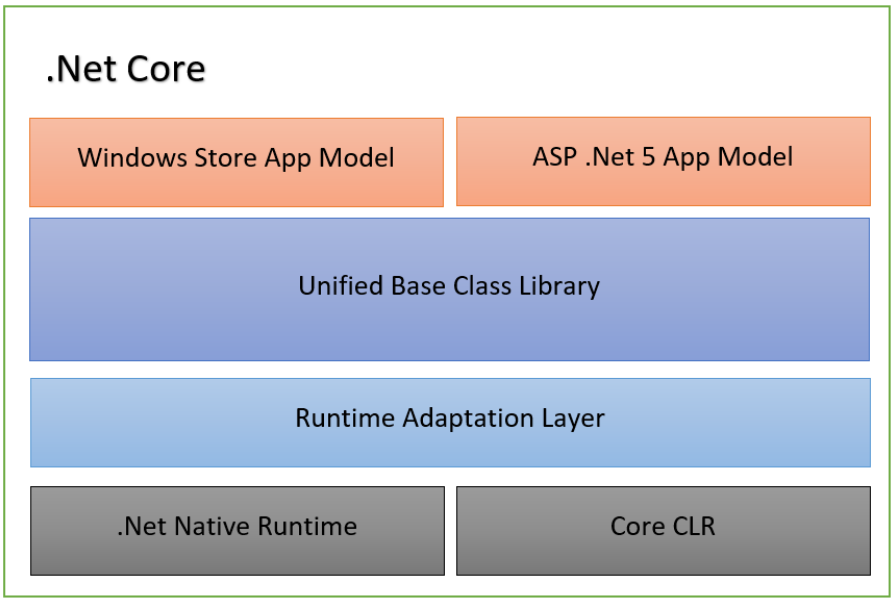
2 Użyte technologie

2.1 .Net Core

Popularny, nowoczesny i wydajny framework oparty o otwartoźródłowa implementację, który został wydany w 2016 roku do ogólnego przeznaczenia. Stanowi zestaw bibliotek pozwalający tworzyć wieloplatformowe aplikacje o wysokim stopniu bezpieczeństwa. Framework ten pozwala na pisanie aplikacji między innymi przeznaczonych do obliczeń chmurowych, IoT oraz jak w naszym przypadku do pisania web serwisu.

Rysunek 1: Logo .Net Core

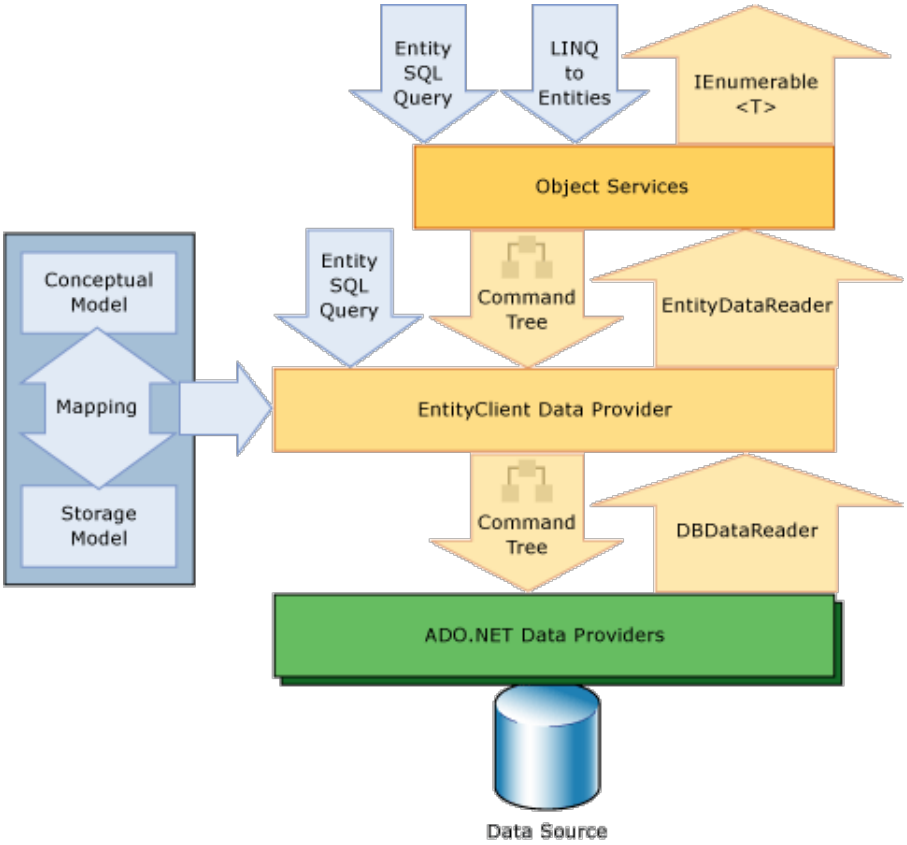
Framework *.Net Core* został przez nas wybrany, ponieważ jest to nowa oraz dobrze prosperująca technologia wprowadzająca dużą dawkę świeżości podczas tworzenia nowego oprogramowania. Posiada wsparcie dla tworzenia web serwisów opartych o metodykę *REST*, poprzez dodanie nowych i gotowych do działania bibliotek. Platforma *.Net Core* jest znacznie wydajniejsza od .Net Framework. Wprowadza znaczące usprawnienia przekładające się na szybkość działania pisanych programów. Architektura przedstawia się w sposób następujący.



Rysunek 2: Architektura .NET Core

2.2 Entity Framework

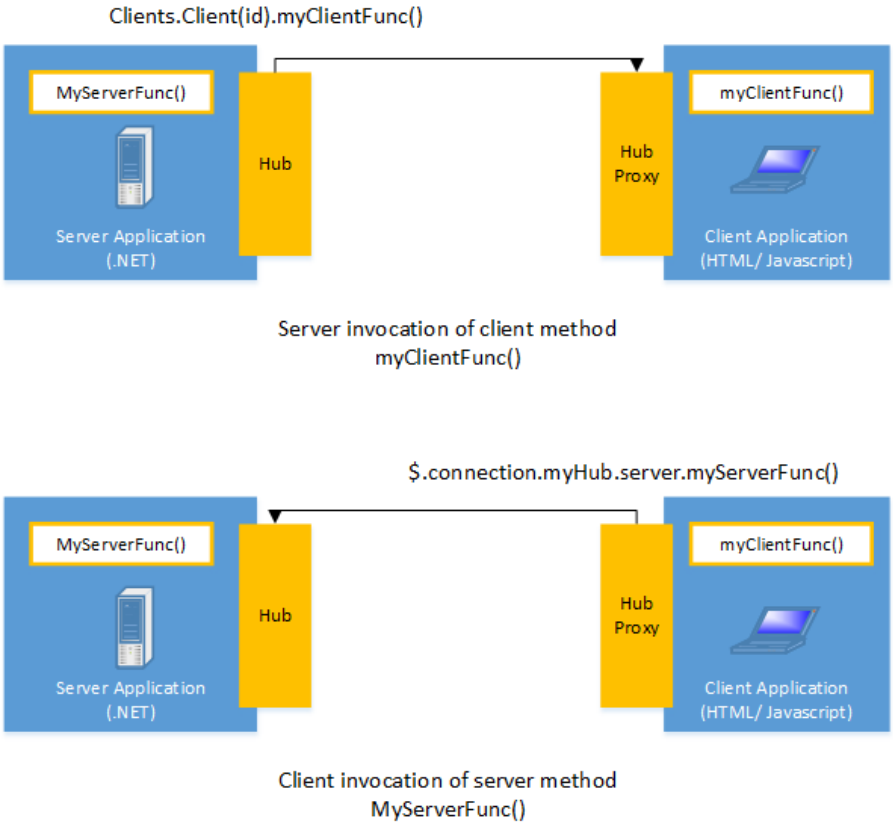
Entity Framework to zestaw technologii *ADO.NET*, obsługujące opracowywanie aplikacji zorientowanych na dane. Framework ten pozwala modelować konkretne jednostki, relację czy też logikę działania bazy danych. Obsługuję wiele systemów magazynowania danych takich jak na przykład *MySQL*, który to został przez nas wybrany do realizacji projektu. Całość jest konfigurowalna z poziomu kodu co jest bardzo wygodnym rozwiązaniem. Pozwala deweloperom na współpracę z danymi w postaci obiektów. Model fizyczny jest rafinowany przez administratorów bazy danych w celu zwiększenia wydajności, ale programiści piszący kod aplikacji przede wszystkim zawężają się do pracy z modelem logicznym, pisząc zapytania *SQL* i wywołując procedury składowane. Modele domen są zwykle używane jako narzędzie do przechwytywania i komunikowania się z wymaganiami aplikacji, często tak jak w przypadku diagramów obojętnych, które są wyświetlane i omówione w wczesnych etapach projektu, a następnie porzucone. Wiele zespołów programistycznych pomija Tworzenie modelu koncepcyjnego i rozpoczyna się od określenia tabel, kolumn i kluczy w relacyjnej bazie danych.



Rysunek 3: Architektura Entity Framework do uzyskania dostępu do danych

2.3 SignalR

Biblioteka dla dewelpoarów *ASP.NET*, która przyśpiesza proces dodawania funkcji sieci web w czasie rzeczywistym do aplikacji. Często wykorzystuje się tą bibliotekę w czatach internetowych, lecz może ona o wiele więcej. *SignalR* może być używany też w takich aplikacjach jak pulpity nawigacyjne, aplikacje do monitorowania czy formularze działające w czasie rzeczywistym. Biblioteka umożliwia również zupełnie nowe typy aplikacji internetowych, które wymagają aktualizacji wysokiej częstotliwości z serwera, na przykład gier w czasie rzeczywistym. Komunikacja między stroną a serwerem odbywa się poprzez tak zwane Hub'y. Bardzo dobrze ukazuje to rysunek poniżej.



Rysunek 4: SignalR przykład działania

2.4 MySql

Baza danych rozwijana przez firmę *Oracle*. *MySql* jest to otwarto źródłowy system zarządzania relacyjnymi bazami danych. System ten obsługuję język zapytań *SQL*, który służy do pisania zapytań do tej bazy. *MySql* jest relacyjną bazą danych. Model relacyjny w prosty i intuicyjny sposób przedstawia dane w tabelach. Każdy wiersz w tabeli jest rekordem z unikatowym identyfikatorem zwanym kluczem. Kolumny tabeli zawierają atrybuty danych, a każdy rekord zawiera zwykle wartość dla każdego atrybutu, co ułatwia ustalenie relacji między poszczególnymi elementami danymi.

Rysunek 5: Logo MySQL

2.5 Angular

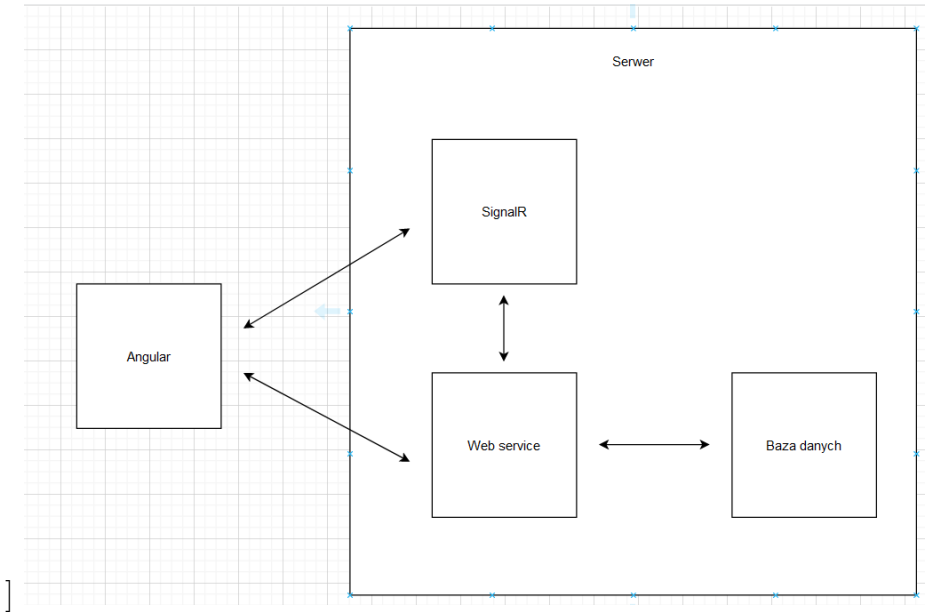
Otwarto źródłowy framework *JavaScript*, zaprojektowany i napisany przez inżynierów z *Google*. Ich celem było zrewolucjonizowanie projektowania części wizualnej stron internetowych. Szybko zyskał popularność wśród programistów JavaScript, którzy zaczęli odstawiać go na rzecz *jQuery*. Jego największą zaletą oraz najbardziej rozpoznawalną cechą jest integracja z atrybutami *HTML*. Framework ten umożliwia proste wdrożenie wzorca *MVC(Model-View-Controller)*, dzięki czemu testowanie jak i rozwój aplikacji nie sprawia wielu problemów.

Rysunek 6: Logo Angular

3 Projekt

3.1 Struktura projektu

Diagram pokązujący architekturę całego projektu opisuje główne komponenty i występujące między nimi połączenia. Strona internetowa napisana w Angularze jest podłączona bezpośrednio z *SignalR* i web serwisem. Miedzy nim występują połączenia dwukierunkowe. Z tym pierwszym strona internetowa utrzymuje stałe połączenie, aby zapewnić natychmiastową wymianę danych. Drugi wymieniony komponent odpowiada na zadane żądania. *SignalR* został wbudowany w web serwis jako integralna część, ale jest traktowany osobno, ponieważ utrzymuje z klientem innego typu połączenie. Między nimi także następuje wymiana danych. Ostatnim komponentem projektu jest baza danych, która jest podłącza tylko do web serwisu. To on stanowi most do pobierania wszelkich zawartych tam informacji.

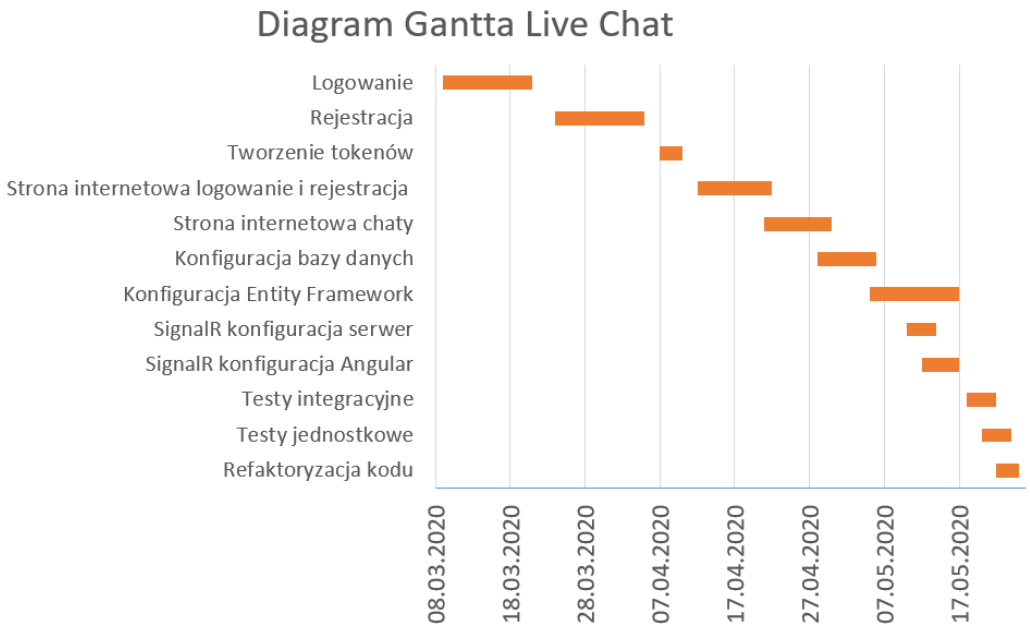


]

Rysunek 7:

3.2 Diagram Gantta

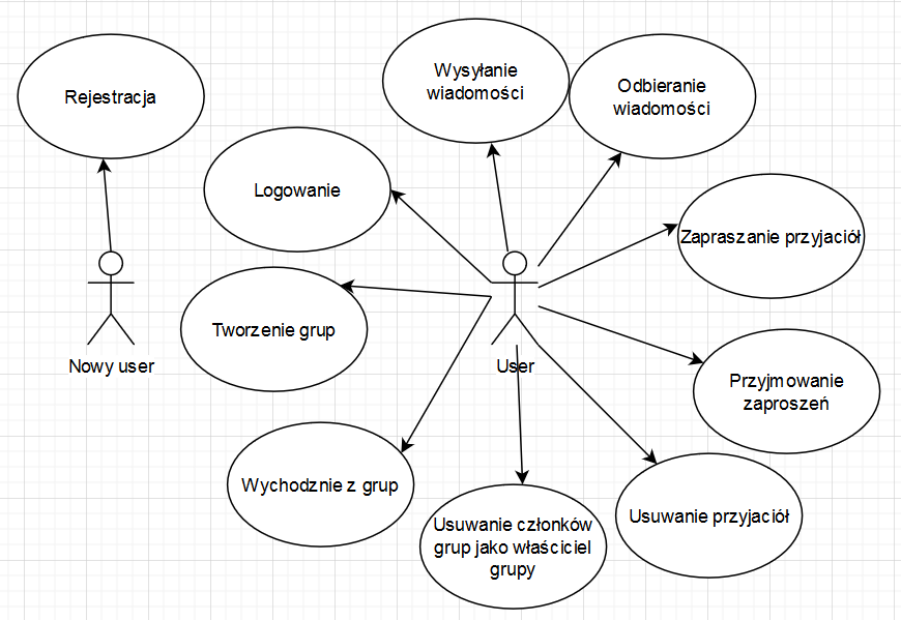
Diagram Gantta dla naszego projektu przedstawia się następująco:



Rysunek 8: Diagram Gantta Live Chat

3.3 Use Cases

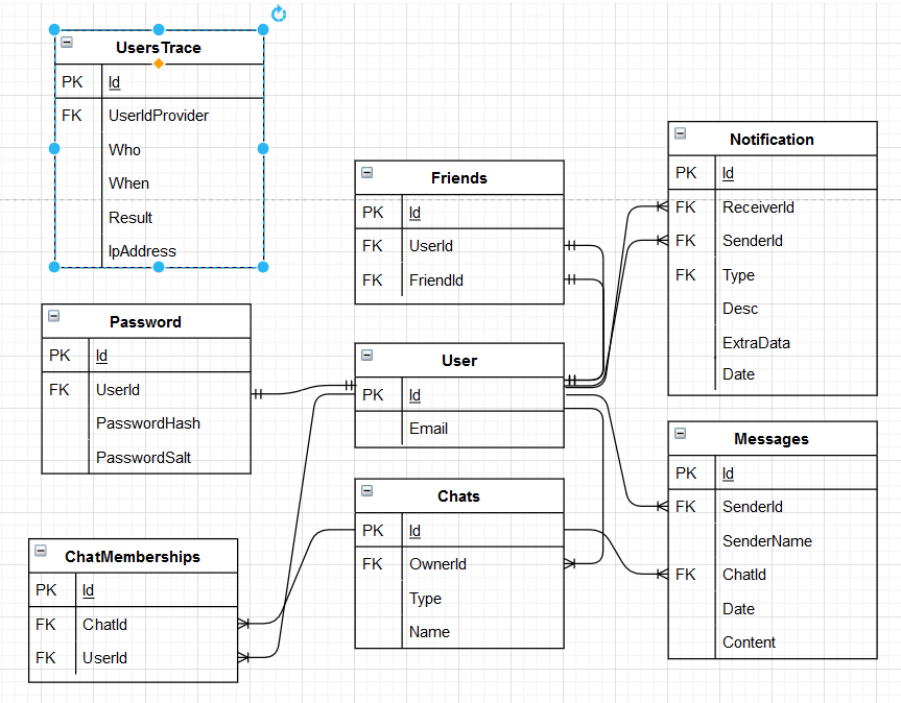
Use case pokazują fukcjonalności projektu z podziałem na rodzaje użytkownik danej aplikacji. W live chat bedziemy wyrózniać dwa rodzaje użytkowników. Będzie to nowy user, który będzie miał możliwość jedynie rejestracji i drugi to będzie już utworzony user, który będzie mógł korzystać ze wszystkich korzyści programu.



Rysunek 9:

3.4 Struktura bazy danych

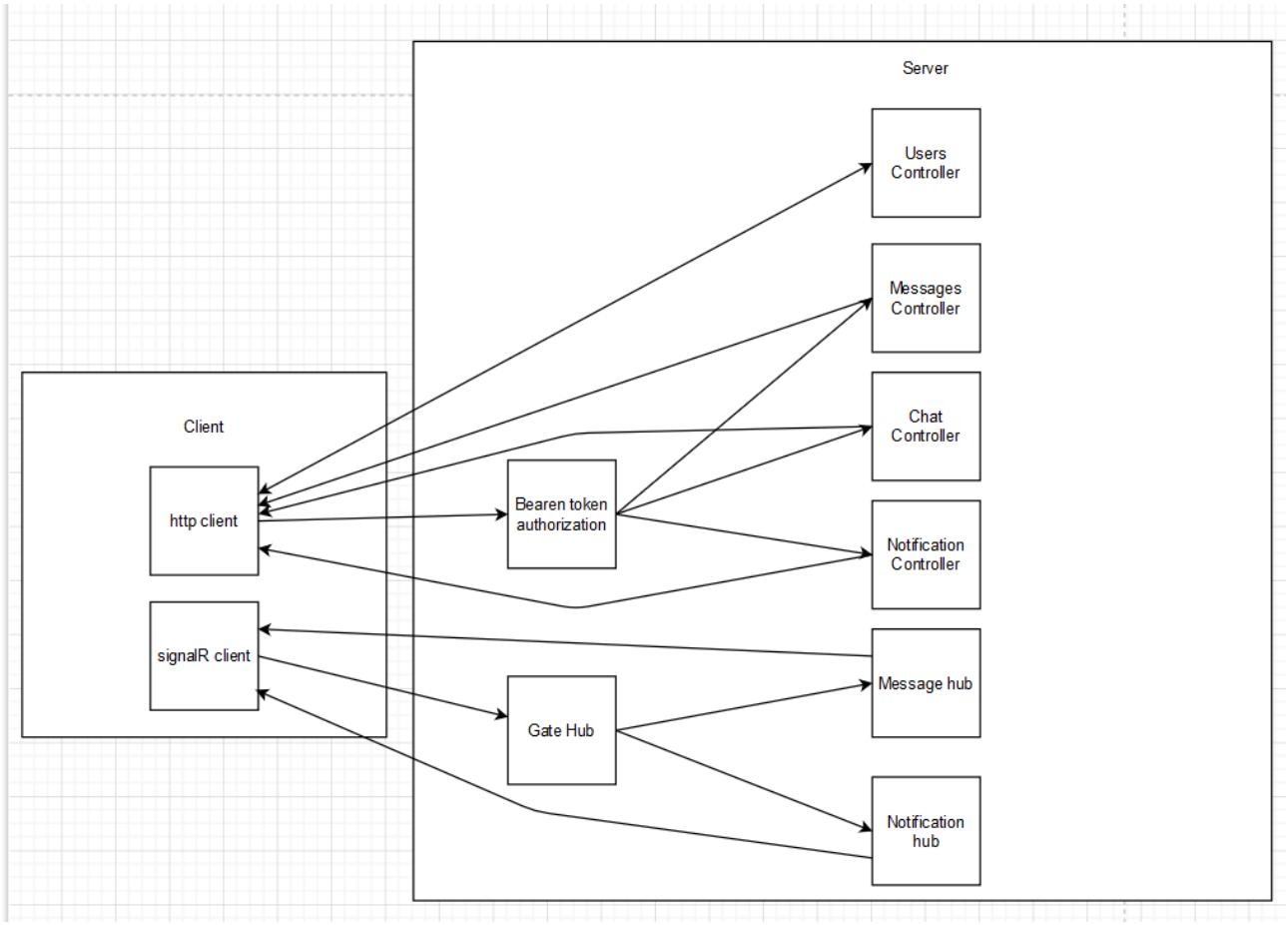
Struktura bazy danych jest prosta i czytelna. Dla takiego projektu baza danych jest fundamentem. Musimy mieć miejsce do przechowywania informacji o użytkownikach, relacjach, wiadmościach czy czatach. Tabele opieraja się na relacjach między sobą. Sama struktura w mysql została wygenerowana przez *Entity Framework Core*, który zrobił w najbardziej optymalny i wydajny sposób.



Rysunek 10:

3.5 Komunikacja z web serwisem

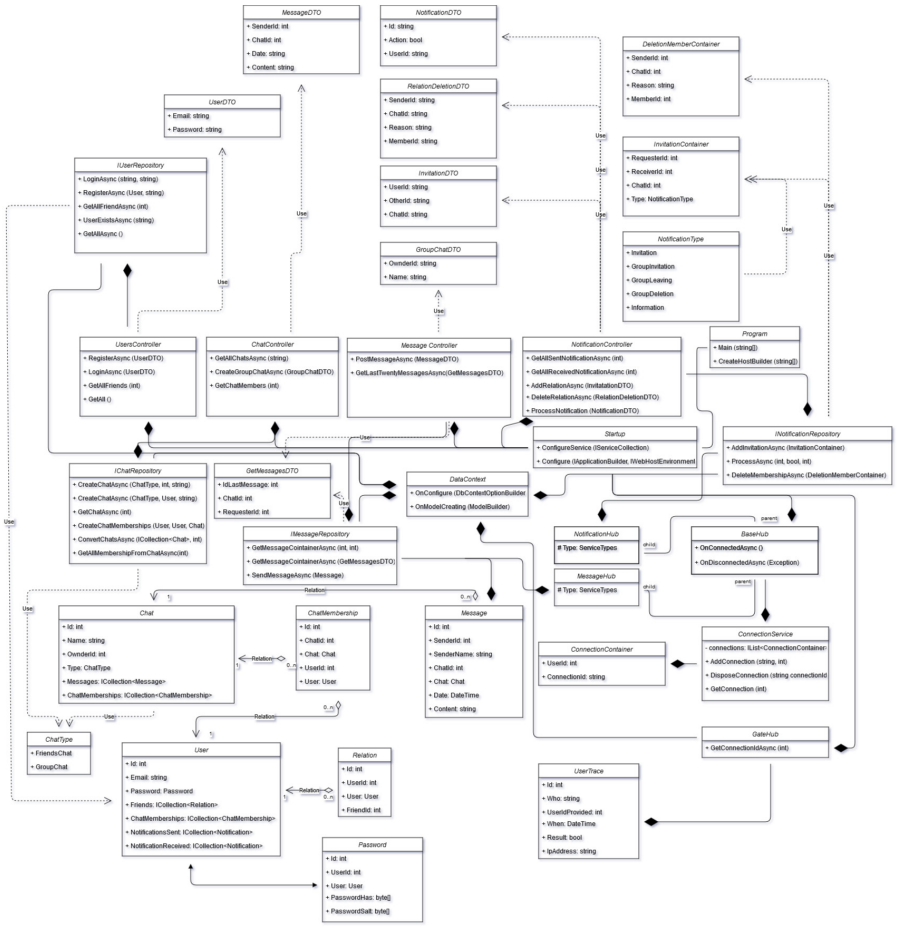
Komunikacja z web serwisem została podzielona na część dla każdego usera i część tylko dla zalogowanych. Po zalogowaniu wytwarzany jest token w *User Controller* i przesyłany z powrotem do klienta. Takowy token jest wykorzystywany do autoryzacji podczas dostępu do pozostałych kontrolerów. W przypadku *SignalR*, tylko zalogowani użytkownicy mogą się podłączyć. Wywoływana jest metoda RPC do walidacji użytkownika. Jest to druga część autoryzacji co czyni ją dwuetapową. Ta część polega na sprawdzeniu czy email zawarty w tokenie zgadza się z id usera. Wywoływana jest wówczas baza danych do pobrania emailu zawartego w rekordzie o danym id i przyrównanie tej wartości z wartością email zawartą w tokenie. Prosty diagram komunikacji z web serwisem jest następujący.



Rysunek 11:

3.6 Diagram klas

Diagram klas przedstawia od strony czysto technicznej połączenia między poszczególnymi klasami, interfejsami czy typami prostymi. Pozwala zauważyć pewne założenia, schematy, które ułatwią implementowanie całego mechanizmu, aby uniknąć powtarzania się kodu czy zminimalizować ilość użytych linijek.



Rysunek 12:

4 Implementacja

4.1 Modele bazy danych

Baza danych dla naszego projektu musiała być bardzo rozbudowana. W trakcie samego tworzenia, modeli ciągle przybywało. Jako że używaliśmy Entity Frameworka zdecydowaliśmy się na użycie adnotacji dla klas modeli. Skorzystaliśmy z bibliotek *System.ComponentModel.DataAnnotations*. Jedenym z przykładowych lecz bardziej rozbudowanych modeli użytych w naszej bazie danych znajduje się na listingu poniżej, dana klasa została przygotowana dla tabeli zawierającej wiadomości.

Listing 1: Przykładowa klasa modelu tabeli - Message

```
public class Message
{
        [Key]
        public int Id { get; set; }

        [Required]
```

```
        [ForeignKey("Sender")]
        [JsonIgnore]
        public int SenderId { get; set; }

        [JsonIgnore]
        public virtual User Sender { get; set; }

        public string SenderName { get; set; }

        [Required]
        [ForeignKey("Chat")]
        public int ChatId { get; set; }

        [JsonIgnore]
        public virtual Chat Chat { get; set; }

        public DateTime Date { get; set; }

        public string Content { get; set; }
    }
```

Jak widać na powyższym listingu. Model ten zawiera takie adnotacje:

- **Key** - określa że dane pole jest kluczem głównym;
- **Required** - informuje żę dane pole musi być wypełnione;
- **ForeignKey** - oznacza daną zmienną jako klucz obcy oraz w nawiasie przyjmuje nazwę tabeli której jest to klucz obcy;
- **JsonIgnore** - adnotacja wskazuje że dane pole bądź metodę należy zignorować podczas deserializacji danych.

4.2 Modele DTO

Model DTO (Data Transfer Object) jest bardzo wygodnym wzorcem projektowym należącym do grupy wzorców dystrybucji. Dzięki DTO można w prosty sposób transferować dane między systemami czy aplikacjami. W naszym projekcie potrzebowaliśmy stworzyć wiele modeli DTO w celu komunikacji *Strona web - Serwer*. Dobrze skonstruowany kontener, bo tak często nazywana jest klasa będąca modelem DTO, często staje się podstawową konstrukcją w wielu rozbudowanych projektach. W naszym projekcie znajduję się aktualnie aż osiem modeli DTO. Posiadamy modele potrzebne do transportu wiadomości czy też powiadomień. Jak wygląda przykładowy model DTO użyty w naszym projekcie znajduje się poniżej:

Listing 2: Przykładowa klasa modelu DTO - Message

```
public class InvitatationDTO
{
```

```
 [Required]
 [RegularExpression(@"^[1-9]\d*$", ErrorMessage = "'0' Can not be used")]
 public string UserId { get; set; }

 [Required]
 [RegularExpression(@"^[1-9]\d*$", ErrorMessage = "'0' Can not be used")]
 public string OtherId { get; set; }

 public string ChatId { get; set; }
}
```

Powyższy listing pokazuje że w projekcie użyliśmy również wyrażeń regularnych w celu sprawdzania poprawności przesyłanych danych. W momencie gdy przesłany przez stronę *Model DTO* zawiera dane nie zgodne z wyrażeniem regularnym, serwer automatycznie zwracał błąd że jakieś dane są nie poprawne. Dzięki temu mogliśmy pominąć sprawdzanie wielu przypadków przesyłania błędnych danych.

4.3 Implementacja kontrolerów

4.4 Problemy i ich rozwiązania

5 Testy

5.1 Testy jednostkowe

5.2 Testy integracyjne

6 Opis wkładu własnego w realizację projektu

6.1 Stworzenie i konfiguracja bazy danych

Złożoność oraz poziom zaawansowania naszego projektu był bardzo duży co wymagało rozbudowanej bazy danych. Budowę oraz połączenie między tabelami w bazie danych ukazuje rysunek numer 10. Praktycznie każda tabela posiada klucz obcy innej tabeli. Spowodowane to jest tym iż specyfika naszego projektu wymaga od nas takiego połączenia. Każdy czat musi być przypisany do konkretnych użytkowników, każda wiadomość do konkretnego czatu. Powiadomienia w podobny sposób co wiadomości czy czaty muszą posiadać przypisanego konkretnego użytkownika, a do tego wszystkiego jeszcze dochodzą czaty grupowe co wymagało od nas dodatkowego przemyślenia działania całej infrastruktury aplikacji.

Po wielu problemach i próbach ich rozwiązania udało nam się skonfigurować *Entity Framework* do oczekiwanego przez nas stopnia. Większość tabel i połączeń między nimi bardzo dobrze się skonfigurowało poprzez adnotacje nadane polom w modelach bazy danych. Sam nasz *DbContext* wyglądał w sposób następujący:

Listing 3: DbContext Entity Framework

```
public DbSet<Password> Passwords { get; set; }
public DbSet<User> Users { get; set; }
public DbSet<Message> Messages { get; set; }
public DbSet<Relation> Friends { get; set; }
public DbSet<Notification> Notifications { get; set; }
public DbSet<Chat> Chats { get; set; }
public DbSet<ChatMembership> ChatMemberships { get; set; }
public DbSet<UserTrace> UsersTrace { get; set; }
```

Powyższa część odpowiada za utworzenie tabel *DBSet* z nazwą modelu we wnętrzu trójkątnych nawiasów. Niestety nie wszystkie tabele chciały się w ten sposób utworzyć. Jedyną tabelą, którą musieliśmy utworzyć w trochę inny sposób okazała się tabela *Notyfication* odpowiadająca za przetrzymywanie informacji na temat powiadomień. Tą jedną tabelę utworzyliśmy używając wbudowanych dodatkowych funkcji *Entity Frameworka*, nadpisując funkcję *OnModelCreating* byliśmy w stanie utworzyć tabelę wraz jej połączeniami. Poniższy listing ukazuje naszą rozbudowę funkcji:

Listing 4: OnModelCreating tabela Notyfication - Entity Framework

```
protected override void OnModelCreating(ModelBuilder modelBuilder)
{
        base.OnModelCreating(modelBuilder);

        modelBuilder.Entity<Notification>()
        .HasOne(t => t.Sender)
        .WithMany(m => m.NotificationsSent)
        .HasForeignKey(p => p.SenderId);

        modelBuilder.Entity<Notification>()
        .HasOne(t => t.Receiver)
        .WithMany(m => m.NotificationsReceived)
        .HasForeignKey(p => p.ReceiverId);
}
```

6.2 Stworzenie systemu logowania i rejestracji

Stworzenie przez nas systemu logowania i rejestracji było bardzo skoplikowanym procesem. Przemyśleć musieliśmy jakiego algorytmu szyfrowania haseł użyć by hasła użytkowników przechowywane w bazie danych były bezpieczne. Do szyfrowania haseł użyliśmy wbudowanego w język *C#* algorytmu wyznaczania wartości skrótu zwangeo *HMAC-SHA512*, który to zbudowany jest z funkcji skrótu *SHA-512* oraz oparty jest o uwierzytelnianie wiadomości opartych o skróty *HMAC*. Proces *HMAC* miesza klucz tajny z danymi komunikatów i miesza wynik. Wartość skrótu jest ponownie mieszana z kluczem tajnym, a następnie poddana skrótu po raz drugi. Wynikowy skrót ma długość 512 bitów.*HMAC* działa w sposób następujący:

$$\mathrm{HMAC}_K(m) = h\Big((K \oplus \mathrm{opad}) \| h\big((K \oplus \mathrm{ipad}) \| m\big)\Big),$$

Rysunek 13: HMAC Signature

Podczas rejestracji szyfrowane jest hasło po stronie serwera oraz zaszyfrowane zapisywane jest w bazie danych. W celu zapobiegnięcia odszyfrowania, hasło jest szyfrowane w jedną stronę. Dzięki temu nawet my jako twórcy nie jesteśmy w stanie od szyfrować dla własnych potrzeb hasła użytkownika. Logowanie przeprowadza podobny proces co rejestracja lecz nie zapisuje hasła w bazie. Hasło wpisane przez użytkownika jest szyfrowane po stronie serwera i już zaszyfrowane hasło jest porównywane z zaszyfrowanym hasłem w bazie danych. Jeśli wartości są takie same użytkownik zostaje poprawnie zarejestrowany w aplikacji i uzyskuje dostęp do wszystkich funkcji systemu.

6.3 Autoryzacja i autentykacja użytkowników

W celu autoryzacji oraz autentykacji użytkowników po stronie serwera. Tworzony jest token. Token jest to ciąg znaków identyfikujący aktualnie zalogowanego użytkownika. Tworzony jest w taki sposób by nie było możliwości powtórzenia się tokena.

Listing 5: Tworzenie tokena przy logowaniu

```
var tokenDescriptor = new SecurityTokenDescriptor
{
        Subject = new ClaimsIdentity(claims),
        Expires = DateTime.Now.AddHours(12),
        SigningCredentials = creds
};

var tokenHandler = new JwtSecurityTokenHandler();
var token = tokenHandler.CreateToken(tokenDescriptor);
```

Jak widać na powyższym listingu, do tworzenia tokena uwierzytelniającego użytkownika wykorzystujemy klasę *SecurityTokenDescriptor*. Dzięki tej klasie jesteśmy w stanie przekazać jej wszystkie potrzebne informacje do utworzenia tokena. Token jest ważny przez 12 godzin ale jeśli użytkownik zamknie kartę z otwarta naszą stroną automatycznie token jest usuwany. Natomiast gdy użytkownik przekroczy czas dwunastu godzin zostanie poproszony o ponowne zalogowanie. Po utworzeniu tokena przesyłamy w formacie *JSON* token wraz z informacjami o zalogowanym użytkowniku do aplikacji w przeglądarce.

6.4 Konfiguracja środowiska i serwera

Konfiguracja aplikacji rozrastała się w raz z powstawaniem nowych funkcji. Przed rozpoczęciem działania aplikacji odpalana jest konfiguracja, która trzeba najpierw skonfigurować. Klasa *Startup* metody takie jak *ConfigureService* oraz *Configure*. Zacznijmy od tej pierwszej. Metoda *ConfigureServices* jest metodą opcjonalną. Wywoływana jest przez hosta przed uruchomieniem metody *Configure*. W metodzie tej wszystkie opcje konfiguracyjne ustawiane są wraz z konwencją przedstawianą w dokumentacji firmy.

6.4.1 ConfigureServices

W tej metodzie jako pierwsze ustawiamy dostęp do bazy danych oraz wskazujemy do jakiej bazy chcemy się łączyć. W naszym przypadku łączymy się do bazy *MySQL*.

Listing 6: Dodanie bazy danych do konfiguracji

```
services.AddDbContext<DataContext>(option =>
{
 option.UseLazyLoadingProxies();
 option.UseMySql(Configuration.GetConnectionString("DefaultConnection"));
});
```

ConnectionString jest pobierany z pliku konfiguracyjnego. Opcja *UseLazyLoadingProxies* powoduje tak zwane Leniwe Ładowanie, które polega na każdorazowym odpytywaniu bazy o interesujące nas dane. Ten typ ładowania jest wykorzystywany gdy chcemy pobrać jakieś konkretne dane z bazy a nie chcemy zaśmiecać sobie pamięci masą innych niepotrzebnych danych.

Jako drugie ustawiamy zakres. Zakresy są potrzebne do bazy danych. Informujemy w ten sposób które interfejsy oraz klasy należą do kontroli bazy danych. Dodajemy je w następujący sposób:

Listing 7: Dodanie klas Repository

```
services.AddScoped<IUserRepository, UserRepository>();
services.AddScoped<INotificationRepository, NotificationRepository>();
services.AddScoped<IMessagesRepository, MessageRepository>();
services.AddScoped<IChatRepository, ChatRepository>();
```

Powyższy listing przedstawia w jaki sposób dodajemy klasy oraz interfejsy, które są repozytoriami dla danych tabel w bazie danych.

Następną częścią jaką dodajemy do naszej konfiguracji są wzorce projektowe *Singleton*. *.Net Core* posiada wbudowane metody pozwalające na tworzenie konkretnych klas na serwerze jako *Singletony*. W jaki sposób to się robi przedstawia poniższy listing z naszego programu:

Listing 8: Wzorzec Singleton w konfiguracji

```
services.AddSingleton<MessageConnectionService>();
services.AddSingleton<NotificationConnectionService>();
services.AddSingleton<Func<ServiceTypes, IConnectionService>>(provider => s
{
        switch(serviceType)
        {
        case ServiceTypes.MessageConnectionService:
                return provider.GetService<MessageConnectionService>();
        case ServiceTypes.NotificationConnectionService:
                return provider.GetService<NotificationConnectionService>(
        default:
                return null;
        }
});
```

Kolejną bardzo ważną częścią jak nie najważniejszą w konfiguracji jest autentykacja i autoryzacja. W naszej aplikacji użyliśmy tak zwanego *BearerTokena*. Określamy wszelkie ustawienia jego jak i to jakim kluczem jest szyfrowane oraz podajemy token potrzebny do tworzenia klucza. Tak jak w przypadku *ConnectionString* tutaj pobierana jest wartość z pliku zawierającego dane konfiguracyjne. Poniższy listing przedstawia jak skonfigurowany jest nasz *BearerToken*.

Listing 9: BearerToken - konfiguracja

```
services.AddAuthentication(JwtBearerDefaults.AuthenticationScheme)
 .AddJwtBearer(options =>
 {
 options.TokenValidationParameters = new TokenValidationParameters
 {
  ValidateIssuerSigningKey = true,
  IssuerSigningKey = new  SymmetricSecurityKey(Encoding.ASCII.GetBytes(
  Configuration.GetSection("AppSettings:Token").Value)),
  ValidateIssuer = false,
  ValidateAudience = false,
 };
 options.Events = new JwtBearerEvents
 {
  OnMessageReceived = context =>
  {
   var accessToken = context.Request.Query["access_token"];
  if (string.IsNullOrEmpty(accessToken) == false)
  {
   context.Token = accessToken;
  }
   return Task.CompletedTask;
  }
 };
});
```

Ostatnią częścią tej metody jest dodanie tak zwanej *Policy*. Ta część pozwala na ustawienie metod, nagłówków oraz ustawienie jaki adres jest tym domyślnym, bazowym. W naszym przypadku jako że to projekt, adres bazowy posiada u nas wartość *http://localhost:4200*. Na sam koniec dodajemy obsługę bibliotek *SingalR*. Poniższy listing przedstawia jak to robimy w kodzie:

Listing 10: Polityka oraz dodanie SingalR w konfiguracji

```
services.AddCors(o => o.AddPolicy("CorsPolicy", builder =>
{
        builder
        .AllowAnyMethod()
        .AllowAnyHeader()
        .WithOrigins("http://localhost:4200")
        .AllowCredentials();
}));
```

```
services.AddSignalR();
```

6.4.2 Configure

W tej metodzie w przeciwieństwie do metody wyżej opisanej, bardzo ważną role gra kolejność wywoływanych metod. Przepływ zwany również *Pipeline*, w tej części programu wszystko musi być ustawione w odpowiedniej kolejności, by zapewnić bezawaryjne działanie. Poniższy listing przedstawia jak wygląda nasza metoda *Configure*:

Listing 11: Metoda Configure

```
if (env.IsDevelopment())
{
        app.UseDeveloperExceptionPage();
}

app.UseRouting();
app.UseAuthentication();
app.UseAuthorization();
app.UseCors("CorsPolicy");
app.UseForwardedHeaders(new ForwardedHeadersOptions
{
        ForwardedHeaders = ForwardedHeaders.XForwardedFor |
        ForwardedHeaders.XForwardedProto
});

app.UseEndpoints(endpoints =>
{
        endpoints.MapControllers();
        endpoints.MapHub<MessagesHub>("/messagechart");
        endpoints.MapHub<NotificationHub>("/notificationchart");
        endpoints.MapHub<GateHub>("/connection");
});
```

Na samym początku informujemy serwer że jeśli aplikacja jest włączana w trybie deweloperskim to aktywujemy *DeveloperExceptionPage*, stronę odpowiedzialną za pokazywanie szczegółowych informacji w momencie wystąpienia poważnego błędu po stronie serwera. Następnie włączamy możliwość *Routingu*, autoryzację oraz autetykację. Kolejnym krokiem jest aktywowanie polityk, które w metodzie *ConfigureServices* ustawialiśmy szczegółowo. Następnie informujemy serwer że zezwalamy na przekierowania informacji takich jak na przykład adresy IP czy porty. Wykorzystywane przy przełączaniu serwerów proxy. Ostatnią częścią można powiedzieć że nawet najważniejszą są tak zwane *EndPoints*. W tym miejscu mapujemy wszystkie kontrolery działające w aplikacji oraz ścieżki do nich.