Modelowanie i analiza systemów informatycznych

dokumentacja projektu
System wspomagania decyzji

inż. Bartosz Ociepka
inż. Beniamin Stecuła

15 listopada 2020

Podział pracy

inż. Bartosz Ociepka - backend
inż. Beniamin Stecuła - frontend

Udokumentowanie pracy

Dokumentowanie pracy odbyło się na kilka sposobów:

- utworzenie niniejszej dokumentacji,
- podział zadań na serwisie Trello:
  https://trello.com/b/se2oXQzD/polap-wspomaganie-decyzji
- przechowywanie kopii poprzednich wersji programu:
  https://github.com/BartoszOciepka/DiabetesNeuralNetwork

Instrukcja obsługi

Instrukcja wdrożenia

Aby wdrożyć projekt należy wykonać poniższą listę kroków:

1. zaimportowanie projektu w Visual Studio 2015,
2. import danych do bazy danych MySql (dołączono plik dump.sql zawierający potrzebne tabele),
3. zmiana connectionString w kodzie na odpowiadające używanej bazie, danych (dokonanie zmiany klas gdy używana jest inna baza niż MySql),
4. uruchomienie projektu.

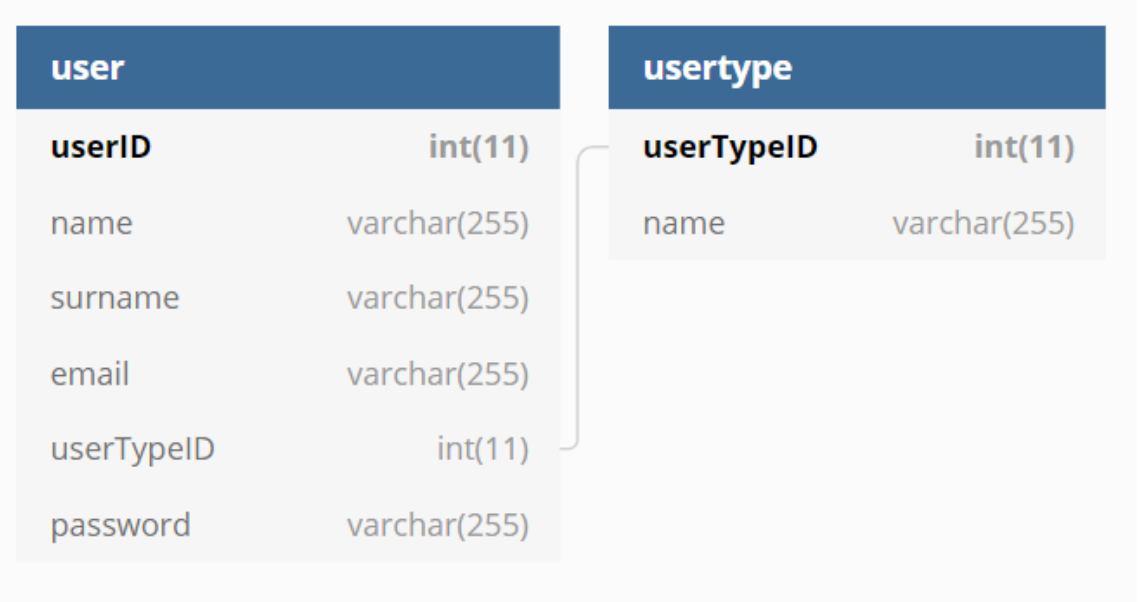
Część testowa

Baza danych

Komponenty systemu

Algorytm szyfrowania

W naszym programie do rejestracji i logowania użyliśmy klasy Membership z System.Web.Security. Do szyfrowania haseł użyty został algorytm TLS 1.3. Nic nie stoi na przeszkodzie aby ten sposób zmienić. W samej konfiguracji można ustawić haszowanie, szyfrowanie lub zapisywanie haseł w trybie plain text (nie jest to zalecany sposób). Po wybraniu rodzaju można



Rysunek 1: Diagram klas.

wybrać konkretny sposób enkrypcji. Poniżej przykład zmiany haszowania na SHA256 w pliku web.config poprzez atrybut hashAlgorithmType.

```
1     <membership
2     defaultProvider =" provider name "
3     userIsOnlineTimeWindow =" number of minutes "
4     hashAlgorithmType =" SHA256 ">
5     <providers >... </ providers >
6     </ membership >
```

TLS wykorzystuje Algorytm Rivesta-Shamira-Adlemana (RSA) – jest to jeden z pierwszych i najpopularniejszych asymetrycznych algorytmów kryptograficznych o kluczu publicznym. Może być stosowany i do szyfrowania, i cyfrowego podpisywania plików.

Polega on na liczeniu funkcji Eulera dla dużych liczb pierwszych, a jego bezpieczeństwo opiera się na trudności faktoryzacji dużych liczb złożonych.

Każdy z rozmówców posiada parę kluczy: prywatny i publiczny. Pierwszy z nich służy do deszyfrowania wiadomości przychodzącej, a drugi do szyfrowania wychodzącej. Aby nawiązać komunikację rozmówcy muszą wymienić się swoimi kluczami publicznymi. Klucze prywatne nigdy nie są ujawniane.

Model systemu eksperckiego

Przykładowy kod z aplikacji z testami

```
1   Tutaj wklejamy pelen kod.
```