Dokumentacja Wstępna
Szyfrowany Notatnik Medyczny - Aplikacja Webowa

Milena Kuna 325 033
Karol Franczuk 325 001

18 kwietnia 2025

1 Koncepcja projektu

Projekt zakłada stworzenie aplikacji webowej służącej do przechowywania poufnych notatek medycznych pacjentów. Aplikacja będzie działać w przeglądarce internetowej z wykorzystaniem nowoczesnych API przeglądarkowych do szyfrowania danych po stronie klienta. Dane będą przechowywane na zewnętrznym serwerze wyłącznie w formie zaszyfrowanej, przy czym klucze szyfrujące nigdy nie opuszczą przeglądarki użytkownika.

2 Cele projektu

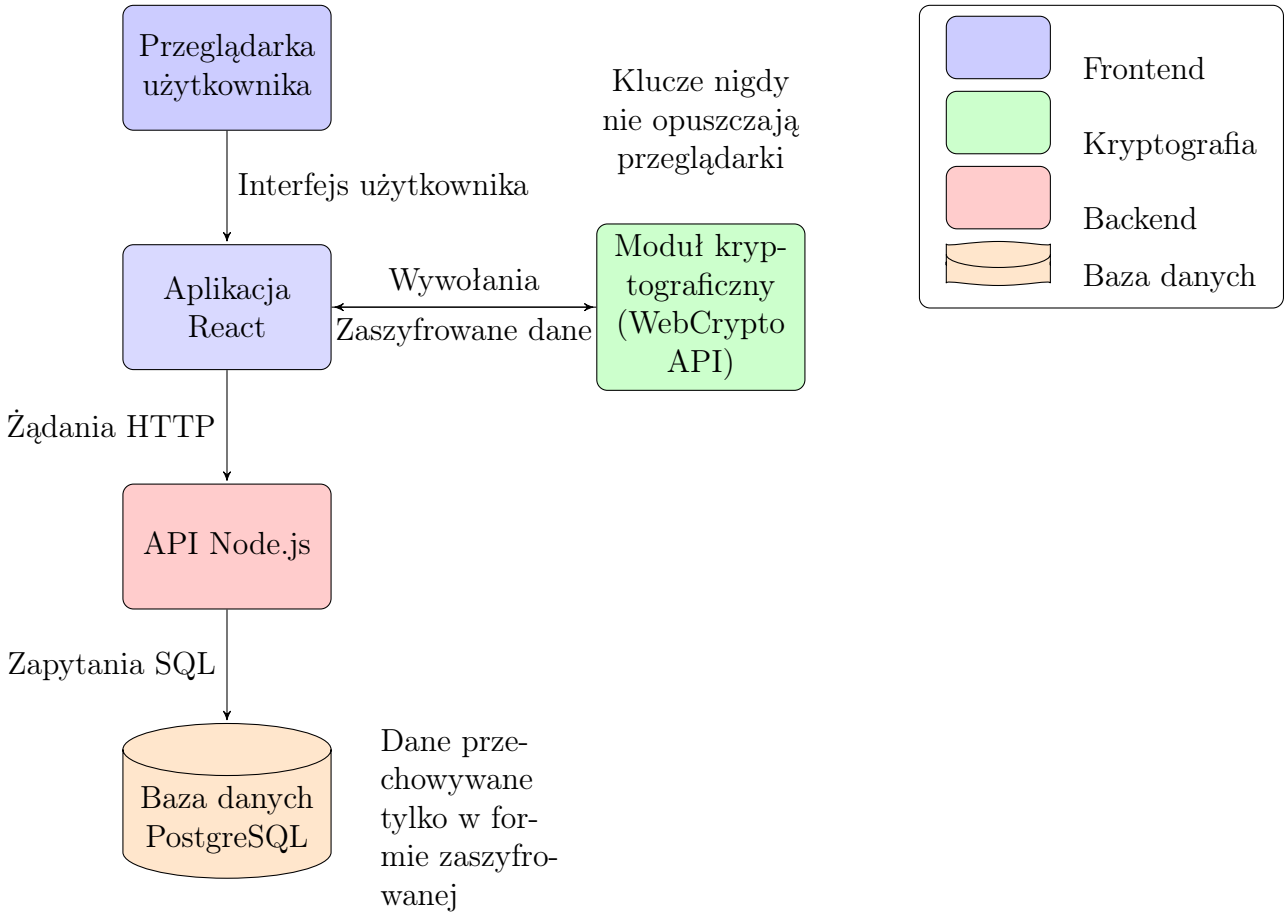
- Stworzenie bezpiecznego systemu przechowywania notatek medycznych w formie aplikacji webowej
- Implementacja mechanizmów szyfrowania end-to-end w przeglądarce
- Zaprojektowanie modelu bezpieczeństwa odpornego na podstawowe ataki
- Zapewnienie pełnej funkcjonalności CRUD na zaszyfrowanych danych
- Analiza ryzyka i potencjalnych wektorów ataku specyficznych dla aplikacji webowych

3 Proponowany stos technologiczny

Warstwa	**Technologie**
Frontend	React.js + TypeScript, Material-UI, WebCrypto API
Backend	Node.js + Express, TypeScript
Baza danych	PostgreSQL z rozszerzeniem pgcrypto
Bezpieczeństwo	WebCrypto API, PBKDF2, AES-GCM 256-bit, JWT
Hosting	GitLab CI/CD, Docker, serwer uczelniany

4 Architektura systemu

4.1 Diagram architektury



Rysunek 1: Diagram architektury systemu szyfrowanego notatnika medycznego

4.2 Komponenty

- **Klient przeglądarkowy**:
  - Generowanie i przechowywanie kluczy w IndexedDB
  - Szyfrowanie/deszyfrowanie danych przed wysłaniem/po odebraniu
  - Interfejs użytkownika do zarządzania notatkami
- **Serwer aplikacyjny**:
  - API REST do operacji na zaszyfrowanych danych
  - Zarządzanie użytkownikami (bez dostępu do treści notatek)
  - Uwierzytelnianie przez JWT
- **Baza danych**:
  - Przechowywanie zaszyfrowanych danych w formie BLOB
  - Metadane notatek (data stworzenia, rozmiar itp.)
  - Tabela użytkowników z solami i haszami haseł

5 Przepływ danych

1. Użytkownik loguje się wprowadzając hasło
2. Aplikacja wyprowadza klucz główny z hasła używając PBKDF2
3. Klucz główny służy do odszyfrowania klucza szyfrującego przechowywanego w IndexedDB
4. Przy tworzeniu notatki:
    - Generowany jest unikalny IV (Initialization Vector) Dane szyfrowane są algorytmem AES-GCM
    - IV + zaszyfrowane dane wysyłane są na serwer
5. Przy odczycie notatki:
    - Pobierane są zaszyfrowane dane z serwera
    - Deszyfrowanie następuje w przeglądarce
    - Odszyfrowane dane wyświetlane są użytkownikowi

6 Bezpieczeństwo

6.1 Mechanizmy zabezpieczające

- **Szyfrowanie**: AES-GCM 256-bit dla danych, PBKDF2 dla kluczy
- **Przechowywanie kluczy**: IndexedDB z ograniczeniami CORS
- **Uwierzytelnianie**: JWT z krótkim czasem życia
- **Ochrona przed XSS**: CSP, sanitizacja danych, HttpOnly cookies
- **Ochrona przed CSRF**: SameSite cookies, tokeny CSRF

6.2 Analiza ryzyka

Ryzyko	**Skutki**	**Środki zaradcze**
Utrata kluczy	Trwała utrata dostępu do danych	Backup kluczy zaszyfrowanych hasłem pomocniczym
XSS	Kradzież danych/sesji	Ścisła CSP, sanitizacja, HttpOnly JWT
MITM	Przechwycenie danych	HSTS, stała weryfikacja certyfikatów
Atak brute-force	Przejęcie konta	Limity prób logowania, CAPTCHA
Wyciek przez cache	Dostęp do danych	Nagłówki Cache-Control, no-store

7 Interfejs użytkownika

7.1 Główne ekrany

- Logowanie/rejestracja
- Dashboard z listą notatek
- Edytor notatek z podglądem formatowania
- Ustawienia bezpieczeństwa
- Panel zarządzania załącznikami

8 Wymagania funkcjonalne

- System uwierzytelniania użytkowników
- Tworzenie, edycja, usuwanie zaszyfrowanych notatek
- System kategorii i tagów
- Wyszukiwanie po metadanych
- Eksport/import danych (zaszyfrowany plik)
- Zarządzanie załącznikami (obrazy, PDF)

9 Wymagania niefunkcjonalne

- Dane szyfrowane przed opuszczeniem przeglądarki
- Brak dostępu serwera do treści notatek
- Wydajność pozwalająca na płynną pracę
- Responsywny design działający na różnych urządzeniach
- Kompatybilność z nowoczesnymi przeglądarkami

10 Podsumowanie

Projekt szyfrowanego notatnika medycznego w formie aplikacji webowej stanowi interesujące wyzwanie z zakresu bezpieczeństwa systemów informacyjnych. Kluczowym aspektem jest zapewnienie, że wszystkie operacje kryptograficzne odbywają się po stronie klienta, a serwer pełni jedynie rolę "przechowalni"zaszyfrowanych danych. Projekt będzie realizowany z wykorzystaniem nowoczesnych technologii webowych, z szczególnym naciskiem na aspekty bezpieczeństwa.