Ćwiczenie laboratoryjne

Bezpieczeństwo danych medycznych

1 Praktyczne aspekty poufności i integralności danych w aplikacjach medycznych opartych na sztucznej inteligencji

1.1 Wprowadzenie teoretyczne

Bezpieczeństwo danych medycznych stanowi kluczowy element budowy systemów informatycznych, w szczególności takich, które wykorzystują algorytmy sztucznej inteligencji (SI). Ze względu na wyjątkową wrażliwość danych klinicznych, konieczne jest zapewnienie trzech fundamentalnych cech bezpieczeństwa informacji:

- **Poufności (Confidentiality)** – ochrona przed nieautoryzowanym dostępem.
- **Integralności (Integrity)** – ochrona przed nieautoryzowaną modyfikacją danych.
- **Dostępności (Availability)** – zapewnienie dostępu do danych, gdy jest to niezbędne.

Systemy oparte na SI, które wykorzystują dane pacjentów, muszą spełniać rygorystyczne wymogi bezpieczeństwa i ochrony prywatności, w tym:

- regulacje prawne (RODO, HIPAA),
- normy bezpieczeństwa (np. ISO/IEC 27001, 27701),
- dobre praktyki kryptograficzne,
- zasady minimalizacji danych oraz anonimizacji.

W kontekście sztucznej inteligencji szczególnego znaczenia nabierają procesy:

- kontroli dostępu do zbiorów danych,
- rejestrowania i audytowania operacji na danych,
- ochrony integralności danych wejściowych i wyników modelu,
- bezpiecznego przechowywania i przetwarzania danych,
- ochrony danych podczas trenowania i inferencji modelu.

1.2 Podstawy prawne i normy bezpieczeństwa

RODO (GDPR). Określa szczególne zasady przetwarzania danych dotyczących zdrowia, wymagając m.in.:

- pseudonimizacji lub anonimizacji,
- minimalizacji danych,
- ograniczenia celu i czasu przetwarzania,
- przejrzystości przetwarzania,
- wdrażania środków technicznych i organizacyjnych adekwatnych do ryzyka.

HIPAA (Health Insurance Portability and Accountability Act). Amerykański odpowiednik regulujący poufność i integralność danych medycznych, w tym:

- szyfrowanie danych w spoczynku i w transmisji,
- kontrolę dostępu,
- audyt aktywności użytkowników.

Normy ISO/IEC 27001 oraz 27701. Określają wymagania dla systemów zarządzania bezpieczeństwem informacji (ISMS) oraz ochroną danych osobowych (PIMS).

1.3 Stosowane technologie i narzędzia

W ramach zajęć studenci wykorzystają narzędzia i techniki umożliwiające zabezpieczanie danych medycznych:

- **Szyfrowanie symetryczne i asymetryczne** (AES, RSA).
- **Haszowanie kryptograficzne** (SHA-256, SHA-3).
- **Kontrola dostępu** (mechanizmy RBAC/ABAC).
- **Pseudonimizacja i anonimizacja** danych medycznych.
- **Wykrywanie manipulacji danych** (np. poprzez funkcje skrótu).
- **Bezpieczne przechowywanie kluczy** (np. poprzez `Fernet`).

1.4 Przebieg ćwiczenia

Etap 1: Przygotowanie i analiza danych

- Zaimportuj przykładowy zbiór danych medycznych (np. dane pacjentów zawierające: wiek, BMI, parametry pomiarowe, diagnozy).
- Zidentyfikuj dane wrażliwe wymagające ochrony: dane identyfikujące, dane kliniczne, zmienne diagnostyczne.
- Oddziel dane osobowe od danych klinicznych.

Etap 2: Szyfrowanie i integralność danych

- Zaszyfruj wybrane kolumny danych przy użyciu szyfrowania symetrycznego (np. AES/Fernet).
- Wygeneruj i zastosuj funkcje skrótu (SHA-256) do weryfikacji integralności plików.
- Sprawdź, jak zmiana jednego bitu w danych wpływa na funkcję skrótu.

Etap 3: Pseudonimizacja i anonimizacja

- Zastosuj pseudonimizację danych pacjentów (np. zamiana identyfikatorów na losowe tokeny).
- Zastosuj anonimizację w oparciu o techniki:
  - usuwanie identyfikatorów,
  - generalizacja (np. grupy wiekowe),
  - maskowanie danych.
- Przeanalizuj wpływ anonimizacji na jakość modelu SI.

Etap 4: Kontrola dostępu i audyt

- Zaimplementuj prosty mechanizm RBAC (Role-Based Access Control), definiując role: **administrator**, **lekarz**, **analityk**.
- Ogranicz dostęp do wybranych kolumn w zależności od roli.
- Zaimplementuj logowanie operacji dostępu do danych (audyt).

Etap 5: Bezpieczeństwo modeli SI

- Zabezpiecz dane wejściowe modelu przed manipulacją (np. dodaj weryfikację skrótu).
- Zaimplementuj walidację danych przed podaniem ich do modelu.
- Przeanalizuj zagrożenia takie jak: poisoning, data tampering, adversarial examples.

1.5 Python – przykładowe fragmenty kodu

Szyfrowanie danych (Fernet, AES)

```
from cryptography.fernet import Fernet
import pandas as pd

key = Fernet.generate_key()
cipher = Fernet(key)

df = pd.read_csv("dane_medyczne.csv")
df["diagnosis_enc"] = df["diagnosis"].apply(
    lambda x: cipher.encrypt(x.encode()).decode()
)
```

Haszowanie (SHA-256)

```
import hashlib

with open("dane_medyczne.csv", "rb") as f:
    content = f.read()
hash_val = hashlib.sha256(content).hexdigest()
print("SHA-256:", hash_val)
```

Pseudonimizacja kolumny

```
import uuid
df["patient_id"] = [str(uuid.uuid4()) for _ in range(len(df))]
```

1.6 Zadania dla studentów

Zaimplementuj bezpieczeństwo danych w miniaplikacji (Etapy 1-5) na porstawie własnego zbioru danych klinicznych - szyfrowanie, skróty, audyt:

1. Porównaj różne algorytmy haszujące i oceń ich odporność na kolizje.
2. Utwórz procedurę pseudonimizacji i sprawdź, jak wpływa ona na model predykcyjny.
3. Zasymuluj manipulację danymi wejściowymi i zaimplementuj detekcję naruszeń integralności.
4. Zaimplementuj system kontroli dostępu RBAC z poziomami dostępu dla różnych użytkowników.
5. Przeanalizuj ryzyka w systemach SI opartych na danych medycznych.
6. Zaimplementuj szyfrowanie całego pliku i obsługę klucza szyfrującego.
7. Wykonaj audyt logów dostępu i zaproponuj ulepszenia polityk bezpieczeństwa.