Микола Сало, Євген Волинець
[1] НЛТУ України, Львів, Україна, ORCID: 0009-0002-2548-5211,
mykola.salo@nltu.edu.ua
[2] НЛТУ України, Львів, Україна. ORCID: 0009-0008-1071-3852,
yevhenvolynets@nltu.edu.ua

Особливості архітектури та безпеки мобільних застосунків у сфері охорони здоров'я

Анотація. *Здійснено опис специфіки проектування та розробки мобільних застосунків у сфері охорони здоров'я (mHealth). Проаналізовано ключові відмінності між комерційним програмним забезпеченням та медичними рішеннями класу SaMD. Основну увагу приділено питанням архітектури безпеки, дотриманню регуляторних норм (GDPR, HIPAA) та проблемам інтероперабельності даних. Результати аналізу можуть бути використані при створенні безпечних медичних інформаційних систем.*

Ключові слова *– mHealth, SaMD, кібербезпека, інтероперабельність, FHIR, GDPR.*

Вступ. У сучасному світі трансформація охорони здоров'я нерозривно пов'язана з концепцією mHealth (mobile health). Мобільні пристрої дозволяють здійснювати безперервний моніторинг стану пацієнта та надавати дистанційні послуги. Проте розробка таких систем стикається з критичними викликами [1]: необхідністю забезпечення конфіденційності пацієнтів (PHI), відповідності суворим регуляторним нормам (GDPR, HIPAA, ISO 13485) та гарантування цілісності клінічних даних. Метою цієї роботи є систематизація інженерних підходів до проектування архітектури мобільних клієнтів, які забезпечують баланс між надійним захистом даних та користувацьким досвідом.

Архітектура mHealth застосунку: Offline-First та Синхронізація. Створення програмного забезпечення для медицини передбачає дотримання жорстких стандартів. Якщо застосунок впливає на лікування або діагностику, він класифікується як "Software as a Medical Device" (SaMD). Архітектура повинна забезпечувати мінімізацію даних, збираючи лише те, що критично необхідно для функціонування, що відповідає принципам GDPR [2].

* науковий керівник

Специфіка мобільного використання передбачає нестабільність інтернет-з'єднання. Для забезпечення безперервності надання медичних послуг пропонується використання архітектурного підходу Offline-First із патерном Store-and-Forward. Дані (наприклад, показники життєдіяльності), зібрані сенсорами, спочатку зберігаються у локальній зашифрованій базі даних (наприклад, Realm або Room із SQLCipher). Синхронізація з сервером відбувається через чергу запитів (Request Queue) лише за наявності стабільного з'єднання, що запобігає втраті критичних даних.

Загальна схема взаємодії компонентів зображена на Рис.1

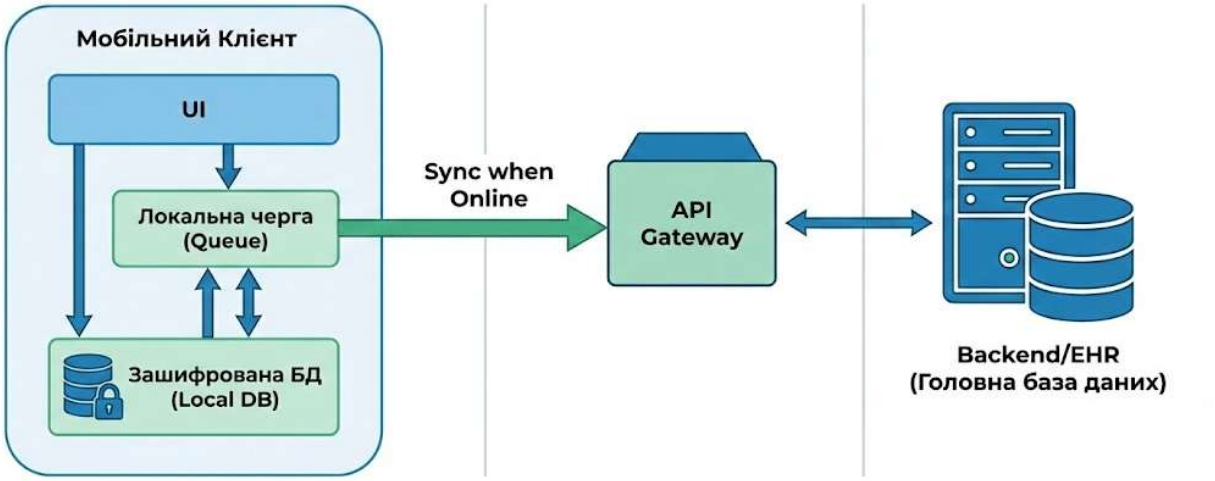

Рисунок 1. Трирівнева архітектура mHealth застосунку з підтримкою offline-режиму

Багаторівнева модель безпеки. Захист даних реалізується на трьох рівнях: дані у спокої, дані під час передачі та захист від витоків через відлагодження.

Захист даних у спокої (Data at Rest): Використання лише програмного шифрування є недостатнім. Архітектура повинна передбачати використання апаратних засобів безпеки. Ключі шифрування (AES-256) генеруються та зберігаються в ізольованих контейнерах ОС: Android Keystore та iOS Keychain (Secure Enclave). Доступ до ключів може бути додатково захищений біометричною аутентифікацією.

* науковий керівник

Захист даних під час передачі (Data in Transit): Окрім стандартного протоколу TLS 1.3, критично важливим є впровадження Certificate Pinning (жорстка фіксація сертифіката сервера в коді додатка) для захисту від атак "Man-in-the-Middle". Для доступу до API рекомендовано використовувати mTLS (Mutual TLS), де сервер також перевіряє криптографічний сертифікат мобільного клієнта (Рис. 2).

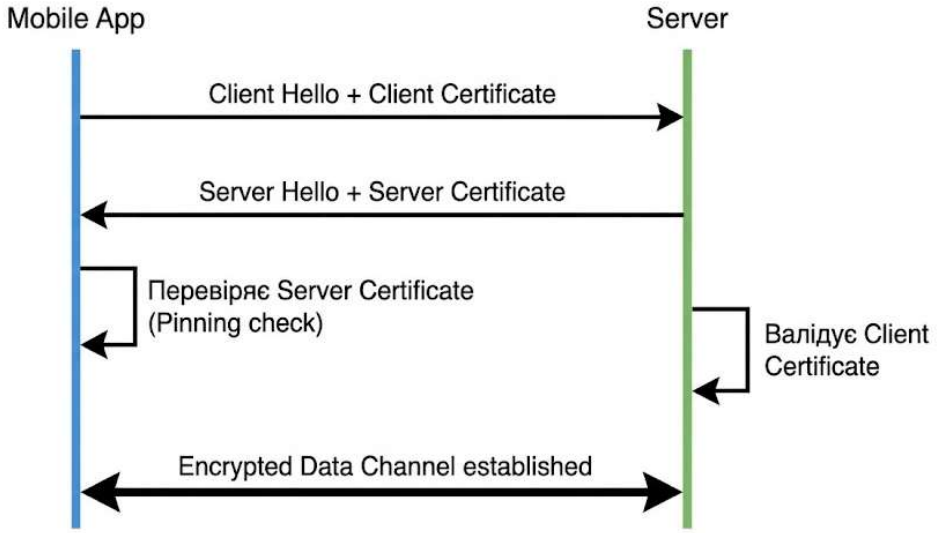

Рисунок 2. Процес взаємної аутентифікації mTLS

Санітизація логів та захист від витоків. Поширеним вектором витоку PHI є системні журнали (logs). Стандартні методи логування можуть випадково зберегти токени доступу або дані пацієнта у відкритому вигляді. Запропоновано впровадження архітектурного шару Log Sanitization Layer (Рис. 3). Усі лог-повідомлення та мережеві запити проходять через спеціальний перехоплювач (Interceptor), який використовує RegEx-правила для виявлення чутливих даних та їх заміни на плейсхолдери (наприклад, [REDACTED]) перед записом у консоль або відправкою в системи краш-аналітики.

Інтероперабельність: FHIR та SMART on FHIR. Для інтеграції з різнорідними госпітальними системами (EHR) використовується стандарт HL7 FHIR [3]. Мобільний додаток виступає як клієнт, що нормалізує зібрані біосигнали у формат ресурсів *Observation* (з використанням кодів LOINC) перед відправкою. Авторизація доступу до медичних даних здійснюється через протокол SMART on FHIR (на базі OAuth 2.0). Це дозволяє делегувати права доступу та отриму-

* науковий керівник

вати гранулярні дозволи (Scopes), наприклад, "читання лише аналізів крові", без передачі пароля користувача самому додатку.

Рисунок 3. Схема процесу санітизації логів

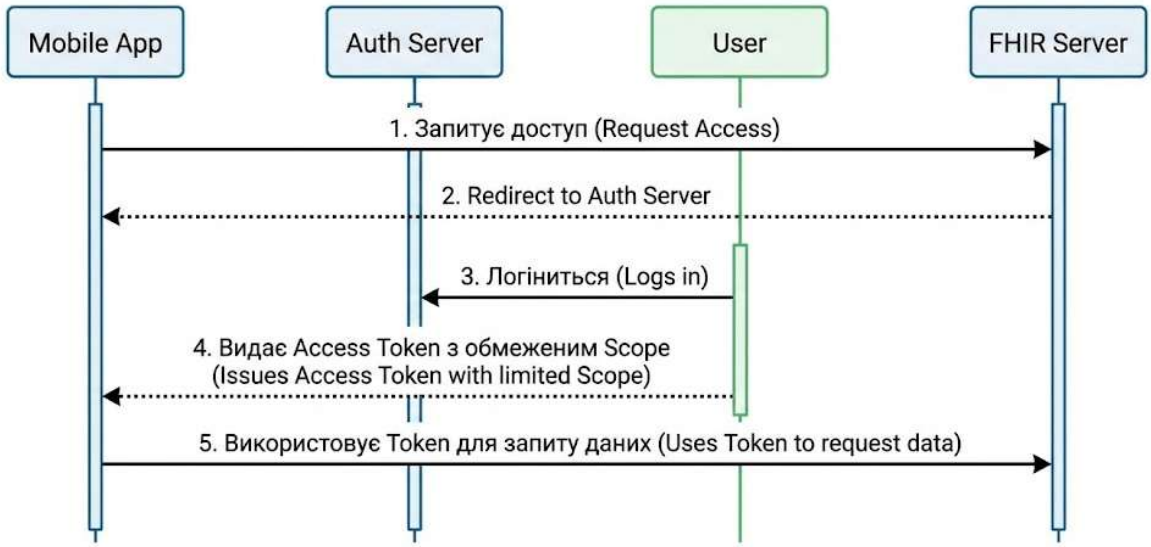

Рисунок 4. Потік авторизації SMART on FHIR

Висновок. Розробка mHealth рішень вимагає синергії між програмною інженерією, правом та медициною. Запропонована архітектура, що включає апаратне зберігання ключів, mTLS, санітизацію логів та підтримку стандарту FHIR, дозволяє створити безпечне середовище для роботи з чутливими даними. Подальші дослідження будуть спрямовані на вдосконалення методів використання штучного інтелекту безпосередньо на мобільному пристрої (On-device ML) для збереження приватності.

* науковий керівник

Список використаних літературних джерел

[1] John R. Patrick (2017). Home Attitude: Everything You Need To Know To Make Your Home Smart. California, US: The Appliance Studio, University Gate East CreateSpace Independent Publishing Platform.

[2] European Commission (2018). General Data Protection Regulation (GDPR). Official Journal of the European Union.

[3] HL7 International (2023). HL7 FHIR Release 4B. Ann Arbor, MI: Health Level Seven International.

Features of developing mobile applications for the healthcare sector

Mykola Salo, Yevhen Volynets

The specific character of designing and developing mobile applications in the healthcare sector (mHealth) is described. Key differences between commercial software and SaMD class medical solutions are analysed. The main focus is on security architecture issues, compliance with regulatory standards (GDPR, HIPAA), and data interoperability problems. The results of this analysis can be used to create secure medical information systems.

* науковий керівник