**Міністерство освіти і науки України**

Національний університет “Львівська політехніка”

Інститут комп’ютерних наук та інформаційних технологій

**Кафедра САПР**



**Лабораторна робота №6**

з дисципліни: “Технології та стандарти інтернету речей”

**на тему:**

“Інтеграція безпеки даних для систем інтернету речей”

**Виконав**:

Ст. групи ПП-44

Верещак Б. О.

**Прийняв**:

асис. Гавран В. Б.

**Львів - 2025**

**Мета роботи**

Ознайомитись з принципами забезпечення безпеки даних у системах Інтернету речей (IoT), навчитися реалізовувати базові методи захисту даних, такі як шифрування, автентифікація та контроль доступу.

**Теоретичні відомості**

Майже кожен пристрій Інтернету речей, який підключений до мережі, може отримати доступ до інфраструктури Інтернету речей, а також до ваших персональних даних. Коли з’являються нові лазівки в безпеці та потенційні вразливості, ризики, пов’язані з Інтернетом речей, виходять на новий рівень через сумісність, програми та автономне прийняття рішень. Тому безпека та конфіденційність даних є життєво важливими.

Інтернет речей – це мережа, яка об’єднує мобільну мережу, соціальні мережі, Інтернет і різні розумні об’єкти, щоб надати користувачам різноманітні послуги та додатки.

Покращуючи безпеку взаємодії об’єктів, надійність і сумісність, безпека на різних рівнях безпосередньо впливає на успіх систем Інтернету речей. Інтенет речей тепер може об’єднувати різні простори (наприклад, фізичне та цифрове), де різні датчики взаємодіють з фізичним простором. Ці датчики вже повністю використовуються практично у всьому, від іграшок до систем охорони здоров’я. Це показує, як різні небезпеки, які виникають у цифровому світі, починають діяти на реальний світ.

Система успішна, якщо вона може забезпечити безпеку від вразливостей. Багато в чому успіх додатків Інтернету речей та інфраструктури Інтернету речей залежить від забезпечення безпеки та уразливості. Вимогами до безпеки Інтернету речей (IoT) є велика кількість нових інструментів, які вбудовані в організацію, а часом і в систему.

Всі пристрої, які є підключеними, мають потенціал отримати доступ до Інтернет-інфраструктури або особистих даних. Такі пристрої можна аналізувати та використовувати. У результаті аналізу цих даних можна створити невидимі посилання, які можуть бути спрямовані на конфіденційність людей або організацій. Незважаючи на те, що проблеми безпеки та конфіденційності є надзвичайно важливими, ймовірність небезпеки для об’єктів підвищиться, оскільки сумісність, гібридні програми та незалежне прийняття рішень створюють складність, прогалини в безпеці та потенційні вразливості.

У сфері інформаційних технологій існує ризик захисту даних, оскільки складність може створити високу вразливість у зв’язку з послугами. Більшість інформації, доступної в Інтернеті речей, пов’язана з нашими особистими даними, такими як дата народження, місце розташування, бюджет тощо. Однією з проблем великих даних є ризики, які застосовуються до кожного набору даних. Інтернет речей має бути реалізований законним, моральним, соціальним і політичним способом. При цьому слід враховувати юридичні, систематичні, технічні та бізнес-проблеми.

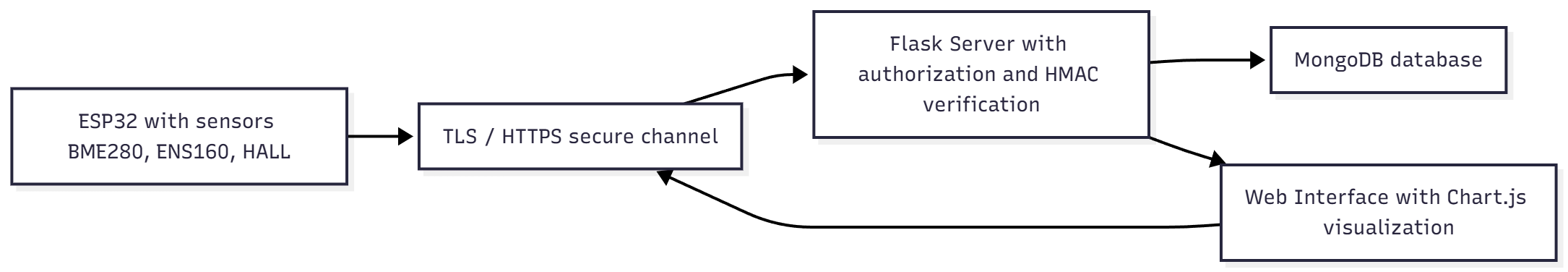
**Лабораторне завдання**

* Ознайомитися з теоретичними відомостями.
* Інтегрувати та описати принципи безпеки даних для ІоТ проекту згідно з варіантом.
  + Розумні парковки: Система моніторингу та резервування місць;
  + Інтелектуальна система керування шторами;
  + Інтелектуальна система керування електроспоживанням будинку;
  + Інтелектуальна система керування та оптимізації домашніх генераторів;
  + Застосунок для керування LED-стрічкою та освітленням;
  + Розумний інкубатор;
  + Система моніторингу периметру і виявлення загрози;
  + Інтелектуальна система догляду за садом;
  + Розумний термостат для опалення;
  + Розумні двері для домашніх тварин.
* Оформити звіт до лабораторної роботи.

**Результати виконання завдання:**

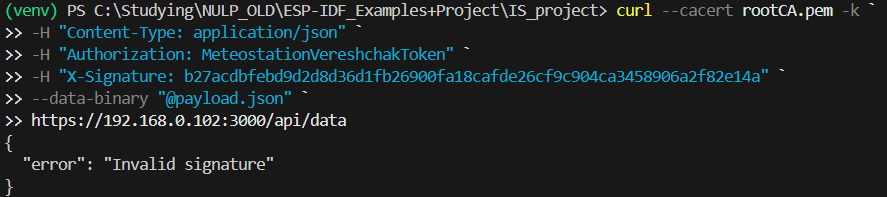
На цій лабораторній роботі було інтегровано та документовано комплекс заходів із захисту даних для IoT-проєкту Метеостанції. Метою було забезпечення конфіденційності, цілісності та доступності даних від сенсора до веб-інтерфейсу, мінімізувати ризики несанкціонованого доступу і атак, а також зробити систему простою для перевірки безпеки під час тестування й демонстрацій.

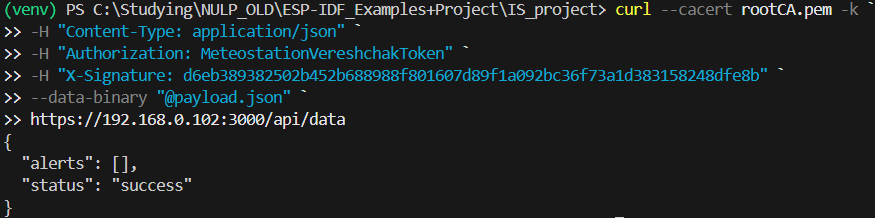
Першим і основним рівнем захисту є канал передачі: всі зв’язки між ESP32 і сервером виконуються через HTTPS (TLS). Це означає, що весь HTTP-трафік (заголовки й тіло повідомлень) передається зашифрованим потоком; перехоплювач бачить лише TLS-записи та IP/домен, але не може прочитати JSON-payload. На пристрої впроваджено перевірку сертифіката сервера: у прошивці або вбудовується кореневий CA (rootCA.pem), або читається з файлової системи (SPIFFS). Таке рішення запобігає MITM-атакам навіть у випадку, коли хтось спробує підмінити сертифікат.



*Рис. 1. Архітектура IoT системи*

Другий важливий рівень – аутентифікація та контроль доступу. Кожна метеостанція має унікальний device-token, який передається в заголовку Authorization; сервер зберігає перелік дозволених токенів і пов’язує кожен токен із конкретним device\_id. Для підвищення гарантій достовірності пакетів використовується HMAC-підпис (SHA256) over raw payload з спільним секретом: клієнт обчислює HMAC(SECRET\_KEY, payload) і посилає результат у заголовку X-Signature. Сервер відтворює підпис по отриманих сирих байтах і порівнює їх захищеним методом hmac.compare\_digest. Така схема гарантує, що навіть у випадку перехоплення зашифрованого потоку зміни в даних або підробка повідомлення будуть виявлені.



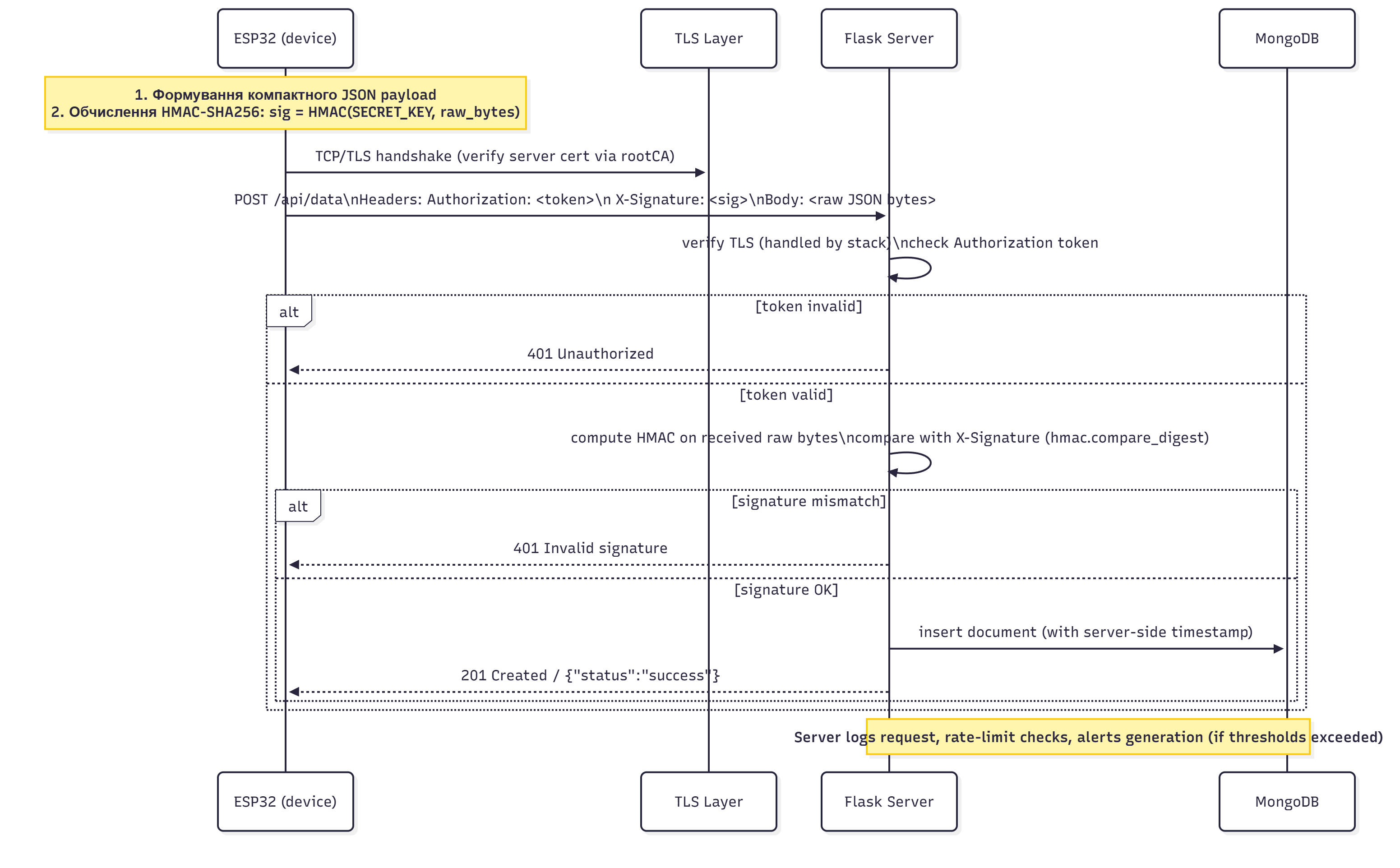


*Рис. 2. Результат відправки неправильного підпису файлу і правильного*

На сервері реалізовано багатоаспектний захист: всі критичні ендпоїнти вимагають Authorization; маршрути, що змінюють конфігурацію (наприклад, /api/config), додатково обмежені правами адміністратора або окремим адмін-токеном; введено перевірку цілісності даних перед збереженням (сервер валідить типи і межі параметрів), логування подій і обмеження швидкості запитів (rate limiting). Дані в MongoDB зберігаються під обліковим записом з паролем, доступ до БД обмежений мережею.

Практична реалізація на ESP32 враховує обмеження пристрою: для стабільності HMAC формується над компактним JSON, на пристрої встановлено перевірку TLS через .cert\_pem = server\_root\_cert\_pem, а всі запити – GET для конфігів і POST для даних – підписуються й відправляються з заголовком Authorization. HMAC-ключ і токени зберігаються в прошивці для лабораторного завдання; у виробничих умовах їх слід тримати у секретному сховищі або використовувати secure element.

Перевірка безпеки виконувалася систематично: TLS-зв’язок контролювався за допомогою openssl s\_client -connect host:port і curl –cacert rootCA.pem, трафік аналізувався у Wireshark – при коректній конфігурації видно TLS-handshake, але не JSON-трафік. Тестування HMAC-перевірки проводилося шляхом генерації підпису локально (OpenSSL або Python hmac) і відправки запиту через curl або Python requests; сервер коректно відхиляв змінені payloads або неправильні сигнатури (HTTP 401).



*Рис. 3. Послідовність: підписування (ESP32) → верифікація (Flask)*

**Висновки**

На даній лабораторній роботі я ознайомився з принципами забезпечення безпеки даних у системах Інтернету речей (IoT), навчитися реалізовувати базові методи захисту даних, такі як шифрування, автентифікація та контроль доступу.

Реалізував багаторівневу систему безпеки для IoT-проєкту Метеостанції. Виконані завдання показали, як комплекс заходів – від захищеного каналу передачі даних до HMAC-підпису і контролю доступу – забезпечує конфіденційність, цілісність і доступність інформації в умовах обмежених ресурсів пристроїв.

Отриманий досвід показав, що навіть на обмежених IoT-пристроях можна реалізувати надійний захист даних, якщо системно підходити до вибору протоколів, методів аутентифікації та перевірки цілісності. Така лабораторна робота сприяє розумінню практичних принципів безпеки даних у реальних IoT-сценаріях і підвищує готовність до проєктування захищених систем у виробничих умовах.