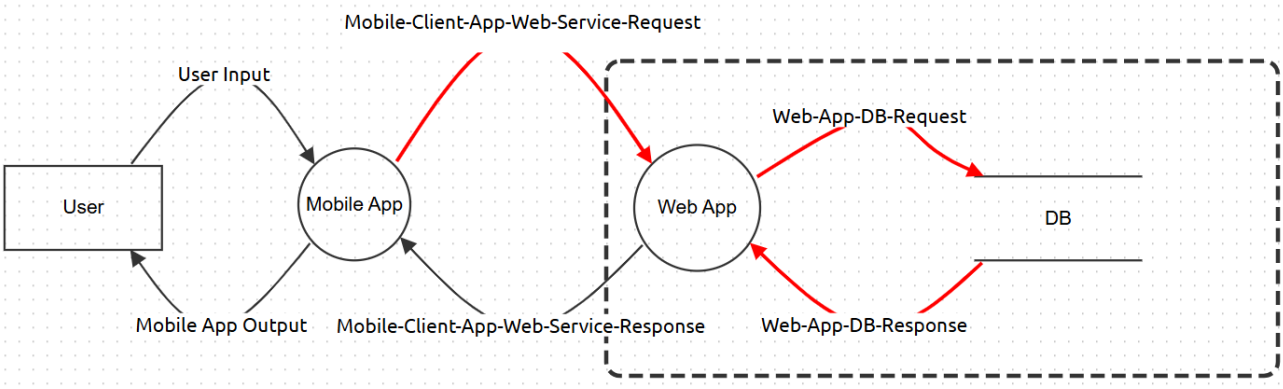

Рисунок 1 – Вигляд схеми застосунку в OWASP Threat Dragon

Система представляє собою розповсюджуваний додаток для мобільних пристроїв та єдиний веб-сервер із власне веб-застосунком та базою даних. Мобільний додаток взаємодіє із веб-застосунком, котрий в свою чергу оброблює запити та оновлює базу даних.

Опис зв’язків між сутностями:

1. User ↔ Mobile App

- Тип зв'язку: Взаємодія через інтерфейс.
- Напрямок: Двосторонній.
- Опис:
    - Користувач здійснює взаємодію з мобільним додатком (вхід у систему, перегляд даних, виконання дій).
    - Mobile App приймає вхідні дані (наприклад, введення через екран) і повертає результат роботи або повідомлення.

2. Mobile App ↔ Web App

- Тип зв'язку: API-запити або сервісна інтеграція.

- Напрямок: Двосторонній.
- Опис:
    - Mobile App може звертатися до Web App через API для отримання додаткових даних або виконання дій, які потребують серверної обробки.
    - Web App повертає результати запитів у форматі (наприклад, JSON, XML).

3. Web App ↔ DB

- Тип зв'язку: Запити до бази даних.
- Напрямок: Двосторонній.
- Опис:
    - Веб-додаток виконує CRUD-операції (Create, Read, Update, Delete) для роботи з даними.
    - База даних обробляє запити (отримує, оновлює, створює або видаляє записи) і повертає результат.

Наведемо таблицю загроз:

No загрози	Назва зв’язку	STRIDE-клас загрози	Назва загрози	Опис загрози
0	Mobile-Client-App-Web-Service-Request	Elevation of Privileges	An adversary may jail break into a mobile device and gain elevated privileges	An adversary may jail break into a mobile device and gain elevated privileges
1	Mobile-Client-App-	Information Disclosure	An adversary can reverse weakly encrypted or hashed content	An adversary can reverse weakly encrypted or hashed content

	Web-Service-Request			
2	Mobile-Client-App-Web-Service-Request	Repudiation	Attacker can deny the malicious act and remove the attack foot prints leading to repudiation issues	Proper logging of all security events and user actions builds traceability in a system and denies any possible repudiation issues. In the absence of proper auditing and logging controls, it would become impossible to implement any accountability in a system
3	Mobile-Client-App-Web-Service-Request	Spoofing	An adversary can spoof the target web application due to insecure TLS certificate configuration	Ensure that TLS certificate parameters are configured with correct values
4	Mobile-Client-App-Web-Service-Request	Tampering	An adversary can reverse engineer and tamper binaries	An adversary can use various tools, reverse engineer binaries and abuse them by tampering
5	Web-App-DB-Request	Elevation of Privileges	An adversary can gain unauthorized access to Azure SQL database due to weak account policy	Due to poorly configured account policies, adversary can launch brute force attacks on Azure SQL Database
6	Web-App-DB-Request	Information Disclosure	An adversary can read confidential data due to weak connection string configuration	
7	Web-App-DB-Request	Repudiation	An adversary can deny actions performed on Azure SQL Database due to a lack of auditing	An adversary can deny actions performed on Azure SQL Database due to a lack of auditing.
8	Web-App-DB-Request	Elevation of Privileges	An adversary can gain long term, persistent access to an Azure SQL DB instance through the compromise of local user account password(s)	An adversary can gain long term, persistent access to an Azure SQL DB instance through the compromise of local user account password(s).
9	Web-App-DB-Request	Elevation of Privileges	An adversary may abuse weak Azure SQL Database configuration	An adversary may abuse weak Azure SQL Database configuration.

Опишемо наведені загрози:

0. Злом мобільного пристрою через джейлбрейк дозволяє атакувальнику отримати контроль над системними функціями, обходити обмеження додатків та отримувати доступ до чутливої інформації.

1. Слабка криптографія дозволяє атакувальникам декодувати чутливу інформацію, наприклад, паролі чи персональні дані, під час передачі між клієнтом і веб-сервісом.

2. Відсутність адекватного логування й аудиту призводить до неможливості забезпечити підзвітність. Це дає змогу атакувальникам уникнути відповідальності за свої дії.

3. Некоректна конфігурація TLS може дозволити атакувальникам підробити веб-додаток і обманом змусити користувачів взаємодіяти з підробленим сервісом.

4. Зловмисники можуть використовувати спеціальні інструменти для аналізу мобільного додатка, змінювати код програми й використовувати його у зловмисних цілях, наприклад, обходячи механізми безпеки.

5. Недостатньо сильна політика паролів або захисту облікових записів може дозволити атакувальнику виконувати атаки типу "brute force" для доступу до бази даних.

6. Неправильно налаштовані або відкриті рядки підключення до бази даних можуть дозволити атакувальникам отримати доступ до конфіденційної інформації, такої як логіни, паролі або бізнес-дані.

7. Відсутність журналів дій та аудиту ускладнює або унеможливлює відстеження того, хто і які дії виконував у системі, що дозволяє атакувальникам уникати відповідальності.

8. Якщо паролі локальних користувачів зламані або викрадені, атакувальник може забезпечити собі довготривалий доступ до бази даних, що дозволить виконувати шкідливі дії.

9. Недостатньо жорстка конфігурація, наприклад, надмірні дозволи для облікових записів, дозволяє атакувальникам отримувати доступ або здійснювати операції, на які вони не мають прав.