УДК 004.031.4
Пундик В. І.– ст. гр. СІм-51
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНОСТІ AZURE IOT HUB

Науковий керівник: к.т.н., доц. Яцишин В.В.

PundykV.I.
TernopilIvanPul'ujNationalTechnicalUniversity

RESEARCHOFAZURE IOT HUB FUNCTIONALITY

Supervisor: PhD, Assoc. Prof. Yatsyshyn V.V.

Ключові слова:інтернет речей,cloud-сервіси.
Keywords: internet of things, cloud-services.

AzureIoTHub – це повністю керований сервіс, який забезпечує надійний і безпечний двосторонній зв'язок між мільйонами пристроїв IoT і back-end рішеннями. До основних функціональних можливостей AzureIoTHub належить:

- забезпечення надійного обміну повідомленнями пристрій-хмара і хмара-пристрій з можливістю масштабування;
- гарантування безпечного зв'язку кожного пристроюна основі облікових даних безпеки та контролю доступу;
- забезпечення моніторингу для підключених пристроїв і управління ідентифікаційними даними пристрою подій;
- включає в себе бібліотеки пристроїв для найбільш популярних мов і платформ.

IoTHubі бібліотеки пристроїв дають змогунадійно та безпечно підключати пристрої до back-end рішень.

IoT пристрої характеризуються наступними критеріями:

- можуть бути представлені, яквбудовані системи без людини-оператора;
- можуть бути у віддалених місцях, де фізичний доступ занадто дорогий;
- можуть бути доступні тільки через back-end;
- можуть мати обмежені ресурси живлення і обробки;
- можутьбути підключеними до мережі через повільне або дороге з'єднання;
- можутьпотребувати використання галузевих (внутрішніх) протоколів.
- можуть бути створеними за допомогою великого набору популярних апаратних і програмних платформ.

Окрім, вище перелічених критеріїв,IoT рішення повинні також забезпечувати масштабованість, безпеку і надійність. При використанні традиційних технологій, таких як веб-контейнери і брокери обміну повідомленнями важко реалізувати підключення з дотриманням наведених вимог.

AzureIoTHub вирішує проблеми підключення пристроїв наступними способами:

- аутентифікація і безпечне підключення.Кожному пристрою надається власний ключ захисту, якийдає змогу підключитися до IoTHub. Реєстр IoTHub зберігає ключі пристрою;
- моніторинг операцій підключення пристрою. Існує можливість одержання детальної інформації про операції управління ідентифікацією і подій підключення пристрою. Це дозволяє легко ідентифікувати проблеми з підключенням, наприклад,

пристрої, які намагаються з'єднатися з неправильними обліковими даними, відправляти повідомлення занадто часто, або відкидати всі повідомлення cloud-device.

- великий набір бібліотек пристроїв. Бібліотеки доступні і підтримуються для безлічі мов і платформ – C для багатьох дистрибутивів Linux, Windows і операційних систем реального часу. Бібліотеки також підтримуються для таких мов як C #, Java і JavaScript.
- IoT протоколи та розширення. Якщо рішення не може використовувати стандартні бібліотеки, IoTHubдає змогунативно використовувати MQTT v3.1.1, HTTP 1.1, або 1.0 AMQP протоколи. Також можна розширити IoTHub для забезпечення підтримки користувацьких протоколів шляхом налаштування шлюзу протоколуAzureIoT;
- масштабованість. AzureIoTHubмасштабується для мільйонів одночасно підключених пристроїв і мільйонів подій в секунду.

Ці переваги є спільними для багатьох моделей комунікації. На рисунку 1 зображена структура та можливі схеми підключення пристроїв до IoTHub.

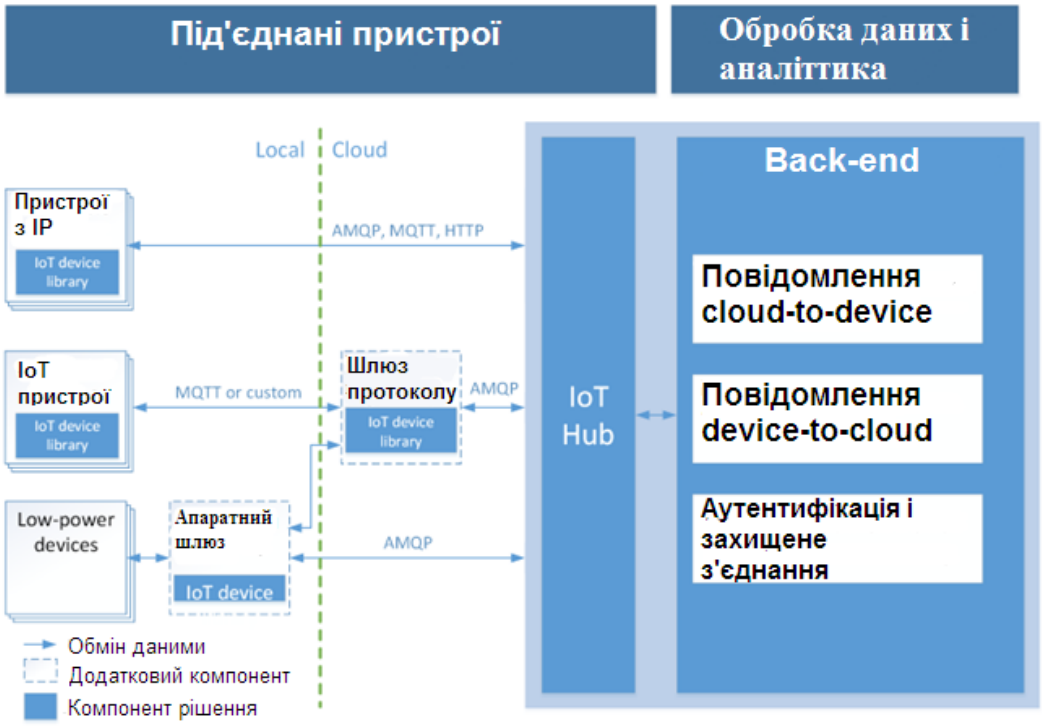

Рисунок 1 – Структура та можливі методи підключення

IoTHubна даний час дозволяє реалізувати наступні конкретні моделі комунікації:

- Повідомлення device-to-cloudна основі подій пристрою. IoT концентратор може надійно отримати мільйони подій в секунду з пристроїв. Потім він може обробляти їх за допомогою процесора подій. Він може також зберігати їх для аналізу. IoTHub зберігає дані про події на термін до семи днів, щоб гарантувати надійну обробку і поглинати піки навантаження.
- Повідомлення cloud-to-device (або команди). Back-end може використовувати IoTHub для відправки повідомлень з гарантією мінімум одноразової доставки на кожен пристрій. Кожне повідомлення має індивідуальні настройки термін існування, і може запросити як підтвердження доставки, так і закінчення терміну існування. Це забезпечує повну видимість в життєвому циклі повідомлення cloud-to-device. Крім того, існує можливість виконання іншихфункцій, таких як завантаження та скачування файлів. Ці функції включають в себе управління пристроями, моніторинг підключення і масштабування.