КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
Факультет радіофізики, електроніки та комп'ютерних систем
Кафедра комп'ютерної інженерії

ВИКОРИСТАННЯ ЗАСОБІВ IOT В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Дипломна робота бакалавра
студента 4 року навчання
спеціальність: 123 «Комп'ютерна інженерія»
Богдана ОВСАКА

Науковий керівник:
доцент, кандидат фіз.-мат. наук
Юрій БОЙКО

Рецензент:
професор, доктор фіз.-мат. наук
Євген ІВОХІН

До захисту допускаю: Завідувач кафедрою
Юрій БОЙКО

Ухвалено на засіданні кафедри ―____‖_____2022 р., протокол № ____

Київ - 2022

РЕФЕРАТ

Обсяг роботи 61 сторінка, 18 ілюстрацій, 5 таблиць, 71 джерел посилань, 4 додатки.

Метою роботи є огляд основних протоколів та технологій Інтернету речей, Інтернет платформ; аналіз можливостей використання засобів IoT в закладах вищої освіти; побудова моделі використання Інтернету речей у закладах вищої освіти.

Результати роботи: Виконано огляд існуючих основних протоколів та технологій Інтернету речей; розглянуто основні IoT-платформи; проаналізовано основні можливості впровадження засобів Інтернету речей в закладах вищої освіти; побудовано модель використання засобів Інтернету речей в закладі вищої освіти.

Впровадження засобів Інтернету речей в закладах вищої освіти наразі знаходиться на початковому етапі розвитку, а можливих засобів Інтернету речей для його реалізації існує велика кількість. Тому заклади вищої освіти мають обирати серед великої кількості різних варіантів, що є доволі обтяжливим та тривалим процесом. Побудована у даній роботі модель може бути використана при розгортанні IoT інфраструктури в закладі вищої освіти.

Побудова інфраструктури Інтернету речей в закладах вищої освіти є етапом розвитку систем Розумного міста, тому вона може бути інтегрована в ці системи. Її використання дозволить зменшити витрати цих закладів на електроенергію та теплопостачання, дозволить покращити безпеку та покращить умови перебування для студентів, викладачів та відвідувачів.

Ключові слова : ІНТЕРНЕТ РЕЧЕЙ, ІНТЕРНЕТ ПЛАТФОРМИ, ЗАСОБИ ІНТЕРНЕТУ РЕЧЕЙ, ЗАКЛАДИ ВИЩОЇ ОСВІТИ, ІННОВАЦІЇ.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧЕННЯ

AMQP – Advanced Message Queuing Protocol;

AWS – Amazon Web Services;

CAGR – Сукупний середньорічний темп росту

COAP – Simple Object Access Protocol;

DDS – Data Distribution Service;

HTTP – Hypertext Transfer Protocol;

HTTPS – Hypertext Transfer Protocol Secure;

IETF – Internet Engineering Task Force

IIoT – Індустріальний Інтернет речей

IoT – Інтернет речей;

ІКТ – Інформаційно-телекомунікаційні технології

ISO – International Organization for Standardization;

IWF – Міжнародний форум з розвитку Інтернету речей;

MQTT – Message Queuing Telemetry Transport;

NFC – Near Field Communication;

OASIS – Organization for the Advancement of Structured Information Standards;

OMG – Object Management Group;

RFC – Request for Comments;

RFID – Radio-frequency identification, радіочастотна ідентифікація;

Smart City – Розумне місто

XMPP – Extensible Messaging and Presence Protocol;

ЗВО – Заклад вищої освіти**;**

HVAC – Опалення, вентиляція та кондиціювання**;**

SLU – Університет Сент-Луїза

ВСТУП

Від початку виникнення мережі Інтернет можна спостерігати поступовий процес проникнення цифрових технологій в повсякденне життя людей. Така тенденція щороку створює нові можливості для цілих галузей. Вже зараз відбувається процес інтеграції підприємств і цифрових платформ, тобто йде впровадження віртуальних платформ у діяльність бізнесу загалом. Даний процес пов'язаний з необхідністю обробки великих обсягів інформації про діяльність бізнесу, розширення каналів передачі цієї інформації всередині та ззовні підприємств, ефективного зв’язку різних відділів між собою.

Концепція була сформульована в кінці XX століття як позначення перспектив широкого використання засобів радіочастотної ідентифікації для взаємодії фізичних об'єктів як між собою, так і з зовнішнім світом [68, 69]. А сам термін «Інтернет речей» був запропонований в 1999 році Кевіном Ештоном [53], який припустив, що можливо зв'язати кілька фізичних об'єктів («речей») на виробництві для обміну інформацією і взаємодії між собою і з зовнішнім середовищем. Відповідаючи на питання, чому була сформульована така концепція варто звернути увагу на бурхливе зростання Інтернету в 90-ті роки, якраз тоді почалося масове впровадження роздрібної торгівлі через Інтернет, тобто тоді починався ринок електронної комерції, і людство почало усвідомлювати які можливості має дана технологія [5]. У 2004 році в науковому журналі Scientific American була опублікована велика стаття [26] присвячена «Інтернету речей». У ній була сформульована концепція IoT, були описані можливості застосування цієї концепції в житті людини загалом. Поняття Інтернету речей має відокремлення, яке називається Індустріальний Інтернет речей [71], який являє собою концепцію обчислювальної мережі фізичних об'єктів або речей, які оснащені вбудованими технологіями для взаємодії із зовнішнім середовищем або між собою, що дозволяє їм працювати без втручання людини.

Інтернет речей являє собою комп'ютерні системи, які працюють у режимі реального часу і складаються з мережі розумних пристроїв і серверу, або декількох серверів, або хмарної платформи, до якої вони підключені за допомогою засобів зв'язку, наприклад WiFi, Bluetooth, Ethernet тощо, і які виконують певну задану функцію.

Можна навести приклади використання таких IoT-систем:

- у побуті (системи розумного будинку);
- у медицині (системи моніторингу стану здоров'я, системи розумних лікарень [25, 55]);
- у транспорті (системи керування автопарком, електронні системи взяття оплати, системи керування транспортними засобами, системи безпеки транспорту [24, 49]);
- у виробництві (системи керування виробничими процесами, системи оптимізації використання електроенергії [65]);
- у сільському господарстві (системи прогнозування опадів, системи прогнозування врожаю, системи розумних теплиць [33]);
- у освіті (системи контролю відвідуваності, системи контролю енергозатрат приміщень [48, 50]).

Отже, можна говорити про всебічне використання Інтернету речей у багатьох сферах, що підтверджує актуальність використання IoT в закладах вищої освіти. Впровадження IoT-систем закладами вищої освіти обумовлене вигодами, які надають такі системи, а саме: економія коштів, покращення умов надання освіти, збільшення ефективності використання електроенергії, покращення безпеки відвідувачів, тощо.

В університеті Стенфорд впроваджується проект "Smart Campus", що являє собою IoT-систему управління енергопостачанням кампусу для покращення енергоефективності корпусів університету, покращення системи обслуговування і зменшення витрат на опалення. Також, університет штату

Аризона (ASU) ефективно впроваджує IoT-системи, наприклад, футбольний стадіон був обладнаний датчиками заповнення трибун, датчиками переповнення сміттєвих бачків [23]. Крім того, ASU створив систему розумного паркування, обладнавши датчиками паркувальні місця і створивши додаток для смартфона, щоб студенти могли відстежувати зайнятість паркувальних місць, бронювати місце для себе, тощо.

Використання IoT-систем є актуальним питанням сьогодення, яке потребує усвідомлення можливостей такого застосування і потребує реалізації IoT інфраструктури відповідно до потреб університету.

Дана робота має наступний вміст: Огляд та структура IoT, можливості використання IoT систем в університеті, розгляд технологій передачі даних IoT системами, аналіз існуючих IoT рішень, модель впровадження IoT рішення в Університеті.

Мета роботи: проведення огляду протоколів та технологій Інтернету речей, аналіз існуючих IoT-рішень, побудова моделі використання IoT в ЗВО.

РОЗДІЛ 1. СКЛАД І СТРУКТУРА ІНТЕРНЕТУ РЕЧЕЙ

1.1 ВИЗНАЧЕННЯ КОНЦЕПЦІЇ IOT

Інтернет речей є новітнім етапом розвитку обчислювальних систем та засобів зв'язку. Під цим терміном прийнято вважати комплекс високотехнологічних пристроїв, які підключені один до одного і виконують певні функції [26]. По суті Інтернет речей це концепція певної мережі передачі даних між фізичними об'єктами, які мають відповідні засоби для взаємодії як між собою, так і з навколишнім середовищем.

Сам термін Internet of Things був запропонований Кевіном Ештоном у 1999 році як певне переосмислення застосування радіочастотної ідентифікації (RFID) для взаємодії фізичних об'єктів між собою [26]. Далі, вже починаючи з 2010-х років, відбувається стійкий розвиток цієї концепції. Причиною тенденції є стрімке поширення Інтернету, розвиток безпровідних технологій зв'язку, поява хмарних обчислень тощо.

В загальному розумінні Інтернет речей (або IoT) можна сприймати як перспективну концепцію, яка має технологічні та соціальні наслідки[25]. З точки зору технічної стандартизації IoT – це інфраструктура для сучасного інформаційного суспільства, яка забезпечує надання більш складних послуг шляхом з'єднання фізичних та віртуальних речей за допомогою сумісних інформаційно-телекомунікаційних технологій (ІКТ)[29].

По відношенню до IoT, речі – це певні фізичні або віртуальні предмети, які можуть бути ідентифіковані в мережі зв'язку. З точки зору концепції, то у цій книжці Designing the Internet of Things [19] зауважено, що IoT характеризується додаванням нового виміру до концепції Інтернету, а саме комунікація між будь-якими речами (Рис. 1).

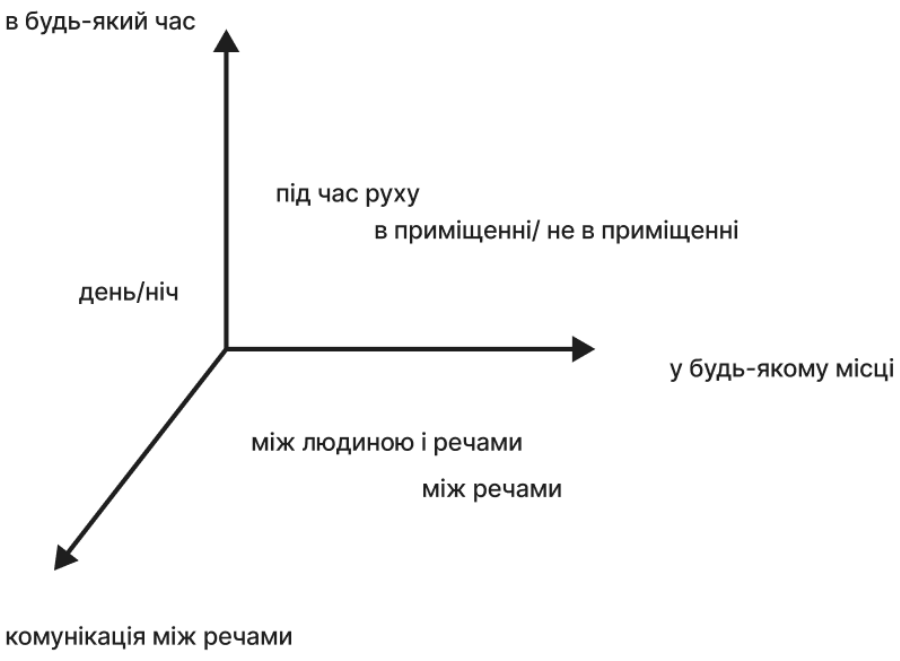


Рис. 1 Новий вимір в концепції Інтернету [19]

Зокрема, в книзі [19] елементи IoT пояснюються простою формулою:

$$\text{Фізичні об'єкти} + \text{контролери, сенсори, механізми} + \text{Інтернет} = \text{IoT}$$

Таким чином один екземпляр IoT складається з наступного набору фізичних об'єктів, кожен з яких:

- містить мікроконтролер, який забезпечує виконання якоїсь функції;
- містить датчик, який вимірює якийсь фізичний параметр або/і виконавчий механізм, який залежить від якогось фізичного параметра;
- має можливість комунікації за допомогою підключеної мережі;
- ідентифікується у мережі (має певний тег).

Інтернет речей є сукупністю певних приладів, які є підключеними до мережі і під керуванням певного програмного забезпечення (ПЗ) виконують певну закладену функцію без втручання людини [66].

1.2 ЕТАЛОННА АРХІТЕКТУРА IOT

Так як Інтернет речей має доволі велику складність технічних рішень, було необхідно стоворити певну архітектуру, яка б описувала його основні компоненти та їх взаємозв'язок. Крім того, наявність архітектури допомогла б адміністраторам мережі краще оцінювати справність роботи такої системи. А також, така архітектура могла б бути основою для стандартизації компонентів IoT, що може забезпечити сумісність і відповідно полегшити процес розробки.

Згідно з Рекомендацією Y.2060 [63] Міжнародного союзу електрозв'язку, еталонна модель IoT характеризується 4-ма рівнями, а саме:

- рівень пристрою (сенсори, виконавчі механізми);
- рівень мережі (Internet getaways);
- рівень підтримки послуг та підтримки за стосунків (аналітика, обробка даних);
- рівень застосунку.

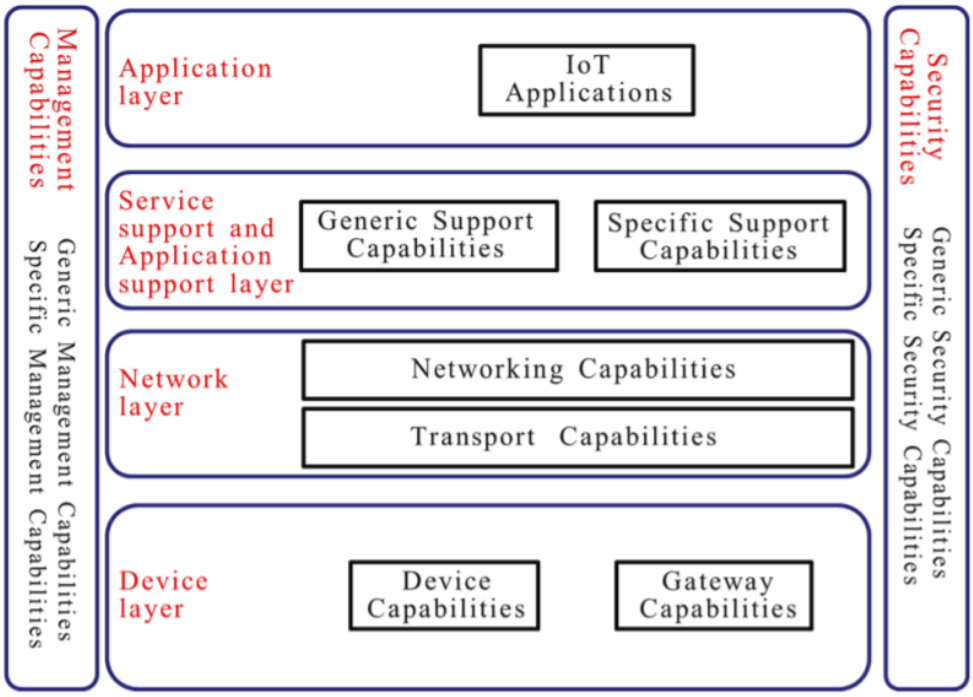


Рис 2. Еталонна архітектура [61]

Рівень пристрою включає в себе датчики та виконавчі механізми, а також механізм перетворення інформації з аналогової у цифрову і підтримку інтерфейсів.

Датчики можна поділити на наступні категорії:

- звукові: мікрофони;
- світлові: PIR датчики, датчики освітлення ;
- теплові: термопари, напівпровідникові датчики, терморезистор;
- електромагнітні сенсори для вимірювання фізичних характеристик (ємність, індуктивність, опір).

Датчики необхідні для того, щоб зчитувати певні дані з навколишнього середовища, далі дані передаються до блоку обробки даних пристрою.

Для перетворення аналогової інформації може використовуватися аналогово-цифровий перетворювач (АЦП) для подальшої її передачі через інтерфейси обміну даних. На рівні пристрою забезпечується підтримка декількох інтерфейсів для обміну даними. Наприклад, шини локальної мережі контролерів (CAN), ZigBee, Bluetooth, WiFi, Ethernet, LTE тощо.

Рівень мережі характеризується двома властивостями:

- організації роботи мережі, а саме надає функції керування з’днанням мережі. Наприклад, функції управління доступом;
- забезпечення сумісності IoT пристрою та програмного забезпечення при передачі даних.

Рівень підтримки роботи застосунків відповідає за підтримку роботи за стосунків і складається з двох основних властивостей:

- базова підтримка роботи за стосунку. До таких функцій належить обробка даних та їх зберігання для коректної роботи застосунків;

- спеціалізована підтримка роботи застосунку, це додатковий функціонал для роботи якогось конкретного за стосунку, це може бути додаткова обробка інформації.

Рівень застосунку містить спеціальні програмні засоби для роботи з IoT пристроями, це верхній рівень еталонної моделі.

Також у цій рекомендації наводяться приклади загальних положень щодо забезпечення безпеки IoT. Такі положення безпеки розглядаються на 3 рівнях еталонної моделі, а саме:

- На рівні застосунку (авторизацію, аутентифікацію, захист даних застосунку, захист від шкідливого програмного забезпечення);
- На рівні мережі (авторизацію, аутентифікацію, конфіденційність даних про використання пристрою, перевірку цілісності даних);
- На рівні пристрою (аутентифікацію, авторизацію, перевірку цілісності пристрою, керування доступом, захист цілісності даних).

Такі положення щодо безпеки необхідні для забезпечення роботи застосунків, наприклад систем оплати послуг, або системи доступу до кампусу.

Окрім Міжнародного союзу електрозв’язку еталонна модель була представлена і на Всесвітньому форумі IoT (IWF), до розробки цієї моделі були залучені лідери індустрії, а саме такі компанії як: IBM, Cisco та Intel. Еталонна модель IoT від Всесвітнього форуму IoT представлена на Рис. 3.

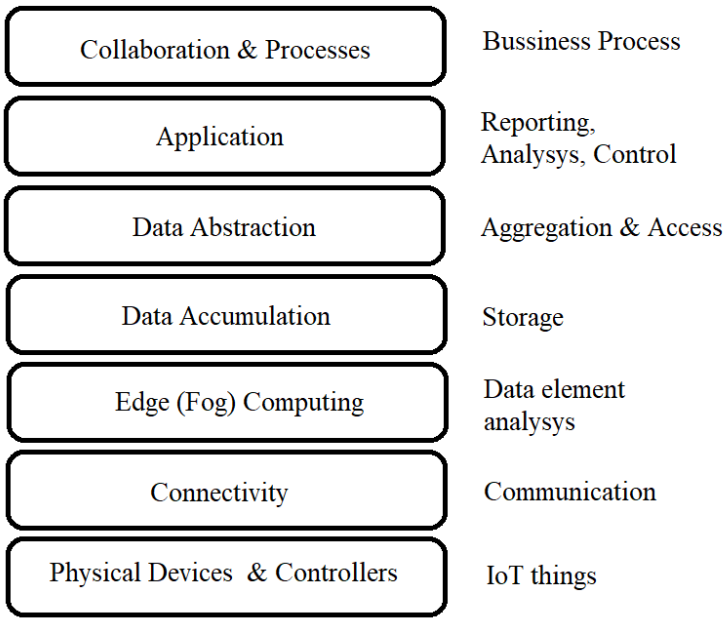


Рис. 3 Еталонна модель IoT World Forum[32]

Згідно з описом Cisco [15], еталонна модель IoT представлена IWF містить 7 рівнів:

1) **Рівень пристроїв та контролерів**. На цьому рівні базово розглядаються фізичні пристрої та контролери, які ще називаються речами в Інтернеті речей. До цього рівня належить величезна кількість різноманітних кінцевих пристроїв, які приймають та відправляють дані.
2) **Рівень сумісності.** Завданням цього рівня є забезпечення сумісності пристроїв для надійного та вчасного обміну інформацією. На цьому рівні розглядаються передача між:
   - пристроями та мережею;
   - між мережами;
   - між мережею та системами рівня 3 цієї моделі.

   Цей рівень забезпечує комунікацію з елементами рівня 1, а також надійну передачу даних по мережі: протоколи, комутація та маршрутизація, трансляція протоколів, безпека на рівні мережі.

3) **Туманні обчислення (Fog computing)**. Цей рівень необхідний для того, щоб забезпечувати форматування даних і виконувати певну частину обробки цих даних для їх подальшого використання на більш високих рівнях цієї моделі. Наприклад, якийсь датчик може генерувати декілька терабайтів даних за годину, тоді завданням рівня 3 стане обробка і форматування цих даних для того, щоб вони займали менше місця і були придатні для подальшої обробки на більш високих рівнях.

   В документі Cisco [31] міститься наступний опис прикладів операцій туманних обчислень:

   - оцінка даних за критеріями щодо того, чи слід їх обробляти на більш високому рівні;
   - форматування даних для їх подальшої послідовної обробки на вищому рівні;
   - обробка даних з додатковим контекстом, наприклад, вихідним кодом;
   - скорочення та/або узагальнення даних для мінімізації впливу даних та трафіку на мережу та системи обробки більш високого рівня;
   - визначення того, чи є дані основними чи тестовими;

4) **Рівень накопичення даних.** Цей рівень необхідний для того, щоб накопичувати дані. Тобто, дані приходять у вигляді мережевих пакетів, які на цьому рівні оброблюються і зберігаються у вигляді реляційних таблиць. Таким чином, такі дані можуть використовуватися застосунками для їхньої роботи, відбувається перехід від обробки подій до обробки запитів.
5) **Рівень абстракцій.** На цьому рівні відбувається обробка зібраної інформації на попередньому рівні для її зручного представлення у застосунку. Тобто, на цьому рівні створюються схеми перегляду, фільтруються, спрощуються, обираються дані для роботи додатку.

6) **Рівень застосунку.** Це рівень програми, де відбувається інтерпретація зібраної інформації. Програмне забезпечення цього рівня взаємодіє з 5-м рівнем, де дані вже зібрані у вигляді таблиць, тому їхнє використання додатком не вимагає якоїсь великої швидкості взаємодії і обмежується лише швидкістю виконання запитів.
7) **Рівень процесів.** Цей рівень необхідний для того, щоб дані, які були представлені на Рівні 6, були вчасно використані іншими системами і була виконана якась певна дія. Саме цей рівень робить Інтернет речей корисним.

Також, у межах даної еталонної моделі представлені основні рекомендації безпеки:

- кожен елемент системи має бути захищений;
- на кожному рівні має бути забезпечений захист процесів ;
- комунікація між рівнями також має бути захищена.

Отже, еталонна модель IoT є важливим першим кроком на шляху стандартизації концепції та термінології IoT. Ця модель визначає функціональні можливості, які має мати елемент IoT, а також проблеми, які мають бути вирішені при розробці такої системи.

1.3 Огляд топології мережі IoT

Однією з найбільш важливих складових інтернету речей є власне передача даних. Як правило, більшість IoT пристроїв не під’єднані до мережі Інтернет напряму, а є під’єднаними опосередковано до певної мережі, яка вже підключаться до Інтернету. Це обґрунтовано специфікою роботи таких пристроїв. У більшості випадків IoT пристрої не потребують високошвидкісного доступу в Інтернет, при цьому більш важливими параметрами для них є надійність з’єднання, енергоефективність та безпека з’єднання. Однак, такі пристрої все ж таки потребують доступу в Інтернет для передачі даних та комунікації з іншими пристроями, серверами, хмарними

сервісами. Для цього використовуються шлюзи, які форматують та передають дані між різними мережами.

Згідно з моделлю OSI топологія мережі належить до першого (фізичного) рівня, так як визначає як саме фізично підключені пристрої один до одного, однак її можна розглядати і з другого (канального) рівня модель OSI, так як розглядається ще і адресація всередині мережі.

Однією з перших і таких що зараз майже не використовується є топологія point-to-point (p2p), коли два пристрої з'єднані напряму один до одного. Самостійні мережі p2p в Інтернеті речей майже не використовуються, так як рідко таких пристроїв буває лише два, зазвичай їх набагато більше.

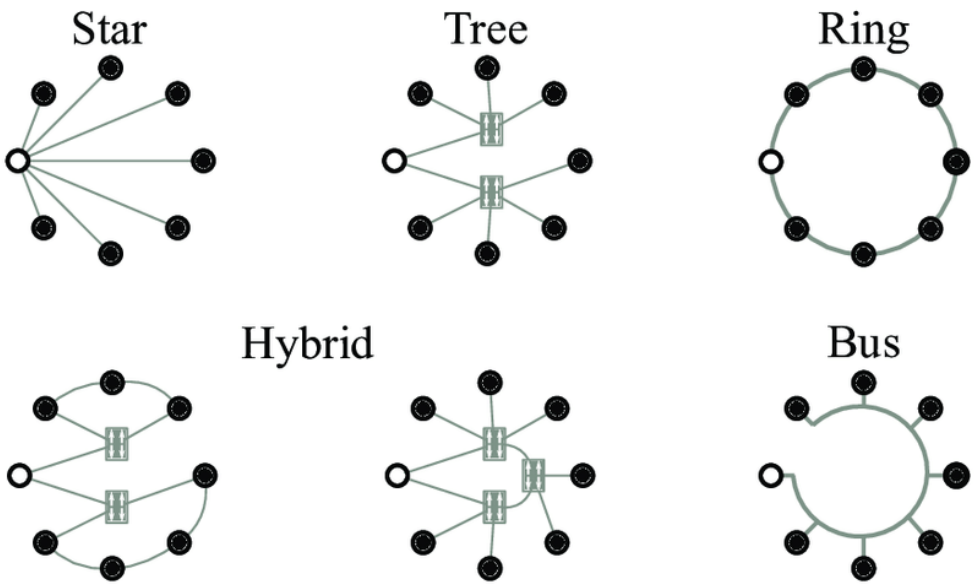


Рис. 4 Традиційні топології мережі [38]

Традиційно використовуються наступні топології:

Кільце (ring) – коли пристрої з'єднані послідовно, при цьому дані передаються від одного пристрою до іншого, тобто також послідовно, поки не дійдуть до потрібного адресата. Також, необхідно додати, що така топологія більш надійна, ніж, наприклад, топологія лінія, так як дані можуть передаватися у різних напрямках кільця.

Лінія (line) – топологія, у якій всі пристрої з'єднані послідовно в лінію. По суті, така топологія є роз'єднаним кільцем.

Шина (bus) – топологія, у якій всі пристрої підключені до загального каналу передачі даних. При такому підключенні дані отримують одночасно всі підключені пристрої. Також, при такій топології дані може передавати тільки один пристрій, щоб не виникало колізій. Таким чином, швидкість при такому з'єднанні є достатньо низькою, але достатньою для датчиків, або, наприклад, не швидкісної системи автоматизації у промисловості [71].

Зірка (star) – по суті це певна сукупність з'єднань p2p, які є об'єднаними концентратором. При цьому обмін даними між пристроями відбувається через посередництво концентратора. Таким чином працюють більшість Ethernet мереж, а також безпровідні мережі Wi-Fi. Варто зазначити, що при такій топології швидкість передачі залежить від здатності концентратора оброблювати таку кількість даних одночасно, а також від пропускної здатності кожного p2p з'єднання.

Дерево (tree) – топологія мережі, при якій деякі пристрої виконують роль концентратора, а також роль кінцевого пристрою. По суті, таке з'єднання є окремим випадком топології Зірка.

Mesh – топологія мережі, у якій окремі вузли можуть динамічно, напряму підключатися до максимального числа інших вузлів. При цьому, така топологія не має якоїсь жорсткої структури і характеризується якраз адаптивністю. Така топологія дозволяє передавати дані між вузлами при цьому використовуючи проміжкові вузли для цієї передачі і робить це найбільш швидким шляхом за допомогою відповідних протоколів. Наприклад, якщо один вузол у такій мережі був відключений, то сусідні вузли автоматично встановлюють нові зв'язки.

Ще існують гібридні мережі (hybrid networks) – тобто мережі, які включають в себе мережі різних топологій. По суті, мережа Інтернет є прикладом такої гібридної мережі, так як включає в себе всі вище описані топології у різних своїх сегментах.

Для впровадження рішень Інтернету речей найкраще підходять і найбільше застосовуються mesh топологія [63], так як вона забезпечує найбільшу адаптивність і надійність мережі, що дозволяє підключати різні пристрої не так залежачи від планування будинку, або від можливостей щодо встановлення пристроїв. Також, поширеними є топології: шина (RS-485), зірка (wifi, ethernet), mesh (Zigbee, LoRa та інші). Всі вони мають свої переваги та недоліки, то ж для вибору топології необхідно підходити залежно від поставлених завдань.

РОЗДІЛ 2. ТЕХНОЛОГІЇ ТА ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ IOT

2.1 ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ IOT

Оскільки сама концепція Інтернету речей передбачає, що розумні пристрої є автономними, тобто мають працювати без втручання людини, то для їх зв'язку з сервером або між собою використовуються протоколи безпровідного зв'язку.

Безпровідні мережі можна розділити на дві великі групи по параметру дальності передачі даних, а саме на групу Безпровідних технологій передачі даних на великі відстані (Дальність передачі >1 км) та на групу Безпровідних технологій передачі даних на короткі відстані. (Дальність передачі <1 км)

До групи Безпровідних технологій передачі даних на короткі відстані належать Z-Wave, ZigBee, NFC, Bluetooth, WIFI (HaLow), розглянемо їх детальніше.

Z-Wave – безпровідна комунікаційна технологія з низькими енерговитратами, яка використовує діапазон частот до 1ГГц і розроблена спеціально для керування, моніторингу, зчитування стану в житлових та невеликих комерційних приміщеннях. Ця технологія широко розповсюджена у сегменті систем розумного дому [61].

Переваги цієї технології:

- підтримка Mesh – мереж;
- використовує частоту 1 Ггц, через це не впливає на інші мережі (WiFi, Bluetooth);
- енергоефективна.

ZigBee - це бездротова технологія, розроблена як відкритий глобальний стандарт для використання у недорогих, малопотужних бездротових мережах IoT. Стандарт Zigbee працює за специфікацією радіо IEEE 802.15.4 і працює в неліцензованих діапазонах, включаючи 2,4 ГГц, 900 МГц і 868 МГц [63].

Специфікація 802.15.4, за якою працює стек Zigbee, була ратифікована Інститутом інженерів з електротехніки та електроніки (IEEE) у 2003 році. Специфікація являє собою пакетний радіопротокол, призначений для недорогих пристроїв, що працюють від батарейок. Протокол дозволяє пристроям працювати в різних мережевих топологіях, а також є доволі енергоефективним, що забезпечить роботу від акумулятора на кілька років. Також можливе використання стаціонарних елементів живлення.

Переваги ZigBee:

- підтримка кількох мережевих топологій, таких як “Point-to-Point”, “Point to Multipoint” і “Mesh”;
- 128-бітове шифрування AES для безпечних з'єднань;
- можливість під єднати до 65 000 вузлів в одну мережу;
- запобігання колізій;
- низька затримка.

Специфікація ZigBee поділена на п'ять рівнів, як показано на Рисунку 5: фізичний (PHY) рівень, рівень керування доступом до середовища (MAC), мережевий рівень (NWK), рівень підтримки додатків (APS) і каркас програми. При цьому варто зазначити, що з цих рівнів PHY і MAC взяті з радіостандарту IEEE 802.15.4. Дана технологія також дозволяє використовувати різні елементи живлення у своїх пристроях.

Така технологія використовується у системах розумного дому, наприклад для забезпечення безпеки приміщення від потрапляння сторонніх осіб, або для вимірювання температури в приміщенні та її регулюванні. У закладі вищої освіти така технологія може використовуватися для будування IoT інфраструктури у лабораторії, або аудиторіях, чи в будь-яких приміщеннях, тобто фактично немає обмежень щодо її застосування.

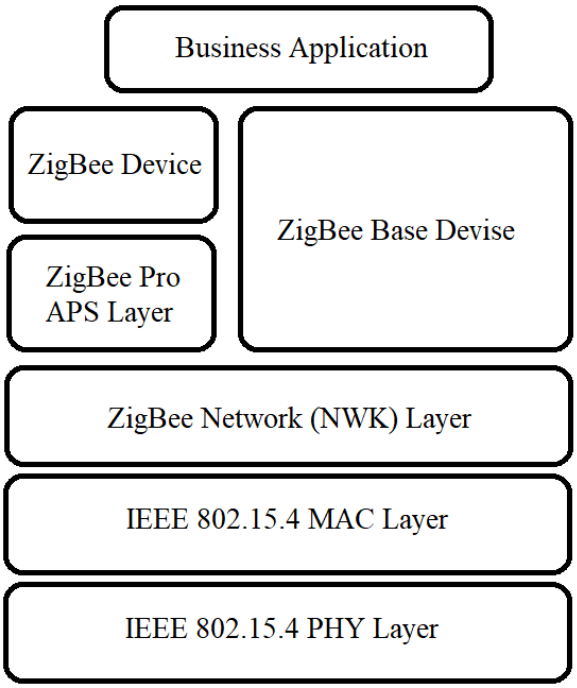


Рис. 5 ZigBee Stack [60]

NFC (Near Field Communication) - це безконтактна технологія зв'язку, заснована на радіочастотному (РЧ) полі з базовою частотою 13,56 МГц. Технологія NFC розроблена для обміну даними між двома пристроями на малій відстані (до 10 см.) [26].

NFC використовується для взаємодії з пристроями радіочастотної ідентифікації RFID, таким чином їх сумісне використання дає можливість створювати системи контролю доступу до приміщень, системи зчитування електронних карток тощо[40].

До переваг NFC належать:

- безпека, через те, що радіус дії NFC сигналу сягає 2 сантиметрів зловмисники не зможуть записати сигнал;
- енергоефективність.

Принципова схема типового NFC пристрою виглядає як показано на Рис. 3. Контролер NFC, підключений до антени, передає та приймає всі кадри

зв’язку NFC, пристрої NFC ініціюють та керують транзакціями NFC за допомогою використання NFC API та NCI (NFC Controller Interface).

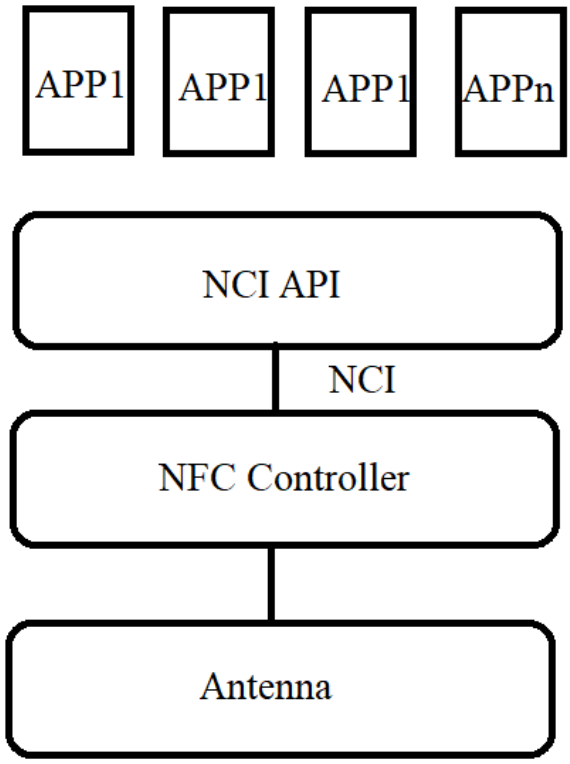


Рис. 6 Типова схема NFC пристрою [40]

Така технологія може використовуватися у системах контролю доступу до кампусу Університету.

BLE – це високошвидкісна бездротова технологія, яка призначена для з’єднання телефонів або іншого портативного обладнання між собою. Технологія базується на специфікації IEEE 802.15.1 і використовує малопотужний радіозв'язок для з'єднання телефонів, комп'ютерів та інших мережевих пристроїв між собою[13]. Зазвичай, Bluetooth сигнал має радіус дії до 30 метрів. Bluetooth мережа має топологію зірка (star), при цьому швидкість передачі даних може сягати 1 Мбіт/сек. [26]. Архітектура системи BLE показана на Рис. 4.

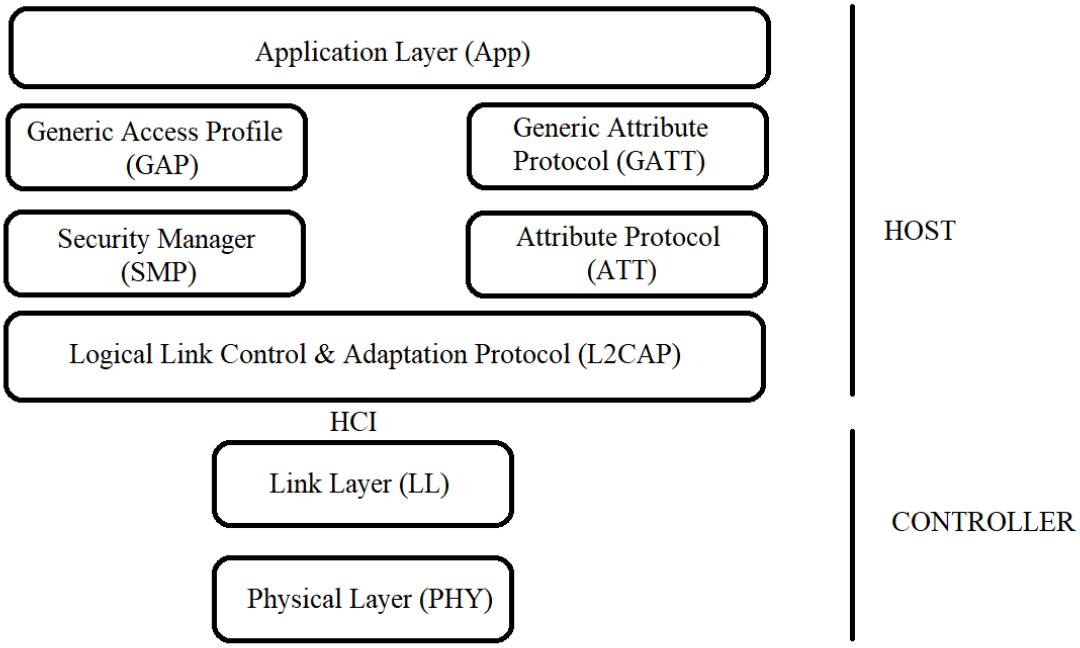


Рис. 7. Bluetooth Low Energy Stack [13]

Основними рівнями стеку BLE є:

- рівень застосунку – на цьому рівні визначаються доступні користувачу функції, логіка роботи тощо;
- рівень хоста – на цьому рівні забезпечується шифрування та дешифрування даних, інкапсуляція та декапсуляція даних тощо;
- рівень контролера – тут відбувається встановлення та керування з’єднань, модуляція сигналу тощо.

Переваги BLE:

- швидкість передачі;
- радіус дії;
- енергоефективний;
- 128-бітове шифрування AES для безпечних з'єднань.

Така технологія може використовуватися для будування інфраструктури Інтернету речей у конференц-залах Університету.

Wi-Fi HaLow – це бездротова технологія зв’язку, що базується на специфікації IEEE 802.11ah і по суті, є меншою по потужності, більшою по дальності сигналу та більш універсальною версією Wi-Fi, що працює в діапазоні, який не підлягає отримання сертифікації, і який працює на частоті нижче 1 ГГц [60, 61]. Унікальна комбінація стандарту Wi-Fi HaLow, що включає енергоефективність, підключення на великій відстані, низьку затримку, швидкість передачі даних HD-відео, функції безпеки та підтримку вбудованої IP-адреси, робить його ідеальним вибором протоколу для бездротових пристроїв Інтернету речей, що живляться від акумулятора[65].

Переваги Wi-Fi Halow:

- радіус дії;
- енергоефективність;
- низька затримка;
- шифрування.

Для узагальнення інформації було створено Таблицю 1 порівняння цих технології за критеріями: швидкість передачі даних/ частота/ радіус дії.

Щодо використання у закладах вищої освіти, ця технологія може бути використана для побудови розумної інфраструктури у їдальнях, де необхідно покрити мережею площу до 60-100м.

Таблиця 1 Порівняння WiFi Halow та WiFi

Параметр	Wi-Fi (IEEE 802.11n/ac/ax)	Wi-Fi Halow (IEEE 802.11 ah)
Робоча частота	2.4 Ггц, 5 Ггц	Європа: 863Мгц
Ширина каналу	20, 40, 80, 160 Мгц	1,2,4,8 Мгц
Максимальна кількість клієнтів на точку доступу	2007	8191

Продовження Таблиці 1

Параметр	Wi-Fi (IEEE 802.11n/ac/ax)	Wi-Fi Halow (IEEE 802.11 ah)
Швидкість передачі даних	6.5 – 150 Мб/с (802.11n)	150 kb/s -86,7 Мб/с
Дальність передачі	~100 м	>1 км

До групи Безпровідних технологій передачі даних на великі відстані належать: LoRaWan, SigFox, LTE-M.

LoRaWan - технологія з низьким енергоспоживанням, яка розроблена для бездротового підключення «речей», що працюють від батареї, до Інтернету в регіональних, національних або глобальних мережах, і націлений на ключові вимоги Інтернету речей (IoT), такі як двонаправлений зв'язок, наскрізна безпека, мобільність та послуги визначення місцезнаходження [36].

LoRaWAN має три різні класи кінцевих пристроїв для задоволення різних потреб, що відображаються в широкому діапазоні застосувань [36]:

Клас А – двонаправлені кінцеві пристрої:

Клас за замовчуванням, який повинен підтримуватися всіма кінцевими пристроями LoRaWAN. Зв'язок класу А завжди ініціюється кінцевим пристроєм і є повністю асинхронним. Кожна передача висхідної лінії зв’язку може бути відправлена в будь-який час і супроводжується двома короткими вікнами низхідної лінії зв’язку, що дає можливість двостороннього зв’язку або, якщо необхідно, команди керування мережею.

Клас В – двонаправлені кінцеві пристрої з детермінованою затримкою низхідної лінії зв’язку:

Пристрої класу B синхронізуються з мережею за допомогою періодичних сигналів і відкривають «ping слоти» низхідного каналу у запланований час. Це надає мережі можливість відправляти зв'язок низхідній лінії зв'язку з детермінованою затримкою, але за рахунок деякого додаткового споживання енергії кінцевим пристроєм.

Клас С – пристрої з найнижчою затримкою з’єднання.

На додаток до структури висхідного каналу класу А, за яким слідують два вікна низхідного каналу, клас С додатково зменшує затримку на низхідній лінії зв’язку, залишаючи приймач кінцевого пристрою відкритим весь час, коли пристрій не передає дані (напівдуплекс). Виходячи з цього, мережевий сервер може почати передачу по низхідній лінії в будь-який момент за умови, що приймач кінцевого пристрою відкритий, саме тому затримки немає.

Архітектура LoRaWAN складається з таких компонентів: Датчик IoT, Шлюз, Мережевий сервер, Сервер за стосунку [30, 36] (Рис. 5).

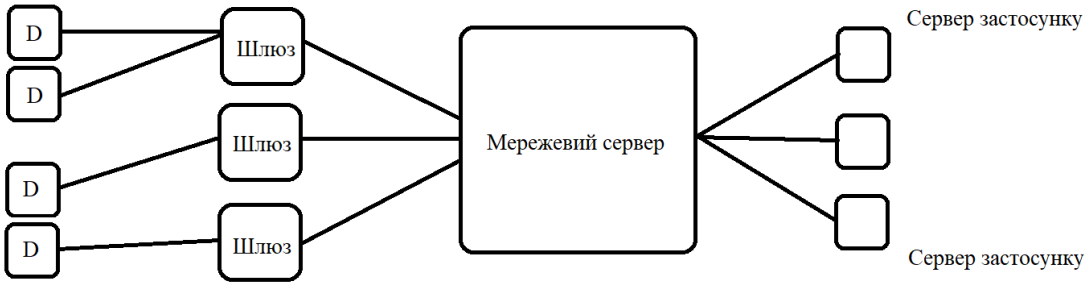


Рис. 8. Архітектура LoRaWAN [30]

SigFox – технологія бездротового низькошвидкісного зв'язку в мережах з низьким споживанням енергії. Для передачі даних SigFox використовує ультразвукову смугу частот.

Архітектура SigFox складається з таких компонентів: IoT пристрої, базова станція SigFox, SigFox Cloud та сервери застосунків (Рис. 6)

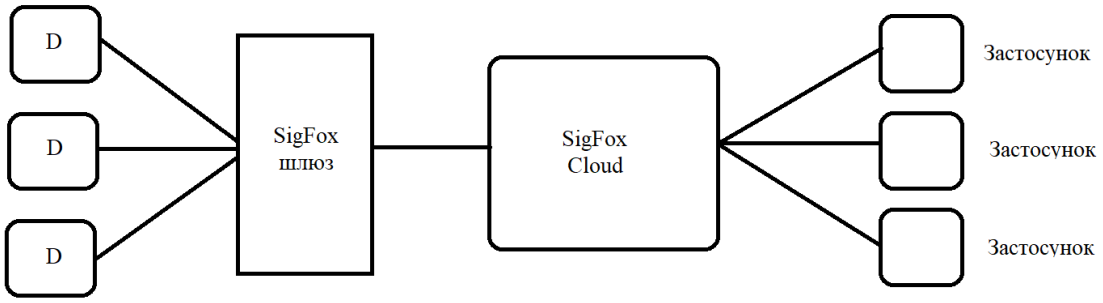


Рис. 9. Архітектура SigFox [28]

LTE-M - це провідна технологія LPWAN для додатків Інтернету речей. Використовується для з'єднання таких пристроїв, як датчики IoT, або інші промислові IoT пристрої [70] за допомогою радіомодулів [27, 39].

2.2 ПРОТОКОЛИ ІНТЕРНЕТУ РЕЧЕЙ

Протоколи інтернету речей діляться на групи в залежності від того, до якої ділянки мережі вони застосовуються. Таким чином, для зв'язку між датчиками зазвичай використовуються протокол DDS, на ділянці датчик – брокер використовується протоколи CoAP, MQTT, XMPP тощо. На ділянці сервер – застосунок переважно використовується протокол SOAP [1, 11].

Розглянемо детальніше кожну ділянку зв'язку та протоколи, які на ній використовуються на прикладі такої топології:

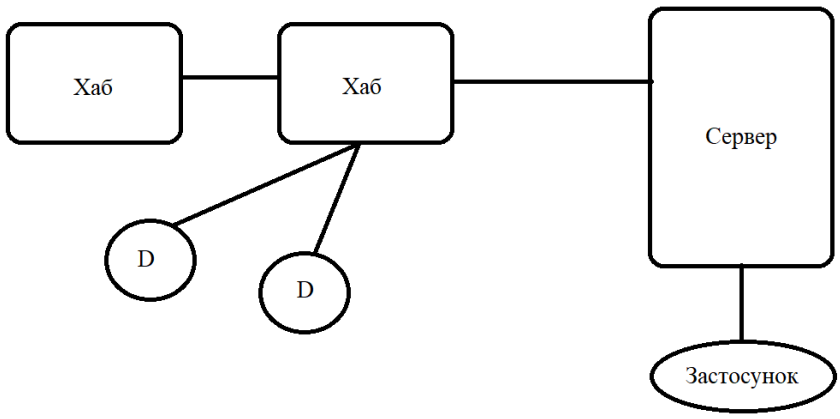


Рис. 10. Топологія яка використовується для аналізу

Дана топологія є реалізацією шаблону проектування передачі повідомлень, який називається “Видавець-Підписник”. Цифрою 1 позначений датчик, який виступає у ролі видавця, цифрою 2 позначений брокер, або сервер, який приймає інформацію від видавців і передає її відповідним підписникам, а також відповідає за її фільтрацію і зберігання, цифрою 3 позначений сервер, який зберігає фільтровані дані і передає дані застосункам користувачів.

Розглянемо ділянку пристрій – пристрій

Найбільш популярним протоколом для ділянки датчик- датчик є DDS (Data Distribution Service) [57]. Задачою цього протоколу є реалізація шинного зв’язку між датчиками, при цьому у якості протоколу транспортного рівня, куди інкапсулюється DDS, використовується протокол UDP (User Datagram Protocol), що дозволяє використовувати багатоадресну систему. Для роботи протокол використовує метод «запит-відповідь», при цьому він реалізовує дві операції, а саме читання та запис. Також, важливо додати, що операції в даному протоколі задаються класами. Для операції читання можуть використовуватися три наступні способи:

- Списки очікування (WaitSets) – реєструється список очікування DDS і якщо настає одна з перелічених подій, тоді відбувається зчитування;
- Запити (Polling) – періодично надсилаються запити DDS на отримання нових даних;
- Слухання (Listening) – реєструються спеціальні класи-слухачі DDS, які отримають інформацію у разі настання певних подій.

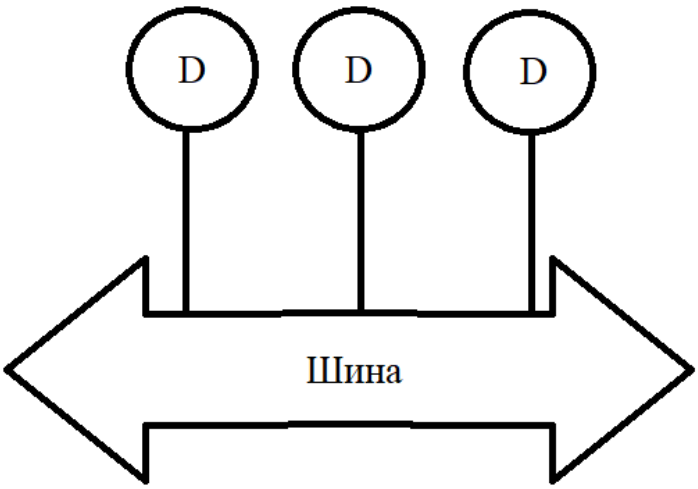


Рис. 11. Принцип з’єднання пристроїв за допомогою протоколу DDS[57]

Розглянемо ділянку пристрій – брокер (хаб)

Як правило, для зв’язку на цій ділянці використовуються два протоколи, це XMPP (Extensible Messaging and Presence Protocol) та COAP (Constrained Application Protocol).

XMPP – це протокол обміну повідомленнями та інформацією про присутність [20]. Для транспорту використовується протокол TCP, дані пересилаються у форматі XML, а ідентифікацію користувачів відбувається за допомогою спеціального ідентифікатора JID. Архітектура мережі XMPP є децентралізованою, тому така мережа може бути легко розширена. Найчастіше такий протокол використовується у домашніх мережах IoT.

Спеціально для використання в IoT, мережах з обмеженими ресурсами та підвищеною потребою в енергозбереженні використовується протокол COAP.

COAP – протокол, який був розроблений для обмежених в ресурсах мережах. Даний протокол є спрощеною версією протоколу http, таким чином він підтримує інтеграцію з ним. Для своєї роботи він використовує метод

«запит-відповідь» за допомогою простих методів аналогічних до http, а саме put, post, get, delete [50].

Таблиця.2 Методи SOAP протоколу

Метод	Функції
GET	Виконує пошук ресурсів, надає дані, що містяться у посиланні URI. Наприклад, дані отримані датчиком
PUT	Задає нову дію для джерела даних
POST	Змінює певну дію для джерела даних
DELETE	Видаляє дані
FETCH	Надає інформацію про джерело даних
PATCH	Частково змінює дію для джерела даних

Ділянка брокер – сервер

На цій ділянці найчастіше використовують протокол MQTT, так як його використання знижує навантаження на канал передачі даних. MQTT (Message Queue Telemetry Transport) – спеціально розроблений протокол для обміну повідомленнями між пристроями. MQTT працює за принципом видавець-підписник. Слово topic відноситься до рядка UTF-8, який брокер використовує для фільтрації повідомлень кожного підключеного клієнта. Даний протокол працює поверх TCP/IP і використовує порт 1883 або 8883 [39]. Для взаємодії з брокером протокол використовує типи повідомлень, які вказані у Таблиці 3.

Таблиця 3. Типи повідомлень MQTT

Тип повідомлення	Для чого використовується
Connect	Встановити з’єднання з брокером
Disconnect	Від’єднатися від брокера

Publish	Опублікувати дані до теми у брокері
Subscribe	Підписатися на тему в брокері
Unsubscribe	Відписатися від теми

Для пояснення цієї взаємодії була створена наступна схема:

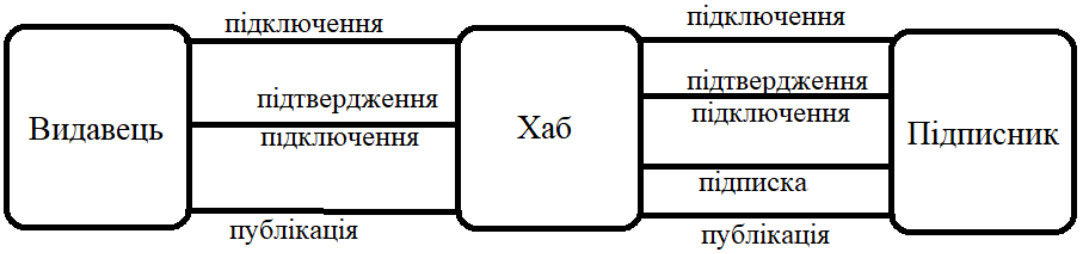


Рис. 12. Схема взаємодії MQTT [39]

Важливо додати, що MQTT забезпечує двосторонній зв’язок між сервером і брокером, а також між брокером та датчиком.

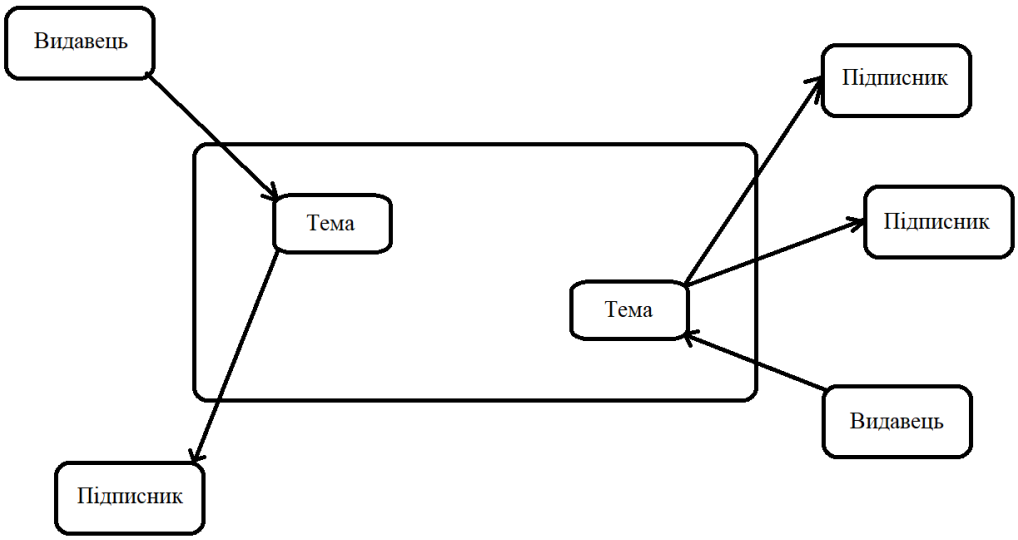


Рис. 13. Принцип роботи протоколу MQTT[39]

Тепер розглянемо ділянку сервер-застосунок

Ця ділянка необхідна для того, щоб забезпечити взаємодію між системою IoT та застосунком користувача, де останній зможе налаштовувати параметри системи IoT, а також отримувати дані із серверу.

Як правило для реалізації цих функцій використовується протокол SOAP. SOAP (Simple Object Access Protocol) – протокол обміну структурованими повідомленнями у форматі XML у розподілених обчислювальних системах, який базується на моделі запит-відповідь. Цей протокол можна використовувати з протоколами прикладного рівня, наприклад з HTTP, HTTPS, FTP, SMTP тощо. Наразі SOAP є стандартом, на якому базуються технології роботи веб-сервісів. Також, SOAP має вбудовані механізми доступу до об’єктів SOAP-PRC та SOAP Message [46].

SOAP-RPC – використовується для віддаленого виклику функцій, базується на об’єкті Call. SOAP Message використовується для обміну повідомленнями і базується на об’єкті Message [20].

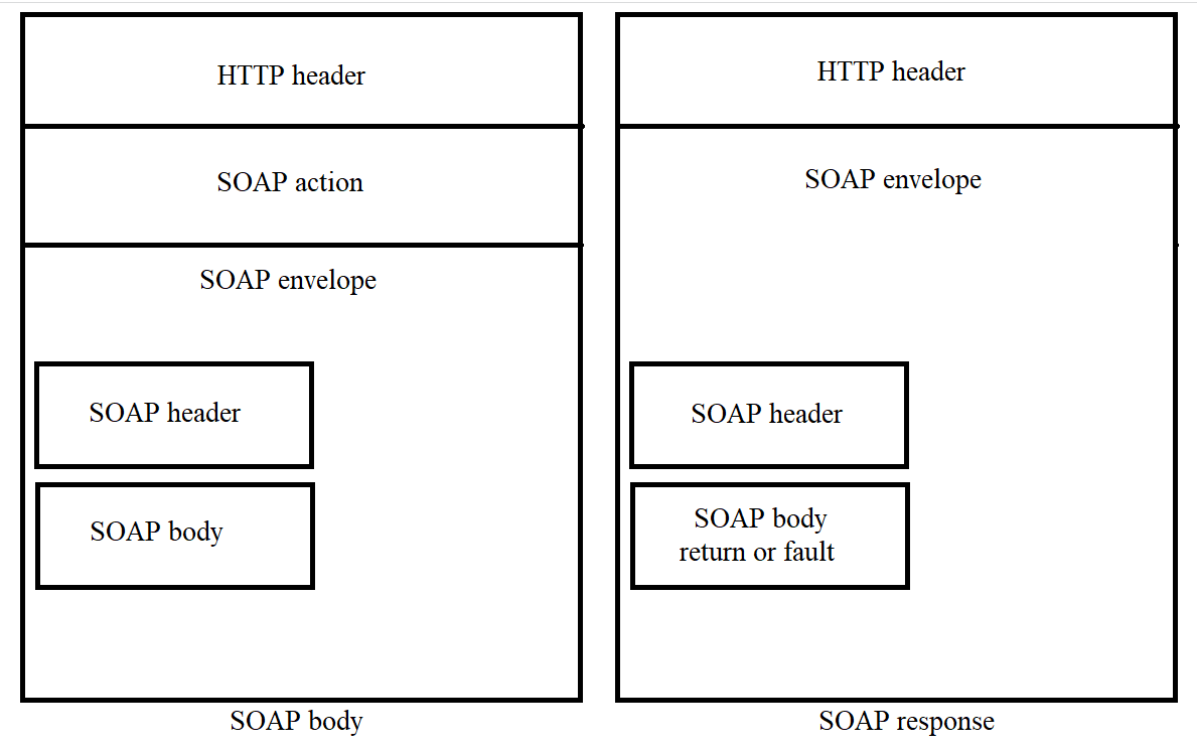


Рис. 14. Модель запит-відповідь SOAP [47]

У зв’язку з тим, що сфера IoT ще формується, протоколи передачі даних стандартизовані різними організаціями, крім того використовують різні протоколи транспортного рівня та архітектуру і, відповідно, можливості. Тому мною була створена наступна оглядова Таблиця 4.

Таблиця 4. Огляд розглянутих протоколів

Протокол	Стандарт	Опис
AMQP	OASIS/ISO	Передача даних між компонентами системи IoT
COAP	IETF	Обмін повідомленнями між пристроями IoT через Інтернет
DDS	OMG	Обмін повідомленнями між пристроями IoT
MQTT	OASIS	Обмін повідомленнями по принципу Видавець-Підписник
HTTP	IETF	Передача даних через Інтернет
WebSocket		
XMPP	XMPPSF	Протокол обміну повідомленнями у режимі реального часу

РОЗДІЛ 3. ОГЛЯД IOT ПЛАТФОРМ

Внаслідок стрімкого розвитку Інтернет речей стає однією з головних технологій у сучасному суспільстві, мережі IoT стрімко зростають, у зв'язку з цим і виникає потреба у забезпеченні інтеграції різних апартних засобів IoT. Згідно із визначенням [31], програмна IoT платформа – програмне забезпечення, призначене для підключення пристроїв Інтернету речей (датчиків, контролерів та інших пристроїв) до хмари та забезпечення віддаленого доступу до них. Завданням IoT платформи є виконання ролі посередника між фізичними пристроями і користувачем, а саме забезпечувати виконання поставлених користувачем вимог. Використовуючи інтерфейси інтеграції зі шлюзом, які надаються платформою, можна передавати зібрані дані IoT в певні системи аналізу та зберігання даних, а також передавати дані на підключені пристрої (конфігурація, повідомлення) або між ними (елементи управління, події), використовуючи різні види користувацьких застосунків [34].

Критерії вибору IoT платформи базуються на технічних характеристиках цих платформ та їх вартості, а саме:

- масштабованість;
- безпека;
- сумісність;
- варіанти розгортання;
- багатофункціональність;
- вартість використання.

До найбільш популярних IoT платформ відносться наступні: Google Cloud IoT, Cisco IoT Cloud Connect, Microsoft Azure IoT Hub, Thingsboard, Oracle IoT.

Компанія Google створила платформу Google Cloud IoT для підключення пристроїв Інтернету речей базуючись на своїй вже існуючій платформі Google Cloud Platform. Фактично ця платформа є інтеграцією вже існуючих сервісів

для Інтернету речей. [17, 22] Основним сервісом платформи є Cloud IoT Core, який забезпечує безпечне підключення, керування та отримання даних з пристроїв IoT. Ця служба складається з Менеджера пристроїв та Моста Протоколів.

Менеджер пристроїв забезпечує підключення пристроїв, їх налаштування, віддалений доступ до них, а також, при підключенні нових пристроїв, надає механізм автентифікації.

Міст протоколів забезпечує балансування навантаження для всіх підключень пристроїв, а також він публікує дані з пристроїв в Cloud Pub/Sub.

Cisco IoT Cloud Connect була створена компанією Cisco як набір хмарних сервісів IoT для індустріального та персонального використання. Також, для функціонування платформи компанія пропонує спеціальне IoT апаратне забезпечення, що дозволяє створювати єдину підтримувану систему [21].

Microsoft Azure IoT Hub – сучасна хмарна платформа для побудови інтернету речей. Ця платформа також являє собою набір хмарних сервісів для обробки, підтримки роботи, контролю Інтернету речей. [43]

Thingsboard – платформа для підключення пристроїв Інтернету речей та яка забезпечує обробку інформації, контролю функцій Інтернету речей та призначена для промислового та персонального використання. [56]

Oracle IoT – платформа для забезпечення роботи Інтернету речей, яка, як і деякі вище названі платформи, складається з набору сервісів для обробки, контролю та підтримки роботи IoT [41].

Для порівняння платформ я обрав базові тарифні плани на кожній з платформ і склав Таблицю 5.

Таблиця.5 Огляд IoT платформ

	Масштабованість	Безпека	Сумісність	Варіанти розгортання	Вартість
Google Cloud IoT	Безлімітно	RSA, Контроль доступу	MQTT, HTTPS	Cloud	Free(1), up to 250Mb
Cisco IoT Cloud Connect	Безлімітно	RSA, контроль доступу	MQTT, HTTPS	Cloud	(3)
Microsoft Azure IoT Hub	Безлімітно	RSA, контроль доступу	HTTPS, AMQP, MQTT, MQTT over WebSocket, AMQP over WebSocket	Cloud	Free(2)
Oracle IoT	Безлімітно	RSA, контроль доступу	HTTPS, MQTT, CoAP, XMPP, AMQP	Cloud (необхідне встановлення додаткового ПЗ)	(3)
Thingsboard	Безлімітно	RSA, контроль доступу	MQTT, CoAP, SNMP, HTTP,LwM2M	Cloud, Personal Server	(4)

Free(1) – безкоштовно до 250Мб в місяць, вартість рахується залежно від кількості витрачених мегабайт в місяць.

Free(2) – безкоштовно до 500 пристроїв та 8000 повідомлень в день.

(3) – вартість залежить від партнера Cisco

(4) – використання самої платформи безкоштовне, вартість підключення до 30 пристроїв становить 10 доларів / місяць

"Станом на 05.2022.

Отже, проаналізувавши інформацію викладену у таблиці 5, можна зробити висновок, що найкращим рішенням для побудови IoT моделі в ЗВО буде платформа Mircrosoft Azure IoT Hub. Так, як ця платформа підтримує більшу кількість протоколів, що дозволить підключати більше різноманітних IoT пристроїв і, таким чином, дозволить побудувати масштабовану інфраструктуру. Також дана платформа має безкоштовний тариф для тестування, а також дозволяє підключати необмежену кількість датчиків до неї.

РОЗДІЛ 4. ІНТЕРНЕТ РЕЧЕЙ У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

Впродовж останніх років Інтернет речей значно розширив межі свого використання. Якщо раніше він використовувався у системах розумного дому та на підприємствах, то зараз він використовується у проектах розумного міста (Smart City), і його використання у закладах вищої освіти не є виключенням. Таким чином, у світі створюються розумні кампуси університетів,у яких широко використовуються можливості IoT.

За даними Cisco, представленими у Cisco Annual Internet Report, 2018 – 2023 [14] до кінця 2023 року кількість M2M підключень зросте до 14.7 мільярдів (Рисунок 15). Зокрема, підключені домашні IoT пристрої, такі як системи автоматизації, домашня безпека та відеоспостереження, підключені побутові прилади та програми для відстеження, становитимуть до 48 відсотків, або майже половину, від загальної кількості M2M – з'єднань до 2023 року, що свідчить про поширеність та необхідність M2M підключень у нашому житті (див. Рисунок 15). Також, використання засобів IoT у транспортній структурі буде швидкозростаючою категорією з 30% CAGR. Застосування IoT у системах Smart City матимуть друге місце за швидкістю зростання – 26% CAGR. Саме у категорію систем Розумного міста входять системи Smart Campus.

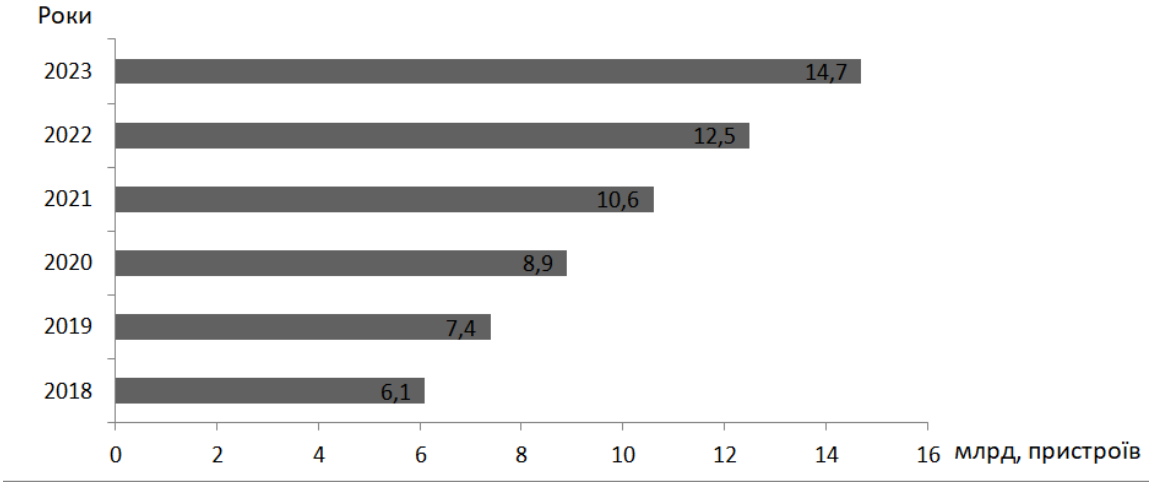


Рис. 15. Ріст числа підключень [13]

Згідно з опитуванням, яке проводилося Центром цифрової освіти США у 2018 році [1], у більшості коледжів та університетів США впровадження IoT ініціатив є стратегічним завданням.

Можна виділити 4 найбільш доцільні сфери використання Інтернету речей у закладах вищої освіти, як показано на Рисунку 16.

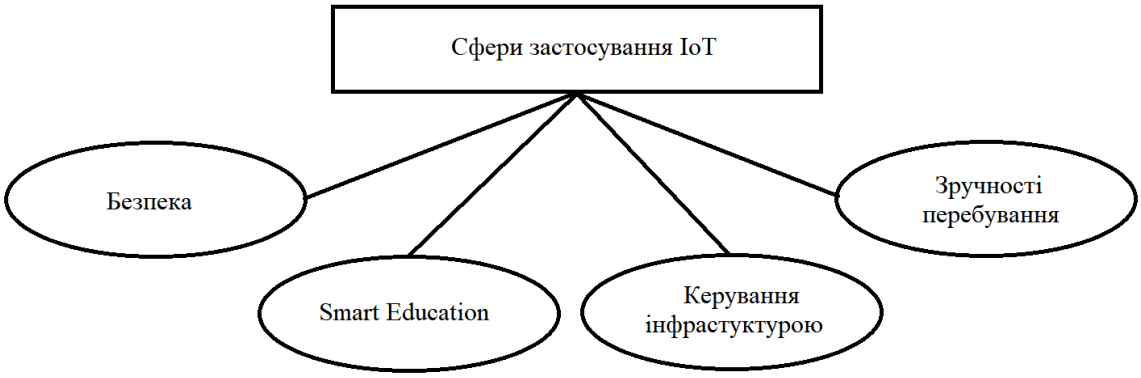


Рис. 16. Сфери застосування IoT в ЗВО[1, 6, 16]

Безпека

Для безпеки перебування відвідувачів світові заклади вищої освіти впровадили цілий ряд рішень, орієнтованих на використання засобів IoT [53], від смарт-карток і контролю доступу до систем оповіщення про надзвичайні ситуації. Наприклад, університет Сан-Франциско встановив систему контролю доступу, яка складається з камер спостереження, а також системи розпізнавання обличчя на вході в гуртожитки, таким чином контролюючи доступ. Такі рішення допомагають підвищити безпеку, не перевантажуючи персонал [17].

Керування інфраструктурою

Ідея централізованого керування системами HVAC та освітленням виникла ще до появи Інтернету, коли контролери були підключені за допомогою комутованого або дротового з’єднання. Але сучасні технології IoT на основі даних створюють нові можливості для економії грошей та

покращення роботи кампуса. В університеті Британської Колумбії (UBC) точки доступу Wi-Fi по всьому кампусу відстежують, коли люди приходять і йдуть — дані, які аналізуються та використовуються для автоматизації температури та інших параметрів у приміщеннях. Така практика дозволяє кампусу економити енергію та обмежувати викиди парникових газів, що є важливим, оскільки UBC має одні з найамбітніших кліматичних цілей серед будь-якої громадської організації у світі. На сьогоднішній день ці системи призвели до 33-відсоткового скорочення викидів парникових газів і щорічної економії [17].

Зручності перебування

Це IoT рішення, які допомагають студентам та викладачам під час перебування на території університету. Наприклад, використання вказівних маячків можуть допомогти студентам орієнтуватися в університетському містечку, або кампусі. В університетських містечках із великою кількістю пасажирів рішення для паркування можуть дозволити студентам резервувати місця для паркування. Університет Сент-Луїса (SLU) у штаті Міссурі розмістив 2300 розумних колонок Amazon Echo Dot у кожній кімнаті гуртожитку на території кампусу, з налаштованою версією розумного помічника Amazon Alexa, запрограмованого відповідати на запитання студентів про години роботи закладу, спортивного залу та розклад заходів та інші аспекти студентського життя [23, 24].

Smart Education

Це IoT рішення направлені на покращення процесу навчання, а саме системи дистанційного навчання, запис лекцій, пристрої покращення продуктивності навчання тощо. Одним із перших таких Розумних кампусів був створений у партнерстві MIT та Microsoft ще у 1999 році MIT iCampus [26]. Це був дослідний проект, метою якого було створення експериментального класу в якому впровадити використання розумних пристроїв в процесі навчання студентів.

Таким чином, використання засобів IoT в ЗВО є актуальним питанням сьогодення, яке необхідно досліджувати і широко впроваджувати, як це відбувається у світових закладах освіти. Найбільш доцільними сферами застосування засобів IoT у ЗВО є сфери: Безпека, Керування інфраструктурою, Зручності перебування, а також Smart Education.

РОЗДІЛ 5. ПОБУДОВА МОДЕЛІ IOT

Базуючись на наведених вище прикладах, а також, оглянутих у Розділах 2 та 3 платформах та технологіях зв'язку для побудови IoT рішень, можливо сформулювати модель використання засобів Інтернету речей у інфраструктурі ЗВО.

Згідно з розглянутими у Розділі 2 технологіями зв'язку IoT пристроїв для побудови такої моделі підходить технологія LoRaWAN, яка серед переваг має велику дальність зв'язку, простоту налаштування, а також економічність. Також, ця технологія є доволі розповсюдженою, відтак можливо використати вже існуючу інфраструктуру міста для нових підключень, що дозволить збільшити і без того, великий радіус покриття мережею LoRa.

Згідно з Розділом 3, як Інтернет платформу доцільно обрати Microsoft Azure IoT Hub, так як дана платформа підтримує більшу кількість протоколів, а також тому, що ця платформа дозволяє реалізувати масштабування у майбутньому. Окрім того, дана платформа забезпечить можливість інтеграції з різними сервісами корпорації Microsoft, а також безпечне зберігання даних, доступ до них, а також можливість для візуалізації отриманих даних.

Однією з найбільш доцільних сфер застосування IoT в ЗВО відповідно до Розділу 4 є сфера зручностей перебування. Відповідно, була взята до уваги необхідність отримання значень вимірів температури та вологості в приміщеннях Університету для покращення умов перебування в них студентів та працівників. Таким чином, була побудована концептуальна модель використання засобів IoT в закладах вищої освіти, яка показана на рисунку 17.

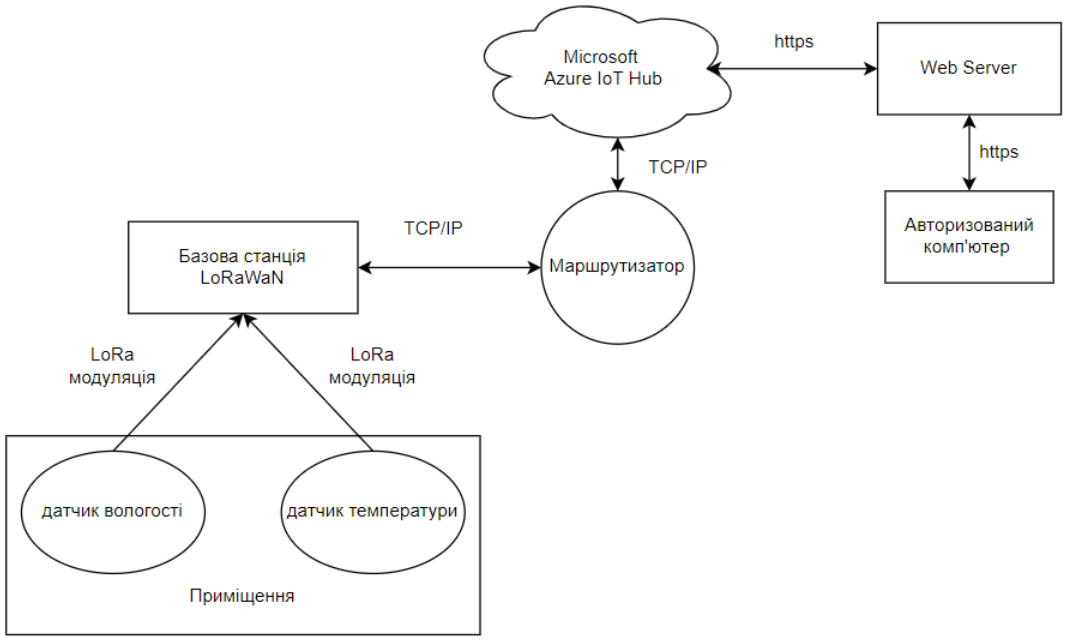


Рис. 17. Модель використання засобів IoT в ЗВО

Дана модель розрахована на використання однієї базової станції LoRaWan, яка мала б потужність антени 6,5 dBi, наприклад LoRa Antenna kit [64] . Відповідно до розрахунків у статті [2], таку антену доцільно розташувати у приміщенні Спортивного комплексу КНУ і покривати мережею LORA для підключення пристроїв IoT у приміщеннях Університету у Голосіївському районі міста Києва, як показано на Рисунку 18. Базова станція пересилатиме отримані дані по каналу Ethernet до IoT платформи.

Базова станція та датчики повинні працювати на частоті 868МГц (неліцензійований діапазон в Україні). Також, на дальність передачі впливають багато факторів, наприклад: погодні умови, розташування базової станції та датчиків, наявність будівель та матеріал, з якого вони побудовані тощо. Залежність дальності передачі від деяких з цих умов наведені у статті [35].

В даній моделі пропонується використати IoT платформу від корпорації Microsoft – Azure IoT Cloud, яка забезпечить обробку та зберігання отриманих з датчиків даних, а також авторизований доступ до цих даних. При використанні безкоштовного плану можливо отримувати до 400000 повідомлень щоденно.

Для візуалізації отриманих даних можна використовувати влаштований інструмент Microsoft Power Bi, або застосунок на Веб-сервері.

Самі датчики пропонується встановлювати у приміщеннях Університету, ці датчики будуть робити виміри, після чого з певним налаштованим інтервалом будуть передаватися до Базової Станції LoRaWAN за допомогою технології LoRa.

Базова станція матиме підключення до внутрішньої мережі Університету, що дозволить забезпечити безпеку та стабільність Інтернет з'єднання з IoT платформою.

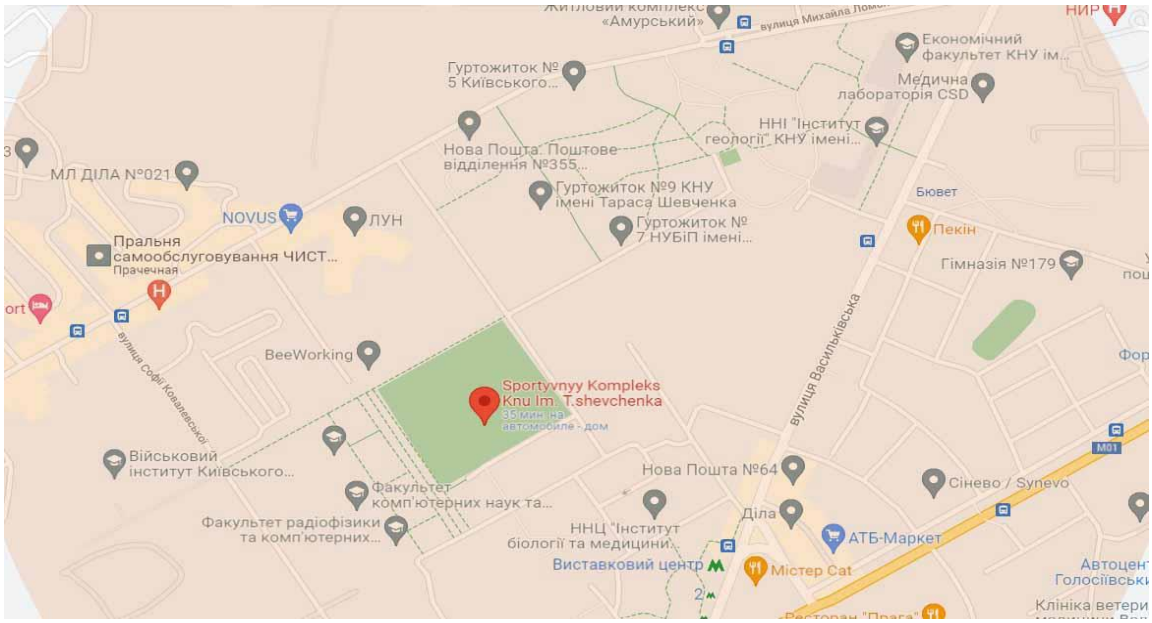


Рис. 18. Покриття мережею LoRaWAN приміщень Університету

Дана модель є масштабованою, відтак, в залежності від можливостей Базової станції можливо підключати достатньо велику кількість IoT датчиків і розміщувати їх у зоні покриття цієї станції.

Для демонстрації результатів впровадження такої моделі було підключено віртуальний датчик до платформи Microsoft Azure IoT Hub і виведено на екран показання температури та вологості у режимі реального часу як показано у Додатках А, Б, В та Г.

Впровадження такої моделі надасть можливості для контролю та інформування відповідальних осіб про значення температури та вологості приміщень Університету, а також покращить рівень інновацій Університету на світовій арені загалом. Окрім того, дану модель можна пристосувати до використання у будь-якому ЗВО України.

ВИСНОВКИ

Згідно сформованих вимог для потреб ЗВО підходить технологія LoRaWan. Ця технологія забезпечує можливість підключення датчиків на площі радіусом до 2 км у міських умовах, а також є економічною та розповсюдженою, відтак це робить можливим використання вже існуючої мережевої інфраструктури для впровадження системи Розумного кампусу в ЗВО.

Серед розглянутих платформ за критеріями визначеними у роботі, рекомендується обрати платформу Microsoft Azure IoT Hub. Ця платформа є частиною екосистеми корпорації Microsoft, відтак вона підтримує інтеграцію з її іншими сервісами, а також дозволяє масштабувати впроваджене рішення у майбутньому.

Згідно з проведеним аналізом сфер застосування для впровадження IoT у інфраструктуру закладів вищої освіти рекомендується: Безпека, Smart Education, Керування інфраструктурою та Зручності перебування відповідно до Розділу 4.

З урахуванням вимог законодавства України щодо ліцензіювання частот у роботі рекомендується частота роботи LoRaWaN датчиків та Базової станції 868 МГц.

У роботі показано доцільність розміщення Базової станції з антеною, яка має підсилення у 6.5 dBi, у приміщенні спорткомплексу кафедри фізичного виховання та спорту КНУ імені Тараса Шевченка. Це забезпечить покриття мережею LoRa приміщення Університету, які знаходяться у Голосіївському районі міста Києва.

Для демонстрації роботи Інтернет платформи було підключено віртуальний датчик температури та вологості і виведено на Веб-сторінку показання вимірювань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Survey on IoT in Education [Електронний ресурс] – Режим доступу до ресурсу: https://lumenpublishing.com/journals/index.php/rrem/article/view/1056 (дата звернення 30.05.2022 р.)
2. Antenna Design Gain and Range Education [Електронний ресурс] – Режим доступу до ресурсу: https://www.lairdconnect.com/resources/white-papers/antenna-design-gain-and-range (дата звернення 30.05.2022 р.)
3. Adding sense to the Internet of Things - An architecture framework for Smart Object systems [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/220141406_Adding_sense_to_the_Internet_of_Things_-_An_architecture_framework_for_Smart_Object_systems (дата звернення 30.05.2022 р.)
4. Adding sense to the Internet of Things sensing [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/251194224_Adding_sense_to_the_Internet_of_Things (дата звернення 30.05.2022 р.)
5. AMQP 0-9-1 Model Explained Platform [Електронний ресурс] – Режим доступу до ресурсу: https://www.rabbitmq.com/tutorials/amqp-concepts.html (дата звернення 30.05.2022 р.)
6. An Integral Pedagogical Strategy for Teaching and Learning IoT Cybersecurity [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/343035783_An_Integral_Pedagogical_Strategy_for_Teaching_and_Learning_IoT_Cybersecurity (дата звернення 30.05.2022 р.)
7. An IoT-Based Thermoelectric Air Management Framework for Smart Building Applications: A Case Study for Tropical Climate [Електронний ресурс] – Режим доступу до ресурсу:

https://www.researchgate.net/publication/339363223_An_IoT-Based_Thermoelectric_Air_Management_Framework_for_Smart_Building_Applications_A_Case_Study_for_Tropical_Climate (дата звернення 30.05.2022 р.)

8. Architecting the Internet of Things [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/314154036_Architecting_the_Internet_of_Things (дата звернення 30.05.2022 р.)
9. AWS IoT – Amazon Web Services [Електронний ресурс] – Режим доступу до ресурсу: https://aws.amazon.com/iot/ (дата звернення 30.05.2022 р.)
10. AWS IoT Core pricing [Електронний ресурс] – Режим доступу до ресурсу: https://aws.amazon.com/iot-core/pricing (дата звернення 30.05.2022 р.)
11. Azure IoT Hub communication protocols and ports [Електронний ресурс] – Режим доступу до ресурсу: https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-protocols (дата звернення 30.05.2022 р.)
12. Bluetooth Introduction [Електронний ресурс] – Режим доступу до ресурсу: https://www.leverege.com/iot-ebook/iot-bluetooth (дата звернення 30.05.2022 р.)
13. Bluetooth Low Energy Stack [Електронний ресурс] – Режим доступу до ресурсу: https://software-dl.ti.com/lprf/simplelink_cc2640r2_sdk/1.00.00.22/exports/docs/blestack/html/ble-stack/index.html (дата звернення 30.05.2022 р.)
14. Cisco Annual Internet Report (2018–2023) White Paper [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (дата звернення 30.05.2022 р.)

15. Cisco IoT Solutions [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html (дата звернення 30.05.2022 р.)
16. Cisco portfolio for education: What can we help you solve today? [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/m/en_us/solutions/industries/portfolio-explorer/portfolio-explorer-for-education.html?s=explore-the-architectures (дата звернення 30.05.2022 р.)
17. Cloud IoT Core overview [Електронний ресурс] – Режим доступу до ресурсу: https://cloud.google.com/iot/docs/concepts/overview (дата звернення 30.05.2022 р.)
18. Definition Internet of things things [Електронний ресурс] – Режим доступу до ресурсу: http://www.gartner.com/it-glossary/internet-of-things/ (дата звернення 30.05.2022 р.)
19. Designing the Internet of Things [Електронний ресурс] – Режим доступу до ресурсу: https://madsg.com/wp-content/uploads/2015/12/Designing_the_Internet_of_Things.pdf (дата звернення 30.05.2022 р.)
20. Extensible Messaging and Presence Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://xmpp.org/ (дата звернення 30.05.2022 р.)
21. Free Trial – Google Cloud Platform [Електронний ресурс] – Режим доступу до ресурсу: https://console.cloud.google.com/freetrial/signup/tos (дата звернення 30.05.2022 р.)
22. Google Cloud IoT solutions [Електронний ресурс] – Режим доступу до ресурсу:

https://cloud.google.com/solutions/iot (дата звернення 30.05.2022 р.)

23. How Arizona State University Built a Smart Campus [Електронний ресурс] – Режим доступу до електронного журналу: https://edtechmagazine.com/higher/article/2019/12/how-arizona-state-university-built-smart-campus-perfcon (дата звернення 30.05.2022 р.)
24. Integration of Smart Phone and IOT for development of smart public transportation system [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/7562698 (дата звернення 30.05.2022 р.)
25. Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards sensing [Електронний ресурс] – Режим доступу до ресурсу: https://www.sciencedirect.com/science/article/pii/S0933365717301367?via%3Dihub (дата звернення 30.05.2022 р.)
26. Internet of Things (IoT) – A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications [Електронний ресурс] – Режим доступу до ресурсу: http://www.sciepub.com/reference/146435 (дата звернення 30.05.2022 р.)
27. Internet of Things (IoT) For Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios sensing [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/338874911_Internet_of_Things_IoT_For_Next-Generation_Smart_Systems_A_Review_of_Current_Challenges_Future_Trends_and_Prospects_for_Emerging_5G-IoT_Scenarios (дата звернення 30.05.2022 р.)
28. Internet of Things (IoT) System Architecture and Technologies, White Paper [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/323525875_Internet_of_Things_IoT_System_Architecture_and_Technologies_White_Paper/figures?lo=1 (дата звернення 30.05.2022 р.)

29. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions sensing [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/228095891_Internet_of_Things_IoT_A_Vision_Architectural_Elements_and_FutureDirections (дата звернення 30.05.2022 р.)
30. IoT Architecture: Topology and Edge Compute Considerations [Електронний ресурс] – Режим доступу до ресурсу: https://www.digi.com/blog/post/iot-architecture-topology-and-edge-compute (дата звернення 30.05.2022 р.)
31. IoT reference model white paper [Електронний ресурс] – Режим доступу до ресурсу: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (дата звернення 30.05.2022 р.)
32. IoT World Forum [Електронний ресурс] – Режим доступу до ресурсу: https://iotforum.org/ (дата звернення 30.05.2022 р.)
33. JRI-MySirius Wireless temperature monitoring solution [Електронний ресурс] – Режим доступу до ресурсу: https://www.jri-corp.com/products/wireless-temperature-monitoring-systems/jri-mysirius (дата звернення 30.04.2022 р.)
34. K. J. Singh and D. S. Kapoor, Create Your Own Internet of Things: A survey of IoT – с. 3-10
35. LoRaWAN Range anf coverage in practice [Електронний ресурс] – Режим доступу до ресурсу: https://smartmakers.io/en/lorawan-range-part-2-range-and-coverage-of-lorawan-in-practice/ (дата звернення 30.04.2022 р.)
36. LoRaWAN для IoT Platform [Електронний ресурс] – Режим доступу до ресурсу: https://www.elko.ua/ru/novosti2/lorawan-elko-smart-center (дата звернення 30.05.2022 р.)

37. Microsoft Campus solutions [Електронний ресурс] – Режим доступу до ресурсу: https://www.microsoft.com/en-us/education/higher-education/campus-solutions (дата звернення 30.05.2022 р.)
38. MQTT: The Standard for IoT Messaging [Електронний ресурс] – Режим доступу до ресурсу: https://mqtt.org/ (дата звернення 30.05.2022 р.)
39. Network-topology [Електронний ресурс] – Режим доступу до ресурсу: https://www.dnsstuff.com/what-is-network-topology (дата звернення 30.05.2022 р.)
40. Nfc and internet of things [Електронний ресурс] – Режим доступу до ресурсу: https://nfc-forum.org/what-is-nfc/nfc-and-the-internet-of-things/ (дата звернення 30.05.2022 р.)
41. Oracle Internet of Things Cloud Service [Електронний ресурс] – Режим доступу до ресурсу: https://docs.oracle.com/en/cloud/paas/iot-cloud/index.html (дата звернення 30.05.2022 р.)
42. Platforms, IEEE Consumer Electronics Magazine. 2017., No. 2 Vol. 6. P. 95-100
43. Pricing – IoT Hub [Електронний ресурс] – Режим доступу до ресурсу: https://azure.microsoft.com/ru-ru/pricing/details/iot-hub/#purchase-options (дата звернення 30.05.2022 р.)
44. Saint Louis University is placing 2,300 Echo Dots in student living spaces [Електронний ресурс] – Режим доступу до ресурсу: https://www.theverge.com/2018/8/15/17693174/saint-louis-university-echo-dots-amazon-student-living-spaces (дата звернення 30.05.2022 р.)
45. Sigfox, the 0g network Networking [Електронний ресурс] – Режим доступу до ресурсу: https://www.sigfox.com/en (дата звернення 30.05.2022 р.)

46. Smart City або «розумне місто» HTTPS [Електронний ресурс] – Режим доступу до ресурсу: https://www.prostir.ua/?news=scho-take-smart-city-i-yak-vyhlyadaje-v-ukrajinskyh-realiyah (дата звернення 30.05.2022 р.)
47. Simple Object Access Protocol HTTPS [Електронний ресурс] – Режим доступу до ресурсу: https://www.ibm.com/docs/ru/rsas/7.5.0?topic=standards-soap (дата звернення 30.05.2022 р.)
48. Smart System: IoT for University [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/304292682_Smart_System_IoT_for_University (дата звернення 30.05.2022 р.)
49. Smart Transport System Based on ``The Internet of Things" sensing [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/258476881_Smart_Transport_System_Based_on_The_Internet_of_Things (дата звернення 30.05.2022 р.)
50. Smart Universities: Concepts, Systems, and Technologies [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/322167374_Smart_Universities_Concepts_Systems_and_Technologies (дата звернення 30.05.2022 р.)
51. The 4 Stages of IoT Architecture [Електронний ресурс] – Режим доступу до ресурсу: https://www.digi.com/blog/post/the-4-stages-of-iot-architecture (дата звернення 30.05.2022 р.)
52. The Constrained Application Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://coap.technology/ (дата звернення 30.05.2022 р.)
53. The Internet of things [Електронний ресурс] – Режим доступу до ресурсу: http://cba.mit.edu/docs/papers/04.10.i0.pdf (дата звернення 30.03.2022 р.)

54. The Internet protocol journal [Електронний ресурс] – Режим доступу до ресурсу: http://ipj.dreamhosters.com/wp-content/uploads/issues/2015/ipj18-4.pdf (дата звернення 30.05.2022 р.)
55. The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing [Електронний ресурс] – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/6091302 (дата звернення 30.05.2022 р.)
56. ThingsBoard Open-source IoT Platform [Електронний ресурс] – Режим доступу до ресурсу: https://thingsboard.io/ (дата звернення 30.05.2022 р.)
57. Usage of the Internet of Things in higher ed [Електронний ресурс] – Режим доступу до ресурсу: https://www.ecampusnews.com/2017/06/14/internet-things-higher-ed/ (дата звернення 20.05.2022 р.)
58. Virtual Temparature and Humidity Sensor [Електронний ресурс] – Режим доступу до ресурсу: https://azure-samples.github.io/raspberry-pi-web-simulator/ (дата звернення 30.05.2022 р.)
59. What id DDS? [Електронний ресурс] – Режим доступу до ресурсу: https://www.dds-foundation.org/what-is-dds-3/ (дата звернення 30.05.2022 р.)
60. Wi-Fi HaLow: Designed for the Internet of Things [Електронний ресурс] – Режим доступу до ресурсу: https://iot.eetimes.com/wi-fi-halow-designed-for-the-internet-of-things/ (дата звернення 10.05.2022 р.)
61. Wi-Fi Solutions [Електронний ресурс] – Режим доступу до ресурсу: https://www.silabs.com/wireless/wi-fi (дата звернення 30.05.2022 р.)
62. Zigbee Wireless Mesh Networking [Електронний ресурс] – Режим доступу до ресурсу:

https://www.digi.com/solutions/by-technology/zigbee-wireless-standard (дата звернення 30.02.2022 р.)

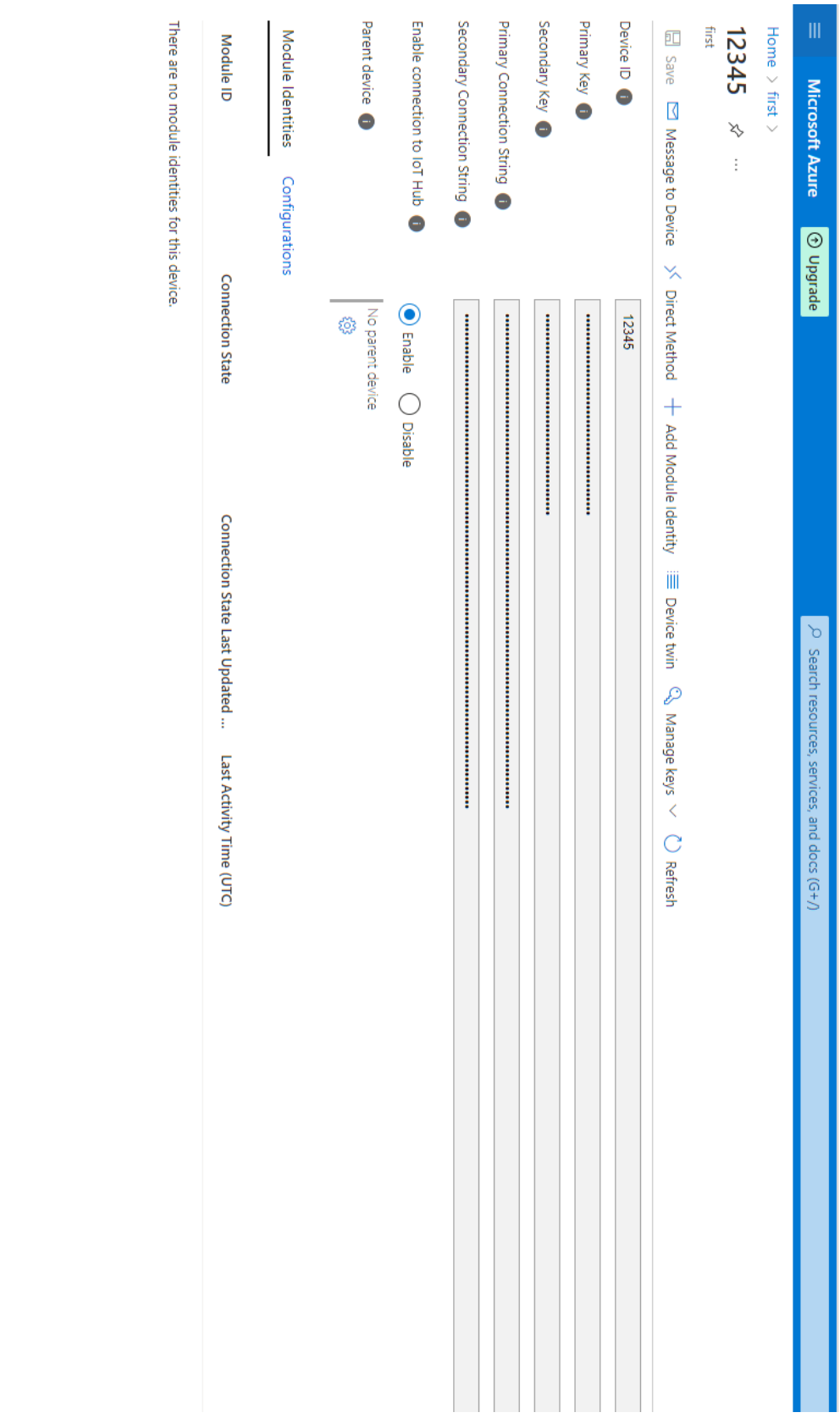
63. Z-Wave IoT technology [Електронний ресурс] – Режим доступу до ресурсу: https://www.z-wave.com/ (дата звернення 30.05.2022 р.)
64. Антена LoRaWaN [Електронний ресурс] – Режим доступу до ресурсу: https://lanmarket.ua/upload/iblock/5d8/5d83967bec5cd3dade78ef7f9da7e836.pdf (дата звернення 30.05.2022 р.)
65. Використання Інтернету речей речей [Електронний ресурс] – Режим доступу до ресурсу: https://www.it.ua/ru/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iot (дата звернення 30.02.2022 р.)
66. Інтернет речей [Електронний ресурс] – Режим доступу до ресурсу: https://www.sas.com/ru_ru/insights/big-data/internet-of-things.html (дата звернення 30.05.2022 р.)
67. Конспект лекцій з курсу “Комп’ютерні мережі” [Електронний ресурс] – Режим доступу до ресурсу: http://eprints.kname.edu.ua/52081/1/2017%20%D1%80%D0%B5%D0%BF%20249%D0%9B%20%D0%BB%D0%BA%D0%9A%D0%BE%D0%BC%D0%BF%D0%A1%D0%B5%D1%82%D0%B8_.pdf (дата звернення 30.05.2022 р.)
68. Концепція Інтернету [Електронний ресурс] – Режим доступу до ресурсу: http://umo.edu.ua/images/content/depozitar/navichki_pracevlasht/elektron_biznn.pdf (дата звернення 30.01.2022 р.)
69. Концепція Інтернету речей [Електронний ресурс] – Режим доступу до ресурсу: https://www.researchgate.net/publication/311863315_Koncepcia_internet_vese (дата звернення 30.05.2022 р.)

70. МСЕ: Глобальна інформаційна інфраструктура, аспекти протоколу Інтернет і мереж наступного покоління Y.2060 Things [Електронний ресурс] – Режим доступу до ресурсу: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-R&type=items (дата звернення 30.02.2022 р.)
71. Промисловий Інтернет речей [Електронний ресурс] – Режим доступу до ресурсу: https://www.it.ua/ru/knowledge-base/technology-innovation/promyshlennyj-internet-veschej (дата звернення 30.01.2022 р.)

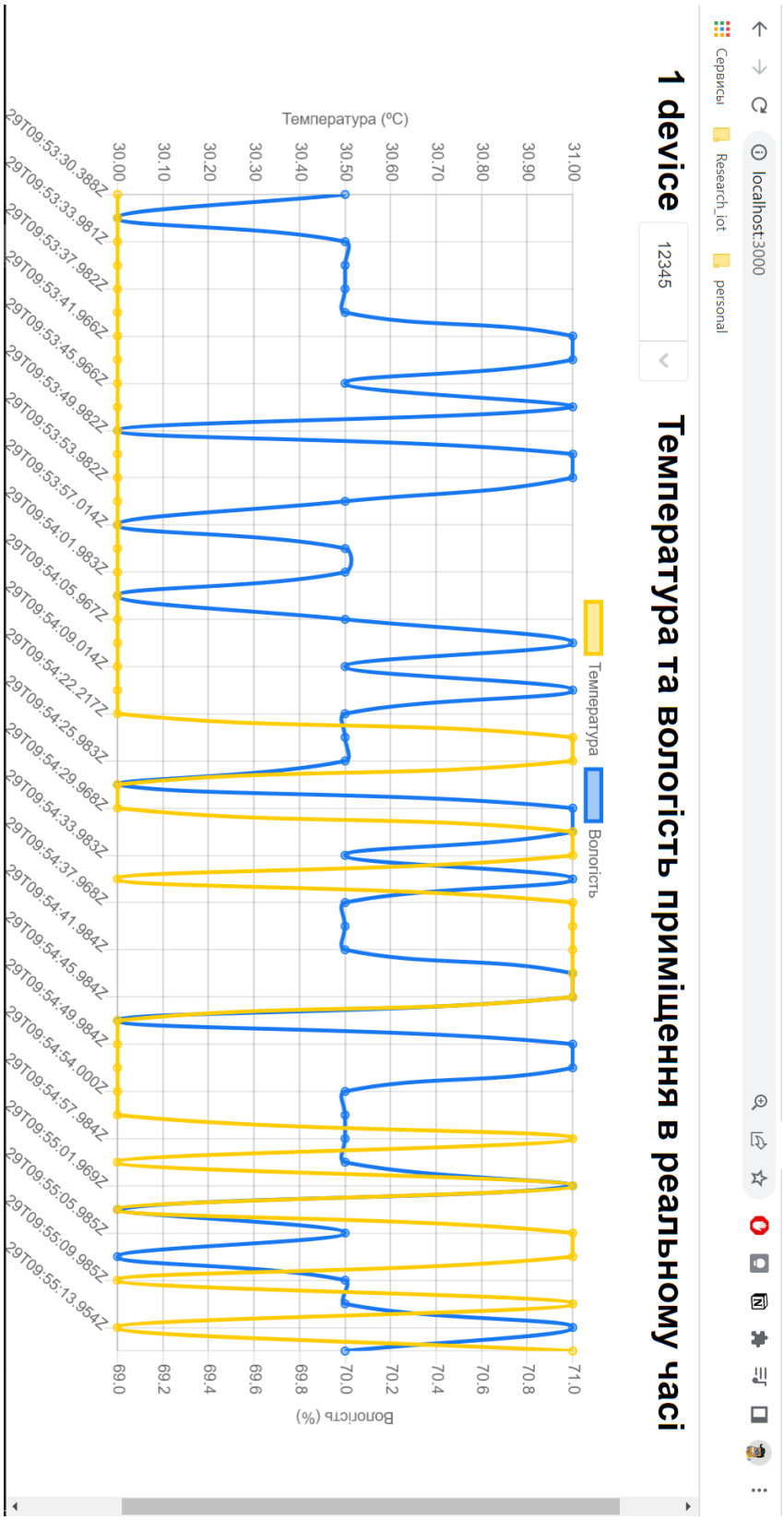
ДОДАТКИ

Додаток А. Метрики підключених датчиків та отриманих повідомлень.

Додаток Б. Підключення датчику до Microsoft Azure IoT Hub.



Додаток В. Результати роботи IoT платформи.



Додаток Г. Віртуальний датчик температури та вологості [57].