МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА

другого (магістерського) рівня вищої освіти

на тему:

«АНАЛІЗ ТЕХНОЛОГІЙ ОБМІНУ ІНФОРМАЦІЇ У МЕРЕЖАХ IoT»

Виконав: здобувач групи ІТ-62
спеціальності 126 «Інформаційні системи та технології»

_____ Денис В.А.
(прізвище та ініціали)

Керівник:_____ Пташник В. В.
(прізвище та ініціали)

Рецензент_____
(прізвище та ініціали)

ДУБЛЯНИ-2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ПРИРОДОКОРИСТУВАННЯ
ФАКУЛЬТЕТ МЕХАНІКИ, ЕНЕРГЕТИКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Другий (магістерський) рівень вищої освіти
Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____
(підпис)
д.т.н., професор, Тригуба А. М.
(вч. звання, прізвище, ініціали)
“____” _____2024 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Денис Віталій Андрійович
(прізвище, ім’я, по батькові)

1. Тема роботи *«Аналіз технологій обміну інформації у мережах IoT»*
керівник роботи *к. т. н., доцент., Пташник В. В.*
(наук.ступінь, вч. звання, прізвище, ініціали)

затверджені наказом Львівського НУП *від 12.09.2024 року № 616/к-с*
2. Строк подання студентом роботи *06 грудня 2024 року*
3. Вихідні дані до роботи: *характеристика сучасних систем інтернету речей; технічна документація до інженерного обладнання інтернету речей: сенсорів, виконавчих механізмів, модулів дротового та бездротового зв’язку; специфікація елементів екосстеми інтернету речей; науково-технічна і довідкова література; довідкова інформація щодо сучасних засобів розробки.*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Аналіз принципів роботи систем інтернету речей
2. Порівняння технологій та протоколів передачі даних в мережах інтернету речей
3. Інтеграція технології Blokchain у систему IoT
4. Охорона праці та безпека в надзвичайних ситуаціях
5. Економічна ефективність
Висновки
Список використаних джерел
5. Перелік графічного матеріалу
Графічний матеріал подається у вигляді презентації

6. Консультанти розділів

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата		Відмітка про виконання
		завдання видав	завдання прийняв	
1, 2, 3, 5	*Пташник В. В., к.т.н., доцент*			
4	*Городецький І. М., к.т.н., доцент*			

7. Дата видачі завдання *13 вересня 2024 р.*

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Відмітка про виконання
1	*Аналіз принципів роботи систем інтернету речей*	*13.09.2024 – 30.09.2024*	
2	*Порівняння дротових та бездротових технологій передачі даних в мережах інтернету речей*	*01.10.2024 – 15.10.2024*	
3	*Впровадження технології Blokchain у системи IoT*	*16.10.2024 – 31.10.2024*	
4	*Розгляд питань з охорони праці та безпеки у надзвичайних ситуаціях*	*01.11.2024 – 10.11.2024*	
5	*Оцінка економічної ефективності прийнятих рішень*	*11.11.2024 – 17.11.2024*	
6	*Завершення оформлення розрахунково-пояснювальної записки та презентаційного матеріалу*	*18.11.2024 – 30.11.2024*	
7	*Завершення роботи в цілому. Підготовка до захисту кваліфікаційної роботи*	*01.01.2024 – 06.12.2024*	

Здобувач _____ *Денис В. А.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Пташник В. В.*
(підпис) (прізвище та ініціали)

УДК 681.521 / 681.518

Аналіз технологій обміну інформації у мережах IoT. Денис В. А. Кафедра інформаційних технологій – Дубляни, Львівський національний університет природокористування, 2024.
Кваліфікаційна робота: 68 сторінок текстової частини, 24 рисунки, 6 таблиць, 24 джерела літератури.

Метою кваліфікаційної роботи є аналіз сучасних технологій обміну інформації у мережах Інтернету речей (IoT), визначення їхніх особливостей, переваг і недоліків, а також обґрунтування вибору оптимальних технологій для підвищення ефективності комунікацій у різних сценаріях використання IoT.

Об'єктом дослідження є мережі Інтернету речей та процеси обміну інформацією між пристроями в цих мережах.

Предмет дослідження вивчає технології та протоколи обміну інформацією, що використовуються у мережах IoT.

Під час виконання кваліфікаційного дослідження ретельно вивчено предметну сферу та проаналізовано методи, інструменти, протоколи низькорівневого зв'язку, такі як Bluetooth, ZigBee, LoRaWAN, і високорівневі стандарти, такі як MQTT, CoAP і HTTP. Особливу увагу приділено ефективності роботи цих технологій в умовах обмежених ресурсів, наприклад, низької потужності пристроїв або обмеженої пропускної здатності мережі. Дослідження також аналізує особливості безпеки передачі даних, враховуючи зростаючу загрозу кіберризиків у мережах IoT. Загалом, предмет дослідження спрямований на визначення найбільш ефективних рішень для різних сценаріїв використання Інтернету речей.

Ключові слова: інтернет речей (IoT), технології обміну інформацією, протоколи комунікації IoT, мережі IoT, MQTT, CoAP, HTTP, ефективність комунікацій, аналіз технологій передачі даних.

ЗМІСТ

ВСТУП

У сучасному світі Інтернет речей (Internet of Things, IoT) стає одним із ключових напрямків розвитку технологій, трансформуючи звичні способи взаємодії між людьми, пристроями та інформацією. Завдяки IoT, створюється можливість об'єднання різноманітних об'єктів у єдину мережу, де вони можуть обмінюватися даними, приймати рішення та адаптуватися до змін у реальному часі. Це відкриває нові перспективи для застосування IoT у різних галузях, включаючи промисловість, транспорт, медицину, сільське господарство та управління інфраструктурою міст. Однак ключовим елементом, що визначає ефективність мереж IoT, є технології обміну інформацією, від яких залежить надійність, швидкість і безпека передачі даних.

Складність сучасних мереж IoT обумовлена їхньою неоднорідністю та великою кількістю пристроїв, які можуть значно відрізнятися за технічними характеристиками, способами підключення та вимогами до енергоефективності. Це створює виклик для розробки технологій обміну інформацією, здатних відповідати цим вимогам і водночас забезпечувати сумісність між пристроями різних виробників. Різноманітні протоколи, такі як MQTT, CoAP, Zigbee, LoRa та інші, пропонують різні рішення для передачі даних, що дозволяє досягати компромісу між енергоефективністю, швидкістю та масштабованістю систем IoT.

Актуальність дослідження цієї теми зумовлена необхідністю створення надійних і безпечних систем для обробки та передачі великих обсягів даних, що постійно генеруються пристроями IoT. Водночас значення мають економічні та екологічні аспекти, адже ефективні технології обміну інформацією можуть суттєво знизити витрати на підтримку мережі та впливати на енергоспоживання пристроїв.

РОЗДІЛ 1
АНАЛІЗ ПРИНЦИПІВ РОБОТИ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ

1.1. Архітектура Інтернету речей

Інтернет речей — це всесвітня інфраструктура для інформаційного суспільства, яка забезпечує потенціал для більшої складності в послугах шляхом поєднання (фізичних і віртуальних) об'єктів з інформаційно-комунікаційними технологіями, які є функціонально сумісними.

Пристрій IoT має мати комунікаційні можливості та забезпечувати додатковий функціонал, наприклад збір, обробку, введення, зберігання й представлення даних.

Структура архітектури пристроїв IoT складається з чотирьох рівнів: сенсорного рівня, мережевого рівня, рівня обробки даних і рівня додатків (див. рис. 1.1). Більш детальний опис кожного рівня архітектури наведено нижче.

Основна функція сенсорного рівня — розпізнавати різні явища навколишнього середовища за допомогою периферійних пристроїв, а також отримувати дані з реального світу. Цей рівень містить кілька різновидів датчиків. Використання комбінації датчиків є однією з найважливіших функцій пристроїв IoT. Датчики в пристроях IoT зазвичай об'єднуються у відповідну мережу. Також на цьому рівні функціонує концентратор датчика, який накопичує інформацію з кількох датчиків. Він також збирає та передає інформацію від датчиків до блоку обробки даних у пристрої. Концентратори зазвичай можуть використовувати кілька механізмів зв'язку, таких як (інтегрований протокол I^2C або послідовний периферійний інтерфейс SPI), щоб передавати дані між датчиками та програмами. Безпосередній вибір механізмів зв'язку залежать від кінцевих пристроїв IoT, які підтримують менше технологій зв'язку ніж концентратори.

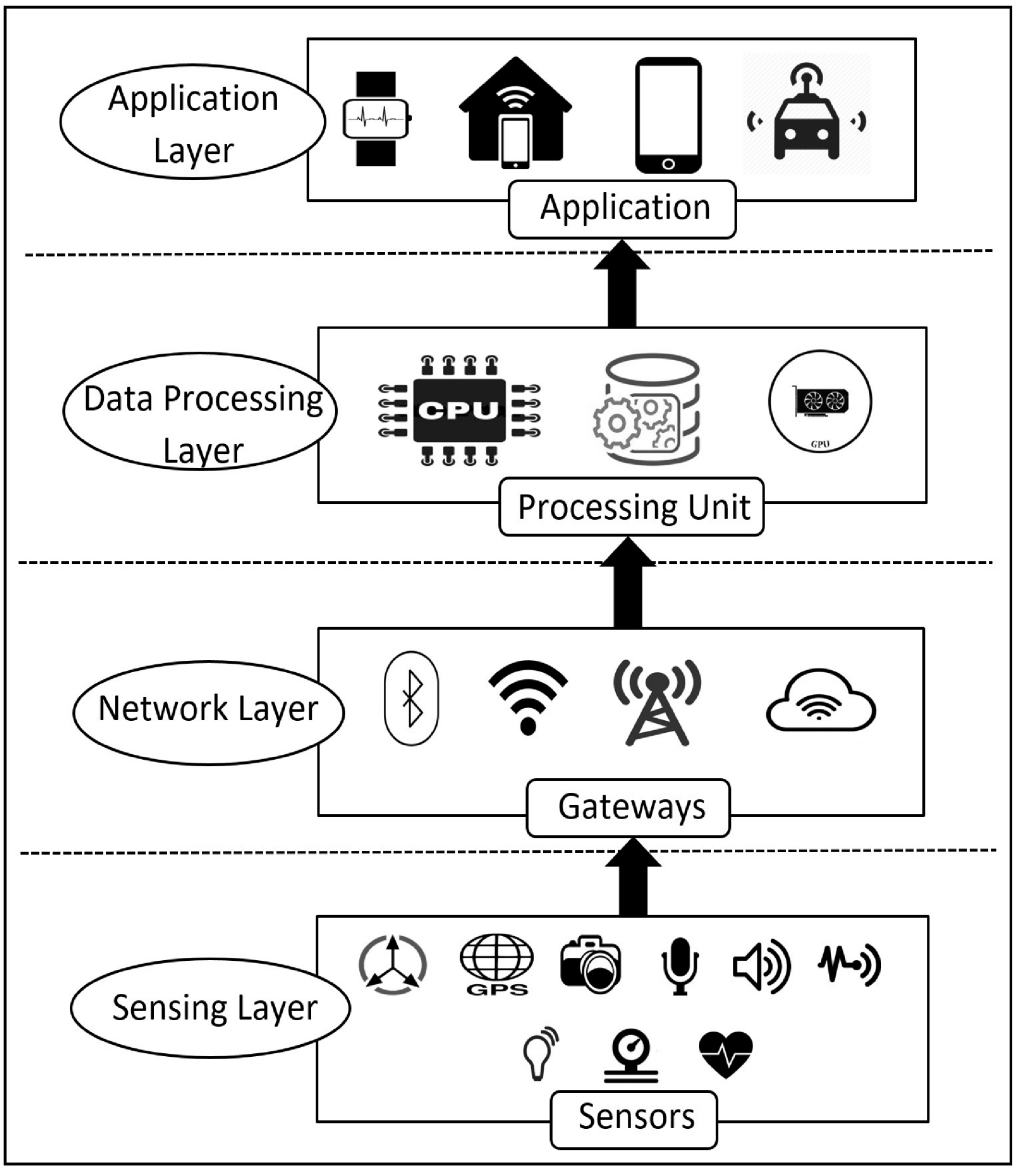

Рисунок 1.1 – Рівні архітектури мережі Інтернету речей

Датчики в пристроях IoT поділяються на кілька великих категоріїй.

Датчики руху аналізують зміну руху, а також орієнтацію пристрою у просторі. За допомогою такого датчика пристрій може контролювати два види руху: прямолінійний рух і кутовий рух.

Датчики навколишнього середовища включають такі пристрої, як датчики світла, тиску, температури, вологості, якості повітря тощо. Інтеграція таких датчиків у IoT пристрої дозволяє їм реагувати на зміни умов навколишнього середовища. Основною метою використання цих датчиків у пристроях IoT є допомога пристроям у прийнятті рішень, які безпосередньо

залежать від змін в навколишніх умовах, але не залежать від інших периферійних пристроїв. Наприклад, датчики навколишнього середовища поширені в більшості програм, які спрощують життя користувачів (наприклад, розумні замки, система домашньої автоматизації, розумне освітлення тощо).

Датчики позиціонування передають дані про фізичне місцезнаходження самого IoT пристрою. Найпоширенішими датчиками позиціонування, які використовуються в IoT, є магнітні датчики та датчики GPS. Магніти використовуються як аналогові годинники та допомагають орієнтувати екран пристрою. GPS-датчики використовуються в IoT для полегшення навігації.

Мережевий рівень IoT використовується як засіб передачі даних для передачі інформації, зібраної датчиками, іншим пов'язаним пристроям. У пристроях IoT мережевий рівень реалізовано для використання кількох комунікаційних технологій (наприклад, Z-Wave, LoRa, Wi-Fi та Bluetooth). які полегшують передачу даних між різними пристроями в самій мережі.

Рівень обробки даних складається з головного блоку для обробки даних у пристрої IoT. Рівень обробки даних отримує інформацію, зібрану на рівні датчика, і аналізує її, потім він обирає дії на основі результатів аналізу. У деяких випадках IoT (наприклад, розумний годинник, розумний домашній концентратор тощо) на цьому рівні також містяться результати попередніх досліджень цих даних для подальшого використання інформації. Крім того, цей рівень здатний передавати результати обробки даних від одного підключеного пристрою до іншого через мережевий рівень. Це забезпечує узгоджену взаємодію між пристроями та сприяє оптимізації їх роботи в реальному часі. Таким чином, рівень обробки даних відіграє принципову роль у забезпеченні інтелектуальних функцій IoT-систем.

Прикладний рівень (або рівень додатків) демонструє результати рівня обробки даних за допомогою різних додатків на основі пристроїв Інтернету речей. Цей рівень, орієнтований на користувача та надає йому необхідні послуги. Різні види використання IoT включають розумні будинки, транспорт та інші програми.

1.2. Принципи роботи систем Інтернету речей

У роботі найпростіших систем IoT виділяють чотири окремі етапивідображені на рис. 1.2:

– зчитування інформації за допомогою датчиків;
– передача даних з датчиків в хмарну систему зберігання;
– обробка даних, зібраних датчиками (об'єднання даних);
– передача інформації в інтерфейс користувача.

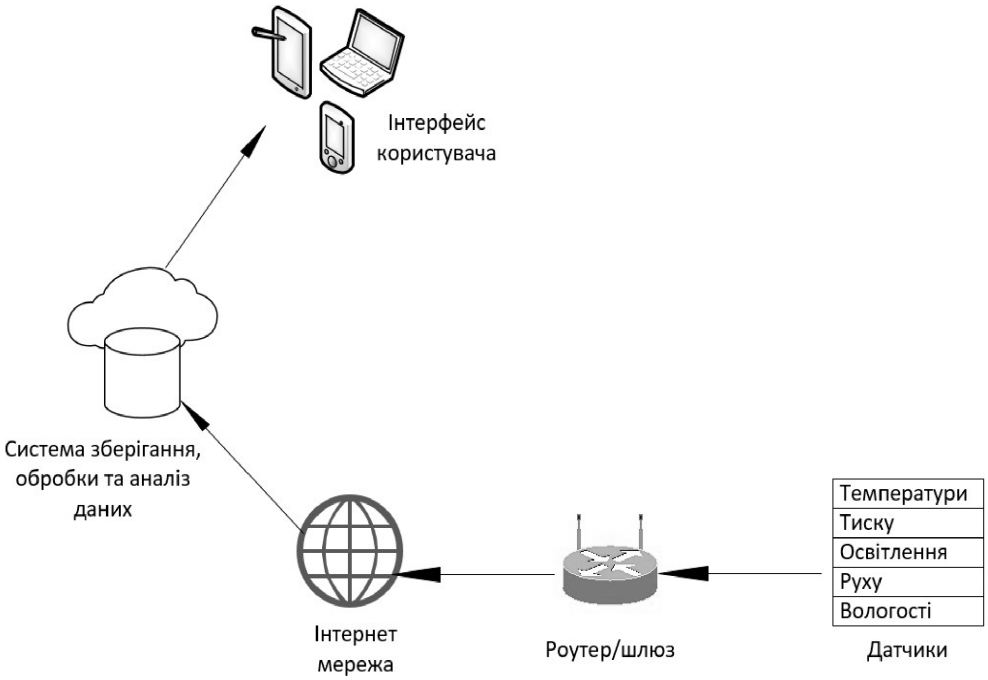

Рисунок 1.2 – Принцип роботи типової IoT мережі

Проведемо детальний аналіз вищезгадних операцій. Спочатку датчики або пристрої знімають сигнали або збирають дані з оточення. Наприклад, це може бути вимірювання температури або зйомка зображень камерою. Це етап, на якому збираються дані з навколишнього середовища.

На етапі передачі даних від датчиків до хмарних сховищ можуть використовуватись різні способи підключення датчиків до хмари: стільникова мережа, супутникова мережа, Wi-Fi, Bluetooth, LPWAN і навіть пряме

підключенні до Інтернету через технологію Ethernet. Кожна з цих альтернатив є компромісом між енергоспоживанням, відстанню та пропускною здатністю. Таким чином, вибір будь-якого конкретного режиму з'єднання залежатиме від конкретного сектору застосування Інтернету речей, але усі технології скеровані на передачу даних у хмару.

Обробка даних отриманих за допомогою датчиків починається коли інформація потрапляє в хмару, тоді програмне забезпечення виконує заздалегідь закладені дії з отриманою інформацією. Наприклад, перевіряє чи знаходяться покази температури в межах певного діапазону прийнятності.

На останньому етапі інформація певним чином передається кінцевому користувачу за його запитом. Це може бути будь-яке сповіщення користувача (електронна пошта, SMS, сповіщення тощо).

Крім того, користувач повинен мати інтерфейс для інтерактивного тестування системи. Наприклад, користувачу може знадобитися дізнатися, чи добре працюють камери відеоспостереження в його будинку; він може зробити це через додаток або веб-сторінку. Такий інтерфейс має бути інтуїтивно зрозумілим і забезпечувати швидкий доступ до ключових функцій, таких як налаштування параметрів або отримання сповіщень про несправності. Крім того, інтерактивне тестування може включати можливість віддалено запускати діагностику пристроїв або перевіряти історію їх роботи, що підвищує зручність і ефективність управління системою. Застосування IoT дозволяє користувачам виконувати певну роботу або альтернативно контролювати систему.

Таким чином можна сказати, що система IoT — це датчики, які комунікують з з хмарою через певний вид зв'язку. Після того, як дані потрапляють у хмару, вони обробляються за допомогою програмного забезпечення, а потім можуть виконувати дії, наприклад передаватись користувачу або ж автоматично змінювати продуктивність датчика без участі користувача.

1.3. Еталонна модель Інтернету речей

На рис. 1.3 представленя еталонна модель IoT, яка наведена в рекомендації Y.2060, вона складається з чотирьох основних рівнів:

- рівень пристроїв;
- мережевий рівень;
- рівень підтримки послуг та додатків;
- прикладний рівень.

Також еталонна модель включає два додаткових рівні: управління та безпеки. Розглянемо детально кожен з цих рівнів.

Прикладний рівень в Рекомендації Y.2060 не розглядається та реалізується на розсуд розробника.

Рівень підтримки послуг та додатків складається з двох груп можливостей, таких як загальні можливості підтримки та спеціалізовані можливості підтримки.

Додатки можуть використовувати різноманітні можливості, зокрема це обробка та зберігання даних. Ці можливості можуть бути активовані за допомогою спеціалізованих можливостей підтримки, наприклад, для створення інших спеціалізованих можливостей та задоволення потреб користувача. Спеціалізовані можливості підтримки реалізують конкретні можливості, які призначені для задоволення вимог різноманітних додатків. Фактично, вони можуть складатися з кількох наборів чітко визначених функцій, щоб забезпечити різні можливості для підтримки різних програм IoT.

Мережевий рівень також надає користувачу два типи можливостей: можливість організації мереж та можливість транспортування. Можливості організації мереж надають відповідні функції управління мережевим з'єднанням, такі як функції управління доступом та ресурсами транспортування, управління мобільністю або автентифікацією, авторизація та облік.

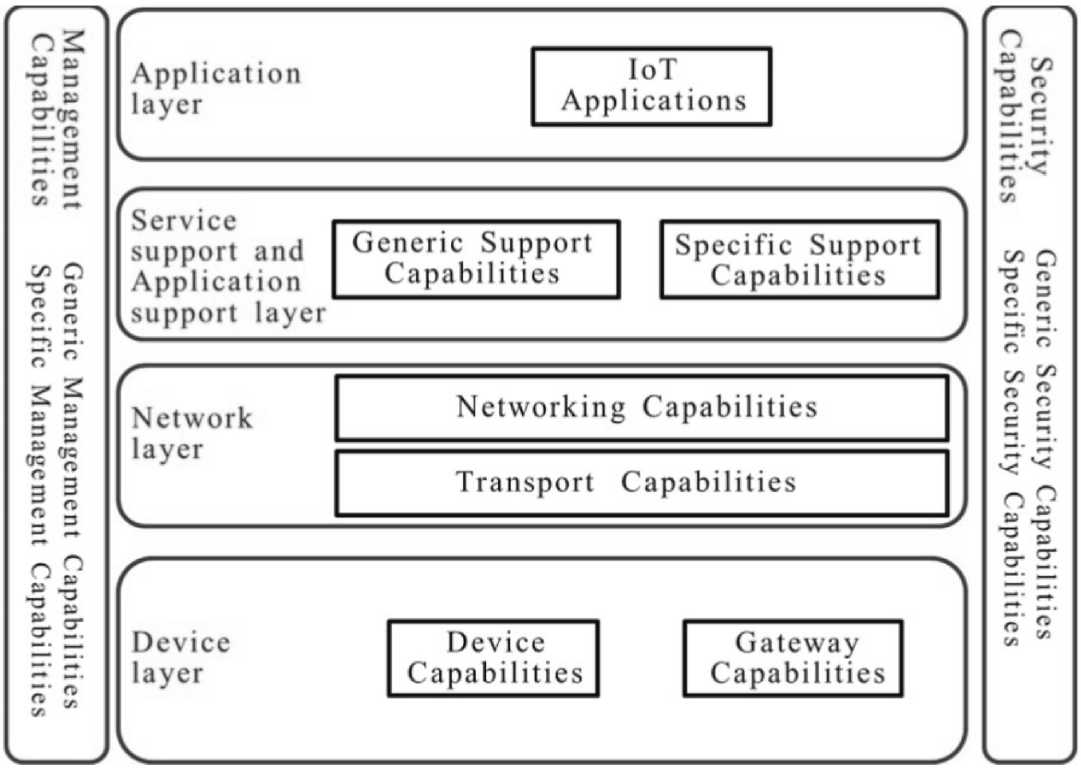

Рисунок 1.3 – Еталонна модель Інтернету речей

Можливості транспортування даних надають з'єднання для транспортування інформації у вигляді даних, що відносяться до послуг і додатків IoT, а також транспортування інформації контролю та управління, що відносяться до IoT.

Можливості рівня пристроїв можна логічно розділити на два види: можливості пристрою та можлвості шлюзу. Можливості пристрою також можна розділити на декілька підкатегорій.

У разі реалізації прямої взаємодії з мережею зв’язку пристрої можуть безпосередньо взаємодіяти з мережею без необхідності передавати сигнла через шлюз, це дозволяє їм отримувати інформацію (наприклад, команди) безпосередньо з мережі.

А у випадку реалізації непрямої взаємодії мережі зв'язку пристрої здатні отримувати та закачувати інформацію в мережі зв'язку непрямим чином, тобто за допомогою можливості шлюзу. На іншій стороні пристрою можуть не прямим чином отримувати інформацію (наприклад, команди) з мережі зв'язку. Організація спеціальних мереж в деяких сценаріях вимагає підвищеної

масштабованості та швидкого розгортання, пристрої можуть мати можливість будувати мережі довільним чином.

Можливості шлюзу повинні забезпечити підтримку інтерфейсу та процесів перетворення протоколів.

Підтримку інтерфейсу слід розглядати з точки зору мультиплексії. Види з'єднань, що існують між пристроєм і шлюзом, можуть використовувати різні дротові і бездротових технологій, наприклад CAN, Bluetooth або Wi-Fi.

На рівні мережі шлюз повинен мати можливість передавати дані між різними прикладними технологіями зв'язку та обміну даними, наприклад, PSTN, мережами на основі 2G або 3G, мережами LTE, Ethernet або DSL.

Можливості шлюзового перетворення протоколу потрібні в двох ситуаціях. Перша ситуація – це коли різні протоколи рівня пристрою використовуються для зв'язку на рівні пристрою, наприклад, протокол технології Z-Wave для якогось пристрою плюс Bluetooth. По-друге, коли з'являється зв'язок, який використовує як рівень пристрою, так і рівень мережі, але з різними технологіями; наприклад, протокол технології Z-Wave рівня пристрою та протокол технології рівня мережі 3G.

Розглянемо також додаткові підрівні екосистеми Інтернету речей. Серед загальних можливостей управління в Інтернеті речей є керування пристроєм, управління топологією локальної мережі та управління трафіком і перевантаженнями.

Керування пристроєм передбачає можливість увімкнення та вимкнення віддаленого пристрою, його діагностика, оновлення програмного та мікропрограмного забезпечення, моніторинг стану пристрою тощо.

А управління трафіком і перевантаженнями включає, наприклад розпізнавання перевантаження мережі та резервування важливих і/або термінових потоків трафіку. Спеціалізовані можливості керування також тісно пов'язані з вимогами додатків.

Можливості забезпечення безпеки розділяють на два види: загальні можливості забезпечення безпеки та спеціалізовані можливості забезпечення безпеки.

Загальні можливості забезпечення безпеки не залежить від додатків і включають на системному рівні процеси авторизації, автентифікації, захисту конфіденційності та цілісності даних, аудит безпеки та антивірусне програмне забезпечення.

На мережевому рівні можливості безпеки пов’язують з процесами авторизації, автентифікації, конфіденційності даних та їх цілісності.

На рівні пристроїв відбувається автентифікація, авторизація, перевірка цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних. Спеціалізовані можливості забезпечення безпеки також тісно пов'язані з вимогами додатків, наприклад вимогам безпеки мобільних платежів.

РОЗДІЛ 2
ПОРІВНЯННЯ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Аналіз технологій та протоколів передачі даних далекого зв'язку

Найближчим часом до багатьох пристроїв буде підключений Інтернет речей. Основним джерелом живлення більшості цих пристроїв буде акумулятор. Одним із основних атрибутів є тривалість часу, протягом якого обладнання працює без допомоги людини – час автономної роботи.

Щоб вирішити цю задачу, розроблені нові мережі та мережеві протоколи спеціально для IoT. Ці мережі відомі як LPWAN (Long Power Wide Area Network). Основними технологіями в цих мережах є NB-IoT, Weightless, LoRa, SIGFOX та інші. Ці технології були створені, оскільки розвиток IoT вимагає підключення все більшої кількості датчиків та пристрої до централізованої бази даних інформації на серверах у хмарі [9].

Мережа LoRa (Long Range) – це технологія і однойменний метод модуляції. Метод модуляції LoRa запатентований компанією Semtech, заснований на технології розширення спектру (spread spectrum modulation) і варіації лінійної частотної модуляції (chirp spread spectrum, CSS), за якої дані закодовано широкосмуговими імпульсами з частотою, що збільшується, або зменшується на деякому тимчасовому інтервалі [11].

LoRa дозволяє демодулювати сигнали на рівні 20 дБ нижче рівня шумів, тоді як більшість систем з частотною маніпуляцією (frequency shift keying, FSK) можуть коректно працювати з сигналами на рівні не нижче 8-10 дБ над рівнем шумів. Схема модуляції LoRa — це фізичний рівень, який можна використовувати в мережах із різними конфігураціями: мережах зірка, точка-точка та сітчаста мережа.

Завдяки своїй високій чутливості (148 дБм) LoRa використовується для пристроїв, які потребують низької потужності та мають велику відстань для переміщення.

Разом з протоколом LoRaWAN можуть працювати декілька видів пристроїв (див. рис. 2.1). Ці пристрої в LoRaWAN поділяються на:

– двонаправлені кінцеві пристрої «класу A» (Bi directional End Devices, Class A);

– двонаправлені кінцеві пристрої «класу B» (Bi directional End Devices, Class B). Від апаратів «класу A» відрізняється тим, що такі пристрої можуть використовувати додаткове вікно прийому;

– двонаправлені кінцеві пристрої «класу C» з максимальним вікном прийому (Bi directional End Devices, Class C). Вони відрізняються вікном практично постійного прийому даних і закривають його тільки під час передачі даних. Цей атрибут дає змогу використовувати їх для вирішення проблем, пов'язаних із великим обсягом даних.

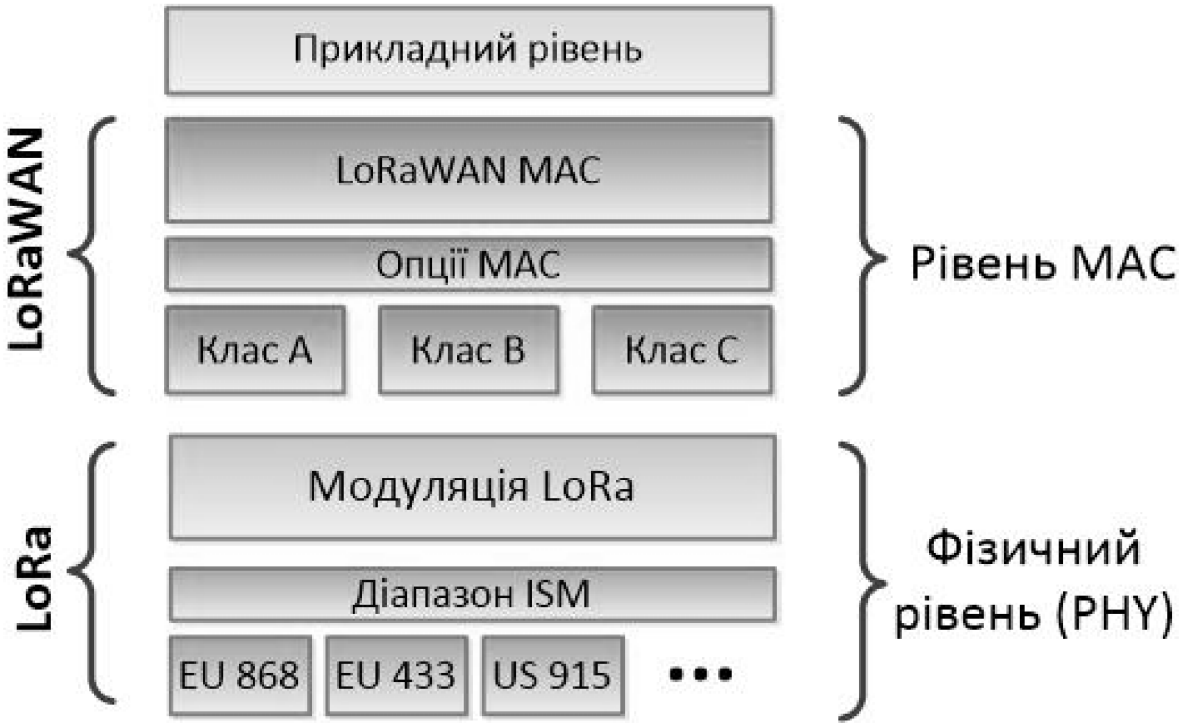

Рисунок 2.1 – Класифікація рівнів та пристроїв LoRaWAN

Конструкція LoRaWAN складається з таких основних компонентів: кінцеві точки, шлюзи, мережевий сервер і сервер додатків (рис. 2.2).

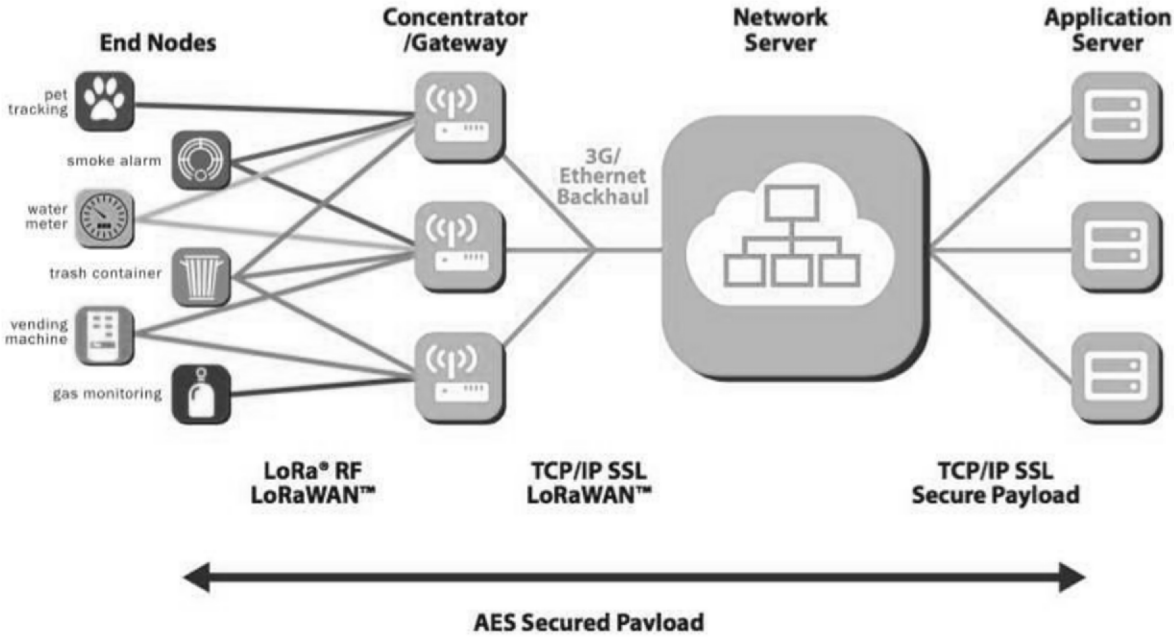

Рисунок 2.2 – Архітектура мережі LoRaWAN

Кінцеві вузли (End Nodes) – пристрої, які здійснюють вимірювання, регулюють і керують. Вузол складається з датчиків і елементів керування, які вимірюють і оцінюють стан системи. Як правило, вони працюють від акумуляторів. З метою економії енергії вузли передають дані протягом обмеженого періоду часу, після чого слідує період очікування для отримання даних.

Шлюз LoRa (Gateway/Concentrator) – це станція, яка отримує інформацію через радіозв'язок від інших станцій, а потім передає її в транспортну мережу. Транзитні мережі включають Wi-Fi, Ethernet, стільникові мережі та будь-які інші канали зв'язку.

Мережевий сервер (контролер) (Network Server) — це віддалений центр керування мережею. Він використовується для регулювання швидкості роботи мережі, аналізу, обробки та зберігання інформації, отриманої на вході.

Сервер додатків (Application Server) – це пристрій, який збирає інформацію з обох кінцевих вузлів і дистанційно керує їхніми діями.

SigFox — це нова форма технології, яка утворилась навколо інформації та комунікації. Розроблений однойменним колективом Labège, Франція, SigFox є мережевим провайдером, який спеціалізується на інтеграції промислового Інтернету речей у бізнес [12]. Конструкція мережі SigFox схожа на операторів стільникового зв'язку, таких як GSM і GPRS, але менш дорога та більш енергоефективна [9].

Покриття, яке забезпечує SigFox, становить приблизно 30-50 кілометрів у містах і селах. У мегаполісах з високим цифровим шумом максимальна робоча відстань становить 3-10 кілометрів.

Пристрої передають свої повідомлення на радіостанцію SigFox. За допомогою протоколу «точка-точка» (P2P) базова станція Sigfox підключається до своєї Інтернет-бази, після отримання та декодування повідомлення дані передаються в її Інтернет-базу. Зрештою, хмарний сервер SigFox спілкується з клієнтськими серверами та IT-платформами через API (рис. 2.3).

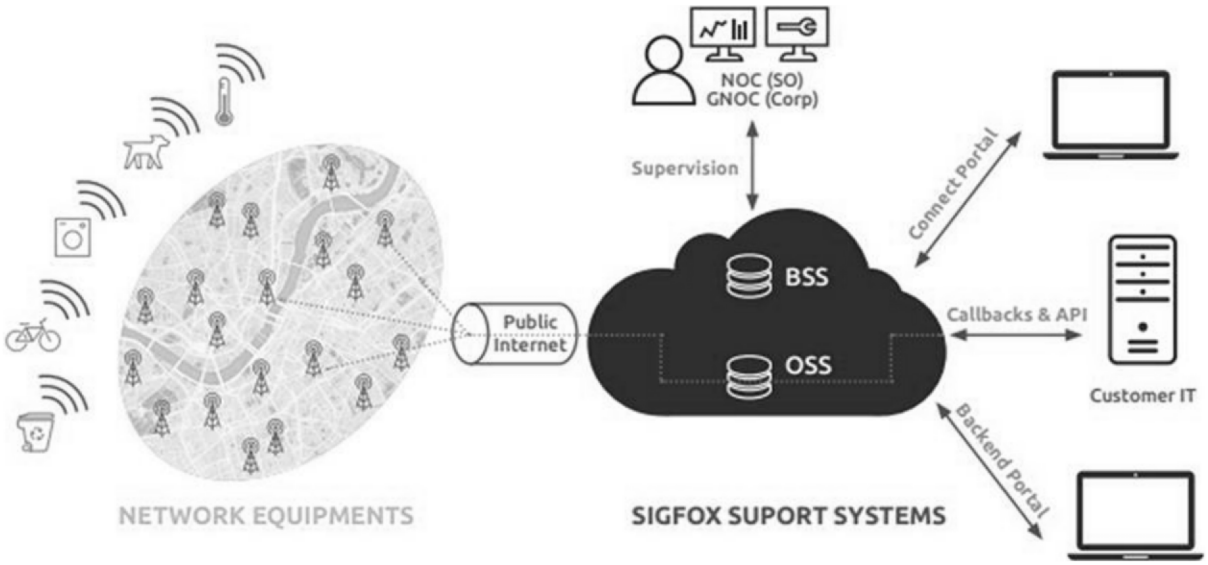

Рисунок 2.3 – Типова архітектура мережі SigFox

Технологія SigFox призначена для недорогих пристроїв, які потребують великої площі покриття [9].

Загальний стандарт має численні переваги порівняно з іншими фундаментальними технологіями в мережах LPWAN, однак у певних вузькоспеціалізованих задачах він поступається конкурентам.

NB-IoT — це протокол стільникового зв'язку, призначений для пристроїв телеметрії з низькою швидкістю передачі даних. Розроблений 3GPP як засіб розробки стільникових телефонів, перша версія стандарту була випущена в 2016 році.[9]

NB-IoT, також відомий як стандарт LTE-CAT.M2, має ряд переваг, серед яких низьке енергоспоживання, що забезпечує час автономної роботи до 10 років, широка зона покриття, можливість швидкої модернізації мережі і високий ступінь надійності.

Виділений частотний канал із смугою пропускання 200 кГц є найефективнішим для NB-IoT, але він також найдорожчий. В цьому випадку необхідно використати 300-600 кГц основного спектру разом із інтервалами безпек. У такому випадку виникає мінімальне стикування з іншими технологіями (рис. 2.4).

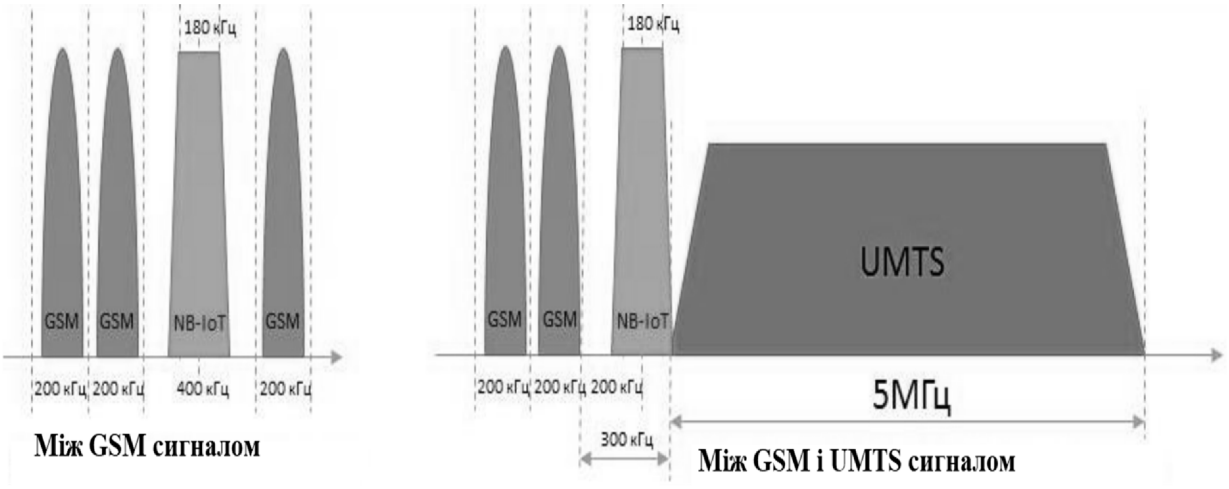

Рисунок 2.4 – Варіанти розміщення сигналів NB-IoT в режимі Stand - Alone

Ресурси призначені для NB-IoT можуть перебувати всередині існуючого спектру LTE, але NB-IoT має вищу потужність на 6 дБ, ніж блоки ресурсів LTE. Цей варіант вигідний для збереження частотного ресурсу, але є проблема взаємовпливу на мережі LTE (рис. 2.5).

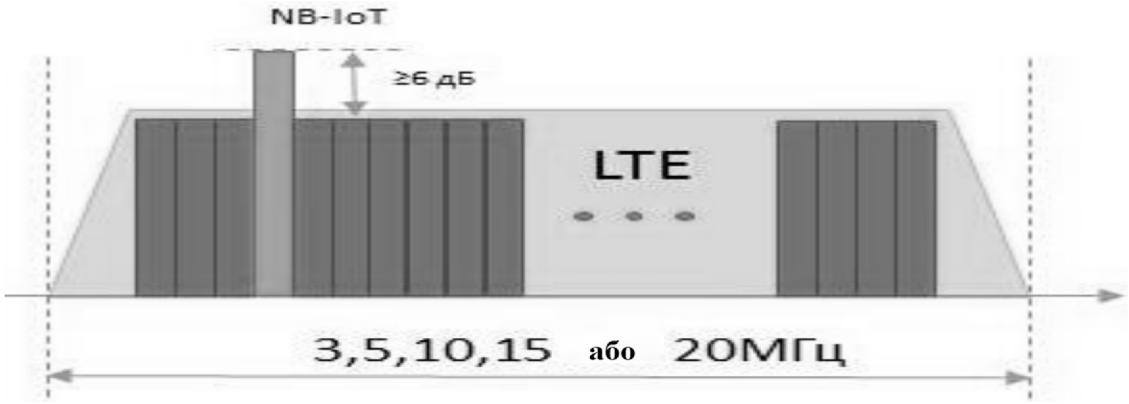

Рисунок 2.5 – Розміщення сигналів NB-IoT в режимі in Band

У разі роботи NB-IoT у захищеному діапазоні частот її спектр розпочнеться у межах так званого запобіжного інтервалу. Наприклад, у діапазоні LTE 10 МГц 500 кГц доступного спектру використовується як запобіжний інтервал. Крім того для роботи NB-IoT у захищеному діапазоні для носій збільшує потужність на 6-9 дБ порівняно з блоками ресурсів LTE (рис.2.6).

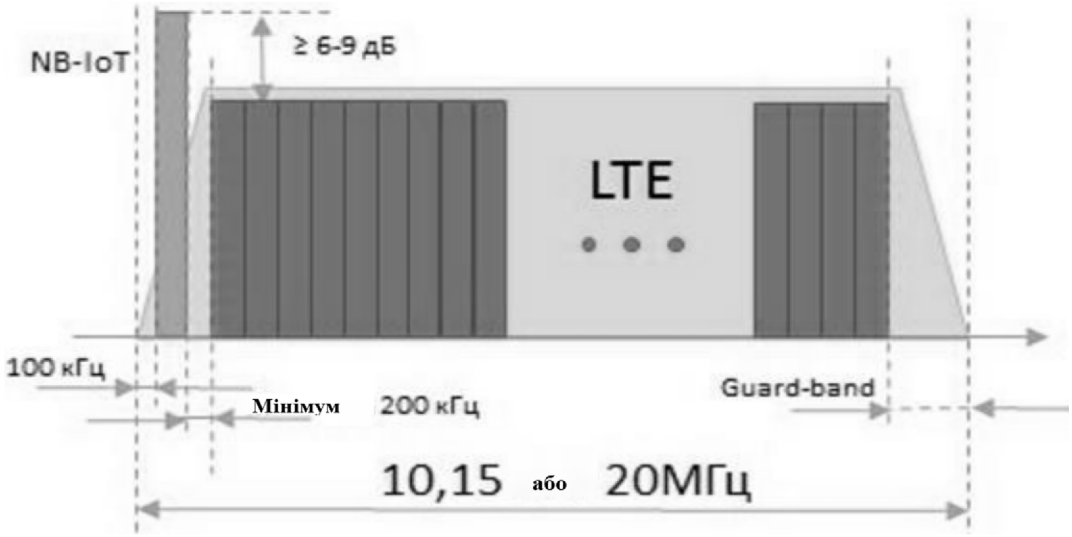

Рисунок 2.6 – Розміщення сигналів NB-IoT в режимі Guard Band

Такий спосіб використання дозволяє одночасно зберегти частотний ресурс і зменшити взаємодію з мережею LTE, однак параметри позасмугових випромінювань LTE будуть погіршені.

Weighless-P — це технологія, яка використовується для реалізації Інтернету речей. Він використовується, коли необхідно забезпечити тривалий час автономної роботи від акумулятора, двонаправлений зв'язок і підтримку пристроїв високого класу [9]. Особливості цієї технології включають велику зону покриття, стабільність мережі, тривалий час автономної роботи та безпеку. Технологія підтримує гарантовану доставку повідомлень, тому не доводиться багаторазово відправляти повідомлення, як в LoRa, SigFox.

Порівняльна характеристика технологій передачі даних на довгі відстані в мережі IoT наведена у таблиці 2.1.

Таблиця 2.1 – Порівняння основних технічних характеристик високочастотних мереж LPWAN

Характеристики	**LoRaWAN**	**SigFox**	**NB-IoT**	**Weightless-P**
Метод модуляції	CSS	DBPSK/GFSK	GFSK/BPSK/QPSK	GMSK/PSK
Діапазон	ISN	ISM	ліцензований	ISM
Швидкість	0.3-50 кбіт/с	100 кбіт/с	UL:1-144 кбіт/с UL:1-200 кбіт/с	0,2-100 кбіт/с
Смуга	широкосмуг. до 500 кГц	вузькосмуг. 100 кГц	вузькосмуг. 200 кГц	вузькосмуг. 12,5 кГц
Час автономної роботи	>10 років	до 20 років	до 10 років	3-5 років
Частота	868,8 МГц (Європа) 915 МГц (США) 433 МГц (Азія)	868,8 МГц (Європа) 915 МГц (США)	800/900/1800 МГц	169/433/470/780/868/915 МГц
Безпека	AES-64/128	AES з HMACs	AES-256	AES-128/256
Дальність	до 2,5 км у місті до 45 км за містом	до 10 км у місті до 50 км за містом	до 2 км	до 2 км у місті

Інші атрибути бездротового Weigthless-P включають підтримку динамічних змін швидкості передачі даних, що забезпечує оптимальну продуктивність мережі та збільшує термін служби батареї в кінцевих пристроях, базова станція регулює швидкість передачі даних на основі близькості кожного пристрою до станції. Чим ближче кінцеві точки до базової станції, тим вища швидкість передачі даних, що призводить до меншого часу передачі та меншої вихідної потужності. І навпаки, вузли, які знаходяться далі від базової станції, використовують найнижчу швидкість передачі даних і найвищу вихідну потужність.

2.2 Технології та протоколи ближнього зв'язку в IoT мережах

Z-Wave — це бездротова технологія пеердачі інформації малої потужності [15]. Z-Wave працює на частотах до 1 ГГц і в основному призначений для передачі простих команд, наприклад, зміна гучності телевізора, вимикання або ввімкнення приладів, зміна яскравості екрана тощо.

Вибір частот був невипадковим. Щоб мінімізувати кількість перешкод від інших уже популярних технологій, наприклад, Wi-Fi який в основному використовується на частоті 2,4 ГГц або 5 ГГц.

Протокол Z-Wave дозволяє реалізувати цілковити контроль над безпекою та енергоспоживанням будинку з мінімальними труднощами [16]. За допомогою технології Z-Wave може функціонувати повнофункціональна система домашньої автоматизації, яка дозволяє програмувати більшість компонентів будинку, включаючи освітлення, опалення, приготування їжі, кондиціонування та навіть безпеку. За своєю суттю та структурою Z-Wave доволі складна система, але вона проста у використанні та економить час, а також енергоефективна.

Технологія NFC (Near Field Communication) розроблена такими компаніями, як Sony і NXP Semiconductors. Вона поєднує в собі комбінацію бездротового зв'язку та радіочастотної ідентифікації [17].

Технологія NFC призначена для передачі різних типів інформації, включаючи зображення, музичні файли, номери телефонів або цифрові ключі для авторизації, між двома обладнаними NFC пристроями, розташованими поруч один з одним. Це може бути кредитна картка, будь-яка портативна технологія або пристрої зчитування RFID. Ця технологія може бути використана як засіб отримання доступу до даних або послуг (електричний ключ або безготівковий платіж).

На відміну від інших безконтактних комунікаційних технологій, NFC може передавати інформацію між двома активними пристроями.

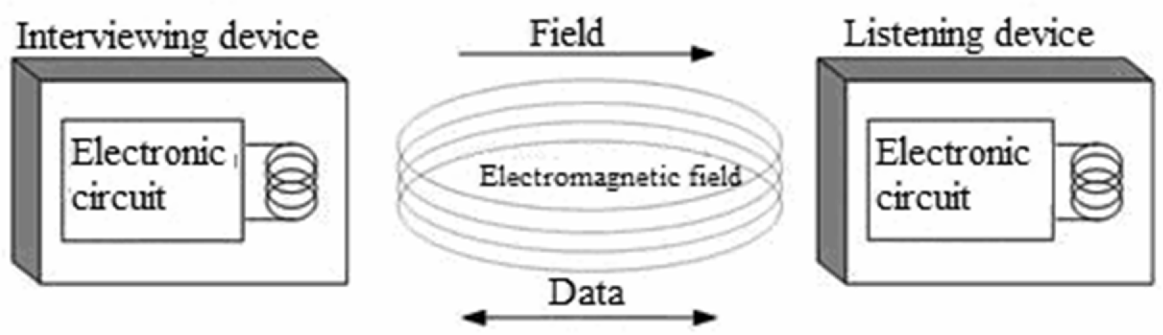

Рисунок 2.7 – Схема роботи NFC пристроїв

При передачі інформації з активного пристрою на пасивний використовується метод ASK. При взаємозв’язку двох пристроїв одного типу слід врахувати, що кожен пристрій має власне джерело живлення, тому сигнал від оператора відразу вимикається після передачі.

RFID (радіочастотна ідентифікація) — це форма автоматичної ідентифікації об’єктів, яка передбачає використання радіочастот для зчитування даних, що зберігаються в транспондерах або RFID-мітках, і подальшого запису інформації [19].

Будь-яка система RFID містить зчитувач, який зчитує інформацію, і транспондер, який також називають RFID-міткою або ідентифікатором.

Більшість систем RFID містять два компоненти. Перший — це складна інтегральна схема, яка обробляє та зберігає інформацію, декодує та модифікує радіочастотний сигнал та виконує інші функції. Другий – це антена, яка приймає і передає сигнали. Крім того, необхідно використовувати програмне забезпечення, яке використовується для аналізу та збирання інформації, зібраної з тегів RFID.

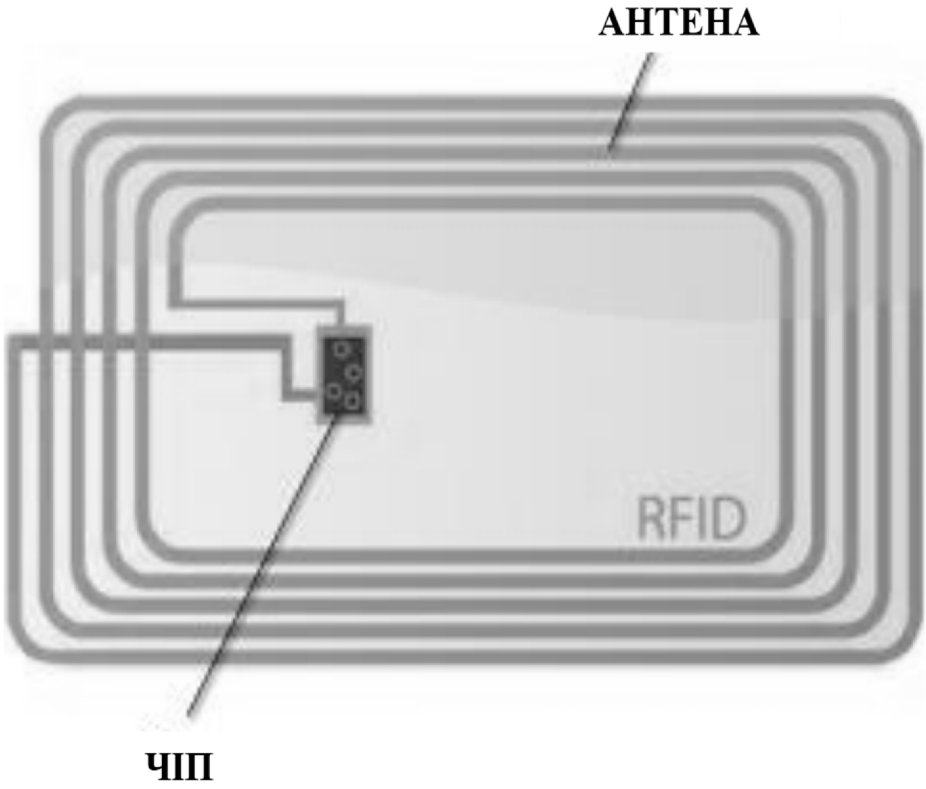

Рисунок 2.8 - Будова RFID-мітки

RFID можна використовувати для управління запасами або відстеження часу спортивної діяльності. Магнітні мітки не беруть на себе роль кодів, але вони мають можливість дистанційного зчитування. Велику рогату худобу можна позначити бірками, в які буде записана інформація про проходження ветеринарного огляду. Транспортні рішення полегшують ідентифікацію автомобілів, навіть коли вони рухаються на високих швидкостях. Деякі

авіакомпанії використовують мітки, щоб ефективно стежити за великими обсягами вантажу. RFID також включено в біометричні паспорти, кредитні картки, які полегшують доступ до зон обмеженого доступу з безпечними засобами ідентифікації.

Бездротова технологія Bluetooth Low Energy (BLE) є невід'ємною частиною стандарту Bluetooth, яказ'явилась починаючи з четвертого покоління Bluetooth і зараз присутня в усіх подальших модифікаціях. Пристрої Bluetooth, які використовують BLE, споживають менше енергії, ніж ті, що використовують інші версії Bluetooth, які були випущені раніше. Багато сучасних IoT пристроїв можуть працювати понад рік від однієї невеличкої батареї, без заміни або перезаряджання. Це полегшує використання невеликих датчиків, які будуть стабільно функціонувати та взаємодіяти з іншими пристроями (рис. 2.9).

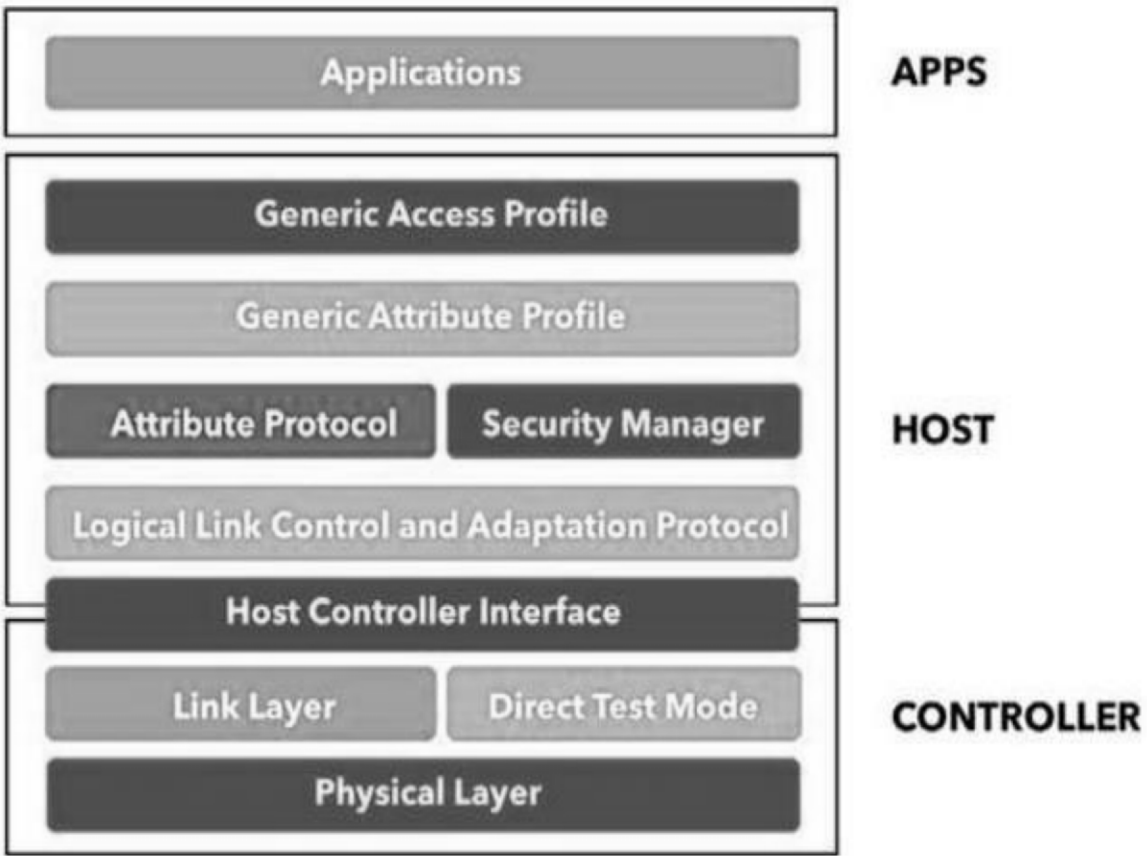

Рисунок 2.9 – Архітектура рівнів BLE

Інтегральними рівнями BLE є:

– функціональність програми корисна для кінцевого користувача;

– основний пристрій, або хост, відповідає за верхні рівні протоколу Bluetooth;

– контролери – відповідають за нижні рівні стека протоколів Bluetooth;

– рівень додатків – найвищий рівень стеку протоколів.

Рівень хосту містить такі підрівні:

– GAP (Generic Access Profile) – профіль загального доступу;

– GATT (Generic Attribute Profile) – профіль загальних атрибуті;

– ATT (Attribute Protocol) – протокол атрибутів;

– SM (Security Manager) – менеджер безпеки;

– L2CAP (Logical Link Control and Adaptation Protocol) – протокол логічного з'єднання та адаптації;

– HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні хосту.

Рівень управління підключається через протокол HCI і має всього три рівні:

– HCI (Host Controller Interface) – інтерфейс хост-контролеру, на стороні контролеру;

– LL (Link Layer) – канальний рівень;

– PHY – фізичний рівень.

BLE призначений для тих пристроїв, які мають невеликі розміри, тобто для пристроїв, у яких важлива компактність і куди не можна встановити повноцінний акумулятор, або батарею великого об'єму. Bluetooth LE споживає в 10-20 разів менше енергії, ніж класичні рішення Bluetooth, і здатний передавати дані в 50 разів швидше і на відстань понад 100 метрів.

Окрім вищезгаданих переваг, BLE має високий рівень безпеки, надійності, малої затримки підключення та низького енергоспоживання. Ще

одним суттєвим аспектом цього стандарту є можливість перенастроювання частоти роботи, тобто є захист від помилок під час передачі сигналів, BLE швидко змінює частоту своєї роботи, вибираючи найбільш ефективну частоту для усунення перешкод, переповнень. і зменшити перешкоди.

Протокол Bluetooth 5.0 був задуманий як засіб зв'язку з Інтернетом речей. Це продемонструвало, що стандарт призначений для захоплення нового ринку пристроїв. В порівнянні з попередньою версією 4.0 була підвищена швидкість передачі даних майже до швидкостей HSPA і LTE ранніх версій, при цьому енергоспоживання залишилося в колишніх межах. На даний момент ця специфікація є мало поширеною. Проте Bluetooth 5 як і всі попередні версії має зворотну сумісність. Цілком можливо, через декілька років кожний мобільний пристрій буде підтримувати 5 версію цього стандарту, що є найважливішою перевагою цієї технології над іншими.

Wi-Fi HaLow — це протокол бездротової мережі, реалізований у 2017 році, як доповнення до стандарту бездротової мережі IEEE_802.11 (рис. 2.10) [18].

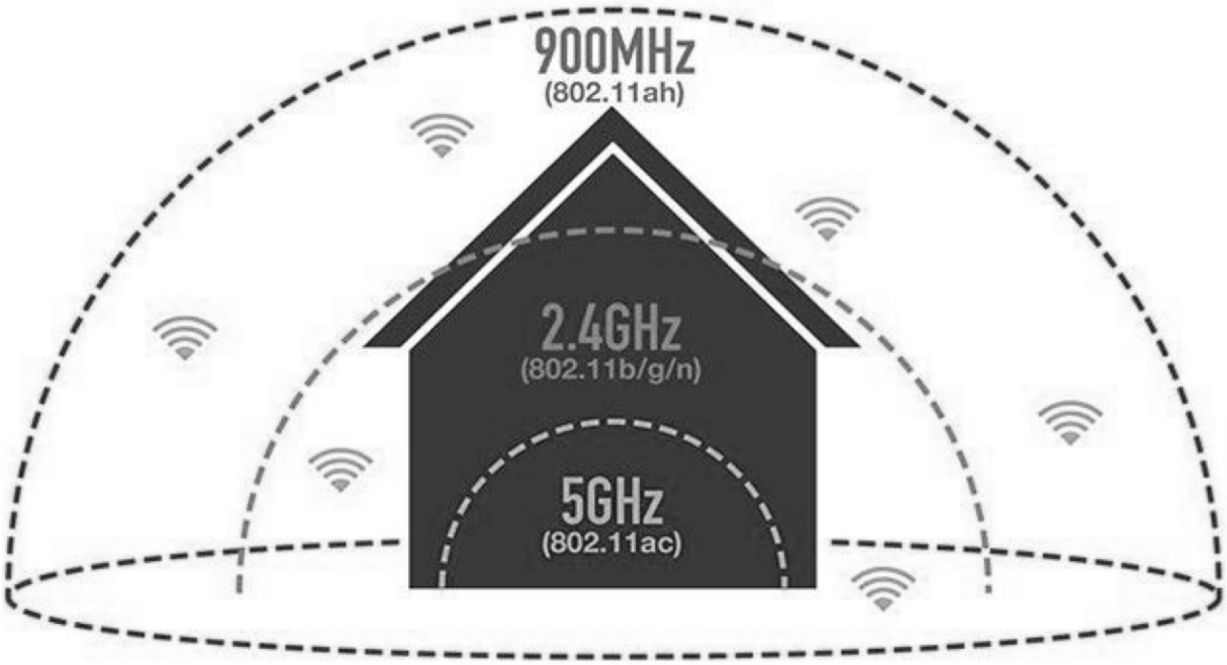

Рисунок 2.10 – Зона покриття різних Wi-Fi протоколів

Цей протокол працює на відкритій частоті 900 МГц, для забезпечення розширеного діапазону мереж, порівняно зі звичайними мережами Wi-Fi, працюючими в діапазонах 2,4 ГГц і 5 ГГц. Його низьке енергоспоживання також є корисним, це дозволяє створювати великі кластери станцій або датчиків, які взаємодіють один з одним відповідно до концепції Інтернету речей (IoT). Протокол має низьке споживання енергії, співмірне з протоколом, Bluetooth LE, але має додаткові переваги у вигляді вищих швидкостей передачі даних і більшого діапазону покриття.

Порівняльна характеристика технологій та протоколів передачі даних на короткі відстані в IoT наведена в (табл. 2.2).

Таблиця 2.2 – Порівняння основних технічних характеристик мереж малого радіусу дії

Параметри	**RFID**	**NFC**	**BLE**	**Z-Wave**	**Wi-Fi HaLow**
Смуга частот	6/13.5/433/863-870/902-928 МГц 2.4/5-27 ГГц	13,56 МГц	2,4 ГГц	868/915 МГц	Піддіапазон 1 ГГц
Швидкість передачі даних	500 кбіт/с	106/212/424/848 кбіт/с	1 Мбіт/с	9.6,40 та 100 кбіт/с	До 4 Мбіт/с
Радіус дії	0.1-5 м	0.1 м	70 м	100 м	100-1000 м
Пропускна здатність на канал		Змінна	40 каналів по 2 МГц		
Модуляція	-	ASK, BRSK	GFSK	FSK/GFSK	BRSK, QPSK, 16-/64-/256-QAM
Топологія	Point to Point Point to Multipoint	Peer-to-Peer	Single-hop	Mesh	Star
Безпека	Шифрування	Шифрування	AES-128	AES-128	WPA

Інші пристрої з можливостями HaLow також працюватимуть у діапазонах 2,4 і 5 ГГц, що полегшить інтеграцію в екосистему, яка наразі налічує 7 мільярдів пристроїв. Крім того, Wi-Fi HaLow матиме можливість підключатися до IP-адрес, це полегшить взаємодію з хмарами, що має вирішальне значення для IoT. Це також дозволить підключити до точки доступу близько 1000 пристроїв.

2.3 Протоколи передачі повідомлень в мережах IoT

Обсяг інформації, що генерується одним сенсорним вузлом, скромний, але більшість служб Інтернету речей побудовані навколо обробки інформації з кількох вузлів. Це принципово відрізняється від підходів, що використовуються в традиційних комунікаційних мережах, наприклад, спосіб доступу до інформації абонентів або передачі даних клієнтам [15].

В результаті ми маємо новий дизайн системи, що складатиметься з кількох джерел і кількох приймачів, а також обсяг трафіку, який генерує один датчик, може бути як малим, так і великим. Загальні протоколи для надсилання повідомлень, які не призначені для цієї мети, не підходять.

Базова топологія, яка використовується для передачі повідомлень в IoT, представлена на рисунку 2.11. До неї входить шаблон проектування для передачі повідомлень, який також відомий як «видавець-передплатник» (Publisher-Subscriber, або pub/sub). У цю концепцію закладено ідею розподілу ролей видавця, який є джерелом інформації, і передплатника, який є одержувачем інформації. Термін підписки пов'язаний з певною процедурою, що виконується учасниками, метою якої є отримання інформації від конкретного видавця, а також організація зберігання інформації – частота отримання та інші подібні (залежно від реалізації) показники.

У такому випадку розглядається ситуація, коли вузол датчика (Node) агрегує інформацію від кількох датчиків (наприклад, дані про вологість повітря), а потім надсилає її на вимогу або через визначений період часу. Як правило, датчики досить прості, їх завдання зводяться до постійної передачі інформації щодо параметрів, які контролюються. У результаті потрібно використовувати комбінацію датчиків і мікроконтролерів, щоб зчитувати виміряні дані та передавати їх на сервер заздалегідь визначеним способом. Крім того, більша частина взаємодії клієнта з системою здійснюється через клієнтську програму (додаток), яка встановлена на персональному комп'ютері, ця програма необхідна для візуального представлення інформації, отриманої від датчиків або вже обробленої сервером і системою. Ця конструкція також передбачає наявність брокера. Брокер – це сервер, який отримує інформацію від видавців і передає її підписаним користувачам.

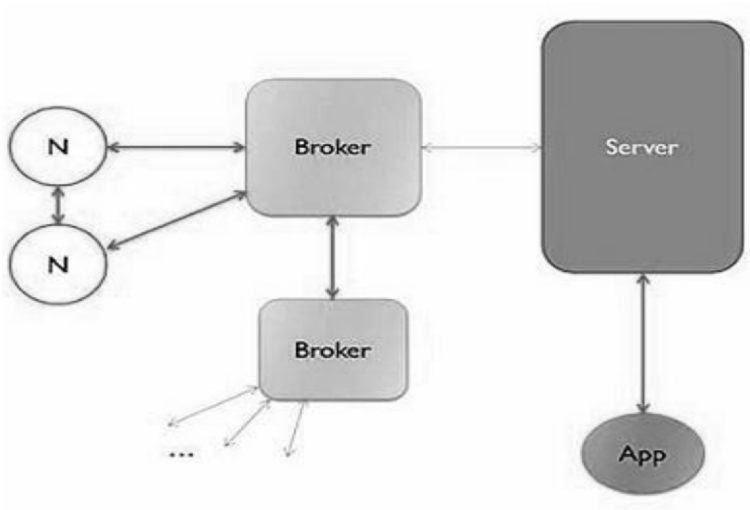

Рисунок 2.11 – Топологія системи передачі даних між вузлами мережі IoT

У складних системах він також може виконувати різні завдання, пов'язані з аналізом і обробкою даних, отриманих сервером. Брокер може зосередитися на підключеннях і створити списки очікування для доставки повідомлень. Це полегшує роль брокера в організації передачі повідомлень, їх зберігані та відборі. Черга повідомлень — це контейнер для повідомлень, які

очікують на передачу. Якщо канал зв'язку обмежений або одержувач не може вчасно отримати повідомлення, черга збереже повідомлення та поверне його відправнику.

DDS (служба розповсюдження даних) — це протокол, який базується на додатках і забезпечує зв'язок у реальному часі. Основа моделі видавець-передплатник. Основною метою протоколу є підключення пристроїв до інших пристроїв через шину обміну повідомленнями (рис. 2.12). Протокол DDS успішно забезпечує ефективну доставку повідомлень і синхронізацію.

Пристрої IoT запитують дані іншим способом, ніж комп'ютери та телефони. Пристрої мають швидкий розгін, масштаб реального часу зазвичай виражається в мікросекундах. Пристроям потрібно спілкуватися з іншими пристроями через складні шляхи, тому простий і надійний двосторонній обмін даними TCP не може працювати з цими пристроями. Натомість DDS сприяє детальному управлінню якістю обслуговування (QoS), груповій розсилці, надійності з можливістю реконфігурації та комплексному резервуванню. Крім того, сегментація даних є сильним компонентом DDS. Протокол DDS пропонує потужні методи фільтрації даних і вибору за призначенням, а кількість синергетичних одержувачів даних можна оцінити в тисячі. Деякі пристрої є відносно невеликими, тому існують полегшені варіанти протоколу DDS, які успішно працюють в обмеженому просторі.

З цієї причини зіркоподібна мережа, яка використовує дані пристрою, зовсім не підходить. Натомість DDS використовує прямий зв'язок між пристроями на основі реляційної моделі даних. Її називають шиною даних (DataBus), оскільки вона нагадує мережу бази даних (рис. 2.12).

Подібним чином база даних відповідає за керування доступом до збереженої інформації, тоді як шина даних відповідає за керування доступом до інформації та її оновлення кількома користувачами паралельно. Це точний склад високопродуктивних пристроїв, які необхідно об'єднати в єдину систему.

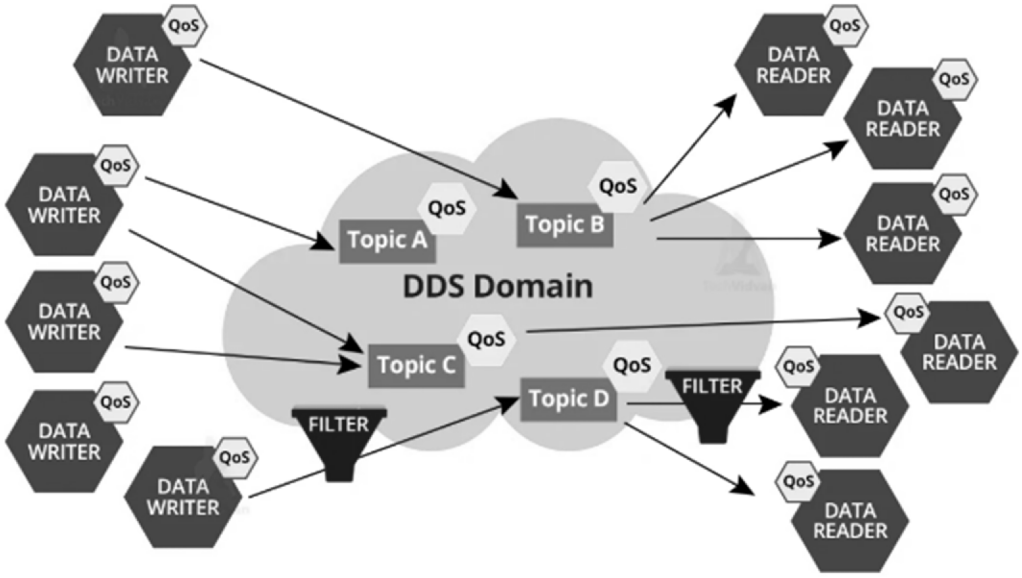

Рисунок 2.12 – Принцип роботи протоколу DDS в мережах IoT

Високопродуктивні системи, які містять інтегровані пристрої, використовують протокол DDS. Ця технологія забезпечує гнучкість, надійність і швидкість, необхідні для створення складних програм у реальному часі. Ці системи використовуються у військовій сфері, вітроенергетиці, інтегрованій охороні здоров'я, діагностиці зображень, відстеженні ресурсів, випробуваннях і безпеці автомобілів.

XMPP (eXtensible Messaging and Presence Protocol) — це загальнодоступний протокол, заснований на XML, який надає засоби передачі інформації про присутність і обмін повідомленнями в режимі реального часу. Спочатку призначений для легкого розширення базової версії, тепер протокол підтримує передачу голосу, відео та файлів через мережу, а також текстових повідомлень.

Протокол XMPP заснований на текстовому форматі для XML, цей протокол забезпечує природне спілкування між окремими особами. Протокол базується на TCP або HTTP на TCP. Його перевагою є метод вирішення проблем Jabber ID, який використовує такі компоненти: вузол, домен і ресурс. Останні два компоненти є необов'язковими. Адреса схожа на_username@gmail.com, що полегшує асоціацію користувачів із величезним

простором Інтернету. XMPP підтримує різні моделі зв'язку (запит-відповідь, публікація, підписка та інші) [15].

XMPP забезпечує простий метод адресації машин. Це особливо корисно для даних, які передаються між віддаленими, часто незалежними джерелами, прикладом цього є спілкування між двома абонентами. Цей протокол має низьку швидкість. На практиці більшість реалізацій цього протоколу використовують метод опитування або перевірки доповнень лише за необхідності.

Переваги цього протоколу також включають його безпеку, масштабованість, і він підходить для невеликих мереж Інтернету речей.

CoAP (Constrained Application Protocol) — це протокол, який спеціалізується на робочій групі IETF-CORE, цей протокол призначений для використання в мережах і пристроях, які мають обмежену кількість ресурсів [15]. CoAP вважається доповненням до HTTP, але на відміну від HTTP, він призначений для використання в пристроях, які мають певні обмеження. CoAP використовує протокол UDP для транспортування.

Повідомлення протоколу обмежені, більшість з них є запитами інформації, включаючи GET, PUT і POST. Крім того, використовуються правила DELETE і CONNECT. Клієнти (кінцеві користувачі) використовують повідомлення як для керування, так і для спостереження за ресурсом. Прапор, який сигналізує про спостереження, встановлюється на запит, і сервер продовжуватиме відповідати на початкове повідомлення після його відправлення. Це полегшує серверам спостереження за станом датчиків.

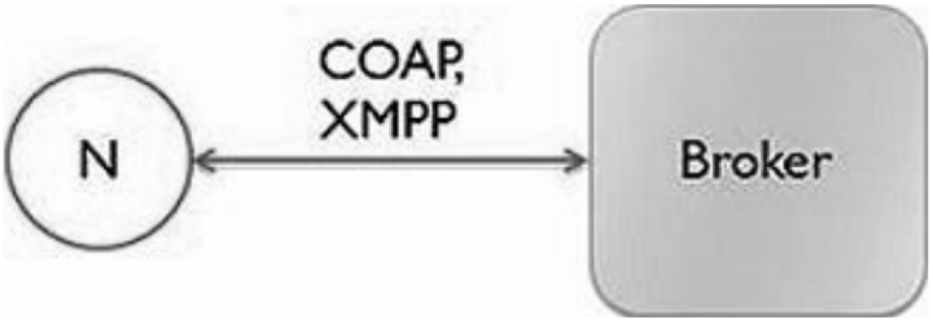

Рисунок 2.13 – Сегмент мережі CoAP та XMPP

Як наслідок, у мережевій частині системи між вузлом датчика та посередником зазвичай використовуються два протоколи: XMPP і CoAP. Ці протоколи використовуються для забезпечення зв'язку між вузлом датчика та брокером, з метою налаштування та передачі інформації між вузлами, а також для реєстрації системи. Фактична процедура протоколу залежить від умов у мережі. Очевидно, що XMPP використовується в системах освітлення та клімату, а також у адресації пристроїв у невеликих персональних мережах. CoAP призначений для використання з пристроями з обмеженими ресурсами та мережами малої потужності. Задокументовано використання протоколу в системах вимірювання температури та інших електронних пристроях.

MQTT (Message Queue Telemetry Transport) – це легкий, компактний і відкритий протокол для передачі даних, створений для ситуацій, коли потрібна невелика кількість коду, а пропускна здатність каналу обмежена [19]. Ці вимоги полегшують його використання в системах M2M (machine-to-machine).

Також існує версія протоколу MQTT-SN (MQTT для сенсорних мереж), раніше відома як MQTT-S, яка призначена для бездротових пристроїв, які не підтримують мережі TCP/IP.

Рисунок 2.15 ілюструє типовий формат повідомлень проколу MQTT загалом. Повідомлення складається з двох окремих заголовків:

– MQTT Fixed Header – заголовок фіксованої довжини;

– Variable Length Header – заголовок змінної довжини (в залежності від типу повідомлення);

– Variable Length Message Payload – поля корисного навантаження змінної довжини.

До заголовка фіксованої довжини входять такі поля:

– Message Type – тип повідомлення;

– DUP – прапор дублювання повідомлення;

– QoS Level – якість надання послуг;

– Retain – спеціальний прапор, який дозволить зберегти останнє повідомлення, отримане брокером;

– Remaining Length – залишкова довжина.

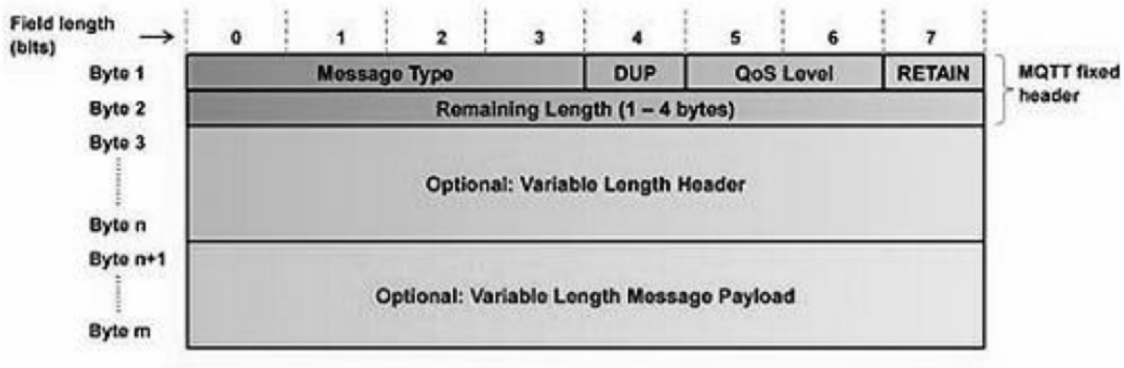

Рисунок 2.15 – Базовий формат повідомлень у протоколі MQTT

Спрощений процес роботи протоколу MQTT передбачає наступні етапи: видавець передає повідомлення з певними даними (наприклад, інформація з датчиків вологості) до брокера, вказуючи при цьому тему (Topic), до якої ці дані відносяться (наприклад, «вологість»). Брокер аналізує, які із підписників мають підписку на певні теми, в даному випадку – на тему «вологість». Підписники, які цікавляться темою «рівень вологості», отримають повідомлення від брокера, що містить інформацію про рівень вологості.

Як наслідок, підписники можуть бути зацікавлені різними темами і, залежно від їх підписки, вони можуть отримувати необхідну інформацію без безпосереднього спілкування з видавцем. На рисунку 2.15 зображена схема передачі інформації за принципом «видавець-підписник».

STOMP — це простий протокол, який передбачає комунікації з кількома мовами, платформами та брокерами. Він також здатний виконувати регулярні оновлення. Цей протокол підходить для стилю «видавець-передплатник» і за допомогою SEND (відправити), SUBSCRIBE (підписатися), UNSUBSCRIBE (відписатися), BEGIN (почати), ABORT (перервати), ACK (підтвердити), NACK (не підтвердити), DISCONNECT (відключити) спілкується з брокером через режим «запит-відповідь».

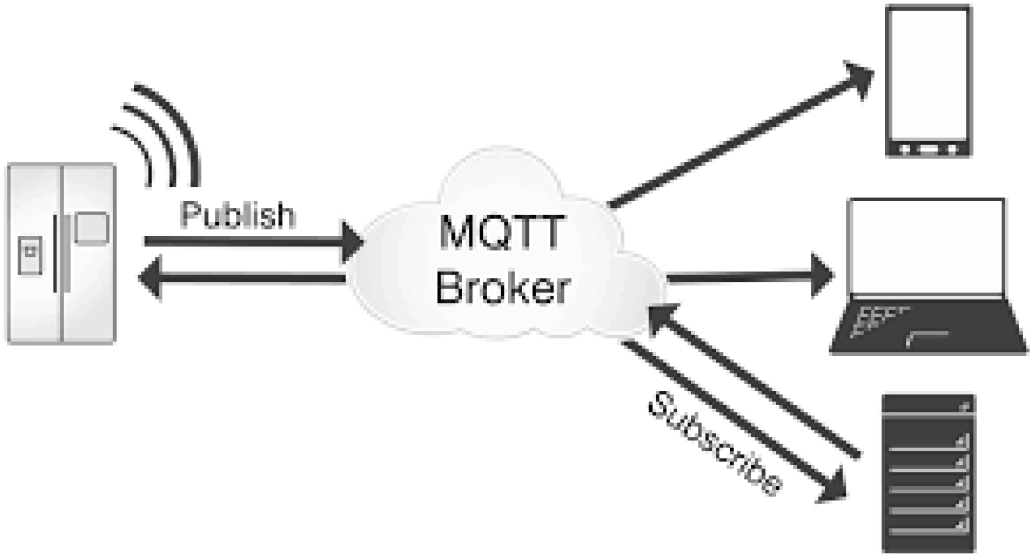

Рисунок 2.16 – Принципова схема роботи MQTT протоколу

Цей протокол використовується в ситуаціях, коли необхідно забезпечити просту передачу повідомлень у мережах, які мають обладнання різних платформ.

Протокол подібний до HTTP, використовує протокол TCP, є простим протоколом, який дозволяє клієнтам STOMP спілкуватися з будь-яким брокером повідомлень, який підтримує цей протокол. Як наслідок, цей метод спілкування призначений для обміну повідомленнями між платформою, розробленою на одній мові програмування, та клієнтом, який розробляє своє програмне забезпечення на іншій. Надає велику кількість бібліотек, сумісних одна з одною (рис. 2.17).

Важливо визнати, що для забезпечення функціонування брокера в мережі Інтернет речей можуть використовуватися обидва протоколи: MQTT і STOMP. Тільки протокол STOMP призначений для взаємодії між брокером і сервером, тоді як протокол MQTT забезпечує повний зв'язок, включаючи як взаємодію брокера з вузлами датчиків, так і взаємодію брокера з сервером.

SOAP (Simple Object Access Protocol) — це протокол, який полегшує обмін структурованими та складними XML-даними в розподіленому обчислювальному середовищі. SOAP використовує базову модель зв'язку, яка

гарантує послідовну передачу повідомлення від відправника до одержувача, це може включати додаткову обробку або розширення повідомлення (рис. 2.18).

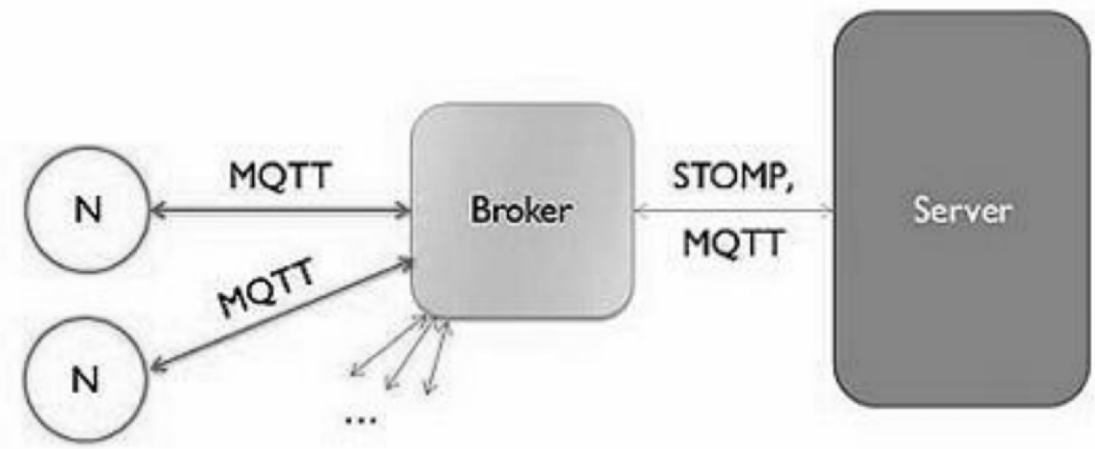

Рисунок 2.17 – Сегмент мережі MQTT та STOMP

SOAP підтримує два режими доступу - SOAP MESSAGE і SOAP RPC.

Режим SOAP MESSAGE використовує об’єкт Message для передачі та обробки повідомлень SOAP. Може використовуватися для зв’язку, який є асинхронним і передбачає негайну або відкладену відповідь.

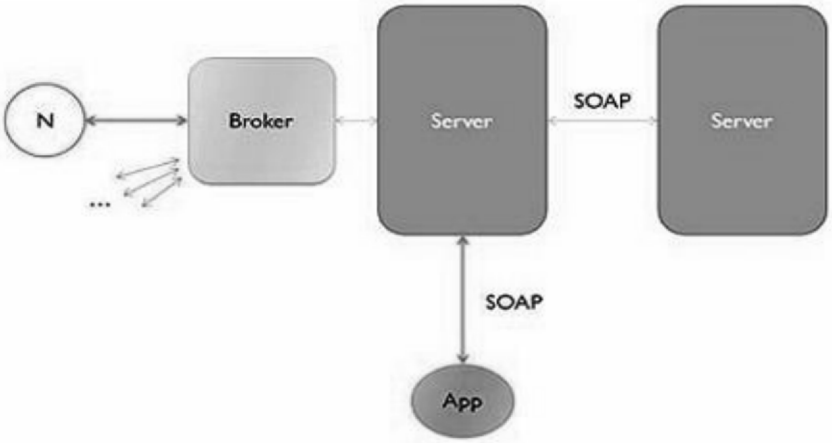

Рисунок 2.18 – Сегмент мережі протоколу SOAP

У режимі SOAP RPC реалізовано передачу запитів та відповіді на виклики. Цей об’єкт призначений для віддаленого виклику процедури та є

синхронним щодо XML. Доступні повідомлення (GET, SOAP_ACTION-REPONSE та SOAP_ACTION) полегшують процес формування запитів та відповідей, тому цей протокол підходить для використання з будь-яким рівнем протоколу, який включає запити: FTP, HTTPS та SMTP.

Порівняльна характеристика протоків передачі повідомлень наведена у табл. 2.3.

Таблиця 2.3 – Порівняльна характеристика розглянутих методів

Протокол	**Транс.**	**Призначення**	**Особливості**
DDS	UDP	Для мереж, що потребують розподіленого навантаження	Реалізує прямий зв'язок між пристроями на базі реляційної моделі
XMPP	TCP	Для адресації в невеликій персональній мережі	Для ідентифікації користувачів використовуються ЛД, по формату схожі на адреса електронної пошти
COAP	UDP	Для мереж з обмеженими ресурсами, низьким електроспоживанням	Враховує різні питання середовища реалізації в обмежених мережах
MQTT	TCP	Для завантажених мереж з великою кількістю пристроїв та брокером	Використання механізму черг повідомлень
STOMP	TCP	Для мереж, в яких є декількох комбінацій різних протоколів, що потребують простий протокол передачі повідомлень через брокера.	Взаємодія з більшістю мов, платформ та брокерами
SOAP	TCP	Для розподіленої обчислювальної мережі	Підтримує два механізми доступу: SOAP RPC та SOAP Message

Окремо здійснено порівняльний аналіз операцій, які підтримують проаналізовані протоколи (табл. 2.4). Визначено спільні можливості протоколів та підкреслено їх унікальні характеристики.

Таблиця 2.4 – Операції, що виконуються за проаналізованими протоколами

Протокол	Операції	Відмінні операції
DDS	Процедури отримання та відправки даних	Реалізує прямий шинний зв'язок. «Зберігання історії» - наявність кешу. Підтримка механізму контролю «життєдіяльності» (Keep-alive та Lifecycle)
XMPP	Процедури запиту інформації/вимог, отримання даних,встановлення нових значень, або заміщення існуючої величини	XML-потоки та XML-строфи забезпечують швидкий асинхронний обмін. Схема адресації JID-набір елементів, що утворюють доменний ідентифікатор вузла та ресурсу
COAP	Процедури запису та отримання необхідних конкретних параметрів	Представляє собою двійкову версію протоколу HTTP, спрощену під задачі транспортування даних по лініям з обмеженою пропускною здатністю
MQTT	Процедури обробки публікацій/підписки	Підтримує різні класи якості обслуговування QoS(1-3) Підтримує механізми черг
STOMP	Процедури публікацій/підписки. Операції з транзакціями	Підтримує операції з транзакціями. Підтримка великої кількості спільних бібліотек.
SOAP	Віддалений виклик методів. Процедури запитів параметрів	Можливість віддаленого виклику методів/функцій за допомогою механізму доступу SOAP RPC. Нейтральний до платформи

РОЗДІЛ 3
ІНТЕГРАЦІЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН У СИСТЕМУ IoT

3.1 Аналіз концепції захисту систем IoT за допомогою блокчейну

У якості додаткового прийому підвищення безпекти та ефективності експлуатації мереж IoT запропоновано інтегрувати у таку мережу елементи технології блокчейн. Розглянемо детально ефективність використання моделі IoT із реалізацією блокчейну. Звичайна архітектура IoT має чотири рівні. Технології блокчейн слід інтегрувати у цю архітектуру як окремий компонент, який існує між мережевим і прикладним рівнями.

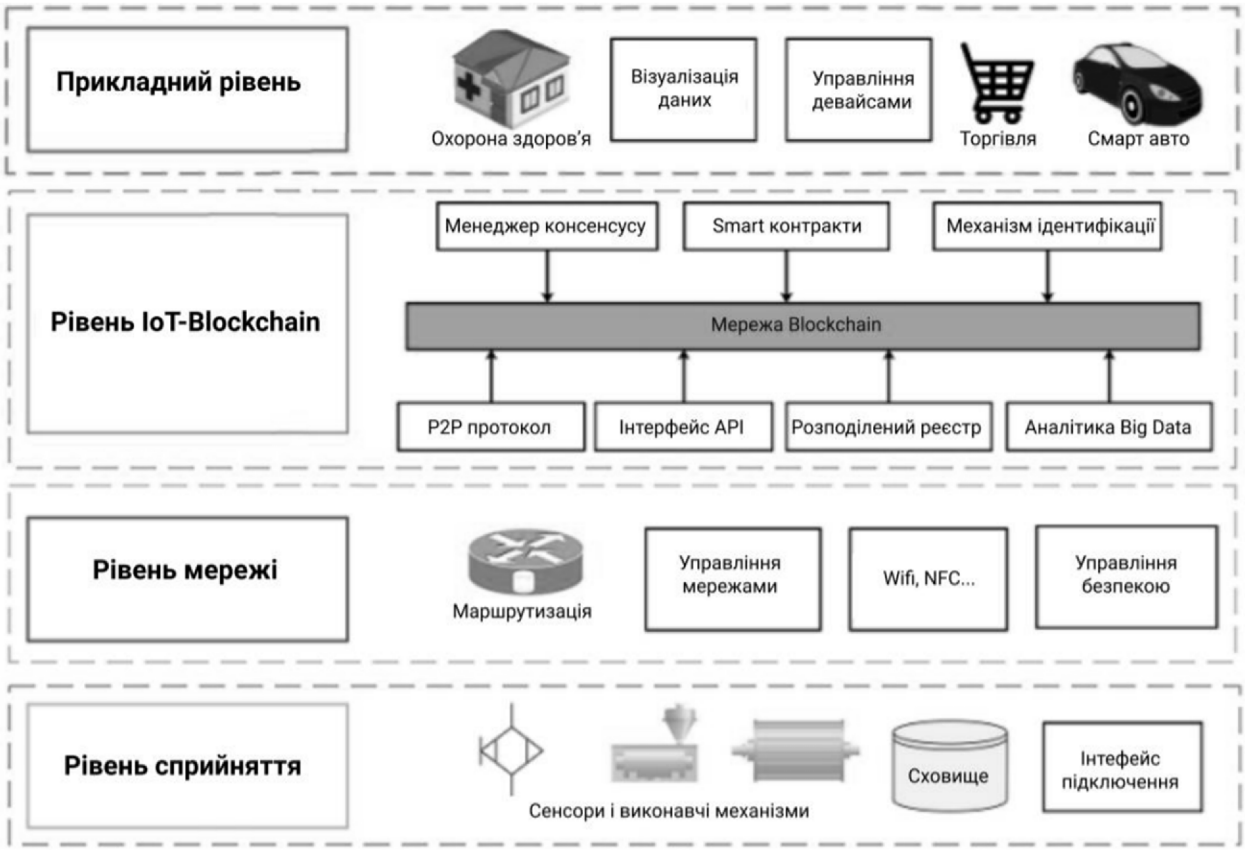

Рисунок 3.1 – Багаторівнева модель IoT з використанням Blockchain

Перший рівень – це рівень сприйняття, який містить речі та об’єкти, які використовуються для сприйняття навколишнього середовища та отримання відповідних даних, які можна використовувати для розуміння навколишнього середовища. Далі йде мережевий рівень, який забезпечує функціонування мережі та маршрутизацію, дозволяє всім об’єктам Інтернету речей підключатися та спілкуватися через Інтернет. Цей рівень включає в себе мережеві компоненти та компоненти безпеки, які полегшують зв’язок і нагляд за безпекою.

Додатковий рівень містить усі модулі, які полегшують різноманітні функції блокчейну в системі IoT. Ці можливості включають зв’язок P2P, розумні контракти, API, аналіз великих даних, формування консенсусу та перевірку особи. Протоколи P2P мають вирішальне значення для забезпечення децентралізованого зв’язку між різними об’єктами IoT. Однією з найважливіших функцій яку кожен пристрій IoT повинен мати є розподілений реєстр. Дублікат такого реєстру може оновлюватись протягом кількох хвилин або секунд у мережі IoT. Однак сам тип реєстру значно відрізнятиметься залежно від сценарію та кількості вузлів у мережі IoT.

Модуль аналізу великих даних дозволяє блокчейну реалізувати ефективне онлайн-зберігання та обробку даних, оскільки система IoT створює великі обсяги даних, які неможливо обробити традиційними методами. Багато транзакцій реєструються в структурованих формах розподіленого реєстру, що вимагає додаткового аналізу даних. Смарт-контракти також вважаються однією з найважливіших частин технології блокчейн, ця технологія використовується для рішень, які автоматизовані на основі заздалегідь визначених умов.

Як правило, смарт-контракт — це фрагмент програмного коду, який виконується в блокчейні для виконання певного завдання, коли виконується або перевіряється певна умова. Також важливим в інтеграції блокчейну з Інтернетом речей є управління консенсусом. Його функція полягає в тому, щоб служити центральним, який підтримує зв'язок між вузлами в мережі.

Управління ідентифікацією використовується для регулювання та диференціації різних частин мережі IoT. Крім того, API полегшує доступ служб на основі блокчейну до програм IoT. Рівень додатків — це верхній рівень, який містить різноманітні додатки, пов'язані з IoT, і забезпечує візуалізацію даних, що створює численні цифрові сервіси та сприяє прийняттю точних і обґрунтованих рішень на основі даних, зібраних із фізичних пристроїв, пов'язаних з IoT.

Традиційні методи забезпечення цілісності даних зазвичай використовують методи шифрування для збереження даних у хмарі, ці методи залежать від довірених третіх сторін (TPA). Схеми перевірки автентичності даних на основі блокчейну можуть успішно обійти проблему довірених сторін, але тоді доведеться боротись з проблемою високих витрат на обчислення та зв'язок. Запропоновано використати схему цілісності даних (BB-DIS) для вирішення згаданих вище проблем на основі блокчейну та білінійного відображення для великих обсягів даних, пов'язаних з IoT. У BB-DIS дані IoT поділяються на фрагменти, а гомоморфні теги (HVT) створюються з метою перевірки. Точність даних може бути досягнута за допомогою властивостей лінійного відображення у формі транзакцій блокчейну.

3.2 Побудова математичної моделі децентралізованих транзакцій

Запропонована модель є децентралізованою, щоб вирішити проблему єдиної точки довіри в традиційній моделі аудиту даних колективної довіри. Протокол полегшує відстеження історії зміни даних. Як наслідок, більшість існуючих методів перевірки цілісності даних, які використовують технологію блокчейн, стосуються питання довіри, а не обсягу даних. Ще одна важлива проблема полягає в тому, що дані, які зберігаються в хмарі, повинні бути актуальними, щоб задовольняти найновіші вимоги різних програм. Як

наслідок, рішення на основі блокчейну повинне мати динамічний характер, необхідний для оновлення інформації, щоб забезпечити цілісність даних.

Технологія Blockchain дозволяє здійснювати децентралізовані транзакції між одноранговими вузлами, а також взаємодіяти окремим вузлам системи без необхідності створення вузла довіри. Це досягається за допомогою шифрування даних, міток часу та розподіленого консенсусу. Такий підхід може вирішити проблему високої вартості, неефективності та інформаційних загроз централізованого зберігання даних IoT. Перелік структурних елементів моделі наведено у табл. 3.1.

Таблиця 3.1 – Структурні елементи моделі

Позначення	**Пояснення**
IVSC	Смарт-контракт для перевірки доброчесності
CRSC	Виклик отримання смарт-контракту
HSSC	Смарт-контракт на зберігання HVT
CSP	Провайдер хмарних послу
DCD	Прилад – користувач даних
DOD	Прилад – власник даних

Структура моделі в основному складається з чотирьох різних сутностей: розумних контрактів, власників даних (DOD), споживачів даних (DCD) і постачальників хмарних послуг (CSP). Для досягнення різних цілей використовуються три типи смарт-контрактів: HSSC, CRSC і IVSC. Усі ці об’єкти можуть функціонувати як частина мережі блокчейн. На практиці перевірки цілісності даних включають кілька учасників: власників даних і споживачів. Перевірка цілісності здійснюється за допомогою смарт-контрактів у системі блокчейн. Користувачі з етичними проблемами можуть використовувати клієнти блокчейну на своїх особистих пристроях або

залишити мережу. Крім того, CSP функціонує як частина мережі блокчейн, що забезпечує децентралізацію та ефективність перевірки цілісності.

Пара DOD і DCD повинна бути додана до мережі блокчейну під час початкового налаштування системи блокчейну для генерації пари ключів. Особа, яка володіє даними, повинна заплатити за зв'язок зі смарт-контрактом і сервісом хмарного зберігання. CSP може функціонувати як вузол майнера в мережі блокчейн, він має право надавати послуги через майнінг і отримувати винагороду. Споживач даних вимагає, щоб дані зберігалися на хмарному сервері, він також оплачує витрати на зберігання. У цьому контексті CSP сприяє загальній службі зберігання даних для власників даних, тоді як нехмарні дані можуть передаватись через однорангову мережу між вузлами мережі.

Процес перевірки показано на рис. 3.2. Протокол перевірки складається з трьох окремих фаз: перша фаза – етап кроку, друга фаза – етап виклику, а третя фаза – етап перевірки. Смарт-контракт і CSP служать верифікатором і постачальником ключів верифікації відповідно.

На етапі кроку DOD створює пряме відображення між двома ключами, вибирає коротку хеш-функцію, яка є специфічною для відображення, вибирає приватний ключ і генерує з нього відкритий ключ. Потім DOD розділяє файл даних на набір кількох фрагментів даних однакової довжини. Після хешування DOD розраховує HVT кожного фрагмента інформації, щоб створити набір метаданих автентифікації даних, що зменшує витрати на зв'язок, але дозволяє публічну перевірку. DOD передає набір компонентів даних і пов'язаних метаданих на сервер зберігання в хмарі. Набір метаданих передається в HSSC через мережу блокчейн як транзакція. DOD стирає файл даних у локальній системі.

На етапі виклику DOD витягує c-елементи з HSSC, які потім використовуються для побудови випадкового індексу фрагментів і надсилання ряду випадкових значень разом з індексом до CSP і CRSC у формі *Chal*, запиту на виклик.

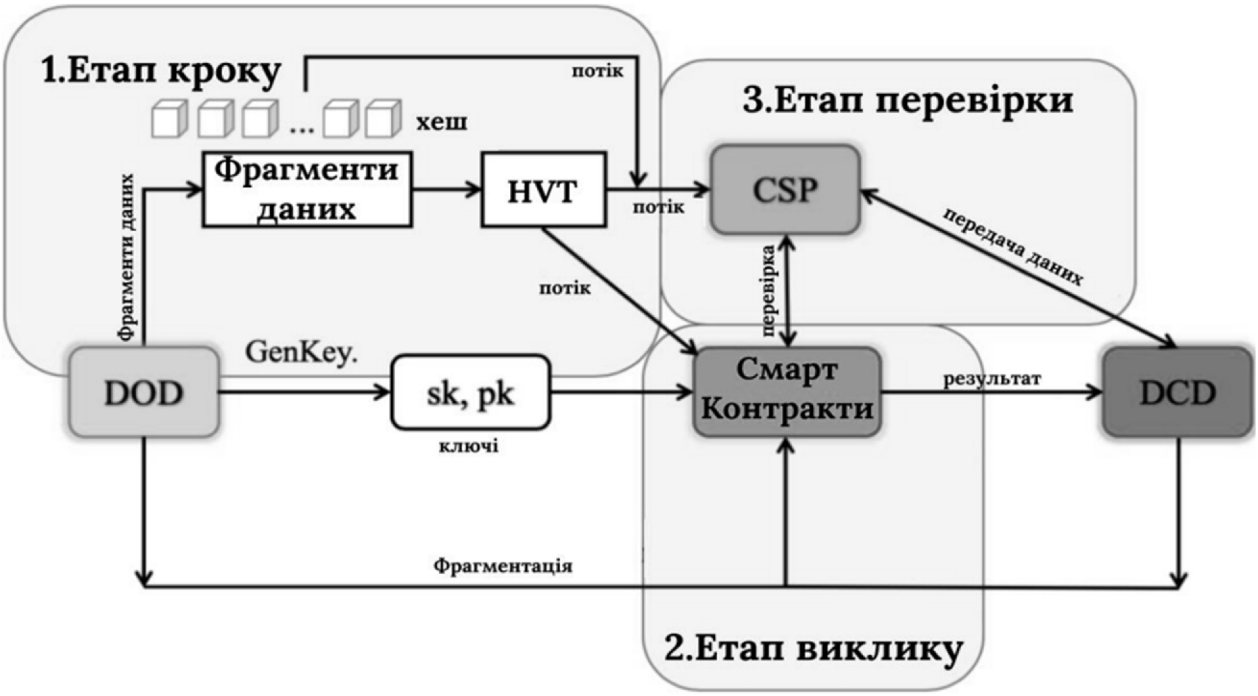

Рисунок 3.2 – Процес перевірки отриманих даних

На завершальному етапі перевірки IVSC отримує HVT і *chal* від HSSC і CRSC відповідно. Після отримання запиту на виклик, CSP обчислює фрагмент {R, μ, η} і передає його до IVSC. IVSC перевіряє, чи є підтвердження правильним. Якщо значення правильні то дані, що зберігаються в хмарі, інтегруються, а IVSC повертає результат до DOD.

DCD також може ініціювати запит на перевірку збережених даних. DCD, який запитує перевірку цілісності, може брати участь у фазі ініціації та фазі перевірки. Коли легітимність даних перевіряється, CSP передає дані з серверів відповідному клієнту через мережу P2P.

Важливо використовувати смарт-контракти в процесі перевірки та алгоритм, який обчислює протокол перевірки, щоб гарантувати автентичність метаданих, пов'язаних з автентифікацією. Розглянемо детально порядок застосування алгоритму перевірки.

На етапі кроку DOD має створити пряме двобічне відображення:

$$e: G_1 \times G_2 \rightarrow G_2, \tag{3.1}$$

де G_1 — циклічна група додавання порядку q;

G_2— циклічна мультиплікативна група порядку Q.

і хеш-функцію захисту короткого підпису:

$$H: \{0.1\}^{*} \rightarrow \{0.1\}^{\lambda}. \quad (3.2)$$

Таким чином отримаємо наступні псевдовипадкові функції: $\varphi(i, j)$: $Z_q^{*} \times \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$, де Z_q^{*} – ціле кільце моди q, $|q| \geq \lambda \geq 160$.

DOD вибирає закритий ключ $\alpha \leftarrow Z_q^{*}$ випадковим чином із відкритого ключа $Y = \alpha P$. Відкритий ключ — pk, а закритий — sk. Неможливо вирахувати приватний ключ із відкритого ключа. DOD розбиває файл даних F на фрагменти однакового розміру: $\{m_1, m_2, m_3, \dots, m_n\}$ та генерує HVT для кожного з цих фрагментів даних m_i. Водночас формується набір метаданих $\Phi = \{\delta_1, \delta_2, \dots, \delta_n\}$.

Зрештою, DOD передає набір фрагментів даних на сервер хмарного сховища, і передає набір метаданих Φ до HSSC. Після цього DOD видаляє файл даних у локальній системі.

На етапі виклику: DOD генерує c-елементи випадковим чином, щоб визначити індекс фрагменту даних з набору $I = \{s_1, s_2, \dots, s_c\}$, $c \in [1, n]$, і генерує псевдовипадкове число для кожного компонента. DOD передає випадкове значення та індекс фрагменту даних на CSP і CRSC у формі запиту виклику $chal = \{(i, v_i)\}$, $s_1 < i < s_c$.

На етапі перевірки після отримання запиту на $chal$ CSP, який є постачальником ключів для верифікації, обчислює:

$$R = \sum_{i=s_1}^{s_c} v_i Y \quad (3.3)$$

$$\mu = \sum_{i=s_1}^{s_c} v_i H(m_i) P \quad (3.4)$$

$$\eta = P - P^2 \sum_{i=s_1}^{s_c} \frac{v_i}{\delta_i} \quad (3.5)$$

Після цього CSP повертає *{R, μ, η}* як доказ IVSC.

Після отримання інформації для верифікації *{R, μ, η}* IVSC визначає, чи інтегровано дані на сервері хмарного сховища: *e (η, P) · e (μ + R, P) = e (P, P)*. Якщо наведена тотожність виконується то передана інформація є вірною. У такому разі розумний контракт підтверджує легітимність верифікованих даних для запитувача.

Відповідно до запропонованої схеми, якщо дані, що зберігаються CSP, не постраждали, а доказ, надісланий CSP, є законним то перевірка наступної математичної тотожності доводить життєздатність запропонованої схеми.

$$e(\eta, P) \cdot e(\mu + R, P) = e\left(P - P^2 \sum_{i=s_1}^{s_c} \frac{v_i}{\delta_i}, P\right) \cdot e\left(\sum_{i=s_1}^{s_c} v_i H(m_i) P + \sum_{i=s_1}^{s_c} v_i Y, P\right) \tag{3.6}$$

$$= e\left(P - P^2 \sum_{i=s_1}^{s_c} \frac{v_i H(m_i) + \alpha}{P}, P\right) \cdot e\left(\sum_{i=s_1}^{s_c} v_i H(m_i + \alpha) P, P\right)$$

$$= e\left(-\sum_{i=s_1}^{s_c} v_i H(m_i + \alpha) P, P\right) \cdot e(P, P) \cdot \left(\sum_{i=s_1}^{s_c} v_i H(m_i + \alpha) P, P\right)$$

$$= e(P, P)$$

З рівняння видно, що алгоритм перевірки здійснений.

Якщо зловмисник хоче пройти перевірку смарт-контракту він повинен згенерувати підпис $\delta_j^* = \frac{1}{H(m_j^*)+\alpha}$, який буде використовуватись для розрахунку наступних елементів верифікації:

$$\mu^* = e\left(\sum_{i=s_1}^{s_c} v_i H(m_i) P + v_i H(m_j^*) P\right), \tag{3.7}$$

$$\eta^* = P - \left(P^2 \sum_{i=s_1, i \neq j}^{s_c} \frac{v_i}{\delta_i}\right) - P^2 \frac{v_i}{\delta_i} \tag{3.8}$$

І вже на їх основі може здійснюватись розрахунок:

$$e(\eta^*, P) \cdot e(\mu^* + R, P) = e(P, P) \quad (3.9)$$

Однак зловмиснику невідомий закритий ключ α, тому підробити підпис m_j^* неможливо і доказ не буде прийнято:

$$\frac{1}{H(m_j) + \alpha} P = \frac{1}{H(m_j^*) + \alpha} P \quad (3.10)$$

Якщо зловмисники спробують стерти дані m_j^* на сервері хмарного сховища, реалізувати верифікацію буде неможливо реалізувати оскільки закритий ключ α невідомий. Зі згаданого вище аналізу можна зробити висновок, що алгоритм перевірки є стійким до зловмисних атак.

Процедура динамічного оновлення даних завершується викликом алгоритму запиту оновлення даних, який називається UpdateReq(), і алгоритмом безпосереднього виконання оновлення під назвою UpdateExec(). Релевантні операції цих алгоритмів включають додавання нових даних до фрагмента даних, зміну даних у фрагменті даних і видалення даних із фрагмента даних.

Алгоритм UpdateReq() ініціюється DOD, вимагає оновлення копії переданого файлу, яка зберігається у віддаленому CSP, і вихідний запит також є оновленням.

DOD запитує нову версію продукту з хмари у вигляді відповідного запиту: $\langle BlockOp, Ind, m_i', \delta'_i \rangle$ де BlockOp — відповідна операція фрагменту даних, Ind — індекс оновленого фрагменту даних, а m_i', δ_i' — це відповідно оновлений фрагмент даних та оновлені метадані.

Алгоритм UpdateExec() реалізується на сервері CSP. Вхідним параметром алгоритму є запит DOD на оновлення, а вихідним – нова версія файлу F' та нові метадані про нього. Після кожної ітерації процесу оновлення DOD ініціює повторну верифікацію даних, щоб перевірити правильність оновлення.

Під час здійснення операції додавання фрагменту даних DOD додає нову частину інформації в позицію *j*. Якщо спочатку є *n* сегментів даних, після операції додавання буде збережено вже *n + 1* сегмент даних. Якщо запит міститиме m_n+1, блок даних то процес перевірки все ще можна завершити, оскільки метадані також доповнено.

У процесі виконання операції видалення певної частини даних усі наступні дані буде переміщено на одну позицію. Якщо конкретну частину даних зі значенням індексу *j* потрібно стерти, DOD просить CSP видалити саме її. Це робиться за допомогою запиту, який надсилається зі сторони DOD до CSP: $\langle Delete, j, null, null \rangle$. Після отримання запиту на видалення набору даних CSP видаляє сегмент даних, індекс якого дорівнює *j*, у резервних копіях.

Для демонстрації ефективності запропонованої схеми цілісності та безпеки даних (BB-DIS) проведено моделювання у MATLab. Для порівняння була використана мережа блокчейн, призначена для безпосереднього зберігання результатів хешування – B-DIS [18]. Мережу, яка багаторазово використовує хеш-функцію дерева Merkle для генерації фрагментів даних на основі блокчейну – BM-DIS [19]. І структуру методу B-DAM [20] з механізмом перевірки даних на основі блокчейну. Середня кількість повторів даних в експерименті склала 30 тестів.

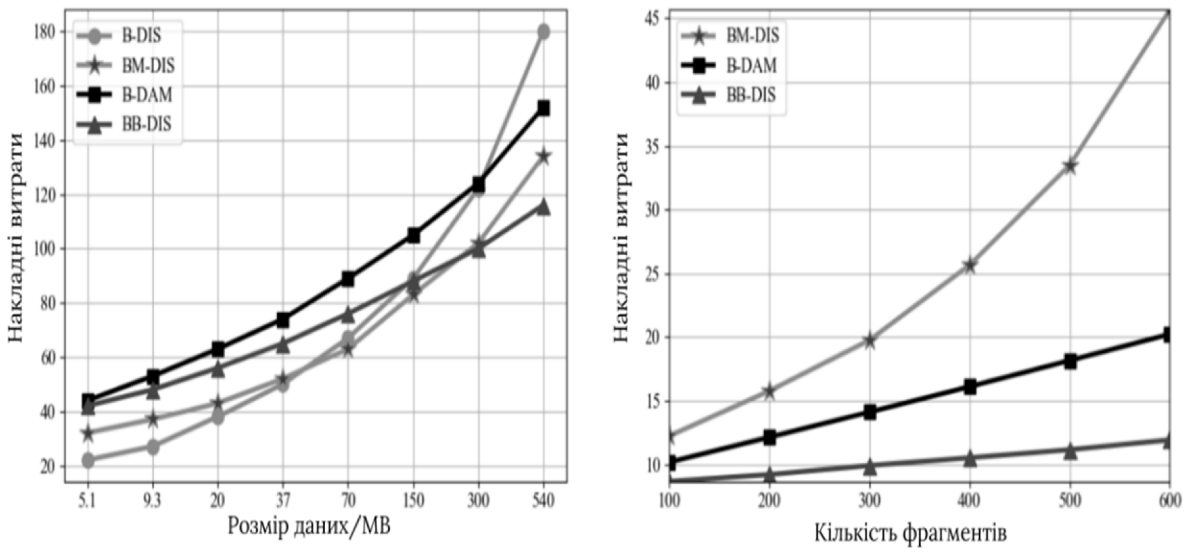

Рисунок 3.3 – Порівняння накладних витрат

На рис. 3.3 показано витрати на перевірки цілісності даних IoT за різними параметрами за умови збільшення масштабу даних IoT. У експерименті підтримувалась постійна загальна кількість фрагментів даних та зберігався їх розмір.

Отримані залежності демонструють, що коли обсяг накопичених даних перевищує 150 МБ, запропонована модель проявляє свою ефективність перед аналогами. Тобто досягається довіра та значно збільшується обсяг перевірки великомасштабних даних, відтак накладні витрати зростають повільніше ніж у аналогів. Крім того встановлено, що у разі використання фрагментів даних фіксованого розміру (20 КБ) BB-DIS вимагає менше накладних обчислювальних витрат порівнно з BM-DIS і B-DAM.

Таким чином розроблена математична модель свідчить про певні переваги запропонованого методу. Використана концепція протидіє враженню даних в мережі IoT, а також полегшує проблему маштабованості.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Чинна класифікація причин електротравматизму не відрізняється від загальноприйнятої класифікації причин нещасних випадків. Найбільш поширеними серед груп причин електротравматизму є організаційні та технічні.

Серед технічних причин слід виділити такі, як недосконаліть конструкції електроустановки і засобів захисту, допущені недоліки при виготовленні, монтажу і ремонті електроустановки, невідповідність будови електроустановок і захисних засобів умовам їх застосування тощо.

Організаційні причини електротравматизму в першу чергу пов’язані з недостатньою кваліфікацією працівників, порушеннями правил безпеки, відсутністю нагляду та контролю за виконанням робіт в електроустановках, несвоєчасним опосвідчення технічного стану електроустановок, відсутністю чи невідповідністю вимогам безпеки засобів захисту, експлуатацією несправних електроустановок тощо.

Серед безпосередніх причин попадання людей під напругу слід виділити такі:

– поява напруги на корпусі електроустановки або на електрично зв'язаних з ним металоконструкціях (далі – корпусі) у результаті пошкодження основної ізоляції;

– поява напруги на ізольованих струмовідних частинах електроустановок у результаті пошкодження додаткової ізоляції;

– доступність неізольованих струмовідних частин електроустановок, які знаходяться під напругою, що призводить до випадкового (прямого) дотику до них;

– потрапляння в зону розтікання струму в землі;

– виникнення електричної дуги між струмовідними частинами і тілом людини.

Струм через тіло людини проходить, якщо вона торкається одночасно двох точок, між якими існує різниця потенціалів, і при цьому виникає замкнене коло. Величина цього струму залежить від схеми включення, тобто від того, яких частин електроустановки торкається людина, а також від параметрів електричної мережі. Серед різноманітних схем включення людини в електричне коло слід виділити такі:

– одночасний дотик до двох полюсів мережі постійного струму або до фази та нуля однофазної мережі чи двох фаз трифазної мережі змінного струму;

– дотик до одного з полюсів чи однієї з фаз мережі змінного струму, при якому коло струму замикається через людину та землю;

– дотик до корпусу електроустановки, який у результаті пошкодження основної ізоляції знаходиться під напругою, за умови, що коло струму замикається через людину та землю;

– одночасний дотик до двох точок на поверхні землі, які в результаті замикань на землю знаходяться під напругою.

Замикання на землю може відбутися внаслідок появи контакту між струмовідними частинами і заземленим корпусом, при падінні на землю обірваного проводу, при порушенні ізоляції устаткування тощо. У всіх цих випадках струм від частин, що знаходяться під напругою, проходить у землю через елементи обладнання, що мають контакт з ґрунтом, або спеціальний металевий електрод, який прийнято називати заземлювачем.

Розміри та форма елементів обладнання та електродів можуть бути різними. Різні можуть бути і електричні властивості ґрунту, особливо за наявності в місті замикання кількох шарів ґрунту з різними питомими опорами.

Засоби та заходи з безпечної експлуатації електроустановок.

При розробці системи засобів та заходів з безпечної експлуатації електроустановок у першу чергу враховується:

– особливості виробничого середовища;

– доступність електрообладнання;

– величина напруги мережі живлення, В;

– величина струму замкнення на землю, А;

– конструктивні особливості мережі живлення – кількість фаз і режим нейтралі;

– величина опору і стан ізоляції провідників відносно землі;

– протяжність і розгалуженість мережі живлення.

Усі засоби і заходи електробезпеки прийнято поділяти на три групи: технічні, організаційні та електрозахисні.

Технічних засоби і заходи з електробезпеки реалізуються в конструкції електроустановок при їх розробці, виготовленні і монтажі відповідно до чинних нормативів. За своїми функціями технічні засоби і заходи електробезпеки поділяються на дві групи:

– технічні заходи та засоби електробезпеки, що використовуються за нормального режиму роботи електроустановок;

– технічні заходи та засоби електробезпеки, що використовуються за аварійних режимів роботи електроустановок.

До основних технічних засобів і заходів першої групи відносяться:

– захист від випадкового (прямого) доторкання до струмовідних частин;

– блокувальні пристрої;

– засоби орієнтації та сигналізації;
– захисне розділення електричних мереж;
– застосування малої (зверхнизької) напруги;
– компенсація ємнісних струмів замикання на землю;
– вирівнювання потенціалів.

Залежно від призначення, умов експлуатації та конструкції в електроустановках можуть застосовуватись одночасно декілька з перелічених технічних засобів і заходів.

Технічні заходи електробезпеки, що використовуються за аварійних режимів роботи електроустановок включають:

– захисне заземлення;
– занулення;
– · захисне відключення;
– подвійна ізоляція.

Електрозахисні засоби – це технічні вироби, що не є конструктивними елементами електроустановок і застосовуються під час виконання робіт в електроустановках з метою запобігання електротравм.

Організаційні заходи і засоби щодо попередження електротравм регламентуються НПАОП 0.00-1.21-98 «Правила безпечної експлуатації електроустановок споживачів».

4.2 Безпека в надзвичайних ситуаціях

Кожній організації властива своє специфічне трудове середовище. Трудова діяльність розробника програм завжди здійснюється в певному просторі і в певний час, з використанням конкретних засобів виробництва (засобів праці і предметів праці). Крім того, в процесі конкретної трудової

діяльності між працівниками складаються і певні соціально-трудові відносини, які також динамічні, і змінюються залежно від зміни умов протікання трудової діяльності людини. Тому трудова діяльність здійснюється в певному середовищі, що розуміється як сукупність умов і впливів, наявних в деякому оточенні.

Під трудовою середовищем розуміються кошти, умови праці та взаємини людей, що беруть участь у трудовому процесі. Трудове середовище включає, як фізичні фактори (тобто санітарно-гігієнічні умови праці в широкому сенсі), так і техніко-технологічні чинники (засоби праці, предмети праці, технологічний процес).

Засоби праці представляють собою знаряддя праці, з допомогою яких люди впливають на предмети праці і, видозмінюючи їх, надають їм корисні властивості, здатні задовольняти певні потреби. До засобів праці відносяться машини й устаткування, інструменти і пристосування, виробничі будівлі та споруди, всі види транспорту, лінії електропередач, засоби зв'язку та сигналізації, засоби захисту працівників.

Основна роль в засобах праці належить саме знарядь виробництва, оскільки саме з їх допомогою людина перетворює предмети природи. Засоби праці та предмети праці у своїй сукупності складають засоби виробництва.

Але, як відомо, самі по собі засоби виробництва функціонувати не можуть. Провідну роль поєднанні засобів праці і предметів праці, тобто функціонування засобів виробництва належить людині. Тому вирішальним фактором процесу виробництва є робоча сила людини.

Засоби праці, предмети праці і люди в трудовій організації знаходяться в постійній взаємодії. Елементи фізичної трудового середовища схильні до постійних змін. Ці зміни відбуваються швидше серед елементів фізичної трудового середовища, що є продуктом людської праці, і породжують цілий ряд соціальних наслідків. Зміна матеріальних елементів фізичної трудового середовища, що є частиною природи, відбувається повільніше і до певного моменту з меншими соціальними наслідками. Положення людини в трудовому

середовищі може бути різним, і залежить від того, переважають чи у фізичній трудової середовищі матеріальні фактори, що є частиною природи, або матеріальні чинники, є продуктом людської праці.

Відносини, в які вступають люди в процесі трудової діяльності, утворюють соціальну трудову середу. З соціологічної точки зору, праця, в першу чергу, являє собою відносини, що виникають між конкретними людьми – учасниками процесу праці. В ході трудової діяльності люди вступають у суспільні відносини, і в рамках цих суспільних відносин формуються міжособистісні відносини, взаємна поведінка індивідів. Характер міжособистісних відносин у трудовому середовищі, визначається соціальним статусом і роллю індивіда в трудовій організації, і має суттєвий вплив на поведінку людини в трудовому середовищі, і досягнення ефекту трудової діяльності.

На поведінку працівників у трудовій середовищі впливають: форми організації та оплати праці, психологічний клімат, виробничо-побутові умови, життєве оточення працівників, позавиробнича діяльність людей.

При організації праці, що пов'язана з використанням ВДТ ЕОМ і ПЕОМ, для збереження здоров'я працюючих, запобігання професійним захворювання і підтримки працездатності слід передбачити внутрішньозмінні регламентовані перерви для відпочинку.

Внутрішньозмінні режими праці і відпочинку мають передбачати додаткові нетривалі перерви в періоди, що передують появі об'єктивних і суб'єктивних ознак стомлення і зниження працездатності.

При виконанні протягом дня робіт, що належать до різних видів трудової діяльності, за основну роботу з ВДТ ЕОМ і ПЕОМ слід вважати таку, що займає не менше 50 % часу впродовж робочої зміни мають передбачатися:

– перерви для відпочинку і вживання їжі (обідні перерви);

– перерви для відпочинку і особистих потреб (згідно з трудовими нормами);

– додаткові перерви, що вводяться для окремих професій з урахуванням особливостей трудової діяльності.

Тривалість обідньої перерви визначається чинним законодавством про працю і Правилами внутрішнього трудового розпорядку підприємства (Організації, установи).

Внутрішньозмінні режими праці і відпочинку при роботі з ВДТ ЕОМ і ПЕОМ розроблено з урахуванням характеру трудової діяльності, напруженості і важкості праці диференційовано для кожної професії.

За характером трудової діяльності виділено три професійні групи згідно з діючим класифікатором професій ДК 003-95 і Зміна № 1 до ДК 003-95:

– розробники програм (інженери-програмісти) – виконують роботу переважно з відеотерміналом та документацією при необхідності і інтенсивного обміну інформацією з ЕОМ і високою частиною прийняття рішень. Робота характеризується інтенсивною розумовою творчою працею з підвищеним напруженням зору, концентрацією уваги на фоні нервовоемоційного напруження, вимушеною робочою позою, загальною гіподинамією, періодичним навантаженням на кисті верхніх кінцівок. Робота виконується в режимі діалогу з ЕОМ у вільному темпі з періодичним пошуком помилок в умовах дефіциту часу;

– оператори електронно-обчислювальних машин – виконують роботу яка пов'язана з обліком інформації одержаної з ВДТ за попереднім запитом, або тієї, що надходить з нього, супроводжується перервами різної тривалості, пов'язана з виконанням іншої роботи і характеризується як робота з напруженням зору, невеликими фізичними зусиллями, нервовим напруженням середнього ступеня та виконується у вільному темпі;

– оператор комп'ютерного набору – виконує одноманітні за характером роботи з документацією та клавіатурою і нечастими нетривалими переключеннями погляду на екран дисплея, з введенням даних з високою швидкістю, робота характеризується як фізична праця з підвищеним навантаженням на кисті верхніх кінцівок на фоні загальної гіподинамії з

напруженням зору (фіксація зору переважно на документи), нервовоемоційним напруженням.

Встановлюються такі внутрішньозмінні режими праці та відпочинку при роботі з ЕОМ при 8-годинній денній робочій зміні в залежності від характеру праці:

– для розробників програм із застосуванням ЕОМ, слід призначати регламентовану перерву для відпочинку тривалістю 15 хвилин через кожну годину роботи за ВДТ;

– для операторів із застосування ЕОМ, слід призначати регламентовані перерви для відпочинку тривалістю 15 хвилин через кожні дві години;

У всіх випадках, коли виробничі обставини не дозволяють застосувати регламентовані перерви, тривалість безперервної роботи з ВДТ не повинна перевищувати 4 години. При 12-годинній робочій зміні регламентовані перерви повинні встановлюватися в перші 8 годин роботи аналогічно перервам при 8-годинній робочій зміні, а протягом останніх 4-х годин роботи, незалежно від характеру трудової діяльності, через кожну годину тривалістю 15 хвилин.

З метою зменшення негативного впливу монотонності є доцільним застосовувати чергування операцій усвідомленого тексту і числових даних (зміна змісту роботи). Чергування вводу даних та редагування текстів.

РОЗДІЛ 5
ЕКОНОМІЧНА ЕФЕКТИВНІСТЬ

5.1 Економічна ефективність інтеграції Blockchain у мережі IoT

Економічна ефективність технології Blockchain у мережах Інтернету речей (IoT) базується на її здатності забезпечувати безпечний, прозорий та децентралізований обмін даними між пристроями. У традиційних системах управління IoT значні витрати виникають через необхідність централізованих серверів, що обробляють великий обсяг даних і контролюють взаємодію між пристроями. Blockchain усуває потребу в такій централізації, створюючи розподілену мережу, де кожен пристрій може автономно підтверджувати транзакції та обмінюватися інформацією без посередників. Це знижує витрати на інфраструктуру, оскільки усувається залежність від централізованих центрів обробки даних.

Використання Blockchain підвищує ефективність IoT-систем завдяки автоматизації процесів через смарт-контракти. Вони дозволяють пристроям виконувати дії на основі попередньо заданих умов без необхідності ручного втручання чи додаткового програмного забезпечення. Це зменшує витрати на обслуговування і технічну підтримку, водночас підвищуючи швидкість і точність виконання завдань. Наприклад, у системах розумного дому смарт-контракти можуть автоматично регулювати споживання енергії або забезпечувати безпеку, що напряму економить ресурси.

Blockchain також вирішує питання безпеки, які є критичними для IoT, особливо у великих мережах із тисячами взаємопов'язаних пристроїв. Кіберзагрози та зломи можуть спричиняти значні економічні збитки, зокрема через втрату даних чи збої в роботі систем. Використання криптографії у Blockchain забезпечує високий рівень захисту даних і знижує ризики

несанкціонованого доступу. Це зменшує витрати на безпеку, які в традиційних системах можуть бути дуже високими, оскільки вимагають значних ресурсів для побудови захищених серверів і мереж.

Крім того, Blockchain оптимізує управління ресурсами в IoT, дозволяючи створювати економічні моделі обміну, де пристрої можуть взаємодіяти напряму, обмінюватися ресурсами чи навіть здійснювати мікротранзакції між собою. Це відкриває нові можливості для монетизації IoT, зокрема у сферах логістики, енергетики чи роздрібної торгівлі. Наприклад, розумні енергосистеми можуть використовувати Blockchain для обліку і торгівлі енергією між будинками, підвищуючи ефективність використання відновлюваних джерел енергії та створюючи економічну вигоду для користувачів.

Загалом, Blockchain додає економічну цінність мережам IoT за рахунок зниження операційних витрат, підвищення безпеки і відкриття нових джерел доходу. Його інтеграція з IoT забезпечує стійкий розвиток технологій у різних галузях, дозволяючи підприємствам і споживачам отримувати більше вигоди від автоматизації та децентралізації процесів.

Зниження витрат на інфраструктуру реалізується через використання децентралізованої моделі Blockchain, що усуває необхідність у централізованих серверах, зменшуючи витрати на їхнє створення, обслуговування та масштабування.

Смарт-контракти дозволяють автоматизувати процеси обміну даними і виконання транзакцій між пристроями, що знижує потребу в ручному управлінні та посередниках. Криптографічний захист і незмінність даних у Blockchain знижують ризики кібератак, усуваючи значні витрати на ліквідацію наслідків зломів та втрату даних.

Взаємодія пристроїв у мережі без використання енергоємних централізованих серверів сприяє зниженню споживання енергії, особливо у великих мережах IoT.

Blockchain забезпечує безпечний обмін даними, що дозволяє користувачам і компаніям продавати їх без посередників, отримуючи додаткові доходи. Розподілений реєстр гарантує точність і незмінність даних, зменшуючи витрати на аудит, перевірки та виправлення помилок у транзакціях.

Можливість точного обліку та прогнозування ресурсів (наприклад, електроенергії в розумних мережах) дозволяє знизити перевитрати і підвищити ефективність використання інфраструктури.

Blockchain дозволяє легко інтегрувати нові пристрої в існуючу мережу IoT без значного збільшення витрат, забезпечуючи стійке зростання системи.

Ці переваги роблять Blockchain важливим інструментом для зниження витрат і підвищення ефективності в мережах IoT, забезпечуючи економічну вигоду для бізнесу та користувачів.

5.2 Ніша Blockchain у мережах Iot

Ніша Blockchain у мережах Інтернету речей (IoT) є однією з найбільш перспективних і швидкозростаючих у сучасному технологічному світі, оскільки вона поєднує переваги децентралізованої технології з широким потенціалом IoT для автоматизації та інтеграції пристроїв. Зростання кількості IoT-пристроїв створює значні виклики, пов'язані з безпекою, масштабованістю та ефективністю обміну даними. Blockchain надає ефективне рішення цим проблемам, відкриваючи нові можливості для розробки інноваційних продуктів і сервісів.

Однією з ключових областей, де Blockchain демонструє свою значущість у IoT, є безпека. Традиційні IoT-системи зазвичай залежать від централізованих серверів, які є вразливими до атак. Впровадження Blockchain усуває цю проблему завдяки своїй децентралізованій природі, де дані

зберігаються у формі блоків, розподілених між учасниками мережі. Це не лише підвищує рівень захисту даних, але й мінімізує ризик збоїв у роботі системи через єдиний вразливий вузол. Для стартапів, що працюють у сфері IoT, це відкриває можливість розробки продуктів із фокусом на кібербезпеку, що є особливо актуальним у галузях, пов'язаних із критично важливими системами, такими як медицина, транспорт чи промисловість.

Іншим важливим аспектом є можливість автоматизації процесів через використання смарт-контрактів. У мережах IoT смарт-контракти дозволяють пристроям виконувати дії автоматично на основі заздалегідь визначених умов. Це спрощує управління складними системами, такими як логістичні ланцюги постачання, енергетичні мережі чи системи управління будинками. Для підприємців у цій ніші з'являється можливість створювати програмні рішення для різних секторів, які інтегрують Blockchain із IoT, дозволяючи пристроям обмінюватися ресурсами чи проводити фінансові транзакції без участі людини.

Значну увагу Blockchain у IoT привертає також у сфері монетизації даних. IoT-пристрої генерують величезні обсяги інформації, яка має значну цінність для бізнесу. Blockchain забезпечує прозорість і захист у процесі обміну цими даними, дозволяючи створювати нові бізнес-моделі, де користувачі можуть безпечно продавати дані або отримувати винагороду за їх використання. Це відкриває перспективи для розвитку децентралізованих платформ, які об'єднують виробників пристроїв, користувачів і бізнеси, зацікавлені у доступі до цих даних.

Загалом, ніша Blockchain у IoT пропонує величезні можливості для інновацій у сферах безпеки, автоматизації, обміну даними та оптимізації витрат. Розробка рішень у цій галузі дозволяє не лише підвищувати ефективність і захищеність систем, але й створювати нові моделі співпраці та монетизації в умовах діджиталізації.

5.3 Порівняння дротових і бездротових технологій IoT

Дротові рішення, такі як Ethernet, Power Line Communication (PLC) або інші провідні протоколи, забезпечують стабільний зв’язок і високу пропускну здатність передачі даних. Вони менш схильні до зовнішніх перешкод, що робить їх ідеальними для критичних інфраструктур або промислових застосувань. Однак їхнє впровадження вимагає значних витрат на прокладення кабелів, а також обмежує мобільність і масштабованість систем. Наприклад, для створення дротової мережі в приміщенні потрібно врахувати вартість кабелів ($0.50–$2 за метр), роз'ємів та монтажу (приблизно $10–$15 за точку). У масштабі фабрики довжиною 500 метрів і 50 пристроями загальні витрати можуть сягати $5,000–$10,000.

Бездротові рішення, такі як Wi-Fi, LoRa, ZigBee, або NB-IoT, забезпечують гнучкість і легкість розгортання. Вони дозволяють швидко створювати мережі навіть у віддалених або важкодоступних місцях. Бездротові технології мають нижчі початкові витрати на обладнання і встановлення, але вимагають періодичної заміни батарей у деяких пристроях та можуть бути вразливими до інтерференцій, що особливо несподівано може проявлятися у виробничих умовах. Наприклад, створення мережі на основі Wi-Fi для 50 пристроїв потребує доступних точок (в середньому $50 за одну) та базової конфігурації, що сумарно коштує близько $3,000.

У довгостроковій перспективі використання бездротових мереж є вигіднішим для динамічних систем, які потребують розширення чи змін конфігурації. Дротові мережі стають економічно доцільними для стаціонарних та критично важливих систем через зменшення рівня зашумленості, спрощення поточного обслуговування та менші енергетичні витрати на підтримку постійного функціонування мережі.

Таблиця 5.1 – Порівняння економічних показників дротової та бездротокої технології зв’язку

Дротові технології	**Бездротові технології**
Початкові інвестиції	
$5,000–$10,000 включає обладнання та монтаж	$2,000–$3,000 за наявності базової інфраструктури
Операційні витрати	
низькі витрати на обслуговування: орієнтовно $100–$200 на рік для середньої мережі	періодична заміна батарей для пристроїв залежно від кількості пристроїв: $500–$1000 на рік

Дротові мережі: промислові підприємства, де потрібна висока надійність і пропускна здатність (наприклад, контроль виробничих ліній через Ethernet).

Бездротові мережі: розумний будинок, сільське господарство (LoRaWAN для моніторингу стану ґрунту), транспортування (NB-IoT для відстеження вантажів).

Вибір між дротовими та бездротовими технологіями залежить від конкретного застосування, бюджету та вимог до надійності та масштабованості системи.

ВИСНОВКИ

Ефективний обмін інформацією є важливим елементом функціонування мереж IoT, оскільки забезпечує працезатність всієї системи, дозволяючи пристроям взаємодіяти та реагувати на зміни в реальному часі. Визначено, що вибір оптимальної технології обміну інформацією є залежним від таких характеристик, як енергоефективність, швидкість передачі даних, надійність, масштабованість та здатність до роботи в умовах різноманітних фізичних перешкод. Такі протоколи, як MQTT та CoAP, показують ефективність у використанні обмежених ресурсів, що робить їх ідеальними для систем із малим енергоспоживанням. Водночас протоколи LoRa та Zigbee забезпечують значну дальність зв'язку, але мають обмеження у швидкості передачі.

Кожна технологія обміну інформацією має свої унікальні переваги та обмеження, які визначають її відповідність певним сферам застосування. Технології з низьким рівнем затримки, такі як Bluetooth Low Energy, краще підходять для пристроїв, які потребують швидкої передачі даних на коротких відстанях, тоді як протоколи з розширеним радіусом дії та мінімальним енергоспоживанням, як-от LoRa, є оптимальними для застосувань у сфері сільського господарства чи моніторингу навколишнього середовища. Крім того, інтеграція різних технологій у межах однієї мережі IoT дозволяє досягти гнучкості й оптимізації ресурсів, забезпечуючи стабільну роботу.

Результати математичного моделюванням у середовища MATLab доводять ефективність запропонованого рішення. Результати моделювання показали, що запропонований метод має високий потенціал протидії і низькі показники затрат, зокрема коли обсяг накопичених даних перевищує 150 МБ, запропонована модель проявляє свою ефективність перед дослідженими аналогами. Також встановлено, що у разі передачі фрагментів даних фіксованого розміру запропоноване рішення на основі блокчейн вимагає менше накладних обчислювальних витрат.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mahmood Z., Ullah F. (2019). The Internet of Things in the Industrial Sector. Springer International Publishing.

2. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

3. Da Xu L., He W., Li S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243.

4. Stankovic J. A. (2014). Research Directions for the Internet of Things. IEEE Internet of Things Journal, 1(1), 3-9.

5. Razzaque M. A., Milojevic-Jevric M., Palade A., Clarke S. (2016). Middleware for Internet of Things: A Survey. IEEE Internet of Things Journal, 3(1), 70-95.

6. Kim S., Helal S. (2016). Extended IoT: Applications and Techniques. Springer International Publishing.

7. Ray P. P. (2018). A Survey on Internet of Things Architectures. Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.

8. Atzori L., Iera A., Morabito G. (2010). The Internet of Things: A Survey. Computer Networks, 54(15), 2787-2805.

9. Zanella A., Bui N., Castellani A., Vangelista L., Zorzi M. (2014). Internet of Things for Smart Cities. IEEE Internet of Things Journal, 1(1), 22-32.

10. Khan M. A., Salah K. (2018). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems, 82, 395-411.

11. IEEE Xplore Digital Library (https://ieeexplore.ieee.org/) – містить багато статей з тематики IoT та комунікаційних технологій.

12. Springer Link (https://link.springer.com/) – доступ до книг і статей про технології обміну даними та архітектури IoT.

13. ScienceDirect (https://www.sciencedirect.com/) – публікації на тему мереж IoT, протоколів передачі даних та безпеки.

14. King, J., Awad, A.I. A Distributed Security Mechanism for ResourceConstrained IoT Devices. Informatica (Slovenia) 2016, 40, 133–143.

15. Ning H. Unit and Ubiquitous Internet of Things; CRC Press, Inc.: Boca Raton, FL, USA, 2013.

16. Miller M. The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities are Changing the World; Que Publishing: Indianapolis, Indiana, 2015.

17. Al-Fuqaha A., Guizani M., Mohammadi M., Aledhari M., Ayyash M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Commun. Surv. Tutor. 2015, 17, 2347–2376.

18. Suryadevara N.K., Mukhopadhyay S.C. Smart Homes: Design, Implementation and Issues; Springer: Cham, Switzerland, 2015.

19. Khan R., Khan S.U., Zaheer R., Khan S. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. In Proceedings of the 10th International Conference on Frontiers of Information Technology, Islamabad, India, 17–19 December 2012; pp. 257–260.

20. Fabi V., Spigliantini G., Corgnati S.P. Insights on Smart Home Concept and Occupants' Interaction with Building Controls. Energy Procedia 2017, 111, 759–769.

21. Harper R. Inside the Smart Home: Ideas, Possibilities and Methods. In Inside the Smart Home; Springer: London, UK, 2003; pp. 1–13.

22. Aarts E., Marzano S. The New Everyday: Views on Ambient Intelligence; 010 Publishers: Rotterdam, The Netherlands, 2003.

23. Nunes R.J.C., Delgado J.C.M. An Internet Application for Home Automation. In Proceedings of the 10th Mediterranean Electrotechnical Conference, Lemesos, Cyprus, 29–31 May 2000; Volume 1, pp. 298–301.

24. Al-sumaiti A.S., Ahmed M.H., Salama M.M.A. Smart Home Activities: A Literature Review. Electr. Power Compon. Syst. 2014, 42, 294–305.