

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА
на тему: «Платформа для моніторингу IoT-пристроїв з
використанням сучасних веб-технологій»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
освітньо-професійної програми «Комп'ютерні системи та мережі»

*Кваліфікаційна робота містить результати власних досліджень. Використання
ідей, результатів і текстів інших авторів мають посилання
на відповідне джерело*

(підпис)

Данило ЄМЕЛІН

Виконав: здобувач вищої освіти групи КСДМ-62
Данило ЄМЕЛІН

Керівник: Анастасія ВСЧЕРКОВСЬКА

к.т.н., доц.,

Рецензент: _____
науковий ступінь, Ім'я, ПРІЗВИЩЕ
вчене звання

Київ 2025

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

Навчально-науковий інститут інформаційних технологій

Кафедра Комп'ютерна інженерія

Ступінь вищої освіти Магістр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Комп'ютерної інженерії

_____ Наталія ЛАЩЕВСЬКА

«_____» _____ 2024 р.

**ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Ємелін Данило Михайлович

1. Тема кваліфікаційної роботи: «Платформа для моніторингу IoT-пристроїв з використанням сучасних веб-технологій»

керівник кваліфікаційної роботи Анастасія ВЄЧЕРКОВСЬКА, к.т.н., доц.,

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15» жовтня 2024 р. № 320.

2. Строк подання кваліфікаційної роботи «20» грудня 2024 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, параметри багатокамерного трекінгу, метод детектування об'єктів, вимоги до точності визначення об'єктів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Дослідження методів які впливають на роботу IoT.

2. Аналіз характеристик які впливають на ефективність мережі.

3. Розробка платформи для моніторингу IoT пристроїв з використанням сучасних віб технологій.

5. Перелік ілюстративного матеріалу: *презентація*

- 1 Мета об'єкта та предмет дослідження.
- 2 Актуальність роботи.
- 3 Розроблена симуляція на мікроконтролері ESP32.
- 4 Створення мобільного додатку для візуалізації.
- 5 Використання брокера для передачі даних.
- 6 Збереження даних у базі даних.
- 7 Відображення даних у інформаційній панелі.

6. Дата видачі завдання «16» жовтня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Аналіз наявної науково-технічної літератури	10.10-20.10.24	
2	Вивчення матеріалів для аналізу IoT	20.10-03.11.24	
3	Дослідження методів глибокого навчання	04.11-15.11.24	
4	Аналіз особливостей впливу методів глибокого навчання на IoT	16.11-21.11.24	
5	Створення додатку для моніторингу	22.11-30.11.24	
6	Організація підключень	01.12-04.12.24	
7	Оформлення роботи: вступ, висновки, реферат	05.12-07.12.24	
8	Розробка демонстраційних матеріалів	08.12-08.12.24	
9	Попередній захист роботи	12.12-12.12.24	

Здобувач вищої освіти

_____ (підпис)

Данило ЄМЕЛІН

Керівник
кваліфікаційної роботи

_____ (підпис)

Анастасія ВЄЧЕРКОВСЬКА

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 67 стор., 9 табл., 1 рис., 27 джерел.

Мета роботи – платформу для моніторингу IoT-пристроїв з використанням сучасних веб-технологій, яка забезпечує ефективне збирання, обробку та відображення даних у реальному часі. .

Об'єкт дослідження – Інтернет речей (IoT) як технологічна система, що інтегрує фізичні об'єкти в цифрове середовище для збору та обміну даними.

Предмет дослідження – методи та засоби розробки платформи для моніторингу IoT-пристроїв із застосуванням сучасних веб-технологій.

Проведено експерименти для визначення впливу на продуктивність системи багатьох взаємопов'язаних факторів, та створено платформу IoT.

КЛЮЧОВІ СЛОВА: АВТОМАТИЗАЦІЯ, БЕЗПЕКА, ІННОВАЦІЇ, ІОТ, ПРИСТРОЇ, ТЕХНОЛОГІЇ, ЦИФРОВІЗАЦІЯ.

ABSTRACT

Text part of the master's qualification work: 67 pages, 1 pictures, 9 table, 27 sources.

The purpose of the work is a platform for monitoring IoT devices using modern web technologies, which provides effective collection, processing and display of data in real time.

Object of research – The Internet of Things (IoT) as a technological system that integrates physical objects into the digital environment for data collection and exchange.

Subject of research – methods and tools for developing a platform for monitoring IoT devices using modern web technologies.

Summary of the work: methods and tools for developing a platform for monitoring IoT devices using modern web technologies.

Experiments were conducted to determine the impact of many interrelated factors on the system's performance, and an IoT platform was created.

KEYWORDS:AUTOMATION, SECURITY, INNOVATIONS, IoT, DEVICES, TECHNOLOGIES, DIGITALIZATION.

ЗМІСТ

ВСТУП.....	7
1.IOT (Internet of Things)	7
1.1 ІСТОРІЯ IOT.....	7
1.1.1 Перші приклади IoT-пристроїв.....	10
1.1.2 Розвиток технологій, що підтримують IoT	13
1.2 ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО IOT	17
1.2.1 Основні компоненти IoT	20
1.2.2 Протоколи зв'язку	25
1.3. РОЗВИТОК IOT	32
1.4. IOT-ПРИСТРОЇ.....	45
1.4.1. ВПРОВАДЖЕННЯ IOT-ПРИСТРОЇВ.....	47
1.4.1.1 Сфери використання IoT-пристроїв	50
1.4.2. ПЕРСПЕКТИВИ РОЗВИТКУ IOT	51
1.4.2.1 Інновації та нові технології в IoT	51
1.4.2.2 Вплив IoT на економіку та суспільство.....	54
1.4.2.3 Екологічні аспекти IoT: Ефективність ресурсів.....	57
2. МЕТОДОЛОГІЯ РОЗРАХУНКУ ПРОДУКТИВНОСТІ	
МЕРЕЖІ.....	60
2.1 AWS IoT	60
2.1.1 Принцип роботи AWS IoT.....	60
2.1.2 Принцип роботи сервісів.....	62
2.2 Фактори, що впливають на продуктивність Web-служб	64
2.3 Опис системи та розрахунок пропускної здатності.....	65
2.4 Середня година відкликання.....	66
2.5 Пропускна здатність при використанні кешуючого проксі-сервера.	67
2.6 Розрахунок використання ЦП серверу додатків при обробці запитів.....	68
2.7 Час обслуговування в різних мережах.....	69
ВИСНОВКИ.....	70
ПЕРЕЛІК ПОСИЛАНЬ.....	73

ВСТУП

У сучасному світі технологічний прогрес невинно трансформує способи, якими люди взаємодіють з навколишнім середовищем. Однією з найзначніших інновацій у цій сфері є концепція Інтернету речей (IoT, Internet of Things). Це поняття охоплює мережу фізичних об'єктів, оснащених датчиками, програмним забезпеченням та іншими технологіями, що дозволяють їм збирати та обмінюватися даними через Інтернет. IoT створює нові можливості для автоматизації процесів, підвищення ефективності і зручності в повсякденному житті, на виробництві, у медичних установах та інших сферах.

Актуальність теми Інтернету речей зростає з кожним роком, оскільки все більше галузей починають впроваджувати IoT-рішення для покращення ефективності та зручності. Згідно з прогнозами, до 2025 року кількість підключених IoT-пристроїв у світі може досягти декількох мільярдів, що свідчить про стрімкий розвиток цієї технології. У світі, де дані стають новим золотом, можливість їх збору та аналізу в реальному часі відкриває нові горизонти для бізнесу та суспільства в цілому [1].

Об'єктом дослідження є Інтернет речей (IoT) як технологічна система, що інтегрує фізичні об'єкти через мережу для збору та обміну даними. Предметом дослідження виступають специфічні аспекти впровадження IoT у різні сфери, зокрема виклики та можливості, що виникають у процесі інтеграції цієї технології в сучасні бізнес-процеси.

Метою даної роботи є комплексний аналіз технологій IoT, оцінка їх впливу на різні галузі, а також вивчення актуальних викликів, пов'язаних із безпекою даних, приватністю та ефективністю систем, що реалізують IoT-рішення.

У дослідженні застосовано методи аналізу літератури, кейс-стаді, опитування експертів та порівняльний аналіз існуючих IoT-рішень. Ці методи дозволили отримати глибше розуміння специфіки технології та її впливу на різні сфери діяльності.

Отримані результати дослідження підтверджують, що IoT здатен суттєво підвищити ефективність у багатьох сферах, але вимагає належного управління ризиками. Новизна роботи полягає в систематизації викликів та пропозицій щодо оптимізації впровадження IoT, що може слугувати основою для подальших досліджень.

Рекомендується використовувати результати дослідження для розробки стратегій впровадження IoT у бізнес-процеси, а також для формування політик безпеки та управління даними, що можуть підвищити ефективність інтеграції IoT-рішень.

Результати дослідження мають значний потенціал для застосування в сферах охорони здоров'я, промисловості, транспорту, енергетики та розвитку розумних міст, що відкриває нові можливості для оптимізації процесів.

Дана робота є важливою для розвитку розуміння IoT як технології, яка може істотно поліпшити ефективність і сприяти сталому розвитку. Вона також допомагає в подоланні існуючих викликів у впровадженні новітніх технологій, що є надзвичайно актуальним у сучасному світі.

1.IOT (Internet of Things)

1.1 ІСТОРІЯ IOT

Концепція Інтернету речей (IoT) виникла на перетині кількох технологічних ідей і інновацій, що розвивалися протягом кількох десятиліть. Основою для формування IoT стали досягнення в галузі комп'ютерних наук, зв'язку, мікропроцесорної технології та автоматизації.

Історично перші кроки до IoT були зроблені ще в 1960-х роках, коли вчені вивчали можливості підключення побутових приладів до комп'ютерних мереж. Одним із ранніх прикладів є проект, реалізований у Массачусетському технологічному інституті (MIT), де дослідники намагалися створити мережу, що об'єднує різні пристрої для забезпечення автоматизації в домашньому середовищі.

Таблиця 1.1 представляє основні етапи розвитку концепції Інтернету речей (IoT) з моменту її виникнення до сучасності. У ній наведені ключові події, що мали суттєвий вплив на формування та поширення IoT, а також технології, які сприяли цьому процесу. Кожен етап відображає важливі інновації та реалізації, які сприяли переходу від теоретичних засад до практичних застосувань, що визначають сучасний стан IoT у різних сферах життя.

У 1982 році університетом Карнегі-Меллона був створений перший "розумний" тостер, який міг підключатися до Інтернету. Тостер міг повідомляти користувачів про статус приготування хліба через мережу, що вказувало на початок ідеї про інтеграцію звичайних об'єктів у глобальну інформаційну мережу. Цей експеримент став одним із перших прикладів того, як побутові пристрої можуть взаємодіяти з користувачами через Інтернет.

Термін "IoT" був вперше вжитий у 1999 році Кевіном Ештоном. У своїй доповіді він зазначив, що для оптимізації процесів в управлінні запасами та постачанням важливо мати системи, які могли б самостійно збирати і передавати дані без участі людини. Ештон підкреслив важливість використання RFID-

технологій, які дозволяють ідентифікувати та відстежувати об'єкти, завдяки чому з'явилася можливість об'єднати фізичні об'єкти з цифровими системами.

Таблиця 1.1 - Основні етапи розвитку IoT

Рік	Подія	Опис
1960-ті	Перші експерименти з підключення приладів	Вчені в МІТ досліджували можливості підключення побутових приладів до комп'ютерних мереж для забезпечення автоматизації в домашньому середовищі.
1982	Розумний тостер	Університетом Карнегі-Меллона був створений перший "розумний" тостер, що міг підключатися до Інтернету і повідомляти про статус приготування хліба.
1999	Введення терміна "IoT"	Кевін Ештон вперше вживає термін "IoT" під час презентації на тему автоматизації в управлінні ланцюгами постачання, підкреслюючи важливість RFID-технологій.
2005	Доповідь ITU	Міжнародний союз електрозв'язку опублікував доповідь про потенційну роль IoT у формуванні глобальної інформаційної інфраструктури та покращення якості життя.
2000-ті	Розвиток бездротового зв'язку	З'явилися стандарти Wi-Fi, Bluetooth і Zigbee, які забезпечили основу для зв'язку між IoT-пристроями.

З моменту введення терміна "IoT" концепція почала набувати популярності. У 2005 році Міжнародний союз електрозв'язку (ITU) опублікував доповідь, у якій розглядалася потенційна роль IoT у формуванні глобальної інформаційної інфраструктури. У документі підкреслювалося, що IoT може суттєво змінити підходи до управління ресурсами, забезпечення безпеки та покращення якості життя.

Розвиток технологій, таких як бездротовий зв'язок, також сприяв поширенню IoT. На початку 2000-х років з'явилися стандарти бездротової комунікації, такі як Wi-Fi, Bluetooth і Zigbee, які забезпечили основу для зв'язку між IoT-пристроями.

Зниження вартості мікропроцесорів та сенсорів зробило технології IoT доступнішими для широкого загалу.

На прикладі ранніх реалізацій IoT можна спостерігати, як концепція поступово переходила від теоретичних ідей до практичних застосувань. Це стало можливим завдяки синергії кількох технологічних досягнень, які надали необхідну інфраструктуру для функціонування IoT-систем. У результаті концепція IoT почала активно впроваджуватися в різні сфери, включаючи охорону здоров'я, промисловість, сільське господарство та інші.

Таким чином, поява концепції Інтернету речей стала результатом тривалої еволюції ідей та технологій, які виявилися спроможними об'єднати фізичний і цифровий світи. Сьогодні IoT займає центральне місце в розвитку інновацій і технологій, продовжуючи трансформувати наше життя та бізнес.

1.1.1 Перші приклади IoT-пристроїв

Перші приклади IoT-пристроїв стали важливими етапами в розвитку концепції Інтернету речей, демонструючи, як звичайні об'єкти можуть інтегруватися в інформаційні мережі. Ці пристрої заклали основи для подальших інновацій у цій сфері. Таблиця 1.2 містить перші приклади IoT-пристроїв, які стали основоположними етапами у розвитку концепції Інтернету речей. Вона ілюструє, як різні пристрої інтегрувалися в інформаційні мережі, закладаючи основи для подальших інновацій. У таблиці наведено інформацію про типи пристроїв, їх особливості та вплив на різні сфери життя, що відображає еволюцію IoT від перших експериментів до практичних рішень.

Одним із перших таких пристроїв був "розумний тостер", розроблений в 1982 році в університеті Карнегі-Меллона. Цей експеримент показав, що побутові прилади можуть бути підключені до комп'ютерної мережі. Тостер міг повідомляти користувачів про стан приготування хліба через комп'ютер, що свідчило про можливість автоматизації побутових процесів. Цей приклад став значущим символом початку розвитку IoT.

У 1999 році, під час презентації Кевіна Ештона, було продемонстровано використання технології RFID для ідентифікації об'єктів. Це дозволило автоматизувати процеси обліку та управління товарами, що стало основою для подальшого розвитку IoT в галузі логістики. Перші реалізації RFID-систем використовувалися на складах для відстеження товарів, що дозволяло знижувати витрати і підвищувати ефективність управління запасами.

Таблиця 1.2 - Перші приклади IoT-пристроїв

Пристрій	Рік	Опис
Розумний тостер	1982	Перший IoT-пристрій, що повідомляв про стан приготування хліба через комп'ютер.
RFID-системи	1999	Використання технології RFID для автоматизації обліку і управління товарами.
Системи "розумного дому"	2005	Рішення для контролю освітлення, температури та безпеки через мобільні додатки.
Розумний холодильник	2000-і	Холодильник, що моніторив запаси продуктів і формувал спски покупок.
Термостат Nest	2010	Пристрій, що вивчав звички користувача та автоматично налаштовував температуру для енергоефективності.
Системи моніторингу в сільському господарстві	2010-і	Пристрої для моніторингу ґрунту і кліматичних умов для оптимізації вирощування.

У 2005 році компанія Cisco представила рішення для "розумних будинків", що включали системи контролю освітлення, температури та безпеки. Ці системи давали можливість користувачам управляти своїм житлом за допомогою мобільних додатків. Це стало першим практичним застосуванням IoT для створення зручних і безпечних умов життя.

Ще одним раннім прикладом IoT-пристроїв є "розумний холодильник", розроблений компанією Samsung у 2000-х роках. Цей холодильник міг моніторити запаси продуктів і автоматично формувати списки покупок, які надсилалися на

мобільний телефон користувача. Це рішення продемонструвало, як IoT може змінити підходи до управління домашніми ресурсами.

У 2010 році була запущена платформа Nest, яка спеціалізувалася на розумних термостатах. Цей пристрій міг вивчати звички користувача та автоматично налаштовувати температуру в домі для підвищення енергоефективності. Nest стала важливою віхою в розвитку IoT, адже її успіх призвів до появи численних аналогічних пристроїв на ринку.

Також варто відзначити застосування IoT в сільському господарстві. У 2010-х роках почали з'являтися пристрої для моніторингу стану ґрунту, вологості повітря та інших параметрів, що дозволяли аграріям оптимізувати процеси вирощування культур. Ці рішення не лише підвищували врожайність, а й знижували витрати на ресурси.

Перші IoT-пристрої заклали основи для подальшого розвитку технології, продемонструвавши її можливості в різних сферах життя. Сьогодні IoT охоплює широкий спектр застосувань, від побутових до промислових рішень, і продовжує впливати на всі аспекти сучасного життя. Цей процес триває, а нові технології і рішення відкривають все більше можливостей для інтеграції пристроїв у глобальну інформаційну мережу [12].

1.1.2 Розвиток технологій, що підтримують IoT

Розвиток Інтернету речей (IoT) залежить від впровадження і вдосконалення ряду технологій, які забезпечують функціонування IoT-систем. Це включає в себе бездротові комунікації, обробку даних, мікропроцесорні технології, а також штучний інтелект і аналітику.

Однією з ключових технологій, що сприяють розвитку IoT, є бездротовий зв'язок. Стандарти, такі як Wi-Fi, Bluetooth, Zigbee та LoRaWAN, забезпечують зв'язок між IoT-пристроями та серверами. Wi-Fi дозволяє передавати великі обсяги даних на короткій відстані, що підходить для домашніх і офісних IoT-рішень. Bluetooth, у свою чергу, використовується для короткочасного зв'язку, наприклад, у

носимих пристроях. Zigbee та LoRaWAN, як технології з низьким споживанням енергії, забезпечують з'єднання між пристроями на великих відстанях, що важливо для розумних міст і сільського господарства.

Сенсори є ще однією основною складовою IoT. Вони здатні збирати дані про навколишнє середовище, такі як температура, вологість, тиск, рівень освітленості тощо. Сучасні сенсори стали компактнішими та дешевшими, що сприяє їх масовому використанню в IoT. Мікропроцесори також еволюціонували, забезпечуючи більшу обчислювальну потужність у малих пристроях. Наприклад, платформи на кшталт Raspberry Pi і Arduino стали популярними серед розробників, оскільки вони дозволяють швидко створювати прототипи IoT-рішень [2].

Обробка великих даних (Big Data) стала критично важливою для IoT, оскільки системи генерують величезні обсяги інформації. Розвиток технологій хмарних обчислень дозволив зберігати і обробляти ці дані на віддалених серверах, що значно знижує витрати на інфраструктуру. Хмара також забезпечує гнучкість і масштабованість, дозволяючи компаніям адаптувати ресурси відповідно до потреб.

Аналітика даних, зокрема використання алгоритмів машинного навчання, дозволяє виявляти закономірності в даних, що генеруються IoT-пристроями. Це, в свою чергу, відкриває нові можливості для автоматизації і оптимізації процесів. Наприклад, у промисловості IoT-датчики можуть передавати дані про роботу обладнання, що дозволяє передбачити необхідність ремонту ще до виникнення проблем.

Штучний інтелект став важливим елементом розвитку IoT, оскільки він забезпечує можливість аналізу даних у реальному часі та прийняття рішень на основі отриманих результатів. Застосування технологій ШІ у IoT дозволяє створювати адаптивні системи, які можуть самостійно коригувати свою роботу відповідно до змін у середовищі. Наприклад, розумні термостати, такі як Nest, використовують алгоритми машинного навчання для оптимізації споживання енергії, враховуючи звички користувачів [7].

З ростом популярності IoT з'явилася потреба в розробці стандартів і технологій безпеки. IoT-пристрої часто є вразливими до кіберзагроз, тому питання

безпеки даних і конфіденційності користувачів стало актуальним. Розробники повинні впроваджувати шифрування даних, аутентифікацію пристроїв і інші механізми захисту для забезпечення безпеки IoT-екосистем.

Розвиток технологій, що підтримують IoT, є комплексним процесом, який включає в себе бездротові комунікації, обробку даних, сенсори, мікропроцесори, штучний інтелект та заходи безпеки. Кожна з цих складових грає важливу роль у забезпеченні ефективності та безпеки IoT-рішень, що, в свою чергу, формує нові можливості для інновацій у різних сферах, від промисловості до повсякденного життя.

1.2 ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ІОТ

Інтернет речей (IoT) базується на концепції інтеграції фізичних об'єктів у глобальну інформаційну мережу, що дозволяє їм збирати, передавати та аналізувати дані. Принцип роботи IoT охоплює кілька ключових етапів, які забезпечують функціонування системи [3].

На першому етапі здійснюється збір даних, який здійснюється за допомогою сенсорів. Ці пристрої вимірюють різноманітні параметри навколишнього середовища, такі як температура, вологість, тиск і рух. Зібрані дані є первинною інформацією, що слугує основою для подальшої обробки.

Другим етапом є передача даних, яка відбувається через мережі. Датчики передають зібрані дані на сервери або хмарні платформи, використовуючи різні протоколи зв'язку. Вибір мережі може включати бездротові технології, такі як Wi-Fi, Bluetooth або Zigbee, а також дротові рішення, такі як Ethernet.

Після передачі дані потрапляють на сервери, де відбувається їх обробка та аналіз. Для цього використовуються алгоритми обробки великих даних, машинного навчання та аналітики, що дозволяє виявити закономірності, тренди та аномалії. Результати аналізу використовуються для прийняття рішень.

Візуалізація даних є наступним етапом, що надає користувачеві можливість отримувати інформацію через веб-інтерфейси або мобільні додатки. Це дозволяє

контролювати стан системи або об'єкта, приймати оперативні рішення та налаштовувати параметри.

Останнім етапом є автоматизація, що відбувається завдяки зворотному зв'язку між даними та системами управління. IoT може автоматизувати певні процеси, зменшуючи потребу в людському втручанні. Завдяки такій структурі принцип роботи IoT забезпечує інтеграцію фізичного і цифрового світу, створюючи нові можливості для моніторингу, управління та оптимізації різних процесів.

1.2.1 Основні компоненти IoT

Інтернет речей (IoT) складається з кількох ключових компонентів, які забезпечують його функціонування та ефективність. Основними з цих компонентів є датчики, мережі, хмарні платформи та пристрої управління

Таблиця 2.1 наводить основні компоненти Інтернету речей (IoT), які забезпечують його функціонування та ефективність. Ці компоненти включають датчики, мережі, хмарні платформи та пристрої управління. Вони взаємодіють між собою, формуючи інтегровану систему, здатну збирати, передавати та обробляти дані, що забезпечує автоматизацію та оптимізацію різних процесів у повсякденному житті та промисловості.

Таблиця 2.1 - Основні компоненти IoT-пристроїв

Компонент	Опис	Приклади використання
Датчики	Відповідають за збір даних з навколишнього середовища. Можуть вимірювати різні параметри.	Температурні, вологості, руху, якості повітря
Мережі	Забезпечують передачу даних між пристроями та серверами. Можуть бути бездротовими або дротовими.	Wi-Fi, Bluetooth, Zigbee, Ethernet
Хмарні платформи	Виконують функцію зберігання та обробки даних, зібраних IoT-пристроями.	Amazon Web Services, Microsoft Azure
Пристрої управління	Інтегрують і автоматизують процеси в IoT-системах, виконуючи команди на основі даних.	Розумні термостати, автоматизовані системи освітлення

Датчики є основою IoT, оскільки вони відповідають за збір даних з навколишнього середовища. Вони можуть бути різного типу, в залежності від параметрів, які потрібно виміряти, включаючи температурні датчики, які вимірюють температуру повітря або поверхонь, датчики вологості, що визначають рівень вологості в повітрі або ґрунті, датчики руху для виявлення присутності об'єктів та аналізатори якості повітря, які вимірюють забруднення. Датчики можуть працювати автономно або бути частиною комплексних систем, що збирають дані в реальному часі.

Мережі забезпечують передачу даних між IoT-пристроями та серверами. Вони можуть бути бездротовими, включаючи технології Wi-Fi, Bluetooth, Zigbee та LoRaWAN, які забезпечують комунікацію на коротких і середніх відстанях, або дротовими, такими як Ethernet, що забезпечують стабільний зв'язок. Вибір мережі критично важливий для надійності, швидкості та енергетичної ефективності систем [15].

Хмарні платформи виконують функцію зберігання та обробки даних, зібраних IoT-пристроями. Вони дозволяють масштабувати ресурси відповідно до змін у навантаженні, забезпечують надійне зберігання даних і пропонують рішення для захисту інформації, що важливо в умовах зростаючих кіберзагроз.

Пристрої управління, або контролери, інтегрують та автоматизують процеси в IoT-системах. Вони отримують дані від сенсорів, обробляють їх та виконують команди на основі алгоритмів. Пристрої управління можуть включати розумні термостати, які автоматично регулюють температуру, автоматизовані системи освітлення, що регулюють яскравість на основі руху, і системи безпеки, які контролюють доступ та сповіщають про аномалії.

Таким чином, основні компоненти IoT — датчики, мережі, хмарні платформи та пристрої управління — працюють разом, формуючи інтегровану систему, здатну ефективно збирати, передавати та обробляти дані, що забезпечує автоматизацію і оптимізацію процесів у повсякденному житті та промисловості.

1.2.2 Протоколи зв'язку

Протоколи зв'язку є критично важливими для ефективної передачі даних між IoT-пристроями, серверами та користувачами, оскільки вони визначають способи передачі інформації, обробки запитів і відповідей, а також застосування методів безпеки для забезпечення конфіденційності і цілісності даних. Серед найбільш поширених протоколів у сфері IoT виділяються MQTT, CoAP та HTTP.

Таблиця 2.2 наводить основні протоколи зв'язку, які використовуються в Інтернеті речей (IoT) для забезпечення ефективної передачі даних між пристроями, серверами та користувачами. Протоколи, такі як MQTT, CoAP і HTTP, мають свої унікальні характеристики, які визначають їхню доцільність у різних контекстах IoT. Розуміння особливостей цих протоколів дозволяє вибрати оптимальний варіант для конкретних вимог системи, враховуючи ресурси, швидкість та безпеку.

Таблиця 2.2 - Протоколи зв'язку в IoT

Протокол	Опис	Використання	Переваги	Недоліки
MQTT	Легковаговий протокол обміну повідомленнями, що використовує принцип "публікації/підписки".	Підключені пристрої, які працюють на батареях.	Низьке споживання енергії, підтримка різних рівнів надійності.	Може бути повільнішим у високонавантажених системах.
	Протокол, спроектований для обмежених пристроїв і малих мереж, використовує механізм запитів і відповідей.	Моніторинг і управління в реальному часі.	Низькі накладні витрати, підтримка UDP для зменшення затримок.	Обмежені можливості у порівнянні з HTTP.
CoAP	Стандартний протокол для передачі даних у веб-середовищі, популярний у веб-технологіях.	Взаємодія з веб-сервісами та API.	Широке використання, підтримка різноманітних веб-додатків.	Високе споживання ресурсів, більші накладні витрати.
HTTP				

MQTT (Message Queuing Telemetry Transport) є легковаговим протоколом обміну повідомленнями, розробленим для малошвидкісних і ресурсно обмежених мереж. Він працює за принципом "публікації/підписки", що дозволяє пристроям підписуватися на теми та отримувати оновлення без необхідності постійного опитування сервера. Це знижує обсяги переданих даних і енергоспоживання, що важливо для IoT-пристроїв, які працюють на батареях. MQTT також підтримує різні рівні надійності доставки повідомлень, що дозволяє користувачам обирати оптимальний баланс між швидкістю та безпекою.

CoAP (Constrained Application Protocol) розроблений для малих, обмежених пристроїв у мережах з низькими ресурсами. Він спроектований з урахуванням обмежень IoT-екосистем, що забезпечує ефективну передачу даних з малими накладними витратами. CoAP використовує механізм запитів і відповідей, схожий на HTTP, але з меншою кількістю даних у заголовках. Протокол підтримує UDP, що забезпечує меншу затримку при передачі даних, що важливо для реальних застосувань, таких як моніторинг і управління.

HTTP (Hypertext Transfer Protocol) є стандартним протоколом для передачі даних у веб-середовищі. Хоча він не є оптимальним для IoT через більші накладні витрати, його популярність обумовлена широким використанням у веб-технологіях. HTTP дозволяє IoT-пристроєм взаємодіяти з веб-сервісами та API, що робить його корисним у багатьох випадках, де потрібна інтеграція з уже існуючими веб-додатками. Однак використання HTTP може бути обмеженим через високе споживання ресурсів, особливо в умовах з обмеженою пропускнуою здатністю або енергоспоживанням.

Таким чином, протоколи зв'язку є важливими елементами IoT, оскільки вони забезпечують ефективну передачу даних між пристроями, серверами та користувачами. MQTT, CoAP та HTTP виконують різні функції в залежності від вимог системи, забезпечуючи оптимальні рішення для передачі інформації в контексті ресурсних обмежень, швидкості та безпеки. Розуміння та вибір відповідного протоколу є критичними для успішної реалізації IoT-проектів.

Таки чином, загальна інформація про IoT охоплює принципи роботи, основні компоненти та протоколи зв'язку, які є критичними для реалізації і функціонування IoT-систем. Збір даних, їх передача, обробка та аналіз, а також безпечна комунікація між пристроями формують основи для розвитку інтелектуальних рішень, що підвищують ефективність і зручність у різних сферах [11].

1.3. РОЗВИТОК ІОТ

Розвиток Інтернету речей (IoT) відбувається на фоні швидкого прогресу технологій, які формують нові можливості в багатьох сферах. Основними тенденціями, що впливають на цей розвиток, є інтеграція з технологіями Big Data, штучним інтелектом (AI) та впровадженням 5G.

Таблиця 3.1 ілюструє ключові тенденції, що впливають на розвиток Інтернету речей (IoT). Ці тенденції, такі як інтеграція з технологіями Big Data, розвиток штучного інтелекту (AI), впровадження 5G, а також акцент на стійкості та безпеці, формують нові можливості для інновацій у різних галузях. Розуміння цих тенденцій є важливим для оцінки майбутніх напрямків розвитку IoT та його впливу на суспільство.

Технології Big Data відіграють важливу роль у розширенні можливостей IoT, оскільки зростання кількості підключених пристроїв призводить до експоненційного збільшення обсягів даних, які вони генерують. Big Data дозволяє зберігати, обробляти та аналізувати ці великі обсяги інформації, виявляючи тренди і закономірності, що критично важливо для прийняття рішень у реальному часі. Це забезпечує оптимізацію процесів у таких сферах, як виробництво, логістика, охорона здоров'я та сільське господарство.

Таблиця 3.1 - Основні тенденції розвитку IoT

Тенденція	Опис	Вплив на IoT	Перспективи розвитку
Інтеграція з Big Data	Використання великих даних для обробки та аналізу інформації, згенерованої IoT-пристроями.	Оптимізація процесів у виробництві, логістиці, охороні здоров'я.	Зростання аналітичних платформ та рішень.
Розвиток штучного інтелекту	Автоматизація обробки даних і вдосконалення прийняття рішень через AI.	Поліпшення прогнозування та автоматизації рутинних завдань.	Збільшення застосування AI у різних сферах.
Впровадження 5G	Збільшення швидкості передачі даних та зменшення затримок для підключення більше пристроїв.	Розвиток розумних міст, автономних транспортних засобів.	Ширше впровадження IoT-рішень у повсякденному житті.
Зростання уваги до стійкості	Акцент на енергоефективності та екологічності технологій IoT.	Підвищення ефективності використання ресурсів.	Розробка нових стандартів і технологій для сталого розвитку.
Безпека	Важливість захисту даних та конфіденційності в умовах зростання кіберзагроз.	Впровадження нових протоколів безпеки та регулярні оновлення.	Покращення кібербезпеки у сфері IoT.

Штучний інтелект стає важливим компонентом IoT, оскільки автоматизує обробку даних і вдосконалює процеси прийняття рішень. AI здатний аналізувати дані, зібрані з різних сенсорів, для прогнозування подій і автоматизації рутинних завдань, таких як оптимізація споживання енергії в розумних будинках або передбачуване обслуговування обладнання в промисловості [6].

Впровадження 5G-технологій сприяє розвитку IoT завдяки високошвидкісній передачі даних і зменшеній затримці, що дозволяє підключати більше пристроїв одночасно. Це є критично важливим для реалізації концепцій розумних міст, автономних транспортних засобів та дистанційної медицини. Також зростає увага

до стійкості та енергоефективності, оскільки уряди і компанії прагнуть зменшити вплив на навколишнє середовище.

IoT-технології можуть використовуватися для моніторингу енергетичних витрат і управління ресурсами, що сприяє сталому розвитку. Безпека стає ще одним важливим аспектом, оскільки збільшення кількості підключених пристроїв супроводжується зростанням кіберзагроз. Виробники пристроїв та постачальники послуг зосереджуються на впровадженні заходів захисту даних і забезпечення конфіденційності через розробку нових протоколів безпеки та регулярні оновлення програмного забезпечення.

Основні тенденції розвитку IoT, такі як інтеграція з Big Data, розвиток AI, впровадження 5G, зростання уваги до стійкості та безпеки, створюють нові можливості для інновацій і трансформацій у різних галузях, відкриваючи перспективи для подальшого розвитку цієї технології.

Прогнози розвитку Інтернету речей (IoT) вказують на продовження швидкого зростання цієї технології в найближчі роки. Очікується, що до 2030 року кількість підключених IoT-пристроїв перевищить 30 мільярдів, що зумовлено зниженням вартості сенсорів і бездротових технологій. Це явище поширить використання IoT у різних секторах, включаючи побутові пристрої, промисловість, охорону здоров'я та інші.

Збільшення обсягів даних, які генерують IoT-пристрої, вимагатиме вдосконалення аналітичних рішень. Використання технологій Big Data та штучного інтелекту для обробки цих даних дозволить виявляти тренди та оптимізувати бізнес-процеси. Це надасть можливість зменшити витрати і підвищити ефективність управлінських рішень.

Впровадження 5G-технологій суттєво вплине на розвиток IoT завдяки високій швидкості передачі даних і зменшеній затримці. Це створить умови для впровадження нових рішень, таких як автономні транспортні засоби та медичні системи, що функціонують у реальному часі. Збільшення надійності з'єднань сприятиме масовому використанню IoT в різних галузях.

Формування нових екосистем стане важливим аспектом розвитку IoT. Компанії в цій сфері співпрацюватимуть з постачальниками програмного забезпечення, аналітичних платформ і сервісів безпеки, що дозволить створювати комплексні рішення, відповідні потребам різних галузей. Інтеграція IoT з іншими технологіями, такими як блокчейн, сприятиме розвитку більш безпечних і ефективних рішень.

Однак зростання кількості IoT-пристроїв створює виклики для регуляції та стандартизації. Очікується, що державні та міжнародні організації розроблять нові нормативні акти, спрямовані на захист даних та безпеку. Також будуть розроблені єдині стандарти, що забезпечать сумісність між пристроями від різних виробників [10].

Прогнози щодо розвитку IoT свідчать про значне зростання кількості підключених пристроїв, інтеграцію з аналітичними технологіями, формування нових екосистем і потребу в регуляції. Ці тенденції відкривають нові можливості для бізнесу і суспільства, забезпечуючи подальший розвиток IoT у різних сферах.

Розвиток Інтернету речей (IoT) супроводжується численними викликами та проблемами, які можуть вплинути на ефективність та безпеку впровадження цієї технології. Основні питання включають безпеку, сумісність, управління даними, регуляторний контроль та енергоспоживання.

Безпека є одним із ключових викликів у сфері IoT. Підключені пристрої часто стають мішенями для кіберзагроз, оскільки можуть мати вразливості, які використовуються зловмисниками для несанкціонованого доступу до мережі. Атаки можуть проявлятися у формах зламу пристроїв, викрадення даних або використання IoT-пристроїв для атак на інші системи. Відсутність єдиних стандартів безпеки для IoT-пристроїв ускладнює ситуацію, оскільки виробники не завжди реалізують належні заходи захисту.

Сумісність між різними IoT-пристроями та платформами є ще одним важливим аспектом. На ринку існує безліч виробників з різними технологіями та протоколами, що може призвести до труднощів в інтеграції пристроїв. Відсутність

єдиних стандартів ускладнює розробку програмного забезпечення, що працює з різними IoT-рішеннями, обмежуючи можливості масштабування технологій.

Значні обсяги даних, які генерують IoT-пристрої, ставлять питання про їх управління та обробку. Потреба в ефективних рішеннях для зберігання, обробки та аналізу великих обсягів інформації є критично важливою. Неправильне управління даними може призвести до втрати або неналежного використання інформації, що негативно вплине на бізнес-процеси. Крім того, виникають питання конфіденційності та захисту особистих даних, оскільки багато IoT-пристроїв збирають чутливу інформацію.

З ростом IoT-технологій постає потреба в нових регуляторних рамках, які можуть адекватно регулювати їх використання. Багато країн ще не мають чітких правил для забезпечення безпеки та конфіденційності даних, що може призвести до правових проблем для компаній, що впроваджують IoT-рішення. Відсутність єдиного підходу до регуляції на міжнародному рівні може створити додаткові труднощі для бізнесу, що прагне працювати на глобальних ринках [5].

Багато IoT-пристроїв функціонують на батарейках, і ефективне управління енергоспоживанням є важливим аспектом їх експлуатації. Зі збільшенням кількості підключених пристроїв виникає необхідність у нових рішеннях для забезпечення енергоефективності. Постійна зарядка або заміна батарей може стати серйозною перешкодою для широкого впровадження IoT [9].

Отже, розвиток IoT стикається з численними викликами, серед яких найзначнішими є безпека, сумісність, управління даними, регуляторний контроль та енергоспоживання. Подолання цих проблем є критично важливим для забезпечення ефективного та безпечного впровадження IoT у різних сферах. Успішне вирішення цих викликів відкриє нові можливості для інновацій та розширення застосування технології.

1.4. ІОТ-ПРИСТРОЇ

ІоТ-пристрої, або пристрої Інтернету речей, є фізичними об'єктами, що оснащені технологіями для збору, обробки та передачі даних через Інтернет. Вони слугують елементами екосистеми, що забезпечує інтеграцію реального світу з цифровими платформами. Основною метою ІоТ-пристроїв є автоматизація процесів, моніторинг стану об'єктів та дистанційне управління.

Кожен ІоТ-пристрій зазвичай містить сенсори або датчики, які фіксують інформацію про навколишнє середовище або стан самого пристрою. Зібрані дані можуть оброблятися локально або на віддалених серверах, після чого передаються через різноманітні мережі, такі як Wi-Fi, Bluetooth або мобільні мережі, для подальшого аналізу та використання.

ІоТ-пристрої характеризуються різноманітними функціональними можливостями: від простих вимірювальних пристроїв до складних систем, які взаємодіють з іншими пристроями та системами. Наприклад, термометри можуть вимірювати температуру в приміщенні і передавати ці дані для регулювання системи опалення, тоді як смарт-камери забезпечують відеоспостереження та виявлення руху.

Однією з ключових характеристик ІоТ-пристроїв є їхня здатність функціонувати автономно, використовуючи технології енергозбереження. Це дозволяє пристроям працювати тривалий час без необхідності в постійному підключенні до джерела живлення.

Крім того, ІоТ-пристрої можуть бути інтегровані в ширші системи, такі як смарт-будинки, промислові рішення або медичні системи, що забезпечує комплексне управління та моніторинг різних аспектів. Це, у свою чергу, сприяє підвищенню ефективності та зниженню витрат.

Класифікація ІоТ-пристроїв здійснюється за кількома критеріями, що дозволяє більш точно визначити їх функціональні можливості, сфери застосування та способи інтеграції в системи (таблиця 4.1). Основними критеріями класифікації є функціональність, застосування, спосіб з'єднання та тип оброблюваних даних.

За функціональністю IoT-пристрої можуть бути класифіковані на кілька категорій. Датчики є пристроями, що вимірюють фізичні величини, такі як температура, вологість, тиск чи світло, і передають зібрані дані для подальшого аналізу. Вони складають основу багатьох IoT-рішень, забезпечуючи інформацію про стан навколишнього середовища. Актори — це пристрої, які виконують фізичні дії на основі отриманих команд. Прикладами можуть бути електронні замки, що відкриваються за сигналом з мобільного додатку, або системи освітлення, які автоматично регулюють яскравість. Гейти (шлюзи) забезпечують з'єднання між IoT-пристроями та Інтернетом [8]. Вони здійснюють збір даних від сенсорів та передають їх до центральних систем для обробки.

Таблиця 4.1 - Класифікація IoT-пристроїв

Критерій	Категорія	Опис
Функціональність	Датчики	Пристрої, що вимірюють фізичні величини (температура, вологість, тиск)
	Актори	Пристрої, які виконують фізичні дії на основі отриманих команд
	Гейти (шлюзи)	Пристрої, що забезпечують з'єднання між IoT-пристроями та Інтернетом
Застосування	Побутові	Розумні термостати, системи безпеки, побутова техніка
	Промислові	Сенсори для моніторингу стану обладнання, системи управління енергією
	Медичні	Носимі пристрої для моніторингу здоров'я, медичні апарати
Спосіб з'єднання	Wi-Fi	Бездротове підключення через локальну мережу
	Bluetooth	Короткобездротові з'єднання для передачі даних на невеликі відстані
	LPWAN	Передача даних на великі відстані з низьким споживанням енергії
Тип оброблюваних даних	Аналогові	Збір та передача аналогових даних (температура, вологість)
	Цифрові	Обробка і передача цифрових даних (цифрові зображення)

IoT-пристрої також поділяються залежно від сфери їх використання. Побутові IoT-пристрої використовуються в домашніх умовах для автоматизації і контролю. До цієї категорії належать розумні термостати, системи безпеки, розумні лампи та побутова техніка. Промислові IoT-пристрої призначені для моніторингу і управління виробничими процесами. Прикладами є сенсори, які слезають за станом обладнання, та системи управління енергією, що оптимізують споживання ресурсів. Медичні IoT-пристрої використовуються для моніторингу здоров'я пацієнтів. Це можуть бути носимі пристрої, які контролюють серцевий ритм, або медичні апарати, що збирають дані про стан пацієнта та передають їх лікарям.

IoT-пристрої також класифікуються за способом з'єднання. Wi-Fi-пристрої підключаються до Інтернету через бездротову локальну мережу, що забезпечує високу швидкість передачі даних. Вони часто використовуються в домашніх умовах та в офісах. Bluetooth-пристрої використовують короткобездротові з'єднання для передачі даних на невеликі відстані. Це часто зустрічається у зв'язку з мобільними пристроями, такими як смарт-годинники або бездротові навушники. LPWAN-пристрої (Low Power Wide Area Network) забезпечують передачу даних на великі відстані з низьким споживанням енергії, що робить їх ідеальними для використання в умовах, де немає доступу до електрики [13].

Класифікація IoT-пристроїв також може ґрунтуватися на типі оброблюваних даних. Аналогові пристрої збирають та передають аналогові дані, такі як температура або вологість. Цифрові пристрої обробляють і передають цифрові дані, які використовуються для аналізу та обробки, наприклад, камери, що передають цифрові зображення.

Таким чином, класифікація IoT-пристроїв за різними критеріями є важливим аспектом для розуміння їх функціональних можливостей та потенційних областей застосування. Це сприяє оптимізації впровадження IoT-технологій у різних секторах, забезпечуючи інтеграцію між різними типами пристроїв. IoT-пристрої відіграють ключову роль у розвитку сучасних технологічних рішень.

1.4.1. ВПРОВАДЖЕННЯ ІОТ-ПРИСТРОЇВ

Впровадження IoT-пристроїв у сучасний світ стало важливою складовою розвитку технологій, що дозволяє інтегрувати фізичні об'єкти в інформаційні системи через Інтернет. Internet of Things (IoT) відкриває нові горизонти для автоматизації та оптимізації різних процесів, значно покращуючи якість обслуговування в різних секторах економіки та повсякденному житті. Сфери використання IoT охоплюють практично всі аспекти сучасного суспільства, включаючи освіту, охорону здоров'я, транспорт, сільське господарство та промисловість.

1.4.1.1 Сфери використання IoT-пристроїв

Впровадження IoT-пристроїв в сучасному світі демонструє значний вплив на різні сектори, завдяки їх здатності інтегрувати фізичні об'єкти в інформаційні системи через Інтернет. Основні сфери використання IoT охоплюють освіту, охорону здоров'я, транспорт, промисловість, сільське господарство та розумні міста. Кожна з цих сфер ілюструє унікальні можливості, що дозволяють підвищувати ефективність, безпеку та якість обслуговування. У таблиці 5.1 окреслені основні сфери використання IoT-пристроїв та їхні переваги.

Таблиця 5.1 - Сфери використання IoT-пристроїв та їхні переваги

Сфера використання	Приклади IoT-пристроїв	Користь
Освіта	Інтерактивні панелі, сенсори активності	Підвищення залученості студентів, адаптація навчального процесу
Охорона здоров'я	Носимі медичні монітори, фітнес-трекери	Моніторинг стану здоров'я в реальному часі, профілактика хвороб
Транспорт	Інтелектуальні транспортні системи	Оптимізація дорожнього руху, підвищення безпеки

Продовження табл. 5.1

Промисловість	Сенсори на обладнанні, системи управління	Моніторинг процесів, зниження витрат, підвищення продуктивності
Сільське господарство	Датчики вологості, автоматичні системи поливу	Оптимізація вирощування рослин, економія ресурсів
Розумні міста	Системи моніторингу повітря, управління освітленням	Поліпшення якості життя, екологічна безпека

У сфері освіти IoT-технології сприяють створенню інтерактивних навчальних середовищ, що підвищують залученість учнів. Оснащені датчиками та інтерактивними панелями, розумні класи дозволяють викладачам моніторити активність студентів і адаптувати навчальні матеріали відповідно до їхніх потреб. Крім того, IoT забезпечує можливість дистанційного навчання, що надає студентам доступ до ресурсів з будь-якої точки світу. Інтеграція IoT у навчальний процес також спрощує адміністративні функції, такі як облік відвідуваності та управління ресурсами.

IoT у медицині змінює підходи до моніторингу здоров'я пацієнтів. Носимі пристрої, включаючи фітнес-трекери, монітори серцевого ритму та пристрої для вимірювання рівня глюкози, здатні передавати дані лікарям у реальному часі. Це дозволяє медичним працівникам оперативно реагувати на зміни в стані здоров'я пацієнтів, а також здійснювати профілактичні заходи. Інтелектуальні медичні системи можуть аналізувати зібрані дані та надавати рекомендації, що підвищує ефективність лікування. Використання IoT також спрощує управління лікарнями, оптимізуючи процеси обліку, планування та моніторингу ресурсів.

IoT-технології в транспортному секторі призводять до значних покращень у безпеці та ефективності. Розумні транспортні системи, що використовують датчики та аналітичні алгоритми, здатні оптимізувати дорожній рух, знижуючи затори та покращуючи час доставки. Наприклад, датчики, встановлені на дорогах, можуть відстежувати швидкість руху транспортних засобів і передавати дані до центральних систем для аналізу. Інтелектуальні автомобілі, оснащені IoT-

пристроями, можуть обмінюватися інформацією про дорожню обстановку, що підвищує безпеку на дорогах.

У промисловості IoT використовуються для моніторингу виробничих процесів, управління ресурсами та підвищення ефективності. Сенсори, встановлені на обладнанні, можуть відстежувати його стан, виявляти несправності та передавати дані до системи управління. Це дозволяє оперативно реагувати на проблеми та планувати технічне обслуговування, що знижує витрати і підвищує продуктивність. IoT також сприяє реалізації концепцій "індустрії 4.0", де автоматизація та інтеграція даних відіграють ключову роль.

IoT-пристрої в сільському господарстві застосовуються для моніторингу стану ґрунту, контролю за поливом і управління врожаєм. Датчики, що вимірюють вологість, температуру та інші параметри, допомагають аграріям оптимізувати процеси вирощування рослин і підвищувати їхню продуктивність. Системи автоматичного поливу, що працюють на основі даних з сенсорів, дозволяють знижувати витрати на воду та енергію, зберігаючи природні ресурси.

Концепція "розумних міст" передбачає інтеграцію IoT у міську інфраструктуру для покращення життя громадян. Це може включати системи моніторингу якості повітря, управління трафіком, освітленням і утилізацією відходів. Датчики, встановлені по всьому місту, збирають дані, які використовуються для оптимізації міських процесів і покращення екологічної ситуації. Наприклад, системи управління освітленням можуть автоматично регулювати яскравість вулиць залежно від часу доби та кількості пішоходів.

Впровадження IoT-пристроїв у цих сферах демонструє значний потенціал для покращення якості життя, підвищення ефективності бізнес-процесів і оптимізації ресурсів. Розвиток технологій IoT відкриває нові можливості для інновацій і прогресу в різних секторах, вносячи істотні зміни в традиційні моделі управління та обслуговування.

Кейс-стаді є важливим інструментом для аналізу успішних проектів, що демонструють практичне застосування IoT-технологій у різних сферах. Вивчення

таких проектів дозволяє оцінити ефективність рішень, виявити можливі проблеми, а також визначити найкращі практики для подальшого використання.

У таблиці 5.2 представлені ключові кейс-стаді, що ілюструють практичне застосування IoT-пристроїв у різних сферах. Кожен проект демонструє унікальні рішення, що використовують IoT-технології, а також результати, яких вдалося досягти завдяки їх впровадженню. Вивчення цих прикладів допомагає оцінити потенціал IoT у покращенні якості життя, підвищенні ефективності бізнес-процесів та оптимізації ресурсів. Таблиця відображає різноманітність застосування IoT в сучасному суспільстві та його значення для інновацій і розвитку.

Таблиця 5.2 - Кейс-стаді впровадження IoT-пристроїв

Сфера	Назва проекту	Опис проекту	Основні результати
Розумні будинки	Розумний будинок	Система автоматизації для контролю освітлення, опалення та безпеки.	Зниження витрат на енергоресурси, підвищення безпеки.
Охорона здоров'я	Телемедицина	Носимі пристрої для моніторингу стану здоров'я пацієнтів.	Покращення якості медичного обслуговування, зниження витрат.
Промисловість	Інтелектуальний виробничий процес	Моніторинг і управління виробничими лініями за допомогою сенсорів.	Підвищення продуктивності на 20%, зниження витрат.
Сільське господарство	Розумне фермерство	Моніторинг умов вирощування культур з використанням датчиків.	Економія води, підвищення врожайності на 30%.
Розумні міста	Розумне місто	Інтеграція IoT у міську інфраструктуру для моніторингу якості повітря.	Зниження енергоспоживання на 25%.

Проект "Розумний будинок" передбачає створення системи автоматизації, яка дозволяє користувачам контролювати освітлення, опалення та безпеку свого житла через мобільні додатки. Встановлені датчики руху, камери спостереження та термостати збирають дані, які передаються на центральний сервер. Користувачі можуть налаштовувати режим роботи системи відповідно до своїх потреб, що сприяє зниженню витрат на енергоресурси та підвищенню рівня безпеки. Інтеграція голосових асистентів, таких як Amazon Alexa або Google Assistant, надає можливість управління пристроями за допомогою голосових команд.

Проект "Телемедицина" реалізує IoT-рішення, що дозволяє пацієнтам, які потребують регулярного моніторингу, залишатися вдома, отримуючи необхідні медичні послуги. Носимі пристрої, оснащені сенсорами, контролюють параметри здоров'я, такі як серцевий ритм, тиск та рівень глюкози. Дані автоматично передаються лікарям, що дозволяє швидко реагувати на зміни в стані пацієнтів. Цей підхід покращує якість медичного обслуговування та знижує витрати на госпіталізацію.

На великому заводі реалізовано проект "Інтелектуальний виробничий процес", у рамках якого впроваджено систему моніторингу та управління виробничими лініями за допомогою IoT-технологій. Сенсори, встановлені на обладнанні, збирають дані про його роботу в реальному часі, що дозволяє виявляти несправності на ранніх стадіях та планувати технічне обслуговування. Завдяки аналітиці даних, компанія змогла підвищити продуктивність на 20% і знизити витрати на обслуговування.

Проект "Розумне фермерство" впроваджує IoT-рішення для моніторингу умов вирощування культур. Датчики, що вимірюють вологість ґрунту, температуру повітря та освітленість, дозволяють аграріям своєчасно отримувати дані про стан рослин. Автоматизовані системи поливу, які базуються на отриманих даних, забезпечують оптимальний рівень вологості, що призводить до економії води і підвищення врожайності на 30%.

Проект "Розумне місто" реалізується в кількох великих містах, де IoT-технології інтегровані в міську інфраструктуру. Системи моніторингу якості

повітря, управління освітленням та контролю за трафіком допомагають знижувати рівень забруднення та покращувати безпеку. Наприклад, у місті Барселона було впроваджено систему розумного освітлення, яка автоматично регулює яскравість вулиць залежно від часу доби та присутності пішоходів, що знижує енергоспоживання на 25%.

Аналіз кейс-стаді впровадження IoT-пристроїв демонструє їх потенціал у покращенні якості життя, підвищенні ефективності бізнес-процесів і оптимізації ресурсів. Ці проекти ілюструють, як IoT-технології можуть змінювати традиційні підходи в різних сферах, відкриваючи нові можливості для інновацій і прогресу. Вивчення успішних прикладів також дозволяє виявити критично важливі фактори для ефективного впровадження IoT-рішень у майбутньому.

1.4.2. ПЕРСПЕКТИВИ РОЗВИТКУ ІОТ

Інтернет речей (IoT) є однією з найважливіших технологічних інновацій сучасності, що швидко змінює спосіб, яким люди взаємодіють із навколишнім світом. IoT охоплює різноманітні пристрої, які здатні збирати, аналізувати та обмінюватися даними через Інтернет. Це технологічне явище не лише спрощує повсякденні задачі, але й відкриває нові горизонти для бізнесу, соціальних відносин і сталого розвитку.

Одним із ключових аспектів, що підкреслює важливість IoT, є його здатність інтегрувати фізичний світ із цифровими технологіями. Це дозволяє реалізувати численні можливості, від автоматизації побутових завдань до оптимізації складних промислових процесів. Поглиблене впровадження IoT в різні сфери діяльності стає важливим чинником для підвищення ефективності, зниження витрат і покращення якості життя.

З розвитком нових технологій, таких як штучний інтелект (ШІ), 5G та блокчейн, перспективи для IoT стають ще більш обширними. Ці інновації не лише покращують продуктивність існуючих систем, але й відкривають нові можливості для їх застосування. Наприклад, завдяки мережам 5G, передача даних між IoT-

пристроями стає швидшою і надійнішою, що дозволяє реалізувати рішення в режимі реального часу.

Однак, незважаючи на численні переваги, розвиток IoT супроводжується певними викликами, такими як питання безпеки, конфіденційності даних і етики. Ці питання потребують ретельного розгляду та створення нових регуляторних рамок, щоб забезпечити баланс між інноваціями та захистом прав споживачів.

Екологічні аспекти також набувають особливого значення в контексті розвитку IoT. Технології IoT можуть відігравати важливу роль у збереженні ресурсів і зменшенні негативного впливу на навколишнє середовище. Завдяки точному моніторингу та управлінню ресурсами, IoT може сприяти зниженню витрат води, енергії та сировини, що в свою чергу позитивно вплине на екологічну ситуацію.

1.4.2.1 Інновації та нові технології в IoT

Розвиток Інтернету речей (IoT) супроводжується постійним впровадженням нових технологій та інновацій, які істотно розширюють його можливості. Ці нововведення не лише підвищують ефективність існуючих IoT-рішень, але й відкривають нові горизонти для їх застосування в різних сферах. Основними напрямками інновацій в IoT є використання штучного інтелекту (ШІ), мереж 5G, технологій блокчейн, аналітики даних та автоматизації. Таблиця 6.1 підсумовує ключові інновації та технології, що сприяють розвитку Інтернету речей (IoT). Ці інновації, такі як штучний інтелект, мережі 5G, технології блокчейн, аналітика даних і автоматизація, не лише підвищують ефективність існуючих рішень, але й відкривають нові можливості для їх застосування в різних галузях. Розуміння цих напрямків є критично важливим для подальшого впровадження IoT-технологій у повсякденне життя та бізнес-процеси.

Штучний інтелект є важливим компонентом розвитку IoT, оскільки дозволяє пристроям обробляти великі обсяги даних, отриманих від сенсорів, і приймати обґрунтовані рішення на основі цього аналізу. Застосування алгоритмів машинного

навчання дає змогу системам адаптуватися до змін у середовищі, оптимізувати роботу та передбачати потреби користувачів.

Таблиця 6.1 - Основні напрямки інновацій в IoT

Напрямок інновацій	Опис	Вплив на IoT	Приклади застосування
Штучний інтелект (ШІ)	Обробка великих обсягів даних для прийняття обґрунтованих рішень.	Поліпшення моніторингу та управління ресурсами.	Контроль життєвих показників у охороні здоров'я.
Мережі 5G	Висока швидкість передачі даних та зменшена затримка.	Підвищення ефективності у миттєвих застосуваннях.	Автономні транспортні засоби, розумні міста.
Технології блокчейн	Забезпечення безпеки та прозорості даних через дистрибуцію по вузлах.	Захист даних та управління правами доступу.	Фінансові транзакції, обмін чутливою інформацією.
Аналітика даних	Потужні інструменти для обробки та аналізу великих обсягів даних.	Підтримка прийняття рішень на основі даних.	Виявлення споживчих уподобань у бізнесі.
Автоматизація	Зменшення ручної праці та підвищення точності виконання завдань.	Оптимізація виробничих процесів і управління ресурсами.	Автоматизовані системи поливу у сільському господарстві.

Наприклад, у сфері охорони здоров'я IoT-пристрої, які контролюють життєві показники пацієнтів, можуть використовувати ШІ для виявлення аномалій у даних, що дозволяє лікарям швидше реагувати на критичні ситуації. У промисловості ШІ може допомогти у моніторингу обладнання, що зменшує ймовірність поломок і знижує витрати на обслуговування.

Технологія 5G відкриває нові можливості для IoT, забезпечуючи значно вищу швидкість передачі даних та зменшену затримку. Це особливо важливо для застосувань, де потрібен миттєвий обмін інформацією, таких як автономні транспортні засоби, інтелектуальні транспортні системи та віддалене управління промисловими процесами.

Завдяки 5G IoT-пристрої можуть безперебійно передавати дані в режимі реального часу, що сприяє покращенню прийняття рішень. Це також дозволяє збільшити кількість підключених пристроїв у межах однієї мережі, що є критично важливим для розумних міст та промислових рішень.

Блокчейн технології забезпечують безпеку даних, переданих між IoT-пристроями, шляхом дистрибуції даних по численним вузлам, що ускладнює їхнє несанкціоноване модифікування. Використання блокчейн-технологій в IoT забезпечує прозорість та надійність у сфері обробки даних, особливо в контексті фінансових транзакцій та обміну чутливою інформацією [14].

Блокчейн також може використовуватися для управління правами доступу до IoT-пристроїв, забезпечуючи контроль над тим, хто може отримувати дані та як їх можна використовувати. Це особливо важливо в умовах зростаючих загроз кібербезпеки.

Аналітика даних є ще одним ключовим аспектом розвитку IoT. Збір великих обсягів даних з IoT-пристроїв створює потребу в потужних аналітичних інструментах, здатних обробляти цю інформацію та виявляти корисні закономірності. Інструменти аналітики можуть допомагати в прийнятті рішень на основі даних, що підвищує ефективність операцій у різних сферах.

У бізнесі аналітика даних може використовуватися для виявлення споживчих уподобань, оптимізації виробничих процесів та управління ланцюгами постачання. У сфері охорони здоров'я вона може допомогти в аналізі результатів лікування та прогнозуванні захворювань на основі історії пацієнтів.

Автоматизація є важливою складовою IoT, оскільки дозволяє зменшити ручну працю та підвищити точність виконання завдань. IoT-пристрої можуть автоматизувати багато рутинних процесів, що зменшує витрати часу і ресурси. Наприклад, у промисловості автоматизовані системи можуть контролювати виробничі лінії, а в сільському господарстві автоматизовані системи поливу можуть реагувати на зміни в погодних умовах.

Таким чином, інновації та нові технології, що розвиваються в контексті IoT, мають значний потенціал для трансформації різних аспектів життя. Вони

дозволяють не лише підвищити ефективність і продуктивність, але й створюють нові можливості для бізнесу та покращують якість життя людей. Цей процес продовжуватиме розвиватися, оскільки з'являються нові технології та відкриваються нові горизонти для застосування IoT.

1.4.2.2 Вплив IoT на економіку та суспільство

Розвиток Інтернету речей (IoT) справляє суттєвий вплив на економіку та соціальну структуру суспільства. Цей вплив реалізується через підвищення продуктивності, зміну бізнес-моделей, поліпшення якості життя, а також через виникнення нових викликів, які потребують уваги та регулювання.

Одним із найбільш помітних аспектів впливу IoT на економіку є підвищення продуктивності у різних секторах. IoT-технології дозволяють автоматизувати численні процеси, що зменшує витрати часу та ресурсів. Наприклад, у промисловості впровадження IoT-систем для моніторингу виробничих процесів може призвести до зниження витрат на обслуговування обладнання та підвищення ефективності виробництва. У агросекторі IoT надає можливість аграріям контролювати умови вирощування культур, такі як вологість, температура та рівень добрив, що забезпечує збільшення врожайності за оптимальних витрат.

IoT сприяє появі нових бізнес-моделей, заснованих на даних та аналітиці. Підприємства використовують інформацію, зібрану з IoT-пристроїв, для розробки нових послуг і продуктів. Наприклад, компанії можуть впроваджувати моделі підписки на послуги, що дозволяють клієнтам сплачувати за доступ до даних або можливостей, які забезпечують IoT-пристрої. У сфері автомобільного транспорту, з розвитком IoT, виникають нові сервіси, такі як каршерінг і використання автономних транспортних засобів, що суттєво змінює підходи до володіння автомобілем. Такі інновації не лише підвищують ефективність використання ресурсів, але й зменшують викиди забруднюючих речовин, що позитивно впливає на екологічну ситуацію.

IoT має потенціал суттєво поліпшити якість життя людей. У сфері охорони здоров'я, наприклад, носимі пристрої дозволяють пацієнтам контролювати свої життєві показники, а лікарям — моніторити стан пацієнтів у реальному часі. Це призводить до підвищення якості медичного обслуговування та зменшення витрат на лікування. У побуті IoT-технології сприяють створенню розумних будинків, де автоматизуються процеси освітлення, опалення та безпеки. Це не лише забезпечує комфорт, але й знижує енергетичні витрати, що є важливим аспектом для багатьох сімей.

Крім економічних переваг, IoT також впливає на соціальну структуру суспільства. Наприклад, технології IoT можуть забезпечити доступ до медичних послуг у віддалених регіонах, де традиційна медицина може бути недоступною. Це зменшує нерівність у доступі до охорони здоров'я і покращує загальне благополуччя населення. У сфері освіти IoT дозволяє реалізувати нові формати навчання, такі як дистанційне навчання, що стає можливим завдяки інтерактивним пристроям і платформам. Це відкриває нові можливості для студентів з різних куточків світу отримати доступ до якісних освітніх ресурсів.

Однак, поряд із перевагами, IoT також несе певні ризики і виклики, які потребують уваги. Питання безпеки даних та конфіденційності стають усе більш актуальними в умовах зростаючої кількості підключених пристроїв. Потреба в надійних механізмах захисту інформації є критично важливою для уникнення зловживань і втрат даних. Важливо враховувати можливі соціальні наслідки автоматизації, які можуть призвести до втрати робочих місць у деяких галузях. Це вимагає розробки нових стратегій навчання та перепідготовки працівників для адаптації до змінюваних вимог ринку праці.

Вплив IoT на економіку та суспільство є багатогранним процесом, що потребує уважного управління. Ця технологія має потенціал суттєво поліпшити якість життя, підвищити продуктивність та створити нові бізнес-моделі. Однак, разом із цими перевагами, виникають нові виклики, які потребують комплексного регулювання та етичного осмислення для забезпечення стійкого розвитку суспільства.

1.4.2.3 Екологічні аспекти IoT: Ефективність ресурсів

Розвиток Інтернету речей (IoT) значно впливає на забезпечення ефективності використання природних ресурсів, що має важливі екологічні наслідки. Впровадження IoT-технологій дозволяє оптимізувати споживання ресурсів, зменшити викиди забруднюючих речовин та сприяти сталому розвитку.

Одним із ключових аспектів екологічної ефективності IoT є моніторинг та управління споживанням енергії. Використання розумних датчиків, які збирають дані про споживання енергії в реальному часі, дозволяє виявляти надмірне використання енергії та вживати заходи для його зменшення. Наприклад, розумні термостати можуть регулювати опалення та охолодження будівель, що забезпечує економію енергії до 30%. Це, в свою чергу, знижує витрати на електрику та зменшує викиди вуглекислого газу, що позитивно впливає на екологію.

IoT-технології також відіграють важливу роль у управлінні водними ресурсами. Системи моніторингу рівня вологості в ґрунті дозволяють аграріям здійснювати полив лише за потреби, що призводить до зменшення витрат води. У міських умовах IoT може використовуватися для виявлення витоків у водопровідних мережах, що сприяє зменшенню втрат води та економії цього цінного ресурсу.

Впровадження IoT у промисловість та транспорт також сприяє зниженню викидів забруднюючих речовин. IoT-системи забезпечують контроль за процесами виробництва, що дозволяє виявляти та усувати причини забруднення в реальному часі. Промислові підприємства можуть використовувати датчики для моніторингу викидів газів, що сприяє вжиттю заходів для їх зниження. Наприклад, автоматизовані системи можуть виявляти аномалії у викидах і реагувати на них, що значно підвищує екологічну відповідальність підприємств.

У транспортному секторі IoT-технології допомагають оптимізувати маршрути, знижуючи витрати пального та викиди CO₂. Використання розумних транспортних систем дозволяє зменшити затори на дорогах і підвищити

ефективність перевезень. Це не лише знижує витрати для перевізників, але й покращує якість повітря у містах.

Інтеграція IoT у різні сфери діяльності також сприяє досягненню цілей сталого розвитку. Технології IoT забезпечують можливості для збору та аналізу даних, що дозволяє ухвалювати обґрунтовані рішення в управлінні ресурсами. Розумні міста, які використовують IoT для моніторингу енергоспоживання, управління водними ресурсами та контролю якості повітря, здатні знижувати свій екологічний слід.

Однак для реалізації цих можливостей необхідно забезпечити належну інфраструктуру та зосередитися на питаннях безпеки і конфіденційності даних у зв'язку зі зростанням кількості підключених пристроїв. Забезпечення захисту даних є критично важливим, оскільки збільшення підключених IoT-пристроїв створює нові виклики для кібербезпеки. Тому важливо розробляти стратегії, що враховують як екологічні, так і технологічні аспекти впровадження IoT.

Таким чином, екологічні аспекти впровадження IoT важливі для забезпечення ефективності використання ресурсів. Моніторинг та управління споживанням енергії, води, а також зменшення викидів забруднюючих речовин можуть суттєво сприяти сталому розвитку, зберігаючи природні ресурси для майбутніх поколінь.

2. МЕТОДОЛОГІЯ РОЗРАХУНКУ ПРОДУКТИВНОСТІ МЕРЕЖІ

2.1 AWS IoT

2.1.1 Принцип роботи AWS IoT

AWS IoT (Internet of Things) — це масштабована та безпечна платформа, яка дозволяє легко підключати пристрої IoT, збирати, аналізувати та обробляти дані в реальному часі. Основна мета цієї платформи — забезпечення стабільного функціонування великих мереж підключених пристроїв. Для оцінки продуктивності мережі IoT, що працює з AWS IoT, необхідно врахувати специфіку архітектури платформи, методи обробки даних і масштабованість.

AWS IoT забезпечує інтеграцію пристроїв із хмарною платформою для обміну даними, їх обробки та зберігання. Основні принципи роботи платформи зосереджені на підключенні пристроїв, маршрутизації даних, забезпеченні безпеки та масштабованості. Пристрої IoT взаємодіють із хмарною інфраструктурою через стандартизовані протоколи зв'язку, такі як MQTT, HTTPS або WebSockets. AWS IoT Core дозволяє кожному пристрою реєструватися, отримувати унікальні сертифікати та криптографічні ключі для безпечної передачі даних.

Обмін повідомленнями здійснюється через брокер повідомлень, який маршрутизує дані за темами. Ця система дозволяє пристроям публікувати дані в певній темі або підписуватися на неї для отримання інформації. Наприклад, датчики можуть надсилати значення температури, які обробляються в реальному часі для автоматизації процесів або прийняття рішень. Хмара AWS IoT забезпечує безперервний моніторинг стану пристроїв та обробку повідомлень через функції обчислення в реальному часі. Використання таких інструментів, як AWS Lambda, дозволяє виконувати динамічну обробку даних безпосередньо під час їх надходження [16].

Система також підтримує збереження стану пристроїв навіть у разі втрати з'єднання, використовуючи функцію тіньового сховища. Це гарантує актуальність даних і стабільність роботи мережі, що є критично важливим для масштабних систем IoT.

AWS IoT надає можливості для аналізу даних, управління політиками безпеки та забезпечення високого рівня надійності мережі незалежно від кількості підключених пристроїв або обсягів трафіку [17].

Основні компоненти AWS IoT

8 AWS IoT Core: Дозволяє пристроям безпечно взаємодіяти з хмарними сервісами. Забезпечує управління з'єднаннями, маршрутизацію повідомлень і управління підписками.

9 Device Shadow: Структура для збереження актуального стану пристроїв, навіть якщо вони офлайн. Це полегшує управління системами з високою кількістю пристроїв.

10 AWS IoT Analytics: Інструмент для збору, зберігання і аналізу даних IoT. Він дозволяє оцінювати продуктивність мережі в режимі реального часу.

11 AWS IoT Device Defender: Система для оцінки продуктивності та безпеки пристроїв IoT.

12 AWS Lambda: Серверлес-функції для обробки даних, що надходять, у реальному часі, що значно підвищує продуктивність обчислень.

Методологія дослідження продуктивності мережі

Для оцінки продуктивності мережі IoT на базі AWS IoT використовуються кількісні та якісні методи аналізу, які включають:

1. Визначення метрик продуктивності

Пропускна здатність мережі (Bandwidth).

Затримки передачі даних (Latency).

Надійність передачі (Reliability): кількість втрат пакетів, повторів або помилок.

Масштабованість (Scalability): здатність обробляти зростаючу кількість підключених пристроїв.

Енергоспоживання (Energy Efficiency): важливо для пристроїв з обмеженим живленням.

2. Моделювання сценаріїв навантаження

Для моделювання роботи мережі IoT створюються сценарії з різними рівнями завантаження мережі. AWS IoT Core використовується для симуляції тисяч одночасно підключених пристроїв. Наприклад, за допомогою генераторів даних можна відправляти повідомлення з різними розмірами та частотою, моделюючи різноманітні умови реального використання.

3. Аналіз даних

AWS IoT Analytics використовується для збору та аналізу даних про продуктивність мережі. До аналізу включають:

- Статистичні методи для обробки великих обсягів даних.
- Візуалізацію метрик у динаміці.
- Машинне навчання для виявлення аномалій у роботі мережі.

4. Оцінка масштабованості

Масштабованість мережі оцінюється за допомогою тестування під різними сценаріями, які включають:

- Збільшення кількості підключених пристроїв до десятків тисяч.
- Обробку даних із різною частотою передачі.

2. Експериментальна перевірка методології

Проводиться на основі наступних етапів:

- Налаштування тестового середовища в AWS IoT Core.
- Підключення емуляторів пристроїв.
- Збір даних про продуктивність мережі.

Новизна підходу

Запропонована методологія акцентує увагу на інтеграції сучасних інструментів AWS IoT для забезпечення ефективного моніторингу та оцінки продуктивності мережі IoT. Це включає використання адаптивних моделей

машинного навчання для прогнозування навантаження на мережу, що дозволяє підвищити ефективність управління мережею [18].

Практичне значення дослідження

Розроблена методологія дозволяє оптимізувати роботу IoT-систем, знижувати витрати на інфраструктуру та забезпечувати високий рівень надійності для мереж із великою кількістю пристроїв. Застосування AWS IoT створює універсальну основу для масштабованих та адаптивних рішень у сфері Інтернету речей.

Приклади використання IoT у сучасних системах.

Розумні автомобілі.

Сучасні транспортні засоби підключаються до Інтернету за допомогою різних пристроїв, таких як відеореєстратори, інформаційно-розважальні системи або вбудовані шлюзи. Ці системи збирають дані про швидкість, гальмування, рівень пального та інші параметри, щоб контролювати стан автомобіля та поведінку водія. Застосування таких технологій включає: контроль витрат пального та зменшення витрат для автопарків; відстеження манери керування підлітків їхніми батьками; автоматичне сповіщення близьких у разі аварії; прогнозування та попередження технічних несправностей автомобіля [19].

Розумний дім.

Технології для дому спрямовані на підвищення безпеки, комфорту та енергоефективності. Наприклад, «розумні» розетки допомагають керувати споживанням електроенергії, а інтелектуальні термостати забезпечують контроль температури. Системи безпеки, що включають камери, датчики води чи диму, захищають житло. Можливості таких систем: автоматичне вимкнення невикористовуваних електроприладів; дистанційне управління орендованим житлом; пошук загублених речей, таких як ключі; автоматизація щоденних завдань, наприклад прибирання чи приготування кави.

Розумні міста.

IoT допомагає оптимізувати міську інфраструктуру, покращуючи екологічну ситуацію та якість життя. Наприклад, системи моніторингу оцінюють рівень

забруднення повітря та радіації, а «розумне» освітлення знижує витрати на електроенергію. Також IoT використовується для: діагностики стану мостів, трубопроводів та доріг; оптимізації використання паркувальних місць; покращення управління комунальними послугами.

Розумні будівлі.

Комерційні об'єкти та університетські кампуси впроваджують IoT-технології для підвищення ефективності роботи. Такі системи допомагають: економити електроенергію; зменшувати витрати на технічне обслуговування; раціонально використовувати робочі простори.

Технології IoT активно розвиваються та знаходять застосування у багатьох сферах, роблячи повсякденне життя більш зручним та екологічним [20].

2.1.2 Принцип роботи сервісів

AWS IoT складається з кількох ключових сервісів, які взаємодіють для забезпечення підключення, обробки даних і управління пристроями IoT. Принципи роботи кожного сервісу визначають їхню роль у загальній архітектурі системи.

Основний сервіс для підключення пристроїв до хмари та обміну повідомленнями. IoT Core забезпечує:

- Маршрутизацію повідомлень між пристроями через систему тем. Кожен пристрій або група пристроїв підписуються на відповідні теми, що дозволяє ефективно передавати дані між ними.
- Реєстрацію пристроїв із використанням сертифікатів для забезпечення безпечної взаємодії.
- Інтеграцію з іншими сервісами AWS, такими як Lambda або DynamoDB, для обробки і зберігання даних.

AWS IoT Device Shadow

Цей сервіс дозволяє створювати "тіньові" копії стану пристроїв.

- Зберігає останній відомий стан пристрою навіть у випадку втрати з'єднання.

- Дозволяє користувачам або системам змінювати стан пристрою через тіньову копію, яка синхронізується з пристроєм після відновлення зв'язку.
- Використовується для управління великими мережами, де пристрої можуть бути недоступні в реальному часі.

AWS IoT Analytics

Сервіс для збору, обробки і аналізу даних, що надходять від пристроїв IoT.

- Збирає дані з IoT Core, фільтрує їх і перетворює у придатний для аналізу формат.
- Підтримує інтеграцію з інструментами машинного навчання для прогнозування і оптимізації роботи системи.
- Дозволяє створювати звіти та візуалізувати ключові показники продуктивності.

AWS IoT Device Defender

Сервіс для моніторингу безпеки та продуктивності мережі IoT.

- Аналізує поведінку пристроїв для виявлення аномалій або порушень політик безпеки.
- Здійснює аудит налаштувань пристроїв, перевіряючи їх відповідність рекомендованим стандартам.
- Дозволяє автоматично вживати заходи, наприклад, блокувати підозрілі пристрої.

AWS Lambda

Використовується для виконання серверлес-функцій у реальному часі.

- Обробляє дані, які надходять від пристроїв IoT, без необхідності створення або управління серверами.
- Дозволяє створювати автоматичні правила для обробки подій, наприклад, реагування на зміни стану пристрою або запуск алгоритмів аналізу.

Amazon DynamoDB

Сервіс для зберігання структурованих даних.

- Використовується для зберігання історичних даних, що надходять від пристроїв.

- Забезпечує високу швидкість зчитування і запису даних, що важливо для систем IoT з великим навантаженням.

Amazon S3

Хмарне сховище для великих обсягів даних.

- Використовується для зберігання файлів, журналів і резервних копій даних IoT.
- Забезпечує довготривале збереження даних із можливістю доступу до них у будь-який час.

Координація цих сервісів дозволяє створювати адаптивні, безпечні та масштабовані IoT-системи, які можуть ефективно обробляти великі обсяги даних і забезпечувати безперервну роботу підключених пристроїв [21].

Очевидно, як було зазначено раніше, комплексний підхід до вирішення проблеми безпеки вже зараз можна побачити на прикладі сучасних хмарних обчислень. Давайте більш детально розглянемо в цьому плані технології Amazon IoT. Хмара Amazon Web Services (AWS) доступна для тестування в рамках «безкоштовного рівня». Наприклад, для AWS IoT, протягом першого року після реєстрації, буде доступно 250 000 повідомлень (опублікованих або доставлених) на місяць. Для безлічі інших сервісів доступна лінійка подібних лімітів. На жаль, Amazon не дає можливості «бездумно» експериментувати протягом пробного використання. Користувач цієї хмари завжди повинен давати собі звіт, що запускає або як генерує певні дії. Все, що буде перевищувати поріг безкоштовного використання доведеться оплатити згідно з діючими тарифами.

Реєстрація в хмарі AWS досить проста. Однак, відразу сервіс запросить \$1 USD з картки клієнта для підтвердження можливості оплати рахунків цією картою. Також для нового користувача сервіс перевірить існування реального телефону, і тут його може очікувати невеликий сюрприз. Підтвердити телефон можна автоматично після дзвінка сервісу. Але для власників смартфонів, дзвінок може пролунали не в додатку телефону, а в Viber. Кількість введення коду підтвердження обмежена, якщо не здогадатися де в Viber потрібно ввести заповітні цифри, можна просто вичерпати ліміт і очікувати порядку доби до нової спроби.

Ось, чомусь так і сталося. У будь-якому випадку, техпідтримка Amazon завжди допоможе, навіть на безкоштовному тарифі. Описавши проблему в чаті, буквально за лічені хвилини, цілком можна вирішити подібне питання після живого дзвінка оператора. Можна припустити, що і всі інші питання по роботі з сервісом можна дуже оперативно вирішувати з техпідтримкою. А в масштабах використання ресурсів хмари, коли буде потрібно безпрецедентну якість, сервіс надає платні тарифи технічної підтримки.

Отже, починаючи працювати з хмарою, багато хто відразу приступають до експериментів з віртуальними машинами, файловими сховищами і т.п. але у нас завдання розглянути сервіс AWS IoT і зрозуміти наскільки таке рішення є захищеним. Оскільки AWS IoT-це лише частина сервісів Хмари Amazon, то так чи інакше цей сервіс інтегрується з багатьма іншими рішеннями Хмари (AWS Services). Для цього існує механізм rules Engine, який дозволяє побудувати набір правил взаємодії підключених пристроїв та інших ресурсів хмарних обчислень. Наприклад, можна реалізувати взаємодію AWS IoT і сервісу запуску програмного коду Aws Lambda, нереляційною базою даних Amazon DynamoDB або сервісом обробки і аналізу поточкових даних Amazon Kinesis Streams [22].

2.2 Фактори, що впливають на продуктивність Web-служб

Продуктивність Web-служб є критично важливим параметром, який впливає на якість роботи системи, рівень задоволення користувачів і загальну ефективність бізнес-процесів. У контексті роботи з IoT-платформами, такими як AWS IoT, продуктивність визначає, наскільки швидко й ефективно система здатна обробляти запити, передавати дані та підтримувати підключення пристроїв.

На продуктивність Web-служб впливає низка факторів, які можна умовно розділити на апаратні, програмні, архітектурні та зовнішні.

Апаратні фактори

Обчислювальні ресурси відіграють ключову роль у забезпеченні швидкої роботи Web-служб. Продуктивність залежить від таких параметрів:

- Потужність серверів: кількість ядер процесора, обсяг оперативної пам'яті та швидкість зберігання даних впливають на обробку запитів і виконання завдань.
- Пропускна здатність мережі: швидкість передачі даних між серверами, клієнтами та пристроями IoT впливає на час відповіді.
- Інфраструктура зберігання: SSD-накопичувачі забезпечують вищу продуктивність у порівнянні з HDD, особливо для операцій читання/запису великих обсягів даних.

Програмні фактори

Продуктивність Web-служб залежить від ефективності програмного забезпечення та оптимізації його роботи.

- Оптимізація коду: погано написаний або нефункціональний код може значно знизити продуктивність.
- Алгоритми обробки запитів: вибір алгоритмів для маршрутизації, обробки та аналізу даних впливає на швидкість роботи.
- Базы даних: продуктивність залежить від архітектури баз даних, індексування, стратегій кешування та розподілу навантаження.
- Масштабованість програмного забезпечення: можливість обробляти зростаючу кількість запитів за рахунок горизонтального або вертикального масштабування.

Архітектурні фактори

Вибір архітектури Web-служб визначає, наскільки ефективно система здатна працювати під час великого навантаження.

- Архітектура мікросервісів: дозволяє децентралізувати обробку запитів, що покращує масштабованість і надійність системи.
- Кешування: використання кешу для зберігання часто використовуваних даних зменшує навантаження на сервери.
- Балансування навантаження: рівномірний розподіл запитів між серверами дозволяє уникнути перевантаження окремих вузлів.

Принципи REST або GraphQL: вибір протоколу передачі даних впливає на швидкість і зручність роботи [23].

Зовнішні фактори

Робота Web-служб також залежить від умов, що перебувають поза контролем розробників.

- Мережеві затримки: залежність від швидкості Інтернет-з'єднання клієнтів та пристроїв.
- Кількість користувачів: зростання кількості одночасних запитів може викликати затримки у відповіді.
- Динаміка трафіку: пікові навантаження у певні періоди часу.
- Середовище виконання: хмарні сервіси або локальні сервери можуть мати різні характеристики продуктивності.

Інші фактори

- Безпека: використання протоколів шифрування (TLS/SSL) впливає на продуктивність через додаткові витрати обчислювальних ресурсів.
- Моніторинг і управління: своєчасне виявлення проблем і оптимізація роботи системи.
- Інтеграція з іншими сервісами: взаємодія з зовнішніми API може знижувати швидкість через затримки у відповідях.

Продуктивність хостингу значною мірою залежить від рівня апаратного забезпечення. Сучасне й потужне обладнання забезпечує швидку обробку запитів, що сприяє покращенню позицій сайту в пошукових системах. Чим менше часу витрачається на генерацію та передачу даних, тим краще це оцінюється пошуковими алгоритмами.

Варто інвестувати в якісний хостинг із сучасною апаратною базою. Безкоштовні сервіси, як правило, не забезпечують належного рівня стабільності та швидкості, оскільки їхнє обладнання часто застаріле або перевантажене. Для тривалого та успішного функціонування ресурсу варто обирати надійного провайдера, навіть якщо це вимагає додаткових витрат. При виборі тарифного плану рекомендується звертати увагу на характеристики серверів, зокрема обсяг

дискового простору та наявність технічної підтримки. Зазвичай ці дані доступні на офіційному сайті хостинг-компанії [24].

Деякі хостинг-провайдери пропонують модуль PageSpeed, який допомагає покращити продуктивність сайту. Він оптимізує графіку, аналізує HTML-код і надає рекомендації щодо його вдосконалення. Цей інструмент може стати корисним доповненням до основного функціоналу хостингу. Наявність інструментів серверного кешування, таких як Memcached, OpCache та Redis, значно підвищує швидкість роботи сайту. Ці технології дозволяють зберігати повторювані операції в оперативній пам'яті, знижуючи навантаження на сервер. Завдяки цьому динамічні елементи сайту завантажуються швидше, оскільки дані не витягуються щоразу з жорстких дисків.

Доступність сайту безпосередньо залежить від аптайму серверів. Аптайм відображає відсоток часу, протягом якого сайт залишається онлайн. Наприклад, аптайм у 95% означає, що сервер може бути недоступний протягом 5% часу на рік. Це еквівалентно 438 годинам простою, що може негативно вплинути на відвідуваність та довіру до ресурсу.

Для забезпечення надійної роботи рекомендується вибирати хостинг із високим рівнем аптайму (наприклад, 99.9%). Це дозволить мінімізувати простої та забезпечити стабільний доступ до сайту для користувачів.

Швидкість завантаження сайту залежить не лише від оптимізації контенту та коду, а й від якості хостингу. Вибір потужного обладнання, використання технологій кешування та забезпечення безперебійної роботи сервера — це ключові аспекти для досягнення високої продуктивності вашого ресурсу.

Для підвищення продуктивності Web-служб розробники використовують комбінований підхід, який включає оптимізацію апаратної інфраструктури, впровадження ефективних алгоритмів обробки даних, вдосконалення архітектури та моніторинг зовнішніх факторів. Це дозволяє створювати високопродуктивні системи, здатні забезпечувати стабільну роботу в умовах динамічного навантаження.

Забезпечення безпеки передачі даних в умовах відкритого Інтернет-простору є ключовим завданням, яке необхідно враховувати під час розробки та експлуатації будь-якої технології, пов'язаної з Інтернетом речей (IoT). На відміну від традиційних підходів до побудови Інтернет-комунікацій, IoT-мережі перебувають на початковому етапі свого розвитку. На перший погляд може здатися, що для забезпечення безпеки IoT достатньо гарантувати надійність серверних систем, користувацьких пристроїв і шифрування даних. Однак це не зовсім так.

Наприклад, можна створити систему, в якій дані з камери домашнього асистента шифруються під час передачі на сервер, де вони розпаковуються та архівуються в захищеному сховищі. Проте до цього архіву може бути відкритий доступ через незахищений протокол, такий як FTP. У цьому випадку зловмиснику не потрібно зламувати самі пристрої чи сервери – достатньо скористатися відомими вразливостями протоколу. Таким чином, безпека – це багатогранна концепція, де не можна ігнорувати навіть найменші нюанси. Захист IoT-пристроїв втрачає сенс, якщо є можливість отримати доступ до відкритих даних через вразливості операційної системи IoT-шлюзу чи іншого елемента в IoT-ланцюжку [25].

Розробники таких складних розподілених систем, як IoT, повинні передбачати надійні рішення для захисту всієї інфраструктури. Це означає не лише унеможливлення атак на пристрої, але й забезпечення конфіденційності персональних даних користувачів і захист інформації про власників пристроїв. Під час проєктування IoT-системи слід

комунікація між IoT-пристроями;

надійне зберігання, обробка та представлення даних.

Використовуючи сучасні платформи, наприклад AWS IoT, можна «з коробки» отримати готове рішення для забезпечення безпеки взаємодії пристроїв. Додаткові сервіси AWS також допомагають забезпечити захист даних та програмних компонентів. Проте слід пам'ятати, що вузьким місцем IoT лишається пропускну здатність каналів зв'язку, оскільки стабільний доступ до Wi-Fi, 3G або LTE доступний не всюди.

У промислових чи домашніх мережах можна гарантувати стабільну швидкість передачі даних, але для мобільних пристроїв це завдання складніше. У таких умовах шифрування може стати викликом, оскільки ускладнює пристрої та збільшує розмір пакетів даних. Наприклад, складно уявити реалізацію сучасних алгоритмів шифрування на 8-бітному мікроконтролері Arduino Uno. Але не варто забувати про закон Мура і швидкий прогрес у розвитку електроніки [26].

2.3 Опис системи та розрахунок пропускної здатності

Пропускна здатність системи є ключовим параметром, який визначає її здатність обробляти та передавати дані у мережі. У контексті IoT-систем, зокрема побудованих на основі AWS IoT, пропускна здатність визначає ефективність взаємодії між пристроями, шлюзами та хмарними сервісами. Вона характеризується кількістю даних, які система може обробити за одиницю часу, і впливає на продуктивність усієї інфраструктури.

Опис системи

Розроблена система моніторингу IoT-пристроїв базується на використанні AWS IoT Core та супутніх сервісів, таких як AWS Lambda, Amazon DynamoDB, та AWS IoT Analytics. Архітектура системи побудована з урахуванням принципів масштабованості, безпеки та мінімізації затримок.

Система складається з наступних основних компонентів:

- Пристрої IoT: датчики та виконавчі пристрої, які передають дані через MQTT або HTTPS.
- Шлюзи IoT: локальні пристрої, що збирають дані з IoT-пристроїв і передають їх у хмару через AWS IoT Core.
- Хмарна інфраструктура: AWS IoT Core обробляє та маршрутизує повідомлення, використовуючи тему для кожного типу даних. Інші сервіси AWS виконують функції зберігання, аналізу та візуалізації даних.
- Інтерфейс користувача: веб-додаток, який відображає стан пристроїв у реальному часі, графіки, звіти та історичні дані.

Методологія розрахунку пропускної здатності

Розрахунок пропускної здатності базується на аналізі обсягів даних, які передаються у системі, частоті обміну повідомленнями та обмеженнях інфраструктури. Основні параметри, які враховуються:

- Середній розмір повідомлення: дані від пристроїв зазвичай мають невеликий розмір (декілька десятків або сотень байтів).
- Частота передачі даних: визначається кількістю повідомлень від одного пристрою за секунду.
- Кількість пристроїв: загальна кількість IoT-пристроїв у системі.
- Затримки в мережі: впливають на час доставки повідомлень.
- Обмеження AWS IoT Core: наприклад, максимальна кількість одночасних з'єднань або оброблених повідомлень.

Формула для оцінки пропускної здатності системи виглядає так:

$$B=n \cdot f \cdot s$$

де:

- B — пропускна здатність у байтах за секунду,
- n — кількість пристроїв,
- f — частота передачі повідомлень від одного пристрою (у повідомленнях за секунду),
- s — середній розмір одного повідомлення (у байтах).

Приклад розрахунку

Припустимо, що система має 10 000 IoT-пристроїв. Кожен пристрій надсилає дані зі швидкістю 1 повідомлення на секунду, а середній розмір одного повідомлення становить 512 байтів. Тоді:

$$B=10,000 \cdot 1 \cdot 512=5,120,000 \text{ байт/с (5 МБ/с)}.$$

Це означає, що система повинна бути здатна обробляти щонайменше 5 МБ даних за секунду, щоб забезпечити стабільну роботу.

Аналіз обмежень і оптимізація

Продуктивність системи може бути обмежена такими факторами:

- Пропускна здатність мережі, яка залежить від фізичних характеристик з'єднання між пристроями та хмарою.

- Максимальна швидкість обробки повідомлень у AWS IoT Core.
- Затримки під час збереження даних у базі даних або виконання аналітичних завдань.

Для оптимізації пропускної здатності застосовуються такі підходи:

- Агрегація даних: зменшення кількості повідомлень шляхом об'єднання кількох даних у один пакет.
- Кешування: використання локального кешу для зберігання проміжних даних.
- Використання компресії: зменшення розміру даних перед передачею.
- Розподілене обчислення: використання AWS Lambda для паралельної обробки великих обсягів даних.

Розрахунок пропускної здатності є критичним етапом під час проектування системи IoT, оскільки дозволяє забезпечити її стабільну роботу, адаптацію до змінних умов і ефективне використання ресурсів [27].

2.4 Середня година відкликання

Середня година відкликання (Mean Time to Respond, MTTR) — це ключовий показник ефективності системи моніторингу та управління IoT. Цей параметр визначає середній час, необхідний для реагування на подію чи проблему в системі після її виявлення. Для IoT-платформ, таких як AWS IoT, MTTR охоплює кілька аспектів, зокрема виявлення проблеми, передавання інформації до відповідного модуля, обробку даних і виконання коригувальних дій.

Фактори, що впливають на MTTR

1. Час виявлення проблеми

Залежить від частоти моніторингу системи, точності налаштувань сповіщень та ефективності алгоритмів аналізу даних. IoT-платформи

використовують механізми реального часу для виявлення аномалій, що знижує час виявлення.

2. Швидкість передачі даних

Впливає на час доставки повідомлення від пристрою до хмарної інфраструктури. Затримки можуть виникати через мережеву інфраструктуру, протоколи передачі (MQTT, HTTPS) або недостатню пропускну здатність.

3. Обробка даних

Час, потрібний для аналізу повідомлення в системі. Використання серверлес-функцій (AWS Lambda) дозволяє зменшити затримки, забезпечуючи обробку в реальному часі.

4. Час виконання коригувальних дій

Визначається складністю дії (наприклад, перезавантаження пристрою, зміна конфігурації) та швидкістю виконання команд пристроєм.

Методика обчислення MTTR

Наприклад, якщо система за день обробила 10 подій із такими часами відкликання: 15 хвилин, 20 хвилин, 12 хвилин і так далі, середній час розраховується як середнє арифметичне цих значень.

Приклад розрахунку

Припустимо, що система зафіксувала такі часи відкликання для 5 подій (у хвилинах): 12, 15, 18, 10, 14. Середній час відкликання:

$$MTTR = 12 + 15 + 18 + 10 + 14 = 13.8 \text{ хвилин}$$

Зниження MTTR

Зменшення середньої години відкликання є важливим завданням для підвищення ефективності системи. Основні підходи включають:

- Автоматизація обробки подій: використання AWS IoT Rules Engine для автоматичного виконання дій у разі виявлення певної події.
- Оптимізація алгоритмів моніторингу: впровадження алгоритмів машинного навчання для швидшого виявлення аномалій.

- Покращення комунікації: використання високошвидкісних протоколів, таких як MQTT, для мінімізації затримок передачі даних.
- Масштабування ресурсів: додавання обчислювальних потужностей для обробки великої кількості подій одночасно.

Роль MTTR у забезпеченні продуктивності системи

Скорочення MTTR дозволяє:

- Зменшити втрати, пов'язані з простоєм системи.
- Підвищити рівень довіри до системи з боку користувачів і клієнтів.
- Оптимізувати використання ресурсів, забезпечуючи швидке усунення несправностей.

Середня година відкликання є важливим показником стабільності IoT-системи, що забезпечує своєчасне реагування на проблеми та підтримує її безперервну роботу.

2.5 Пропускна здатність при використанні кешуючого проксі-сервера.

Пропускна здатність при використанні кешуючого проксі-сервера є одним із ключових параметрів, що визначає ефективність роботи мережевої системи. Кешуючий проксі-сервер виконує роль посередника між клієнтами та основними сервісами, зберігаючи копії часто запитуваних даних. Це дозволяє значно зменшити навантаження на основні сервери, підвищити швидкість обробки запитів та покращити загальну продуктивність мережі [16].

Принцип роботи кешуючого проксі-сервера

Основна функція кешуючого проксі-сервера полягає у тимчасовому зберіганні (кешуванні) результатів запитів клієнтів до основних серверів. Коли клієнт надсилає запит, сервер перевіряє, чи є відповідні дані у локальному кеші. Якщо дані доступні (так звана *кеш-потрапляння*), вони негайно повертаються клієнту, минаючи звернення до основного сервера. У разі відсутності даних (так звана *кеш-промах*), запит передається до основного сервера, після чого отримані дані кешуються для подальшого використання.

Фактори, що впливають на пропускну здатність

1. Розмір кешу. Обсяг пам'яті, виділеної для зберігання кешованих даних, має значний вплив на продуктивність проксі-сервера. Більший кеш дозволяє зберігати більше унікальних запитів, що збільшує ймовірність кеш-потрапляння.

2. Алгоритми управління кешем. Використання ефективних алгоритмів, таких як LRU (Least Recently Used) або LFU (Least Frequently Used), оптимізує процес зберігання та видалення даних з кешу. Це забезпечує актуальність кешу і зменшує кількість кеш-промахів.

3. Характер трафіку. Пропускна здатність залежить від того, наскільки часто запити користувачів повторюються. Якщо трафік має високу частоту повторюваних запитів, кешуючий проксі-сервер може значно підвищити ефективність системи.

4. Розташування сервера. Місце розташування проксі-сервера відносно клієнтів і основного сервера впливає на затримки у передачі даних. Розміщення проксі ближче до клієнтів дозволяє зменшити час відповіді та покращити користувацький досвід.

5. Пропускна здатність мережі. Мережеві обмеження можуть впливати на ефективність проксі-сервера. Навіть за високого рівня кеш-потрапляння вузькі місця у мережевій інфраструктурі можуть стримувати продуктивність.

6. Частота оновлення даних. Якщо дані часто змінюються, сервер може витрачати більше ресурсів на оновлення кешу, що потенційно знижує ефективність.

Переваги використання кешуючого проксі-сервера

1. Зменшення навантаження на основні сервери. Основний сервер отримує менше запитів, оскільки значна їх частина обробляється на рівні проксі-сервера. Це знижує використання обчислювальних ресурсів і покращує продуктивність системи загалом.

2. Швидше обслуговування запитів. Дані, що знаходяться у кеші, можуть бути надані клієнту набагато швидше, ніж у разі звернення до основного сервера. Це зменшує затримки та покращує загальний досвід користувача [27].

3. Економія мережевих ресурсів. Кешуючий проксі знижує обсяг трафіку між клієнтами та основними серверами, що зменшує загальні витрати на використання мережі.

4. Підвищення надійності системи
У разі недоступності основного сервера проксі може продовжувати обслуговувати клієнтів, використовуючи дані, що залишилися у кеші.

Обмеження кешуючих проксі-серверів

1. Актуальність даних. Кешуючі проксі можуть надавати застарілі дані, якщо не реалізовано належну політику оновлення.

2. Обмеження пам'яті. Розмір кешу є кінцевим, тому не всі дані можуть бути збережені для подальшого використання.

3. Затримки при кеш-промахах
Якщо запитаний ресурс відсутній у кеші, затримки можуть бути навіть більшими, ніж при прямому зверненні до основного сервера.

4. Складність налаштування
Ефективне налаштування кешуючого проксі потребує ретельного аналізу трафіку, вибору оптимальних алгоритмів і визначення відповідних політик кешування.

Налаштування представлено малюнку 1.

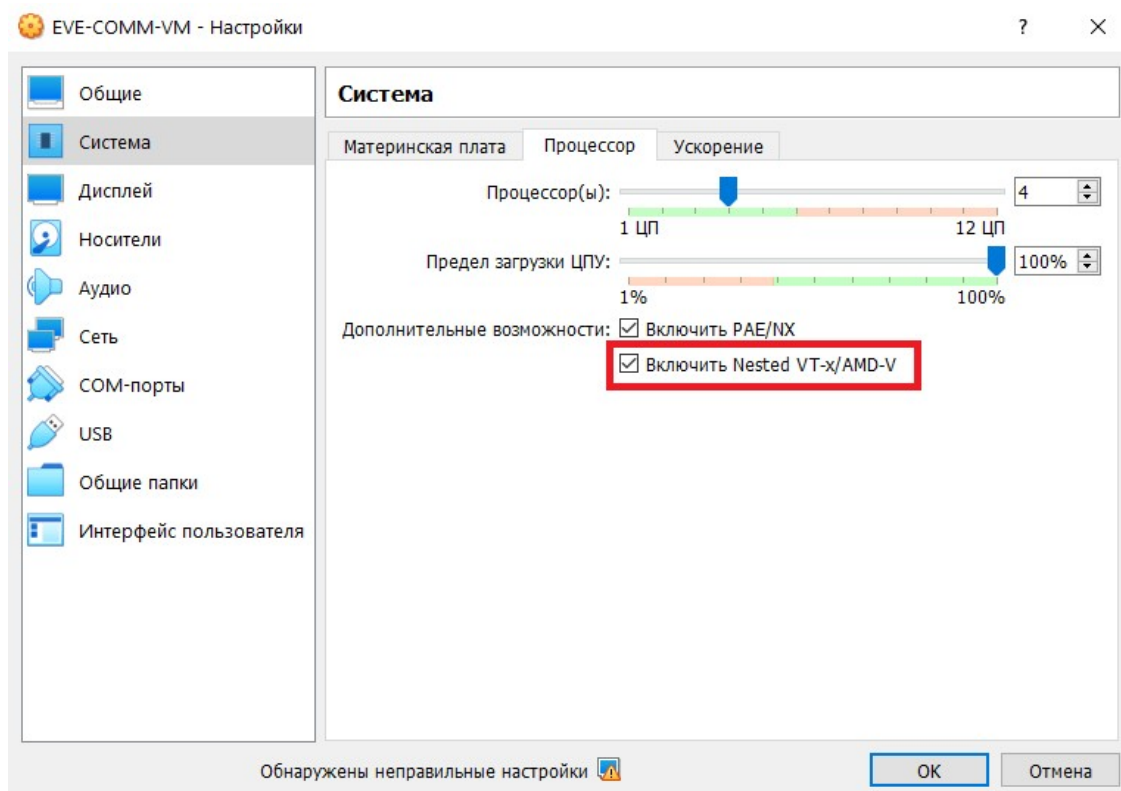


Рисунок
2.5.1 –

Налаштування маршрутизатора

Як клієнта були обрані звичайні персональні комп'ютери, кожному з яких було задано ір адресу. Адреса задана відповідно до поділу на підмережі.

Налаштувати порти комутатора таким чином:

E0/0: trunk, дозволені vlan 12,14,16

E0/1: trunk, дозволені vlan 12,23

E0/2: trunk, дозволені vlan 12,23,34

E0/3: trunk, дозволений vlan 14,34

E1/0: access, vlan 16

На всіх інтерфейсах відключити cdp, усі незадіяні інтерфейси відправити до стану admin-down

Насамперед створимо потрібні нам влади:

```
Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch (config) # vlan 12
```

```
Switch(config-vlan)#vlan 14
```

```
Switch (config-vlan) # vlan 16
```

```
Switch(config-vlan) # vlan 23
```

```
Switch(config-vlan)#vlan 34
```

```
Switch(config-vlan)#end
```

```
Switch#
```

Призначимо вищевказаним інтерфейсам режим роботи та номери vlan'ів відповідно до завдання:

```
Switch(config)#int e0/0
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan 12,14,16
```

```
Switch(config-if)#no cdp enable
```

```
Switch(config-if)#int e0/1
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan 12,23
```

```
Switch(config-if)#no cdp enable
```

```
Switch(config-if)#int e0/2
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan 12,23,34
```

```
Switch(config-if)#no cdp enable
```

```
Switch(config-if)#int e0/3
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#switchport trunk encapsulation dot1q
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan 14,34
```

```
Switch(config-if)#no cdp enable
```

```
Switch(config-if)#end
```

Тепер залишилося відключити незадіяні інтерфейси:

```
Switch#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)#int range e1/1-3
```

```
Switch(config-if-range)#shutdown
```

```
Switch(config-if-range)#end
```

1. IPsec. Додати в топологію підприємства філію та організувати її зв'язок із центральним офісом по IPSec із шифруванням у режимі мережа між маршрутизаторами.

Налаштувати протокол динамічної маршрутизації EIGRP між вузлами R4 та R5:

вказати номер AS 101

на R5 оголосити всі доступні мережі

на R4 оголосити лише мережі, що дивляться у бік R5

зробити всі інтерфейси на обох маршрутизаторах пасивними за умовчанням, окремо активувавши потрібні інтерфейси

відключити автоматичне підсумовування

R4:

```
R4#conf t
```

Enter configuration commands, one per line.

```
R4(config)#router eigrp 101
```

```
R4(config-router)#passive-interface default
```

```
R4(config-router)#netw 10.0.0.0 0.0.0.3
```

```
R4(config-router)#netw 10.0.0.4 0.0.0.3
```

```
R4(config-router)#no auto-summary
```

```
R4(config-router)#no passive-interface s1/0
```

```
R4(config-router)#no passive-interface s1/1
```

```
R4(config-router)#end
```

R5:

Після введення конфігів видно, що EIGRP-сусідство встановилося і R1 видно всі мережі R6:

```
R1#sh ip eigrp neighbors
```

Спостерігач. Розмістити у внутрішній мережі пастку, яка інформуватиме адміністратора при будь-якій спробі її сканування (на ширококомовні пакети та на протокол ARP вона реагувати не повинна).

Налаштування роутера ISP:

- На роутері налаштовані статичні маршрути до мереж 10.0.0.0/18, 192.168.0.0/16 через інтерфейс Fa0/0

- IP-адреси на інтерфейсах налаштовані відповідно до логічної топології

З таблиці топології видно, що метрики різні інтерфейси відрізняються. Для того щоб обидва шляхи потрапили в таблицю маршрутизації, скористаємося командою `variance multiplier`. Як я розповідав раніше, при зазначеному `multiplier` роутер множить FD на `multiplier` і додає до таблиці маршрутизації всі шляхи, відстань до яких потрапляє в діапазон від FD до $FD * Multiplier$. У нашому випадку FD і вартість шляху через інтерфейс S1/1 відрізняються більш ніж у 2 рази, отже, `Multiplier` у нашому випадку має дорівнювати 3. Перевіримо це, вказавши `variance 2`:

R4:

```
R4#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R4(config)#router eigrp 101
```

```
R4(config-router)#variance 2
```

```
R4(config-router)#end
```

```
R4#
```

```
R4#sh ip route eigrp 101 | begin Gateway
```

```
Gateway of last resort is 10.0.34.1 to network 0.0.0.0
```

```
D 192.168.254.0/23 [90/2346496] via 10.0.0.2, 00:00:14, Serial1/0
```

Так і сталося, новий маршрут не з'явився. Збільшимо множник на 1:

```
R4#conf t
```

Кешуючий проксі-сервер є ефективним інструментом для оптимізації пропускної здатності мережі. Завдяки зниженню навантаження на основні сервери, зменшенню затримок і покращенню досвіду користувачів він дозволяє значно підвищити продуктивність системи. Однак для досягнення максимального ефекту необхідно враховувати всі фактори, що впливають на його роботу, та впроваджувати оптимальні алгоритми управління кешем [20].

2.6 Розрахунок використання ЦП серверу додатків при обробці запитів.

Ефективність використання центрального процесора (ЦП) серверу додатків є ключовим параметром, який визначає здатність системи обробляти запити від користувачів у реальному часі. Високий рівень завантаження ЦП може призвести до затримок у роботі системи, тому правильний аналіз і розрахунок використання ЦП є важливими для забезпечення стабільної продуктивності.

Фактори, що впливають на використання ЦП

1. Частота запитів

Кількість запитів на одиницю часу (зазвичай запити на секунду). Чим більше запитів, тим більше ресурсів ЦП витрачається на їх обробку.

2. Складність обробки

Кожен запит вимагає певного часу виконання, який залежить від складності виконуваних операцій, таких як доступ до бази даних, обробка бізнес-логіки чи робота з кешем.

3. Навантаження на мережу

Витрати ЦП на приймання та передачу даних через мережу також впливають на загальний рівень використання процесора.

4. Інші сервіси

Додаткові задачі, які виконує сервер (логування, моніторинг, резервне копіювання), також впливають на завантаження ЦП.

Формула для розрахунку використання ЦП

Використання ЦП можна розрахувати за формулою:

$$UCPU = T_{total} \cdot N \cdot T_{proc} \cdot 100\%$$

де:

- $UCPU$ — використання ЦП у відсотках,
- N — кількість запитів за одиницю часу,
- T_{proc} — середній час обробки одного запиту (у секундах),
- T_{total} — загальний доступний час ЦП (у секундах) за цей же період.

Приклад розрахунку

Припустимо, що сервер отримує 500 запитів на секунду, середній час обробки одного запиту становить 0.005 секунди, а сервер має 4 ядра з частотою 3.0 ГГц. Загальний доступний час ЦП на секунду дорівнює:

$$T_{total} = 4 \text{ ядра} \cdot 1 \text{ секунда} = 4 \text{ секунди.}$$

Рівень завантаження ЦП:

$$UCPU = 4500 \cdot 0.005 \cdot 100\% = 62.5\%.$$

Це означає, що сервер використовує 62.5% своїх обчислювальних ресурсів для обробки запитів.

Вплив оптимізації на використання ЦП

Оптимізація обробки запитів може суттєво зменшити завантаження ЦП.

Основні методи включають:

- Використання кешу: зменшення кількості звернень до бази даних і повторних обчислень.
- Розподіл навантаження: використання балансувальників навантаження для рівномірного розподілу запитів між серверами.
- Оптимізація бізнес-логіки: мінімізація складності виконуваних операцій.
- Впровадження асинхронної обробки: використання асинхронних механізмів для виконання операцій, які не потребують миттєвої відповіді.

Моніторинг і аналіз

Моніторинг використання ЦП в реальному часі є критично важливим для забезпечення продуктивності. Інструменти, такі як Amazon CloudWatch,

Prometheus чи Grafana, дозволяють відстежувати метрики використання ЦП, аналізувати аномалії та здійснювати профілактичні заходи.

Розрахунок використання ЦП при обробці запитів є необхідним кроком для проєктування та підтримки ефективних серверних систем. Впровадження оптимізацій і правильний розподіл ресурсів дозволяють забезпечити стабільну роботу навіть за умов високого навантаження [26].

2.7 Час обслуговування в різних мережах

Час обслуговування у мережах визначає, як швидко система може обробити запит від моменту його отримання до моменту повернення відповіді. Цей показник є критичним для забезпечення високої продуктивності, стабільності та надійності системи, особливо у контексті мереж з різними характеристиками, такими як локальні (LAN), глобальні (WAN), бездротові та хмарні мережі.

Основні етапи обслуговування запитів у мережах

1. Час передачі запиту

Включає затримки на маршрутизацію, переключення між мережевими вузлами та фізичну передачу даних. Цей показник залежить від типу мережі (LAN, WAN) та її пропускної здатності.

2. Час обробки запиту

Містить період, протягом якого сервер або інший обробник запиту виконує необхідну обчислювальну роботу (пошук даних, виконання бізнес-логіки тощо).

3. Час передачі відповіді

Як і час передачі запиту, він залежить від типу мережі, об'єму даних відповіді та топології мережі.

Час обслуговування в різних типах мереж

1. Локальні мережі (LAN)

Локальні мережі забезпечують низький час обслуговування завдяки високій пропускній здатності (зазвичай 1 Гбіт/с і вище) та мінімальним затримкам передачі. LAN використовуються в офісних і домашніх умовах для забезпечення швидкого обміну даними між пристроями.

- Середній час затримки: 0.1–1 мс.
- Використання: системи обміну даними в межах одного об'єкта.
- Вплив факторів: завантаженість мережі та якість обладнання.

2. Глобальні мережі (WAN)

WAN охоплюють великі географічні відстані та забезпечують з'єднання між

різними локаціями. Час обслуговування у WAN значно вищий, ніж у LAN, через більші затримки передачі даних, викликані маршрутизацією через численні вузли.

- Середній час затримки: 10–100 мс (залежно від відстані).
- Використання: корпоративні мережі, інтернет-з'єднання.
- Вплив факторів: пропускна здатність каналів, стан маршрутизаторів.

3. Бездротові мережі (Wi-Fi, LTE, 5G)

Бездротові мережі пропонують високу мобільність, але їх продуктивність залежить від сигналу, інтерференції та числа підключених пристроїв.

- Wi-Fi: час затримки 1–10 мс у стабільних умовах.
- LTE: час затримки 20–50 мс.
- 5G: потенційно 1 мс, що значно підвищує можливості реального часу.

4. Хмарні мережі

Хмарні обчислення передбачають передачу даних до віддалених серверів для обробки. Час обслуговування тут залежить від якості мережі між клієнтом і хмарию, а також продуктивності серверів.

- Середній час затримки: 50–200 мс (залежно від розташування дата-центрів).
- Використання: SaaS, PaaS, IaaS.
- Вплив факторів: фізична відстань до дата-центру, завантаженість хмарних ресурсів.

Методи зменшення часу обслуговування

1. Оптимізація мережевої інфраструктури. У LAN використовувати високошвидкісні комутатори та маршрутизатори. Для WAN застосовувати технології стиснення даних та оптимізації маршрутизації.

2. Застосування кешування

Використання кешуючих проксі-серверів або локального кешу на клієнтському пристрої для зменшення кількості звернень до серверів.

3. Масштабування ресурсів

У хмарних і глобальних мережах масштабування серверних ресурсів дозволяє знизити час обробки запитів.

4. Мінімізація обсягу даних

Стиснення файлів і оптимізація протоколів передачі (наприклад, використання HTTP/2 або gRPC) допомагають зменшити час передачі.

Час обслуговування в різних мережах суттєво залежить від типу мережі, її пропускної здатності, топології та кількості вузлів. Оптимізація мережевої інфраструктури та обчислювальних ресурсів, застосування сучасних протоколів і технологій кешування дозволяють значно зменшити час затримок і підвищити продуктивність системи. Розуміння та врахування цих аспектів є важливими для проектування високоефективних мережевих і хмарних рішень [27].

Висновки до розділу 2

У третьому розділі було проведено детальний аналіз факторів, що впливають на продуктивність систем у різних мережевих умовах, а також розглянуто методологію розрахунку пропускної здатності, використання ЦП серверів та часу обслуговування запитів. Одержані результати дозволяють зробити наступні висновки:

1. Продуктивність системи залежить від багатьох взаємопов'язаних факторів. Основними з них є пропускна здатність мережі, обробка запитів на сервері, час передачі даних між вузлами, а також ефективність використання серверних ресурсів, зокрема ЦП.

2. Кешування є ключовим методом оптимізації. Використання кешуючих проксі-серверів дозволяє значно зменшити затримки в обробці запитів та знизити навантаження на основні сервери. Це особливо ефективно у випадках із частими повторюваними запитами.

3. Різні типи мереж мають свої особливості впливу на час обслуговування. Локальні мережі забезпечують найшвидший час передачі даних завдяки високій пропускній здатності та мінімальним затримкам, у той час як глобальні та бездротові мережі демонструють більшу чутливість до завантаженості та фізичної відстані між вузлами.

4. Оптимізація обчислювальних ресурсів. Розрахунок і моніторинг використання ЦП є критично важливими для забезпечення стабільної роботи серверів. Запропоновані методи, такі як асинхронна обробка, балансування навантаження та оптимізація бізнес-логіки, дозволяють ефективно зменшити навантаження на сервери.

5. Пропускна здатність є основним обмежуючим фактором у складних системах. Її розрахунок та аналіз є необхідними для проєктування ефективної мережевої інфраструктури. Запропоновані формули розрахунку дозволяють точно оцінити можливості системи та передбачити потенційні вузькі місця.

6. Удосконалення методів розрахунку. Представлені теоретичні моделі та розрахунки базуються на сучасних підходах до аналізу продуктивності. Вони можуть бути адаптовані для різних мережевих архітектур, включаючи хмарні рішення, що забезпечує їх універсальність та практичну цінність.

Таким чином, отримані результати створюють основу для подальшої оптимізації роботи мережевих систем, що використовуються для моніторингу IoT-пристроїв. Ефективне поєднання теоретичних розрахунків, сучасних технологій та оптимізаційних методів дозволяє підвищити продуктивність, надійність і швидкість роботи таких систем у реальних умовах.

3. Платформа для моніторингу IoT-пристроїв

У третьому розділі ми налаштуємо підключення ESP32. Забезпечення бездротового з'єднання мікроконтролера з мережею для передачі даних на платформу.

Зчитування даних із сенсора DHT22: Створення андроїд додатку та керування для отримання показників температури та вологості. Форматування даних: Підготовка отриманих значень у форматі JSON для передачі. Передача даних через MQTT: Налаштування з'єднання з MQTT-брокером та відправка даних.

3.1 Було розроблено симуляцію на базі мікроконтролера ESP32 для демонстрації функціонування IoT-платформи. Ця симуляція імітує роботу реальних IoT-пристроїв, генеруючи дані, які надалі передаються до платформи через протокол MQTT за допомогою брокера HiveMQ.

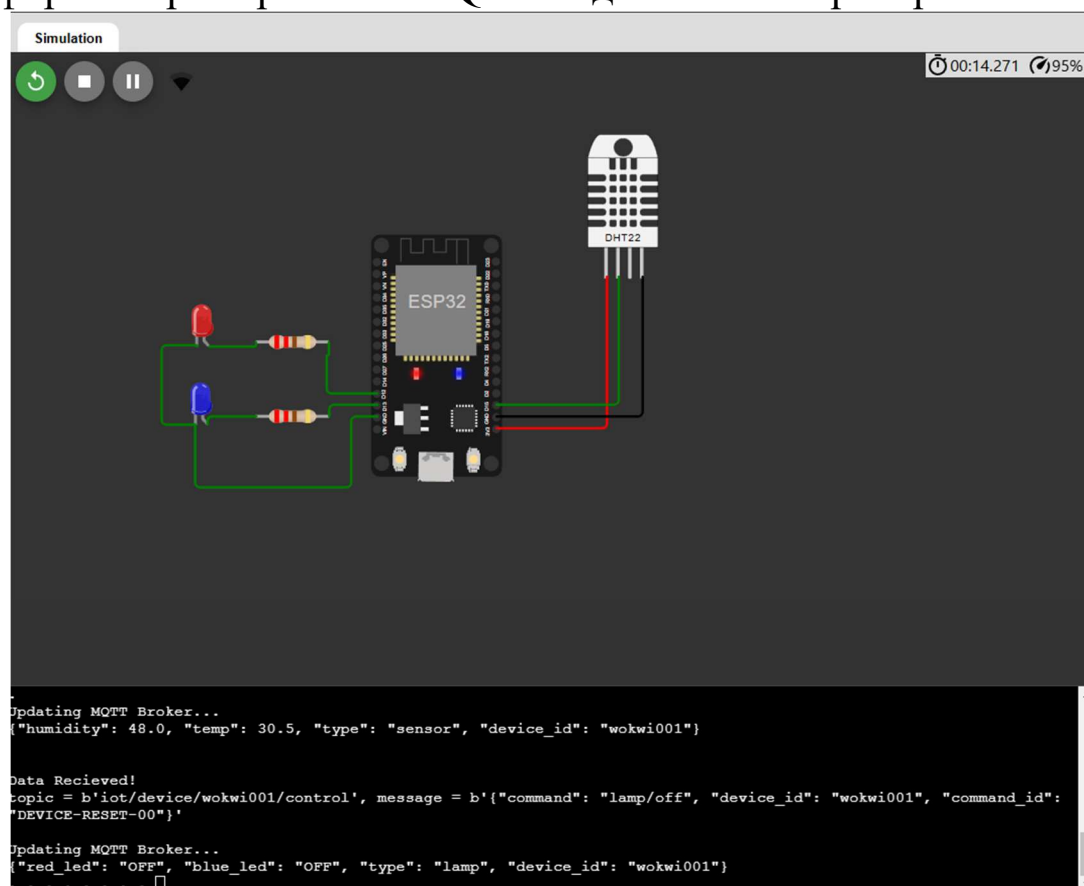


Рисунок 3.1 – Симуляція ESP32

3.2 Було розроблено мобільний додаток, який слугує інструментом для візуалізації показників роботи IoT-пристроїв та здійснення управління їх окремими компонентами. Завдяки цьому додатку користувачі отримують можливість в реальному часі моніторити ключові параметри пристроїв

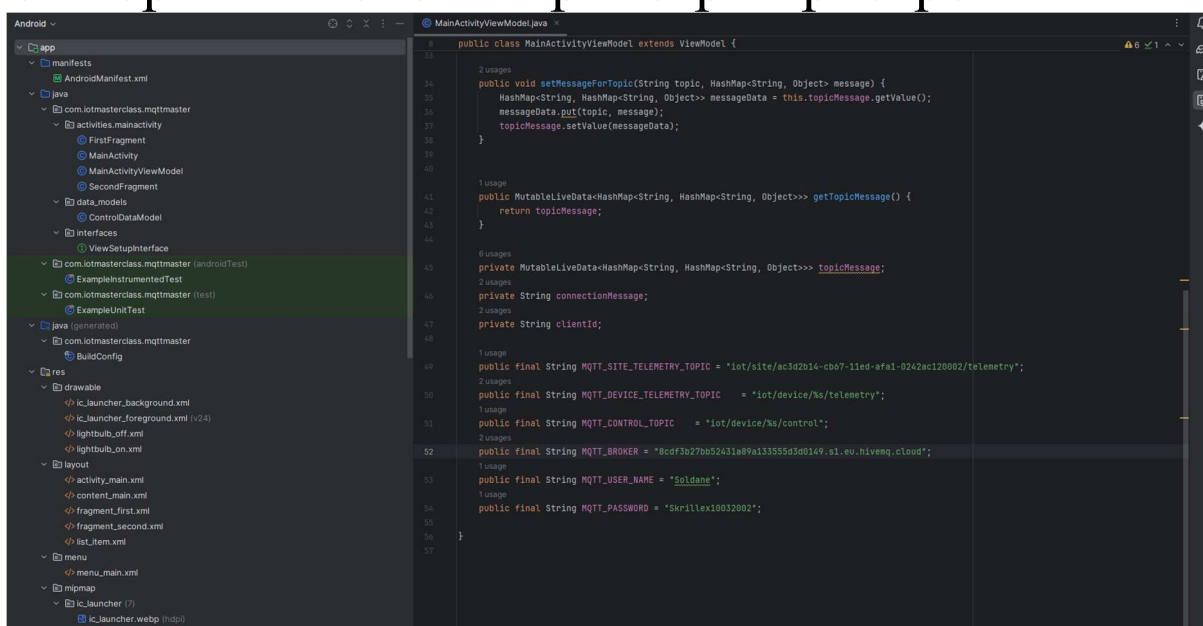


Рисунок 3.2 – код андроїд застосунку

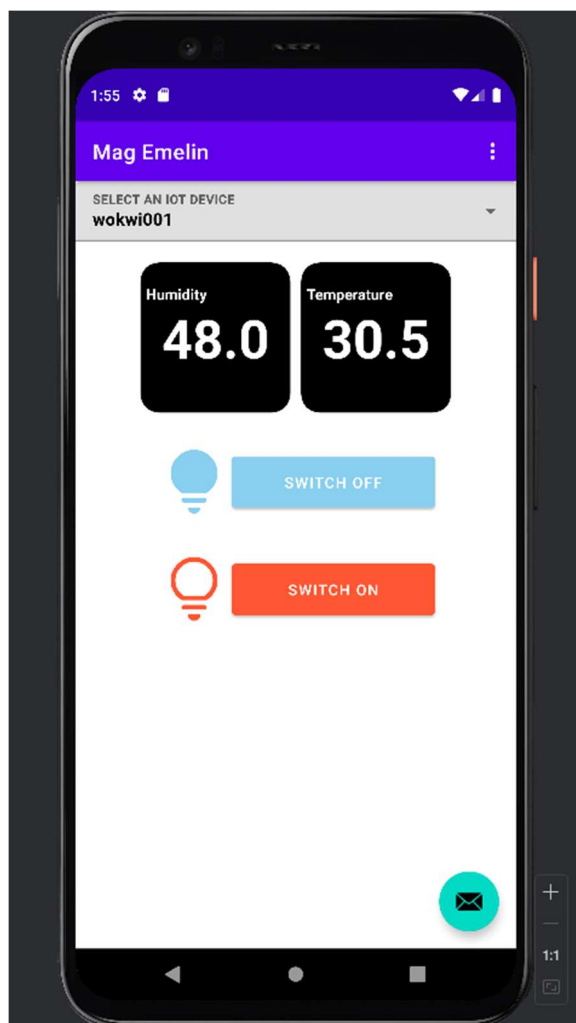


Рисунок 3.3 – вигляд андроїд застосунку

3.3 Через брокера HiveMQ здійснюється передача даних від симуляції IoT-пристроїв до мобільного застосунку. Цей механізм базується на протоколі MQTT, який забезпечує легкість, надійність і ефективність обміну повідомленнями між пристроями.

Cluster Details
Basic information about your cluster environment

Name: 8cdf3b27bb52431a89a133555d3d0149 Plan: Serverless Cloud Provider: aws

Connection Details
Comprehensive details and statistics for your cluster

URL: 8cdf3b27bb52431a89a133555d3d0149.s1.eu.hivemq.cloud

Port: 8883

Websocket Port: 8884

TLS MQTT URL: 8cdf3b27bb52431a89a133555d3d0149.s1.eu.hivemq.cloud:8883

TLS Websocket URL: 8cdf3b27bb52431a89a133555d3d0149.s1.eu.hivemq.cloud:8884/mqtt

Current Usage
Real time cluster statistics

Sessions: 3 / 100
Traffic: 7.95 KB / 10 GB

Access Management
Cluster access statistics

Credentials: 1
Permissions: 0

Рисунок 3.4 – налаштування брокера

3.4 Зібрані дані передаються для зберігання у базу даних InfluxDB, яка є частиною екосистеми InfluxData. Для автоматизації процесу збору та передачі даних використовується інструмент Telegraf.

Telegraf виступає посередником, який отримує дані, що надходять від IoT-пристроїв через брокер HiveMQ, обробляє їх та записує до бази даних InfluxDB у структурованому вигляді. Завдяки цьому забезпечується швидкий і ефективний запис великих обсягів часових рядів, що є критично важливим для моніторингу в реальному часі.

Data Explorer

+ New Script OPEN SAVE

Schema Browser SQL Sync

Bucket: mqtt-data-all

Measurement: mqtt_consumer

Search fields and tag key

Fields: blue_led, device_id, humidity, red_led, temp, type

Tag Keys: host, topic

Query: `SELECT * FROM "mqtt_consumer" WHERE time >= now() - interval '1 hour' AND time <= now()`

Ready (115ms) -1h to now() RUN

1 tables 44 rows

table	blue_led	device_id	host	humidity	red_led	temp
_result	no group string	no group string	no group string	no group double	no group string	no group double
0	ON	wokwi001	local.mqtt.telegraf		ON	
0	OFF	wokwi001	local.mqtt.telegraf		ON	
0	OFF	wokwi001	local.mqtt.telegraf		OFF	

1 11 12 13 15

Рисунок 3.5 – зберігання даних у базі даних

3.5 Через веб-додаток Grafana була створена інформаційна панель для візуалізації даних, які зберігаються в базі даних InfluxDB. Ця панель надає користувачам можливість переглядати ключові показники роботи IoT-пристроїв у зручному та наочному форматі.

Grafana дозволяє будувати графіки, діаграми та інші інтерактивні елементи для представлення часових рядів даних, отриманих через Telegraf. Інформаційна панель підтримує динамічне оновлення даних у режимі реального часу, що забезпечує постійний моніторинг стану IoT-пристроїв.



Рисунок 3.6 – інформаційна панель

Висновки до розділу 3. Було розроблено платформу для моніторингу IoT-пристроїв із використанням сучасних веб-технологій, яка забезпечує ефективну роботу з даними в режимі реального часу.

Створена симуляція на базі ESP32 дозволила перевірити функціональність платформи та її готовність до роботи з реальними IoT-пристроями.

Здійснено інтеграцію ключових компонентів: протоколу MQTT через брокер HiveMQ, бази даних InfluxDB та інструмента Telegraf для передачі й зберігання даних.

Для візуалізації даних розроблено інформаційну панель у Grafana, що забезпечує зручний моніторинг показників у реальному часі.

Результати роботи мають практичне значення і можуть бути використані для створення IoT-рішень у різних галузях.

ВИСНОВКИ

Дослідження Інтернету речей (IoT) підкреслює його значний вплив на сучасні технології та суспільство. IoT визначається як система, що об'єднує фізичні об'єкти з інтернетом для збору, обробки та обміну даними, що робить цю технологію актуальною в умовах стрімкого розвитку цифрових технологій. Актуальність теми підкріплюється широким спектром застосувань та зростаючими можливостями, які вона відкриває в різних сферах.

Історичний розвиток IoT демонструє еволюцію концепції, починаючи з експериментальних проектів у 1980-х роках і до сучасних складних систем. Перші приклади IoT-пристроїв заклали основи для подальшого розвитку технологій, що підтримують IoT, таких як бездротові мережі, хмарні обчислення та аналіз великих даних.

Основні компоненти IoT, такі як датчики, мережі та хмарні технології, забезпечують функціонування системи. Датчики збирають дані про навколишнє середовище, мережі забезпечують їх передачу, а хмарні платформи здійснюють зберігання та обробку даних. Протоколи зв'язку, зокрема MQTT, CoAP та HTTP, грають критичну роль у забезпеченні надійного обміну даними між пристроями.

Розвиток IoT супроводжується численними тенденціями, такими як Big Data, штучний інтелект та технології 5G. Ці інновації відкривають нові можливості для аналізу даних, автоматизації процесів і підвищення ефективності використання ресурсів. Водночас з цими можливостями виникають виклики, пов'язані з безпекою даних та сумісністю між різними пристроями і платформами, що підкреслює необхідність розробки нових стандартів і політик.

Класифікація IoT-пристроїв та їх різноманітність, включаючи розумні будинки, промислові IoT та медичні пристрої, свідчать про широкий спектр застосування технологій IoT. Впровадження IoT у сферах освіти, охорони здоров'я та транспорту демонструє їхню ефективність, підтверджену успішними кейс-стаді. Наприклад, системи моніторингу здоров'я дозволяють здійснювати віддалений нагляд за пацієнтами, а в освіті — створювати інтерактивні навчальні середовища.

Перспективи розвитку IoT включають нові технології та інновації, що можуть суттєво вплинути на економіку і суспільство. IoT має потенціал для трансформації бізнес-моделей, підвищення продуктивності та оптимізації витрат. Екологічні аспекти, зокрема ефективність використання ресурсів, підкреслюють важливість сталого розвитку в умовах зростання використання IoT. Оптимізація споживання енергії та води, а також зменшення викидів забруднюючих речовин можуть сприяти реалізації цілей сталого розвитку.

Отже, IoT має величезний потенціал для подальшого розвитку і трансформації різних аспектів життя. Проте для успішної реалізації можливостей необхідно зосередитися на питаннях безпеки, сумісності та екологічної стійкості. Розробка нових стандартів, підвищення обізнаності користувачів і активне співробітництво між учасниками ринку стануть ключовими чинниками для досягнення успіху в цій динамічній галузі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Абдураманов Р. А., Хлапонін Ю. І., Намір Хашім Касім. Метод квантильної регресії для прогнозування стану телекомунікаційних мереж. *Вісник інженерної академії*. 2017. Вип. №3. С. 32-37.
2. Абрамов В. О. Захищені кабельні інтерфейси сенсорних мереж інтернету речей. *Кібербезпека: освіта, наука, техніка*. 2019. № 1. С. 73-82. URL: http://nbuv.gov.ua/UJRN/cest_2019_1_9 (дата звернення: 23.10.2024).
3. Алексіна Л. Т., Шевченко О. О. Дослідження технологій інтернету речей. *Зв'язок*. 2019. № 4. С. 24-26.
4. Артеменко М. Ю., Беркман Л. Н., Толюпа С. В. Нейронні мережі та їх застосування в телекомунікаційних системах. *Радіотехніка: Всеукр. міжвід. наук.-техн. зб.* 2007. Вип. №134. С. 45–53.
5. Баранов О. А. Інтернет речей і освіта. *Інтернет речей: теоретико-методологічні основи правового регулювання*: монографія. 2-ге вид. Харків, 2018. С. 81-89.
6. Баранов О. А. Інтернет речей і промисловість. *Інтернет речей: теоретико-методологічні основи правового регулювання*: монографія. 2-ге вид. Харків, 2018. С. 36-64.
7. Брайчевський С. М. Зворотні зв'язки в системах Інтернету речей з елементами штучного інтелекту. *Інформація і право*. 2019. № 2. С. 32-39. URL: http://nbuv.gov.ua/UJRN/Infpr_2019_2_6 (дата звернення: 23.10.2024).
8. Гіоргізова-Гай В. Ш., Шеренковський А. О. Шлюз у системі інтернету речей/. *Вчені зап. ТНУ ім. В. І. Вернадського*. Серія: Техн. науки. 2019. Т. 30 (69), ч. 1, № 1. С. 31-37. URL: <https://cutt.ly/dpoJJpm> (дата звернення: 23.10.2024).
9. Іванченко Н. О., Лисенко І. О. Впровадження корпоративних рішень на основі концепції «Інтернет речей». *Наук. вісн. Ужгород. нац. ун-ту. Серія: Міжнар. екон. відносини та світ. госп-во*. 2018. Вип. №19 (1). С. 161-164. URL: <https://cutt.ly/6ppbNA8> (дата звернення: 23.10.2024).

10. Про захист інформації в інформаційно-телекомунікаційних системах Закон України від 05.07.1994 № 80/94-ВР. URL: <http://zakon2.rada.gov.ua> (дата звернення: 23.10.2024).
11. Срібна І. М., Савчук Є. В. Веб-сервіси AWS для розгортання пристроїв IoT. *Зв'язок*. 2019. № 4. С. 18-23.
12. Ткачук Т. Інтернет-речі: від фантастики минулого до реалій сьогодення. *Інтернет речей: проблеми правового регулювання та впровадження: матеріали III наук.-практ. конф., 21 листоп. 2019 р., м. Київ, 2019*. С. 16-19. URL: <https://cutt.ly/Morl2Hv> (дата звернення: 23.10.2024).
13. Юдін О. М., Хлапонін Ю. І. Контроль захищеності бездротових комп'ютерних мереж. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. № 2 (19). С. 92–96.
14. Вергун А. І. Розробка модифікованої архітектури мережі Інтернету речей із використанням LP-WAN. *Зв'язок*. 2019. № 4. С. 15-17.
15. Kulchin Yu. N., Zakasovskaya E. V. Optimizing algebraic and neural methods for information processing in distributed fiber-optical measuring systems. *Optical Memory & Neural Networks (Information Optics)*. 2010. Vol. 19. N 3. P. 237–247.
16. Жук О. В. Інтернет речей: концепції та технології. Київ: Наукова думка, 2019.
17. Шевченко І. О. Безпека в мережах Інтернет речей: проблеми та вирішення. Харків: ХНУРЕ, 2018.
18. Тищенко В. І. Основи захисту інформації в Інтернеті. Київ: Академвидав, 2020.
19. Петренко В. П. Моделі та методи безпеки у Інтернеті речей. Львів: Інститут комп'ютерних наук, 2017.
20. Савченко О. М. Технології IoT та їх застосування в розумних містах. Одеса: ОНУ, 2021.
21. Денисенко А. В. Захист даних у системах Інтернет речей. Київ: Науково-технічний центр, 2019.

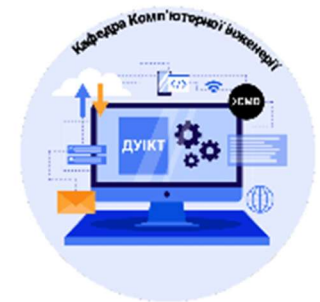
22. Василенко І. Л. Інтернет речей у контексті безпеки інформаційних технологій. Харків: ХДАУ, 2018.
23. Ashton, K. That 'Internet of Things' Thing. RFID Journal, 2009.
24. Miorandi, D., Sicari, S., Pellegrini, F., & Chlamtac, I. Internet of Things: Vision, Applications and Research Challenges. Ad Hoc Networks, 10(7), 1497-1516, 2012.
25. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645-1660, 2013.
26. Borgia, E. The Internet of Things Vision: Key Features, Applications and Open Issues. Computer Communications, 54, 1-31, 2014.
27. Sicari, S., Rizzardi, A., & Grieco, L. A. Security in the Internet of Things: Challenges and Solutions. International Journal of Computer Science and Engineering, 7(4), 140-149, 2015.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ



**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ**



КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Магістерська робота

**«Платформа для моніторингу IoT-пристроїв з використанням сучасних
веб-технологій»**

Виконав: студент групи КСДМ-62 Ємелін Данило Михайлович

Керівник: к.т.н., доц., Вечерковська Анастасія Сергіївна

Київ - 2025

МЕТА, ОБ'ЄКТА ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи – платформу для моніторингу IoT-пристроїв з використанням сучасних веб-технологій, яка забезпечує ефективне збирання, обробку та відображення даних у реальному часі. .

Об'єкт дослідження – Інтернет речей (IoT) як технологічна система, що інтегрує фізичні об'єкти в цифрове середовище для збору та обміну даними.

Предмет дослідження – методи та засоби розробки платформи для моніторингу IoT-пристроїв із застосуванням сучасних веб-технологій.

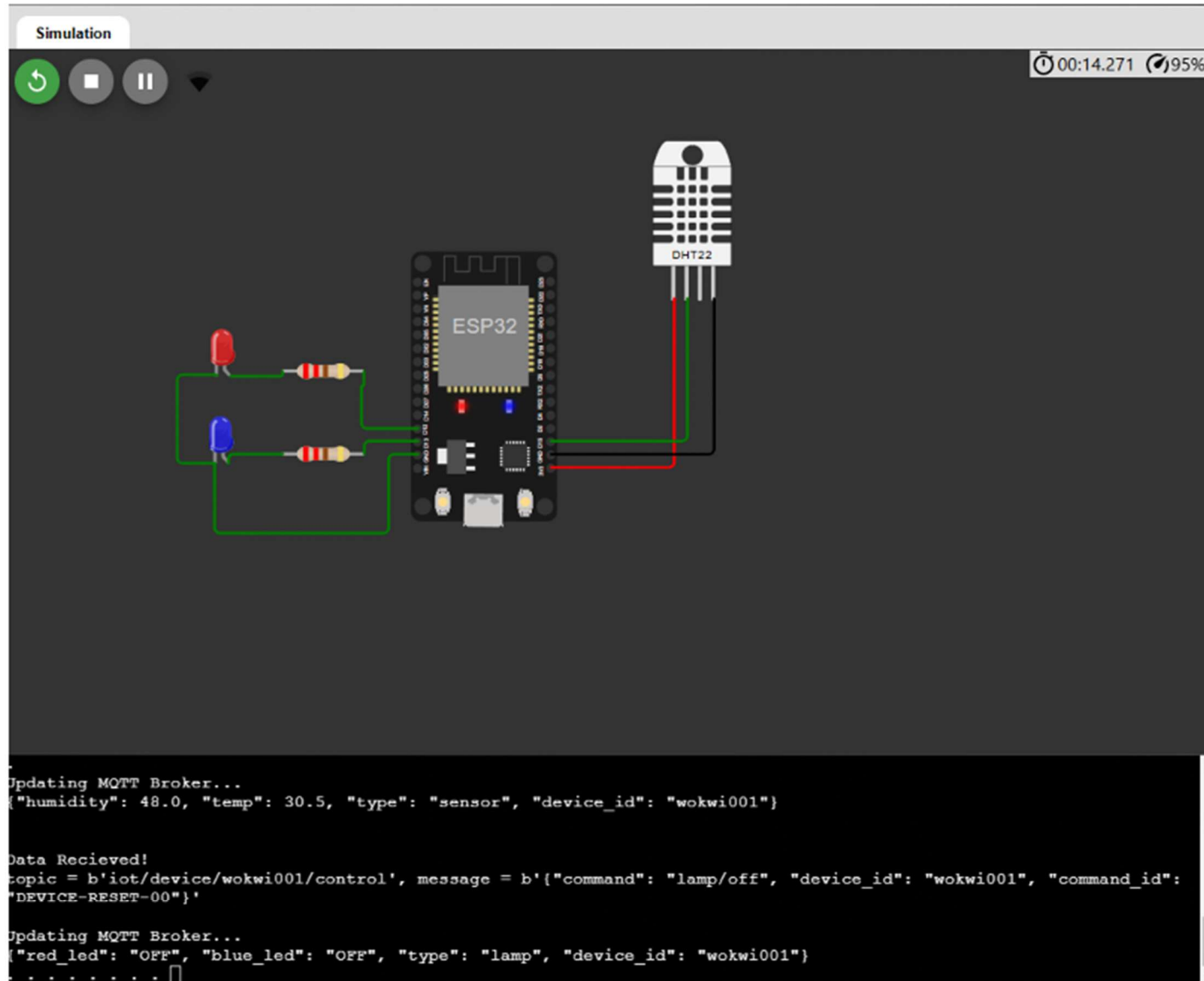
АКТУАЛЬНІСТЬ РОБОТИ

У сучасному світі технологічний прогрес невпинно трансформує способи, якими люди взаємодіють з навколишнім середовищем. Однією з найзначніших інновацій у цій сфері є концепція Інтернету речей (IoT, Internet of Things). Це поняття охоплює мережу фізичних об'єктів, оснащених датчиками, програмним забезпеченням та іншими технологіями, що дозволяють їм збирати та обмінюватися даними через Інтернет. IoT створює нові можливості для автоматизації процесів, підвищення ефективності і зручності в повсякденному житті, на виробництві, у медичних установах та інших сферах.

АКТУАЛЬНІСТЬ РОБОТИ

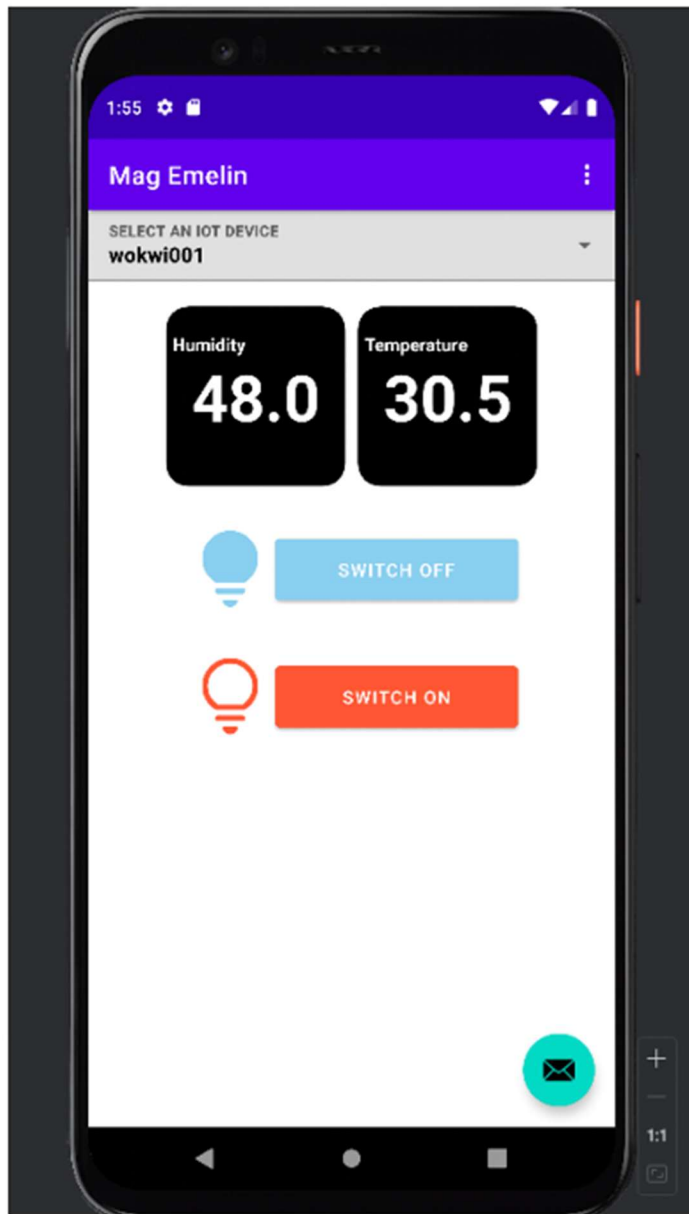
Актуальність теми Інтернету речей зростає з кожним роком, оскільки
все більше галузей починають впроваджувати IoT-рішення для
покращення ефективності та зручності. Згідно з прогнозами, до 2025
року кількість підключених IoT-пристроїв у світі може досягти
декількох мільярдів, що свідчить про стрімкий розвиток цієї технології.
У світі, де дані стають новим золотом, можливість їх збору та аналізу в
реальному часі відкриває нові горизонти для бізнесу та суспільства в
цілому

IoT ПЛАТФОРМА



Було розроблено симуляцію на базі мікроконтролера ESP32 для демонстрації функціонування IoT-платформи. Ця симуляція імітує роботу реальних IoT-пристроїв, генеруючи дані, які надалі передаються до платформи через протокол MQTT за допомогою брокера HiveMQ.

ІоТ ПЛАТФОРМА



Було розроблено мобільний додаток, який слугує інструментом для візуалізації показників роботи ІоТ-пристроїв та здійснення управління їх окремими компонентами. Завдяки цьому додатку користувачі отримують можливість в реальному часі моніторити ключові параметри пристроїв

IoT ПЛАТФОРМА

Cluster Details

Basic information about your cluster environment

Name	Plan	Cloud Provider
8cdf3b27bb52431a89a133555d3d0149	Serverless	aws

Connection Details

Comprehensive details and statistics for your cluster

URL

8cdf3b27bb52431a89a133555d3d0149.s1.eu.hivemq.cloud

Port

8883

Websocket Port

8884

TLS MQTT URL

8cdf3b27bb52431a89a133555d3d0149.s1.eu.hivemq.cloud:8883

TLS Websocket URL

8cdf3b27bb52431a89a133555d3d0149.s1.eu.hivemq.cloud:8884/mqtt

Current Usage

Real time cluster statistics

Sessions: 3 / 100

Traffic: 7.95 KB / 10 GB

Access Management

Cluster access statistics

Credentials: 1

Permissions: 0

Через брокера HiveMQ здійснюється передача даних від симуляції IoT-пристроїв до мобільного застосунку. Цей механізм базується на протоколі MQTT, який забезпечує легкості, надійності і ефективності обміну повідомленнями між пристроями

IoT ПЛАТФОРМА

The screenshot displays the Wokwi IoT platform interface, which is divided into three main sections:

- Mobile App (Left):** A smartphone screen showing a web application titled "Mag Emelin". It features a header with a settings icon and a dropdown menu labeled "SELECT AN IOT DEVICE" with "wokwi001" selected. Below this, there are two large digital displays for "Humidity" and "Temperature", both showing "0.0". There are two light bulb icons; the top one is blue with a "SWITCH ON" button, and the bottom one is red with a "SWITCH ON" button. A green circular button with a white envelope icon is at the bottom right.
- Code Editor (Middle):** A window titled "main.py" showing Python code for an ESP32 microcontroller. The code includes imports for Pin, MQTTClient, ujson, network, utime, and dht. It sets up device ID, WiFi credentials, MQTT broker and topics, and initializes a DHT sensor and two LEDs (red and blue). A method `def did_receive_callback(topic, message)` is defined to handle incoming MQTT messages, parsing JSON commands to control the LEDs. The code is currently in "Simulation" mode, as indicated by the "Simulation" tab and the "Restart the simulation" button.
- Hardware Simulation (Right):** A visual representation of the ESP32 board and its components. The board is connected to a DHT22 temperature and humidity sensor. Two LEDs, one red and one blue, are connected to the board's pins. The simulation status bar at the top right shows a timer at "00:01.266" and a battery level at "99%".

```
1 from machine import Pin
2 from umqtt.simple import MQTTClient
3 import ujson
4 import network
5 import utime as time
6 import dht
7
8
9 # Device Setup
10 DEVICE_ID = "wokwi001"
11
12 # WiFi Setup
13 WIFI_SSID = "wokwi-GUEST"
14 WIFI_PASSWORD = ""
15
16 # MQTT Setup
17 MQTT_BROKER = "8cdf3b27b"
18 MQTT_CLIENT = DEVICE_ID
19 MQTT_TELEMETRY_TOPIC = "iot/device"
20 MQTT_CONTROL_TOPIC = "iot/device"
21
22 # DHT Sensor Setup
23 DHT_PIN = Pin(15)
24
25 # LED/LAMP Setup
26 RED_LED = Pin(12, Pin.OUT)
27 BLUE_LED = Pin(13, Pin.OUT)
28 FLASH_LED = Pin(2, Pin.OUT)
29 RED_LED.on()
30 BLUE_LED.on()
31
32 # Methods
33 def did_receive_callback(topic, message):
34     print('\n\nData Received! \ntopic: ' + topic + '\nmessage: ' + message)
35     if topic == MQTT_CONTROL_TOPIC:
36         #Get the command message from json
37         command_message = ujson.loads(message)
38         if command_message == "lamp/red":
39             RED_LED.on()
40         elif command_message == "lamp/blue":
41             BLUE_LED.on()
```

ІоТ ПЛАТФОРМА

The screenshot shows the InfluxDB Data Explorer interface. On the left, the 'Schema Browser' is open, showing the 'mqtt-data-all' bucket and the 'mqtt_consumer' measurement. The 'Fields' section lists 'blue_led', 'device_id', 'humidity', 'red_led', 'temp', and 'type'. The 'Tag Keys' section lists 'host' and 'topic'. The main area displays a SQL query: `SELECT * FROM "mqtt_consumer" WHERE time >= now() - interval '1 hour' AND time <= now()`. Below the query, the status is 'Ready (115ms)' and the time range is '-1h to now()'. The 'RUN' button is visible. The results are shown in a table with 44 rows. The table has columns: 'table', 'blue_led', 'device_id', 'host', 'humidity', 'red_led', and 'temp'. The data rows show 'blue_led' as 'ON' or 'OFF', 'device_id' as 'wokwi001', and 'host' as 'local.mqtt.telegraf'.

table	blue_led	device_id	host	humidity	red_led	temp
_result	no group	no group	no group	no group	no group	no group
	string	string	string	double	string	double
0	ON	wokwi001	local.mqtt.telegraf		ON	
0	OFF	wokwi001	local.mqtt.telegraf		ON	
0	OFF	wokwi001	local.mqtt.telegraf		OFF	

Зібрані дані передаються для зберігання у базу даних InfluxDB, яка є частиною екосистеми InfluxData. Для автоматизації процесу збору та передачі даних використовується інструмент Telegraf.

Telegraf виступає посередником, який отримує дані, що надходять від IoT-пристроїв через брокер HiveMQ, обробляє їх та записує до бази даних InfluxDB у структурованому вигляді. Завдяки цьому забезпечується швидкий і ефективний запис великих обсягів часових рядів, що є критично важливим для моніторингу в реальному часі.

IoT ПЛАТФОРМА



Через веб-додаток Grafana була створена інформаційна панель для візуалізації даних, які зберігаються в базі даних InfluxDB. Ця панель надає користувачам можливість переглядати ключові показники роботи IoT-пристроїв у зручному та наочному форматі.

Grafana дозволяє будувати графіки, діаграми та інші інтерактивні елементи для представлення часових рядів даних, отриманих через Telegraf. Інформаційна панель підтримує динамічне оновлення даних у режимі реального часу, що забезпечує постійний моніторинг стану IoT-пристроїв.

ВИСНОВКИ

Було розроблено платформу для моніторингу IoT-пристроїв із використанням сучасних веб-технологій, яка забезпечує ефективну роботу з даними в режимі реального часу.

Створена симуляція на базі ESP32 дозволила перевірити функціональність платформи та її готовність до роботи з реальними IoT-пристроями.

Здійснено інтеграцію ключових компонентів: протоколу MQTT через брокер HiveMQ, бази даних InfluxDB та інструмента Telegraf для передачі й зберігання даних.

Для візуалізації даних розроблено інформаційну панель у Grafana, що забезпечує зручний моніторинг показників у реальному часі.

Результати роботи мають практичне значення і можуть бути використані для створення IoT-рішень у різних галузях.

ПУБЛІКАЦІЇ ТА АПРОБАЦІЯ РОБОТИ

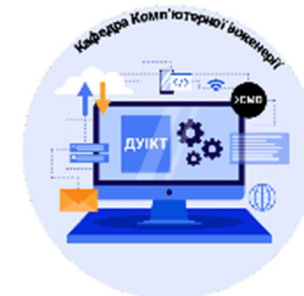
Статті:

1. ІННОВАЦІЙНІ МЕТОДИ ВІДОБРАЖЕННЯ ІНФОРМАЦІЇ У
ВЕБ-БРАУЗЕРАХ <https://doi.org/10.32782/tnv-tech.2024.1.1> DOI:
[10.32782/tnv-tech.2024.1.1](https://doi.org/10.32782/tnv-tech.2024.1.1)



**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-
КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ**



КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Магістерська робота

**«Платформа для моніторингу IoT-пристроїв з використанням сучасних
веб-технологій»**

Виконав: студент групи КСДМ-62 Ємелін Данило Михайлович

Керівник: к.т.н., доц., Вечерковська Анастасія Сергіївна

Київ - 2025