

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЗАПОРІЗЬКА ПОЛІТЕХНІКА»

Факультет комп'ютерних наук та технологій
Кафедра комп'ютерних систем та мереж

Пояснювальна записка

до дипломного проекту (роботи)

магістра

(ступінь вищої освіти)

на тему БУДОВАНА СИСТЕМА ДЛЯ ЗАБЕЗПЕЧЕННЯ
БЕЗПЕЧНОГО СЕРЕДОВИЩА БУДИНКУ

Виконав: студент 2 курсу, групи КНТ-612м
спеціальності _____

123 Комп'ютерна інженерія

(код і найменування спеціальності)

Освітня програма (спеціалізація)

Спеціалізовані комп'ютерні системи

КОЛЯНКІВСЬКИЙ Д.В.

(ПРИЗВИЩЕ та ініціали)

Керівник КАСЬЯН К.М.

(ПРИЗВИЩЕ та ініціали)

Рецензент САМОЙЛИК С.С.

(ПРИЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Комп'ютерних наук і технологій
Кафедра «Комп'ютерні системи та мережі»
Ступінь вищої освіти магістерський
Спеціальність 123 Комп'ютерна інженерія
(код і найменування)
Освітня програма (спеціалізація) «Спеціалізовані комп'ютерні системи»
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Зав. кафедри Кудерметов Р.К.

“ ” 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

КОЛЯНКІВСЬКОГО Дмитра Вікторовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Вбудована система для забезпечення безпечного середовища будинку

керівник проєкту (роботи) к. т. н., доцент, КАСЬЯН Костянтин Миколайович

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом вищого навчального закладу від “24” жовтня 2023 року № 400

2. Строк подання студентом проєкту (роботи) 10 грудня 2023 року

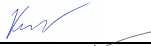
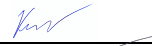
3. Вихідні дані до проєкту (роботи) опис технічного завдання

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

Опис предметної області. Аналіз концепції IoT. Розробка вимог системи. Аналіз існуючих системних рішень «Розумний дім». Дослідження МК для розробки системи. Моделювання системи безпеки. Тестування та дослідження системи.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

6. Консультанти розділів проєкту (роботи)

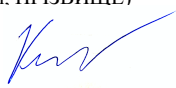
Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-4	КАСЬЯН К. М., доцент		
нормоконтроль	ЩЕРБАК Н. В., ст. викл.		

7. Дата видачі завдання 01.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Аналіз наявних методів та алгоритмів використання IoT для вбудовних систем безпечного середовища	10.10.2023 р.	
2	Розробка вимог для системи	15.10.2023 р.	
3	Вибір мережевого протоколу	20.10.2023 р.	
4	Реалізація вбудованої системи	05.10.2023 р.	
5	Дослідження моделі безпечного середовища	20.11.2023 р.	
6	Оформлення отриманих результатів у ПЗ	25.11.2023 р.	
7	Оформлення графічного матеріалу	01.12.2023 р.	
8	Оформлення допоміжного матеріалу	10.12.2023 р.	

Студент  Дмитро КОЛЯНКІВСЬКИЙ
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник проєкту (роботи)  Костянтин КАСЬЯН
(підпис) (ім'я, ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 70 с., 24 рис., 9 табл., 18 джерел.

ІНТЕРНЕТ РЕЧЕЙ, РОЗУМНИЙ ДІМ, ВБУДОВАНА СИСТЕМА, БЕЗПЕЧНЕ СЕРЕДОВИЩЕ, СИСТЕМНІ РІШЕННЯ, МІКРОКОНТРОЛЕР, МЕРЕЖЕВІ ПРОТОКОЛИ, СТРУКТУРА СИСТЕМИ, СЦЕНАРІЇ РОБОТИ, ТЕСТУВАННЯ, ДОСЛІДЖЕННЯ.

Об'єкт дослідження - вбудовані системи на основі Інтернету речей.

Предмет дослідження - методи та засоби створення безпечного середовища будинку за допомогою вбудованої системи.

Мета дослідження: підвищення безпеки та ефективності управління домашнім середовищем за допомогою вбудованої системи на основі Інтернету речей.

Практичні результати: розроблено модель вбудованої системи для забезпечення безпечного середовища будинку на основі Інтернету речей.

Наукова новизна: вдосконалено методи розробки вбудованих систем шляхом застосування сучасних мережевих протоколів та хмарних технологій.

ABSTRACT

Explanatory note to the master's work: 70 pages, 24 figures, 9 tables, 18 sources.

INTERNET OF THINGS, SMART HOME, EMBEDDED SYSTEM, SECURE ENVIRONMENT, SYSTEM SOLUTIONS, MICROCONTROLLER, NETWORK PROTOCOLS, SYSTEM STRUCTURE, WORKING SCENARIOS, TESTING, RESEARCH.

The object of research is embedded systems based on the Internet of Things.

The subject of research is methods and means of creating a safe environment at home using an embedded system.

The purpose of the study: improving the safety and efficiency of managing the home environment using an embedded system based on the Internet of Things.

Practical results: a model of an embedded system has been developed to provide a secure home environment based on the Internet of Things.

Scientific novelty: methods of development of embedded systems have been improved by applying modern network protocols and cloud technologies.

ЗМІСТ

Вступ.....	7
1 Опис предметної області	9
1.1 Аналіз концепції IoT	9
1.2 Галузь застосування IoT	18
1.3 Вбудована система будинку.....	28
1.4 Аналіз переваг та недоліків організації безпечного середовища будинку технологією IoT	33
1.5 Висновки за розділом.....	35
2 Розробка вимог до системи	36
2.1 Аналіз існуючих системних рішень «Розумний дім».	36
2.2 Дослідження МК для розробки системи.....	41
2.3 Визначення та аналіз вимог до програмного забезпечення.....	43
2.4 Вибір мережевого протоколу	46
2.5 Висновки за розділом.....	49
3 Моделювання системи безпеки	50
3.1 Структура системи	50
3.2 Апаратна частина системи	53
3.3 Сценарії роботи	55
3.4 Висновки за розділом.....	58
4 Тестування та дослідження системи	59
4.1 Тестування функцій системи	59
4.2 Дослідження роботи системи через протоколи Wi-Fi та Z-wave.....	61
4.3 Висновки за розділом.....	66
Висновки	67
Перелік джерел посилання	68

ВСТУП

Останнім часом інтелектуальні системи являють собою сектор інформаційних технологій, що постійно розвивається. Розширення їхнього функціонального діапазону та можливостей прискореної обробки даних вимагає більш складного перерозподілу мережевих ресурсів і підвищення обчислювальної потужності для роботи суттєвих систем обробки даних [1]. Сучасні інформаційні системи, як правило, працюють на структурах, які включають людський нагляд і ґрунтуються на конструкціях попереднього століття. Хоча ці технології адекватно задовольняють системні вимоги, вони також призводять до використання надмірного часу для виконання завдань. Прогресивний підхід до управління центрами обробки даних та інформаційними системами передбачає інтеграцію інтелектуальних агентів та «Інтернету речей» (IoT) в операційні процеси [2].

Розширення IoT значно покращило інтерфейс користувача для безлічі взаємопов'язаних «розумних» пристроїв. Створення безперебійної взаємодії між пристроями, навіть від одного бренду, є складним завданням для розробників і дизайнерів. Незважаючи на різноманітність фізичних інтерфейсів, для користувача вкрай важливо сприймати єдину концепцію в рамках пропонованої послуги [3].

Термін «Інтернет речей» у 2019 році поширився за межі домашніх програмних і апаратних систем і охопив промислові підприємства. Еволюція «розумних будівель» призвела до створення «Інтернету речей» (BIoT), що представляє «Інтернет речей у будівлях», тоді як прогрес у розподіленій мережевій інфраструктурі в автоматизованих системах управління (ACS) породив «Промисловий Інтернет речей» (IIoT) [4].

Забігаючи вперед, очікується створення конвергентної екосистеми, що складається з традиційних технологій керування даними, систем промислового керування (ICS) і систем SCADA (систем диспетчерського

контролю та збору даних). Ця інтеграція може призвести до гібридних програмно-апаратних систем або навіть до складних соціально-технічних систем.

Інтеграція інтелектуальних систем і помічників може призвести до значної економії коштів на підтримку центрів обробки даних та інформаційних систем. Така інтеграція може оптимізувати процес виконання завдань, прискорити час відповіді на обробку запитів, покращити доступ користувачів до послуг і покращити безпеку за рахунок мінімізації помилок людини. Крім того, це може сприяти впровадженню нових методів програмного забезпечення для керування мережею, тим самим підвищуючи гнучкість і контроль над цими системами.

Інтернет речей та інтелектуальні системи — це не лише ефективність; вони також стосуються забезпечення вищого рівня взаємозв'язку між пристроями та системами. Завдяки IoT пристрої можуть спілкуватися та співпрацювати без втручання людини, що веде до розумнішого прийняття рішень і автоматизації в різних галузях. Наприклад, у розумному домі термостат може регулювати температуру на основі даних про погоду в реальному часі, або на виробництві датчики можуть передбачити збій обладнання до того, як він станеться, запобігаючи простоям [5].

Ще однією важливою перевагою є потенційний вплив на навколишнє середовище. Інтелектуальні системи можуть оптимізувати використання енергії та зменшити відходи, сприяючи більш екологічним практикам. Наприклад, будівлі з підтримкою IoT можуть ефективніше керувати ресурсами, використовуючи датчики для керування освітленням і опаленням залежно від кількості людей.

Сфера інтелектуальних систем та Інтернету речей швидко змінює те, як ми взаємодіємо з технологіями, керуємо ресурсами та ведемо бізнес. Постійний розвиток цих технологій обіцяє не лише підвищення ефективності, але й створення майбутнього, яке буде більш зв'язаним, стійким і чуйним на потреби промисловості та суспільства в цілому.

1 ОПИС ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз концепції IoT

Інтернет речей, який зазвичай скорочено називають IoT, являє собою розгалужену мережу обчислювальних пристроїв, механічних і цифрових пристроїв, об'єктів і навіть живих істот кожному з яких ідентифіковано унікальними кодами і які мають здатність обмінюватися інформацією між мережами. Підприємства в різних секторах все частіше застосовують технології IoT для підвищення ефективності роботи, поглиблення розуміння клієнтів, уточнення пропозицій послуг, сприяння прийняттю рішень і підвищення загальної вартості своїх підприємств.

IoT - це технологічна синергія різноманітних елементів, таких як бездротовий зв'язок, розширені алгоритми навчання, автоматизовані процеси, мікроелектромеханічні системи (MEMS) і підключення до Інтернету. Це об'єднання відіграло важливу роль у подоланні розриву між операційними технологіями (OT) та інформаційними технологіями (IT), надаючи засоби для аналізу величезних обсягів неструктурованих даних, отриманих від машин, щоб отримати інформацію, яка стимулює інноваційні прориви. Починаючи з 1982 року, концепція взаємопов'язаних інтелектуальних пристроїв зробила свій перший подих із підключеною до Інтернету кока-колою в Університеті Карнегі-Меллона, яка могла повідомляти про свій запас і температуру напоїв. Розгалужена взаємопов'язана мережа, яку ми сьогодні називаємо Інтернетом, багато в чому завдячує баченню Марка Вайзера щодо повсюдних обчислень, яке передбачає світ, у якому обчислення настільки плавно інтегровані в наші повсякденні середовища, що їх неможливо від них відрізнити [6]. У «Нових технологіях для навчання» Девід Бекта узагальнює цю концепцію, уявляючи обчислювальну потужність, непомітно вплетену в тканину світу, доступну

через інтелектуальні інтерфейси та настільки інтуїтивно вбудовану, що її присутність ледве помічається [7].

Щоб заглибитися в особливості, екосистема IoT характеризується кількома основними особливостями:

- штучний інтелект (AI) – наділяє IoT «інтелектуальними», покращуючи життя безліччю способів завдяки стратегічному використанню даних, взаємопов'язаним мережам і складним алгоритмам. Це може проявлятися як просте оновлення вашого холодильника, оснащеного датчиками, які виявляють і замовляють продукти, як-от молоко та яйця, коли запаси закінчуються, або більш складні програми, як-от прогнозне обслуговування на виробництві [8];

- підключення. Хоча широкомасштабні мережі є звичайним явищем, IoT процвітає завдяки можливості створювати менші, економічно ефективні мережі, які не погіршують функціональність. IoT чудово створює складні мережі між пристроями в системі, сприяючи безперебійному спілкуванню;

- датчики. Датчики є основою IoT, основою його успіху. Вони перетворюють потенціал IoT з концепції в реальну, активну мережу, що дозволяє збирати дані в реальному часі та механізми реагування в різноманітних програмах [9];

- активне залучення. На відміну від традиційних технологій, які покладаються на пасивну взаємодію, IoT є піонером ери активного залучення користувачів. Платформи IoT не просто реагують, але розроблені, щоб ініціювати дії, будь то доставка вмісту, надання послуг або використання продукту.

Крім того, вплив IoT виходить за рамки просто технологічного вдосконалення. Це прокладає шлях до розумніших міст з оптимізованими системами руху, більш ефективним управлінням відходами та покращеною громадською безпекою. У сфері охорони здоров'я IoT полегшує віддалений моніторинг, надаючи дані в режимі реального часу, що може призвести до кращих результатів для пацієнтів та більш персоналізованого догляду.

Екологічний потенціал IoT також заслуговує на увагу, оскільки розумні мережі та пристрої IoT сприяють зменшенню споживання енергії та меншому викиду вуглецю.

У ширшому розумінні майбутнє, сформоване Інтернетом речей, обіцяє не лише ландшафт, де зручність і ефективність є першорядними, але й такий, де кордони між людьми та технологіями дедалі більше розмиваються. Наслідки для суспільства величезні, оскільки IoT може революціонізувати доступність, створюючи розумніші та інклюзивніші середовища та потенційно переосмислюючи спосіб нашого життя та взаємодії з навколишнім світом. Реалізація повного потенціалу IoT полягає в нашій здатності долати виклики, такі як безпека та конфіденційність, і його успішну інтеграцію в повсякденне життя, роблячи його таким же всюдисущим і важливим, як сам Інтернет [10] (рис. 1.1).

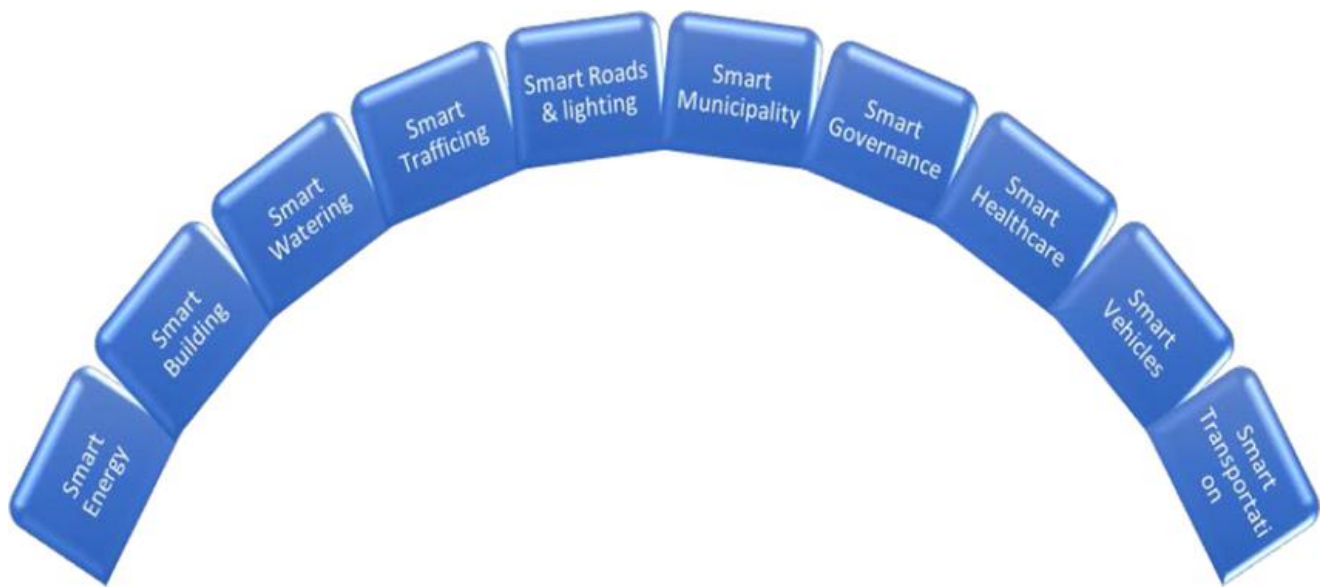


Рисунок 1.1 - Додаток на основі IoT в архетипах розумного міста [1]

Пристрої. Оскільки технологічний прогрес робить пристрої дедалі потужнішими, економічно ефективнішими та компактнішими, Інтернет речей використовує ці невеликі пристрої, щоб збільшити охоплення, гнучкість і точність. [2] Еволюція IoT Термін «Інтернет речей» вперше ввів Кевін Ештон, співзасновник Auto-ID Center Массачусетського технологічного

інституту, під час презентації в Procter & Gamble (P&G) у 1999 році. Метою Ештона було привернути увагу до технології радіочастотної ідентифікації (RFID), і він пов'язав свою презентацію з тенденцією епохи, що розвивається: Інтернетом. Хоча Ніл Гершенфельд, професор Массачусетського технологічного інституту, не використовував термін «Інтернет речей» у своїй книзі «Коли речі починають думати» 1999 року, його прогнози точно віддзеркалювали траєкторію IoT. Розвиток IoT можна віднести до злиття різних технологій, включаючи бездротовий зв'язок, мікроелектромеханічні системи (MEMS), мікросервіси та Інтернет. Це злиття зменшило різницю між оперативними та інформаційними технологіями, уможлививши аналіз неструктурованих даних, створених машинами, для отримання інформації для вдосконалення. Хоча Ештону приписують авторство цього терміну, концепція взаємопов'язаних пристроїв бере свій початок у 1970-х роках із появою широкого поширення комп'ютерів.

Коріння IoT лежать у зв'язку між машинами (M2M) — машини з'єднуються одна з одною безпосередньо через мережі, оминаючи потребу в втручанні людини. Зв'язок M2M передбачає підключення пристроїв до хмари для керування та отримання даних. IoT покращує комунікацію M2M, створюючи величезну мережу інтелектуальних пристроїв, які об'єднують людей, системи та інші програми, обмінюючись і збираючи дані. Ідея IoT є основою для підключення M2M.

Крім того, IoT розглядається як прогресивне розширення систем SCADA, які призначені для збору та аналізу даних у реальному часі на відстані для моніторингу та керування обладнанням. SCADA об'єднує апаратні та програмні компоненти — апаратне забезпечення збирає та передає дані в систему з програмним забезпеченням SCADA для обробки. Сучасні системи SCADA трансформувалися в ранні форми платформ IoT. Концепція IoT набула значного розвитку в середині 2010-х років, зокрема, коли уряд Китаю прийняв її як ключову ініціативу у своєму п'ятирічному плані розвитку.

Екосистема IoT складається з веб-розумних пристроїв, оснащених вбудованими системами, датчиками та комунікаційним обладнанням, яким поставлено завдання збирати та передавати дані про навколишнє середовище. Ці пристрої IoT передають свої дані на центральний шлюз IoT або інші крайові пристрої, надсилаючи їх у хмару для подальшого аналізу або обробляючи локально. Часом ці пристрої також взаємодіють і реагують на дані один одного. Ці взаємодії відбуваються в основному автономно з мінімальним людським впливом, хоча користувачі можуть змінювати налаштування, вводити команди або отримувати доступ до зібраних даних за потреби.

«Речі» в Інтернеті речей (IoT) охоплюють широкий спектр об'єктів, від персональних фітнес-браслів до самокерованих автомобілів. Незалежно від ролі, яку вони виконують для кінцевого користувача, ці пристрої потребують спеціальних компонентів для ефективного функціонування в їхніх мережах IoT.

Датчики є основними збирачами даних з навколишнього середовища, що є першим кроком у функціонуванні системи IoT. Незалежно від того, чи визначають фізичний стан людини, наприклад частоту серцевих скорочень для фітнес-браслета, чи фіксують близькість об'єктів для автономного автомобіля, ці датчики є невід'ємною частиною роботи пристрою [11].

Підключення та унікальна ідентифікація також мають вирішальне значення. Щоб пристрої брали участь у системах IoT, вони повинні передавати зібрані дані іншим системам або пристроям. Для цього необхідна унікальна цифрова ідентифікація, часто IP-адреса, що забезпечує змістовне спілкування в мережі.

Актuatorи дозволяють пристроям IoT виконувати заплановані дії з мінімальною фізичною взаємодією користувача або без неї. Наприклад, розумна лампочка може засвітитися у відповідь на дистанційну команду, або промисловий клапан може відкриватися або закриватися автономно, реагуючи на дані датчиків уздовж виробничої лінії [12].

Однак належне функціонування пристроїв IoT залежить не тільки від автоматизації; кілька інших технологій забезпечують безперебійну роботу систем IoT. Ключові серед них:

Шлюзи IoT діють як канали, полегшуючи потік даних від пристроїв до хмари. Вони служать для стандартизації різноманітних протоколів пристроїв в єдиний протокол і фільтрації зайвих даних.

Хмара служить центральним сховищем даних пристрою та основним місцем обробки даних. Виконуючи більшість завдань обробки, хмара звільняє окремі пристрої від цього тягаря.

Інтерфейс користувача представляє зібрані дані користувачам, дозволяючи їм вводити команди для пристроїв.

Рада з питань архітектури Інтернету визначила чотири критично важливі комунікаційні моделі, які підкреслюють широкі можливості підключення IoT, демонструючи, як взаємопов'язані пристрої підвищують цінність кожного пристрою та збагачують взаємодію з користувачем:

Зв'язок між пристроями передбачає пряму взаємодію між двома чи більше пристроями, часто за допомогою таких протоколів, як Bluetooth, Z-Wave або Zigbee. Ця модель поширена в пристроях, що носяться, і в розумних домашніх пристроях, де невеликі пакети даних обмінюються напряму.

Підключення пристрою до хмари зазвичай використовує Wi-Fi або Ethernet, підключаючи пристрої безпосередньо до хмари. Це налаштування дозволяє користувачам і їхнім програмам отримувати доступ до пристроїв і керувати ними віддалено, а також полегшує збір даних користувачів для покращення послуг.

Шлюзові пристрої служать посередниками в комунікаціях IoT, часто додаючи до системи рівні безпеки та трансляцію протоколів. Наприклад, у розумних будинках централізований концентратор може з'єднувати різні пристрої, дозволяючи їм працювати разом, незважаючи на різні протоколи зв'язку.

Модель ретроспективного обміну даними базується на структурі «хмара-пристрій», що дозволяє користувачам зберігати доступ і аналізувати зведені дані з кількох розумних пристроїв. Наприклад, компанія може застосувати цей підхід для збору та перегляду даних з усіх пристроїв у межах своїх об'єктів, зібраних у хмарі. Цей метод також допомагає подолати проблеми, пов'язані з портативністю даних.

Інтернет речей (IoT) значно покращує особисте та професійне життя, забезпечуючи повний контроль над різними аспектами. Окрім додатків для розумного дому, IoT має вирішальне значення для бізнесу, пропонуючи їм можливість спостерігати за роботою своїх систем у режимі реального часу. Цей моніторинг у режимі реального часу охоплює широкий спектр, від функціональності машини до ланцюга поставок і управління логістикою. IoT дозволяє компаніям оптимізувати процеси, скоротити витрати на робочу силу, мінімізувати відходи та покращити надання послуг, що призводить до економічно ефективних процесів виробництва та доставки та більшої прозорості у взаємодії споживачів. Охоплення IoT поширюється на кілька секторів, включаючи охорону здоров'я, фінанси, роздрібну торгівлю та виробництво. У міському плануванні ініціативи «розумного міста» допомагають економити енергію, а в сільському господарстві підключені датчики допомагають у моніторингу врожаю та прогнозуванні моделей росту.

IoT є ключовою технологією в повсякденному житті та, як очікується, продовжить своє поширення, оскільки все більше компаній визнають переваги взаємопов'язаних пристроїв для підтримки конкурентоспроможності на ринку (рис. 1.2).

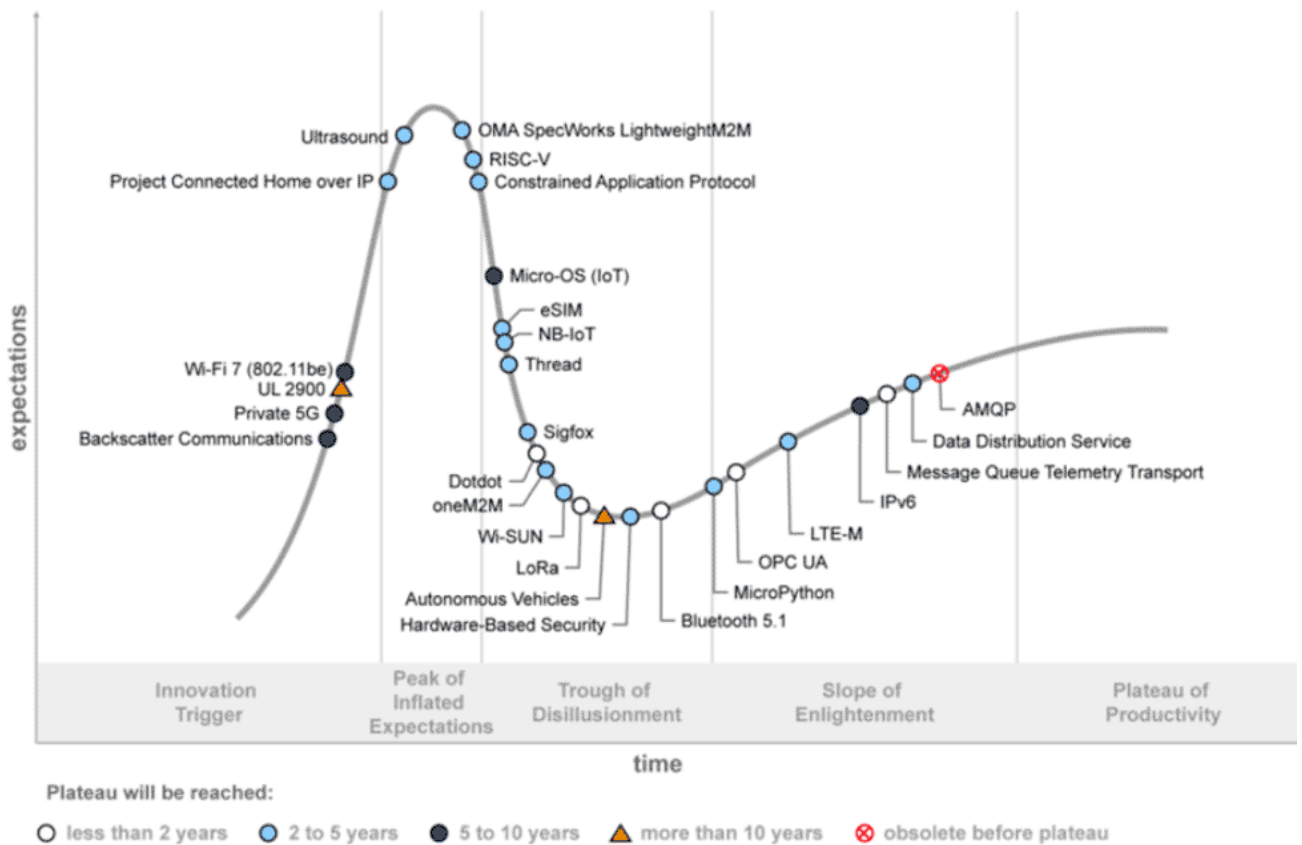


Рисунок 1.2 – Технологічний стек протоколів IoT [5]

Серед нових стандартів IoT:

- Bluetooth, особливо Bluetooth Low Energy (BLE) або Bluetooth Smart, має вирішальне значення для носимих пристроїв і передбачає підключення до мереж IoT, часто через смартфони. BLE розроблено для значного зниження енергоспоживання, зберігаючи радіус дії, який можна порівняти з класичним Bluetooth;

- 6LoWPAN дозволяє малопотужним радіостанціям спілкуватися в Інтернеті та підтримує різні технології, зокрема 802.15.4, Bluetooth Low Energy і Z-Wave, які зазвичай використовуються в домашній автоматизації;

- ZigBee — це бездротова мережа з низькою пропускну здатністю, що використовується переважно в промислових умовах і базується на стандарті IEEE 802.15.4. Альянс ZigBee розробив Dotdot, універсальну мову, яка дозволяє пристроям IoT взаємодіяти в різних мережах;

- LiteOS — це Unix-подібна операційна система для бездротових сенсорних мереж, яка підтримує інтелектуальні пристрої в різних програмах, таких як розумні будинки та Інтернет транспортних засобів (IoV). Це забезпечує основу для розробки розумних пристроїв;

- OneM2M — це глобальна ініціатива, спрямована на створення багаторазових стандартів для полегшення зв'язку між пристроями IoT у різних галузях;

- DDS від Object Management Group (OMG) є стандартом для масштабованого міжмашинного зв'язку в реальному часі;

- AMQP — це відкритий стандарт для асинхронного обміну повідомленнями, що забезпечує зашифрований взаємодіючий обмін повідомленнями між організаціями та програмами, включаючи керування пристроями Інтернету речей;

- LoRaWAN розроблений для малопотужних глобальних мереж (WAN), оптимізований для низького енергоспоживання та великих мереж із великою кількістю пристроїв, пропонуючи швидкість передачі даних від 0,3 Кбіт/с до 50 Кбіт/с;

- Z-Wave спеціалізується на домашній автоматизації, використовуючи простий протокол для швидкої розробки, хоча покладається на одного виробника мікросхем, Sigma Designs.

Платформи IoT включають:

- AWS IoT, розроблений Amazon, допомагає розумним пристроям підключатися до хмари AWS та інших пристроїв;

- ARM Mbed IoT полегшує розробку додатків IoT за допомогою мікроконтролерів ARM;

- Microsoft Azure IoT Suite пропонує послуги для взаємодії та обробки даних із пристроїв Інтернету речей із аналітикою та зручною для бізнесу візуалізацією даних;

- Brillo/Weave від Google, що включає Brillo, ОС на базі Android для вбудованих пристроїв, і Weave, комунікаційний протокол для взаємодії пристрою з хмарою;

- Calvin від Ericsson — це платформа з відкритим вихідним кодом для створення та керування розподіленими програмами, що забезпечує взаємозв'язок між пристроями, містить як структуру розробника, так і середовище виконання.

1.2 Галузь застосування IoT

Інтернет речей (IoT) знайшов свій шлях до широкого спектру додатків, торкаючись усього: від споживчих і бізнес-секторів до сфер виробництва та промисловості. Його вплив поширюється на різні галузі, такі як автомобілебудування, телекомунікації та енергетика.

Дані за 2018 рік свідчать про приголомшливу кількість понад 23 мільярдів пристроїв Інтернету речей у всьому світі, що затьмарює кількість населення Землі, яке на той час становило 7,6 мільярда. Розповсюдження цих підключених пристроїв лише стрімко зростатиме, і очікується, що протягом десятиліття перевищить 75+ мільярдів, як показано на графіку прогнозу підключених пристроїв, рис. 1.3.

Згідно з аналізом Accenture, до 2020 року ринок IoT досягне 14,2 трильйона доларів США. Водночас прогноз IDC передбачає, що компанії можуть витратити понад 1,2 трильйона доларів на IoT, а за прогнозом Бейна, до 2021 року ринок зросте приблизно до 520 мільярдів доларів.

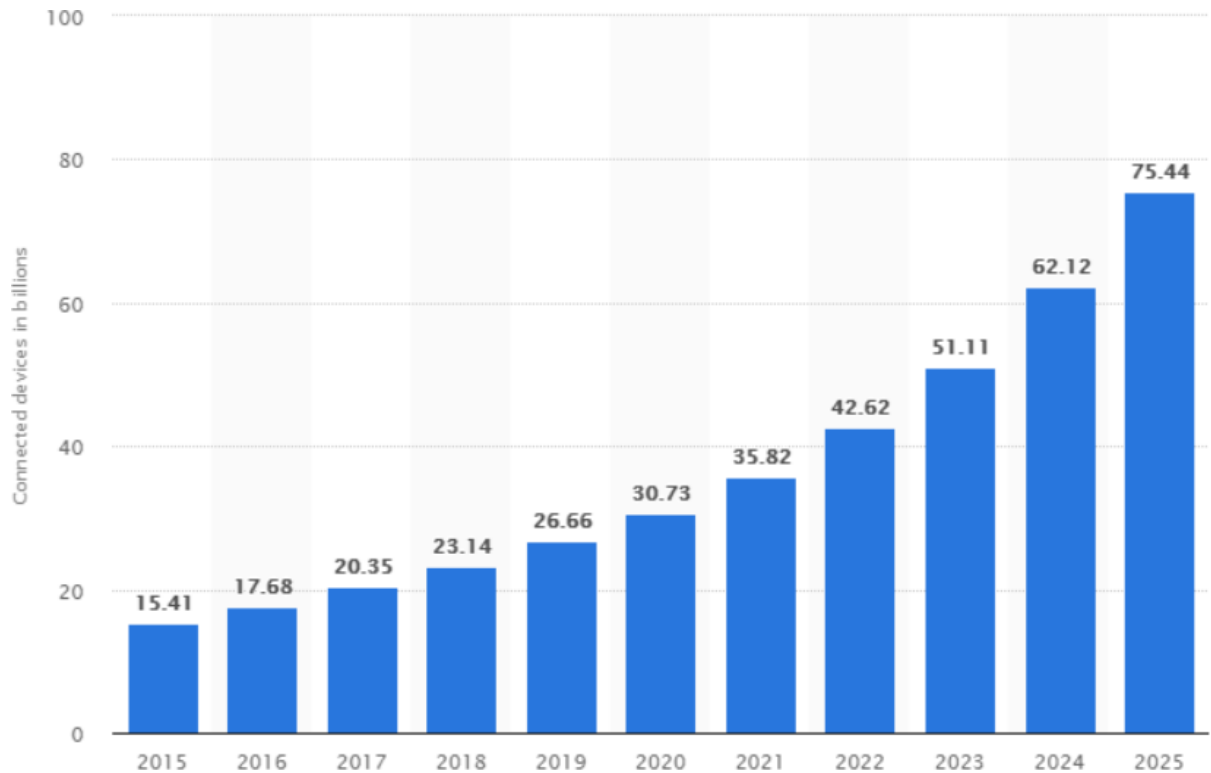


Рисунок 1.3 – Тенденція IoT

У сфері транспорту вплив IoT багатогранний:

- автомобільні компанії все більше інтегрують IoT, передбачаючи майбутнє, де автомобілі будуть «розумними». Ця революція має на меті зробити особисті транспортні засоби не просто транспортним засобом, а складною частиною зв'язаної екосистеми, яку можна порівняти з перевагами систем масового швидкого транспорту (MRT). Окрім простого вдосконалення інфраструктури навколо транспортних засобів, IoT вносить покращення в самі особисті транспортні засоби, перетворюючи їх на приватні простори, оснащені такими ж інтелектуальними функціями та налаштуваннями, які можна знайти в будинку з підтримкою IoT;

- автономні транспортні засоби, також відомі як самокеровані автомобілі або автомобілі без водія, займають перше місце в IoT у транспорті. Ці передові транспортні засоби оснащені набором датчиків, камер, радарів і штучного інтелекту (AI), щоб переміщатися з одного місця в інше без контролю людини. Щоб кваліфікуватись як повністю автономні, ці

транспортні засоби повинні бути здатні рухатися до заздалегідь визначеного пункту призначення стандартними дорогами без втручання людини.

Технології на основі ШІ революціонізують автономну роботу автомобілів. Розробники автономних транспортних засобів використовують широкий масив даних, отриманих із технологій розпізнавання зображень, а також складні можливості нейронних мереж і машинного навчання. Поєднання цих дисциплін дозволяє створювати транспортні засоби, які можуть керувати без участі людини. Нейронні мережі вміють розпізнавати шаблони з величезних обсягів даних, зібраних за допомогою датчиків та інших пристроїв, які потім обробляються алгоритмами машинного навчання. Яскравим прикладом є технологія, яку використовують автономні автомобілі Google, яка об'єднує дані з різних датчиків, щоб виявляти та розуміти навколишнє середовище навколо автомобіля.

Головним завданням транспорту є врегулювання заторів, зниження рівня аварій та оптимізація паркування. IoT пропонує розширені можливості для моніторингу та аналізу потоку трафіку через пристрої, розподілені по всій транспортній мережі. Це покращує керування паркуванням, спрощуючи процес пошуку місця, що є помітним покращенням у порівнянні з традиційними методами, які надають мінімальну інформацію. Аварії часто є наслідком багатьох факторів, у тому числі транспортного потоку. Зони будівництва, погані можливості громадського транспорту та відсутність інформації про дорожній рух у реальному часі – все це сприяє збільшенню аварій. IoT вирішує ці проблеми, покращуючи обмін інформацією як між громадськістю, так і між суб'єктами, які впливають на використання доріг.

У комерційному та промисловому секторах IoT значно підвищує ефективність транспорту. Він покращує керування автопарком, надаючи розширену аналітику та параметри контролю, наприклад моніторинг часу простою, використання палива, умов подорожі та тривалості подорожі. Це трансформує логістичні послуги, роблячи їх більш надійними та

інтегрованими, а не набором незалежних підрядників, як показано на малюнку 1.5 для додатків промислового транспорту.

Сектор охорони здоров'я отримує численні переваги від Інтернету речей, від покращеного моніторингу пацієнтів – завдяки зібраним і проаналізованим даним – до управління запасами фармацевтичних препаратів і медичного обладнання. Лікарні все частіше використовують системи Інтернету речей для виконання різноманітних завдань, таких як відстеження та управління запасами.

Присутність IoT в охороні здоров'я зростає, а його застосування є ключовим у цифровій трансформації сектора. Це включає в себе управління медичними матеріалами, оцифровку медичних записів і оптимізацію клінічних процесів. Використовуючи технологію RFID, IoT почав розширювати свої застосування у візуалізації медичних ланцюжків поставок. Завдяки інтеграції RFID в рішення IoT стає можливим запобігати проблемам охорони здоров'я, пов'язаним із виробництвом, розповсюдженням і відстеженням медичного обладнання та ліків, підвищуючи якість медичної допомоги та одночасно зменшуючи адміністративне навантаження.

Всесвітня організація охорони здоров'я (ВООЗ) повідомляє, що підроблені ліки складають понад 10% фармацевтичних продажів у всьому світі. Зокрема, у Китаї дані Китайської фармацевтичної асоціації свідчать про те, що щонайменше 200 000 смертей трапляються щорічно через неправильне або неправильне використання ліків. Зловживання охоплює від 11 до 26% пацієнтів, які приймають ліки неправильно, з яких приблизно 10% ліків призначаються неправильно. У цьому контексті технологія RFID відіграє вирішальну роль у безпечному відстеженні та перевірці фармацевтичних препаратів і медичного обладнання, допомагаючи регулювати ринок.

Продукти, прикріплені мітками RFID, яким присвоєно чітку ідентичність, яку важко відтворити, будуть корисними для перевірки автентичності та боротьби з підробленими ліками. Такі заходи посилять захист від медичного шахрайства. Наприклад, інформація про ліки може бути

завантажена в загальнодоступну базу даних. Пацієнти або постачальники медичних послуг можуть потім перехресно перевірити інформацію на етикетці з базою даних, щоб легко виявити підробку, як показано на малюнку 1.6, на якому показано використання IoT в медицині.

Інтернет речей має значні перспективи для управління медичною інформацією. Потреба в лікарнях для управління медичною інформацією охоплює ідентифікацію, розпізнавання образів і категоризацію медичних записів. Це включає в себе ідентифікацію пацієнтів, лікарів, ліків, медичного обладнання, лабораторних зразків і медичних записів, які включають категоризацію симптомів і захворювань. Зараз медичним дослідженням часто не вистачає життєво важливих реальних даних, замість цього вони покладаються на надлишки матеріалів, контрольовані умови та добровольців.

Служби екстреної допомоги, які традиційно відчують навантаження через обмеження ресурсів, покращуються завдяки автоматизації та аналітиці з підтримкою Інтернету речей. Сценарії надзвичайних ситуацій можна оцінити здалеку, при цьому служби отримують доступ до історії пацієнтів до їх прибуття, сприяючи швидкому та ефективному лікуванню, таким чином зменшуючи пов'язані з цим ризики та покращуючи реагування на надзвичайні ситуації.

У сфері освіти IoT перетворює традиційні навчальні простори на інтелектуальне середовище, збагачуючи як фізичний простір, так і навчальні процеси, як показано на малюнку 1.7 про застосування IoT в освіті. «Розумні школи» сприяють покращенню особистого досвіду навчання завдяки простому керуванню завдяки пристроям, які спілкуються через мережі Wi-Fi для надсилання та отримання даних.

Сучасні мультимедійні інтерактивні дошки далекі від своїх спрощених попередників. Такі платформи, як Glogster, зробили революцію у створенні цифрових плакатів, дозволивши інтегрувати зображення, аудіо, відео, текст і гіперпосилання, якими потім можна легко поділитися з однолітками чи вчителями в електронному вигляді. Ці цифрові плакати можна поширювати

електронною поштою, отримати доступ через URL-адреси або відображати в блогах класу. Поява розумних дощок дозволила викладачам легко включати онлайн-ресурси та мультимедіа у своє навчання.

Навчання вийшло за рамки статичних текстів і зображень, щоб включити додаткові матеріали, такі як відео, вікторини, анімації тощо, доступ до яких доступний через підручники та додаткові онлайн-платформи. Ці ресурси надають учням ширші перспективи для більш повного вивчення нових концепцій, сприяючи кращій взаємодії з учителями та однолітками. Тепер вчителі привносять реальні виклики в клас, заохочуючи учнів досліджувати та знаходити рішення самостійно.

Інтернет речей (IoT) є ключовим у створенні підключеної мережі за допомогою спеціалізованих систем на основі Інтернету. Він надає педагогам і дослідникам передові інструменти, які відображають академічний прогрес. Такі платформи, як Edmodo, сприяють безперебійній взаємодії між викладачами та студентами, дозволяючи учням отримувати доступ до навчальних матеріалів у будь-який час і з будь-якого місця. IoT сприяє розширеному режиму спілкування, дозволяючи студентам і викладачам перевіряти оновлення та листуватися поза традиційним середовищем у класі, забезпечуючи високий рівень безпеки та конфіденційності для особистого розуміння та академічної роботи.

Впровадження IoT в освітніх середовищах має вирішальне значення, особливо для підвищення безпеки за допомогою найсучасніших технологій реагування. Він охоплює екстрені сигнали, покращення слуху, годинник із підтримкою Wi-Fi та сповіщення для людей із вадами слуху, сприяючи безпечній атмосфері для студентів та персоналу. Технології IoT мають потенціал зменшити шкоду та врятувати життя у важких ситуаціях. Навчальні заклади впроваджують спеціальні заходи безпеки для забезпечення безпеки кампусу. Комунікаційні системи на основі Інтернету речей можна використовувати для різних сповіщень, включаючи унікальні екстрені сигнали, сповіщення в прямому ефірі, кілька розкладів дзвінків і

попередньо записані повідомлення для керівництва персоналом і студентами під час надзвичайних ситуацій.

IoT допомагає розвивати розумні країни та міста, включаючи розвиток інфраструктури, як-от охорона здоров'я та транспорт, зміцнення оборони та покращення муніципальних послуг (рис. 1.4.).

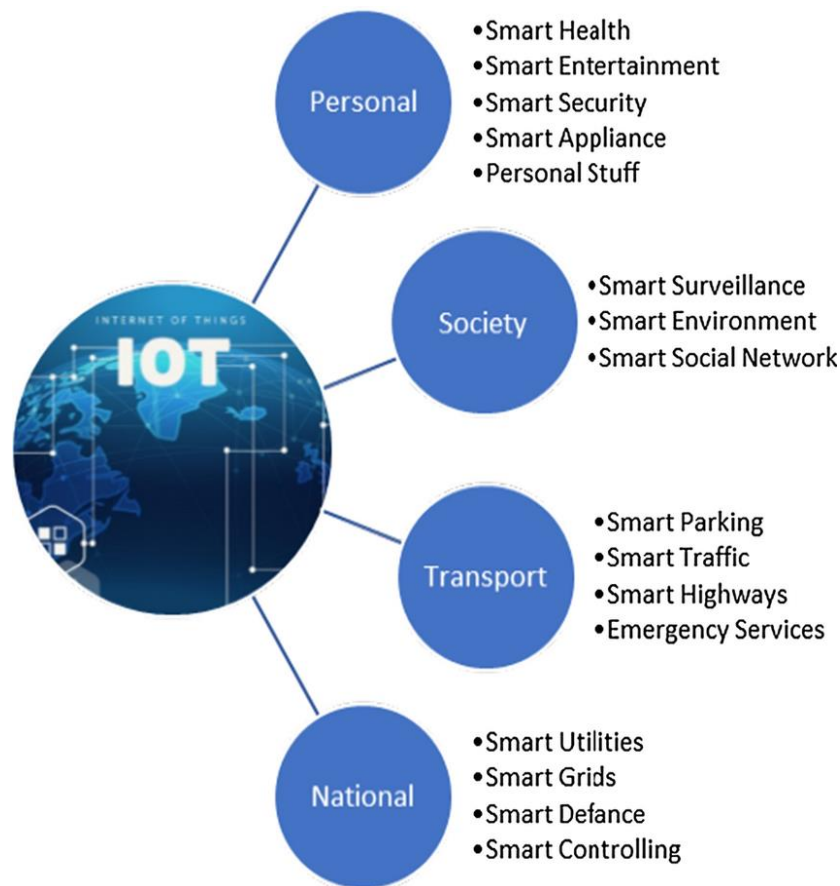


Рисунок 1.4 – Застосування IoT [7]

IoT революціонізує національну оборону, підтримуючи правоохоронні органи та системи національної безпеки за допомогою складних технологій. Це допомагає підвищити безпеку кордону за допомогою рентабельних і високопродуктивних пристроїв, якими також легко керувати. IoT оптимізує операції безпеки, які зазвичай залучають кілька відділів і персоналу, підвищуючи точність і час реакції.

Розумні міста використовують IoT для розвитку фізичної інфраструктури та послуг для покращення якості життя мешканців і

підприємств, а також підвищення ефективності уряду. Він виходить за рамки простої автоматизації процесів, об'єднуючи різні системи та мережі для збору та аналізу даних, які потім використовуються для трансформації операцій у всьому місті. Розповсюдження розумних міст стало більш актуальним із зростанням міграції в міста, що робить сталий розвиток критично важливим. Взаємодія між міськими структурами, громадянами та підприємствами тепер більш динамічно фіксується в режимі реального часу.

IoT є потужним інструментом для міських планувальників та інженерів для вирішення складних аспектів міського розвитку та управління. Він допомагає аналізувати такі фактори, як демографічні зміни, зонування, картографування, розподіл води, транспортні мережі, постачання продуктів харчування, соціальні послуги та землекористування. IoT збирає детальні дані в цих областях, надаючи більш цінну та точну інформацію, ніж звичайна аналітика, завдяки тісній інтеграції з динамікою міста. Інтернет речей в управлінні допомагає розгортати життєво важливу міську інфраструктуру та послуги, такі як транспорт і охорона здоров'я, а також поширюється на управління водними ресурсами, утилізацію відходів і реагування на кризи, як показано на малюнку 1.8 про управління містом за допомогою IoT.

IoT є важливим державним додатком, пропонуючи комплексний економічний аналіз, прояснюючи раніше непрозорі аспекти економіки та покращуючи моніторинг і прогнозне моделювання фінансових тенденцій. Він ретельно вивчає галузі та ринки, щоб точно визначити перспективи зростання та виклики.

Технологія IoT вирішує складні проблеми водної безпеки, дозволяючи урядам оптимізувати розподіл водних ресурсів, задовольняти запити споживачів і вдосконалювати методи управління. Успішне вирішення питань управління водними ресурсами потребує багатогранних внесків, і IoT сприяє цьому шляхом інтеграції даних від різних зацікавлених сторін, деякі з яких можуть не брати безпосередньої участі в зусиллях зі збереження води.

IoT також відіграє вирішальну роль у швидкому реагуванні на надзвичайні ситуації, надаючи урядам дані та комунікаційні інструменти в реальному часі для ефективного управління та пом'якшення кризових ситуацій.

Програми Інтернету речей (IoT) дозволяють швидко отримувати дані про інциденти, що покращує здатність персоналу екстреної допомоги розуміти ситуації, виробляти стратегію реагування та вживати рішучих і своєчасних заходів. Наприклад, датчики навколишнього середовища можуть виявляти та передавати ранні ознаки небезпеки або злочинної діяльності. Такі технології, як ShotSpotter, уже здатні розпізнавати звук пострілу та точно визначати його джерело, сприяючи швидкому реагуванню поліції, не покладаючись лише на звіти очевидців для документування злочину, таким чином допомагаючи розкрити злочин.

У галузі промисловості промисловий Інтернет речей (IIoT) є сферою, що розвивається, і становить значну частину світових витрат на IoT. Промисловці та виробники в різних секторах отримують вигоду не лише від моніторингу, але й від автоматизації складних виробничих процесів. Хоча промислові датчики та системи відстеження вже давно використовуються, IIoT покращує це завдяки більшій деталізації та точності навіть для незначних проблем.

Машини, інтегровані в IIoT, можуть передавати оперативні дані людям, наприклад виробникам оригінального обладнання (ОЕМ) та інженерам, що сприяє автоматизації та оптимізації процесів. Менеджери спрощують дистанційне керування роботою заводу, що покращує командну роботу та точно визначає критичні показники продуктивності та потенційні проблемні області.

Датчики IIoT у виробничому обладнанні запускаються на основі графіків технічного обслуговування. Оскільки машини призначені для роботи в межах певних порогових значень температури та вібрації, датчики Інтернету речей активно відстежують і надсилають сповіщення, якщо ці

параметри перевищуються, що дозволяє заощаджувати енергію, скорочувати витрати, запобігати простоям і підвищувати ефективність завдяки підтримці оптимального робочого середовища.

Системи IoT мають вирішальне значення для моніторингу діяльності ланцюга поставок, пропонуючи глобальне відстеження запасів на рівні товарів. Вони сповіщають користувачів про будь-які значні відхилення від запланованих дій. Це дає широке багатоканальне розуміння запасів, дозволяючи менеджерам отримувати інформацію в реальному часі про поточні запаси, поточну роботу та графіки надходження матеріалів, таким чином оптимізуючи постачання та мінімізуючи надлишкові та зайві витрати.

Безпека працівників на підприємствах забезпечується IoT у поєднанні з аналітикою великих даних. Інфраструктура Інтернету речей відстежує життєво важливі показники здоров'я та безпеки, такі як рівень травматизму, захворювань, дорожньо-транспортних пригод і пошкодження майна під час роботи. Завдяки ефективному моніторингу можна запровадити покращені заходи безпеки, урахувуючи будь-які відстаючі показники та покращуючи загальні стандарти охорони здоров'я, безпеки та навколишнього середовища (HSE).

Датчики IoT збирають різноманітні дані протягом циклу продукту, включаючи склад сировини, умови навколишнього середовища, відходи, вплив транспортування та настрої клієнтів. Аналіз цих складених даних може виявити та вирішити потенційні проблеми з якістю.

Виробники використовують датчики Інтернету речей у продуктах або упаковці, щоб зрозуміти моделі використання та поведінки, відстежувати стан продукту під час транспортування та оцінювати вплив факторів навколишнього середовища, таких як погода та дорожні умови. Ця інформація допомагає вдосконалювати продукти та упаковку, щоб підвищити довговічність і взаємодію з користувачем, оптимізуючи витрати.

Додаток IIoT у логістиці та ланцюзі поставок надає дані в режимі реального часу, відстежуючи матеріали, продукти та обладнання по всьому

ланцюгу поставок. Завдяки ефективному збору даних та інтеграції в такі системи, як ERP і PLM, підключені фабрики та постачальники можуть відстежувати залежності, тривалість циклів і матеріальні потоки, допомагаючи виробникам скорочувати запаси, передбачити потенційні проблеми та мінімізувати вимоги до капіталу.

1.3 Вбудована система будинку

Розумний дім поєднує в собі передові досягнення в області хмарних технологій, підключення до Інтернету, аналізу даних і архітектурного дизайну для підвищення видимості, ефективності та контролю, що забезпечує більш задоволене життя. Концепція інтелектуальних будівель, хоч і не зовсім нова — з огляду на те, що певний час у будинках були вбудовані інтелектуальні елементи, такі як автоматизовані освітлювальні прилади та термостати, — зазнала значного розвитку разом із сучасними технологіями. Сьогодні «розумний дім» поєднує в собі досягнення в Інтернеті речей (IoT), хмарних обчисленнях, підключенні та аналітиці, створюючи проактивне, адаптивне середовище, яке реагує на зміни умов за допомогою взаємопов'язаних систем і набору датчиків і пристроїв.

Дані мережі в розумних будівлях постійно збирають і обробляють величезну кількість цінних даних про навколишнє середовище та його мешканців, включаючи температуру, рівень освітлення, присутність людей і навіть біометричні дані. Дані потім інтегруються з іншими системами для аналізу, сприяючи більш розумним діям і рішенням щодо управління ресурсами, наприклад надсилання попереджувальних сповіщень про потенційні збої обладнання.

Сфера «розумних будівель» стрімко розширюється завдяки технологічним інноваціям і вимогам ринку. Gartner передбачив, що до 2020

року комерційні будівлі матимуть понад мільярд підключених рішень. Ці рішення IoT дозволяють будинкам використовувати дані з безлічі пристроїв, що приносить переваги на рівнях інфраструктури та мешканців і тепер стає економічно доцільним у більших масштабах [13] (рис. 1.5).

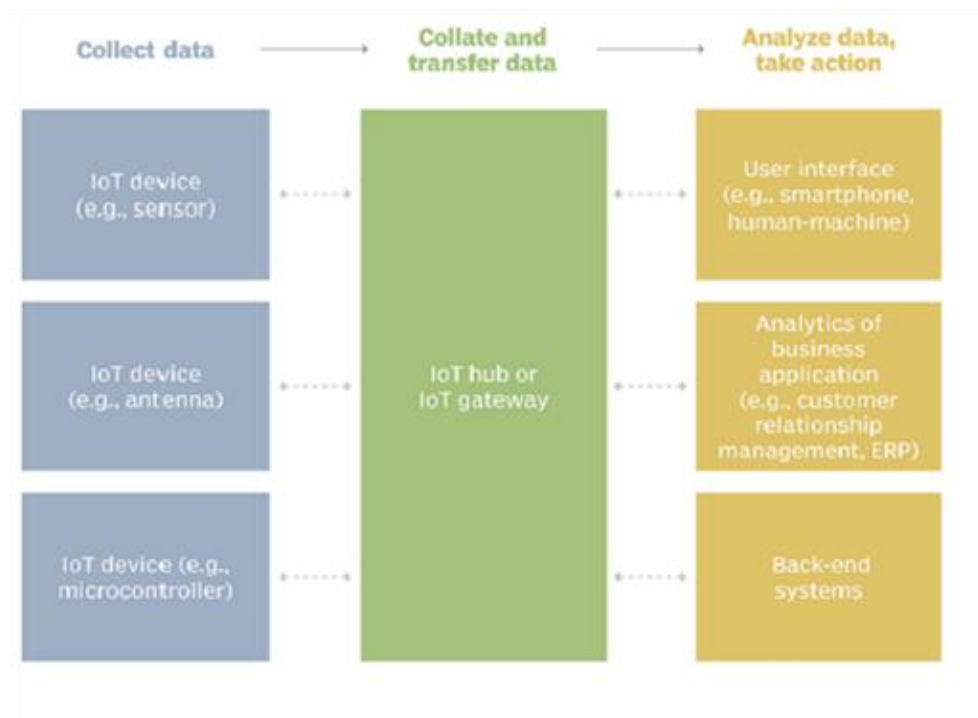


Рисунок 1.5 – Приклад структури сервісу розумного будинку

Значне зниження витрат на апаратне забезпечення зробило можливим встановлення інтелектуальних пристроїв і датчиків як у нових, так і в існуючих будівлях. Завдяки широкому підключенню та стандартизованим протоколам побудови інтеграція стала простішою та швидшою. Хмарна технологія полегшує вилучення значної цінності з великих обсягів будівельних даних. Ці технологічні досягнення каталізують розвиток інтелектуальних будівельних рішень, а також ширшої індустрії Інтернету речей.

Культурні зрушення та демографічні зміни також змінюють очікування мешканців, а такі тенденції на робочому місці, як гарячі столи та комунальні послуги, впливають на корпоративні пріоритети щодо співпраці та адаптації. Ці очікування, що змінюються, зумовлюють попит на рішення для розумних

будівель, які також ґрунтуються на нормах сталого розвитку та нових стандартах оренди приміщень.

«Розумні будівлі» набувають все більшої популярності, задовольняючи критичні потреби забудовників, операторів та мешканців. Власників нерухомості приваблюють інтелектуальні будівельні рішення для покращеного нагляду, який вони забезпечують за експлуатацією будівлі та добробутом, що дозволяє точно керувати витратами та ресурсами, виявляти та виправляти неефективність, а також покращувати використання простору. Власники, як правило, прагнуть отримати всебічний оперативний огляд, який сприяють рішення для розумних будівель, інтегруючи дані між системами, пропонуючи цілісне уявлення про окремі будівлі чи цілі комплекси [14].

Власники нерухомості прагнуть підвищити вартість своїх інвестицій, зберігаючи високий рівень заповнюваності. Вони прагнуть створити привабливе та привабливе середовище для мешканців. Для власників компаній це означає можливості для підвищення продуктивності робочої сили. Для власників комерційної нерухомості це означає надання унікального досвіду орендарям і потенційне відкриття нових доходів за допомогою додаткових послуг. Оператори будівництва переслідують ті ж цілі, що й власники, наприклад прагнення до практичних ідей, які призводять до зменшення використання ресурсів, досягнень сталого розвитку, підвищення ефективності та оптимізації операційних процесів. Оператори, зокрема, цінують інформацію в реальному часі, яка дозволяє швидше вирішувати проблеми, більш проактивно керувати продуктивністю та гарантувати задоволеність мешканців. Провідні рішення для інтелектуальних будівель виділяються тим, що надають такі дані в реальному часі в зручних для користувача форматах, як-от інформаційні панелі та візуалізації.

Концепція «розумного дому» зробила значний стрибок вперед із запровадженням протоколу X10 у 1975 році, зробивши домашню автоматизацію відчутною реальністю, що нагадує футуристичні бачення з серіалів на кшталт «The Jetsons». X10 використовував існуючу електричну

проводку будинку, щоб надсилати цифрові команди підключеним пристроям, керуючи їх роботою. Однак через такі обмеження, як перешкоди та односторонній зв'язок, надійність X10 не була абсолютною, що стало лише початком еволюції до повністю інтегрованих розумних будинків сучасності [15].

Дім із цифровим зв'язком, або розумний дім, використовує найновіші розробки домашньої автоматизації, щоб забезпечити легкий нагляд і керування різними електронними пристроями в домогосподарстві. Розповсюдження смартфонів значно пришвидшило еволюцію та популярність розумних будинків. Смартфон, озброєний комплексним набором додатків, служить універсальним командним центром для інтелектуальних пристроїв, організовуючи та автоматизуючи такі завдання, як регулювання температури, освітлення, електроприладів і систем безпеки. Традиційно такі побутові функції, як відмикання дверей, налаштування сигналізації, регулювання температури та керування розважальними системами, вимагають ручного втручання.

Однак «розумний дім» оптимізує ці завдання в одній інтегрованій системі, якою можна легко керувати за допомогою одного пристрою — часто смартфона. Уявіть, що ви повертаєтеся додому, де двері гаража автоматично відчиняються, вхідні двері, що автоматично відчиняються, освітлювачі, які освітлюють ваш шлях, кліматичні системи, які налаштовуються відповідно до вашого комфорту, і музика, яка починає відтворюватися — все це запускається без натискання жодної фізичної кнопки. Ця зручність не є спонтанною; для цього потрібне стратегічне планування, ретельний вибір сумісних електротехнічних виробів, безпечна та надійна домашня мережа та певне розуміння цифрових систем.

Ілюстрацією цього є «розумні будинки», де основною мотивацією для прийняття є економія енергії та коштів. Багато власників розумних будинків починають із розумних термостатів і освітлення, щоб скоротити споживання енергії, тим самим зменшивши витрати. Дослідження показують, що лише

інтелектуальні термостати можуть зменшити витрати на опалення до 12% і витрати на охолодження до 15%. Окрім енергозбереження, підвищена безпека є вагомою причиною для впровадження технології розумного будинку. Завдяки інтеграції веб-камер, розумних замків, датчиків і систем безпеки власники будинків можуть стежити за своєю власністю з віддалених місць через Інтернет.

Основною перевагою домашньої автоматизації є впевненість, яку вона пропонує власникам будинків, дозволяючи їм перевіряти потенційні ризики, як-от залишені ввімкненими прилади чи незахищені двері, будь-де. Це особливо корисно для людей похилого віку, забезпечуючи рівень моніторингу, який може допомогти їм залишатися вдома безпечно та комфортно. Домашня автоматизація підвищує ефективність — не потрібно залишати кондиціонер працюючим цілий день; розумна система може підлаштуватися під ваш розклад і охолодити ваш дім до вашого повернення. Цей принцип поширюється на всі прилади і навіть на зрошення саду, гарантуючи, що вода використовується лише тоді, коли це необхідно. Результатом є більш ефективне використання ресурсів, що приносить користь як навколишньому середовищу, так і гаманцю власника будинку.

Однак складність систем домашньої автоматизації перешкоджає їх широкому впровадженню. Для деяких складність розумних будинків здається лякаючою; вони можуть бути викликані технологією або знеохочені після початкових труднощів. Виробники та галузеві альянси прагнуть спростити роботу користувача, зробивши її приємною та доступною для людей різного рівня технічної підготовки. Для максимальної ефективності пристрої в системі розумного дому повинні бути сумісні, працювати за загальними або сумісними протоколами — це єдиний стандарт, який ще належить встановити на різноманітному ринку домашньої автоматизації.

Безпека є ще однією проблемою в розумних будинках; дослідження NTT DataCorp. У 2016 році було виявлено, що 80% американців стурбовані безпекою своїх даних у розумних будинках. Інциденти злому не лише

становлять загрозу для вимкнення світла та дезактивації сигналізації, але й ризикують надати хакерам доступ до особистих мереж, що призведе до більш серйозних атак або витоку даних. Крім того, конфіденційність викликає серйозне занепокоєння, і багато людей з обережністю ставляться до даних, зібраних пристроями розумного будинку. Незважаючи на наміри виробників удосконалити продукти або запровадити нові послуги на основі цих даних, довіра споживачів і прозорість є ключовими для виробників, щоб налагодити стосунки з розумними користувачами продуктів.

1.4 Аналіз переваг та недоліків організації безпечного середовища будинку технологією IoT

Створення безпечного середовища будинку на основі Інтернету речей надзвичайно актуальним в сучасному світі, де технології швидко розвиваються і все більше інтегруються в повсякденне життя людей. В таблиці 1.1 показано важливість і актуальність цього напрямку.

Однак, разом з численними перевагами, важливо також звертати увагу на питання приватності та безпеки даних, оскільки збільшення кількості підключених пристроїв може створювати нові вразливості. Тому при розробці IoT-систем для домашнього використання, необхідно включати ретельно продумані заходи забезпечення кібербезпеки та захисту даних.

На сучасному ринку існує велика кількість програмних та апаратних IoT-рішень для створення безпечного середовища вдома (табл. 1.2).

Таблиця 1.1 – Актуальність організації безпечного середовищу будинку технологією IoT

Послуги	Застосування
Безпека і контроль	IoT технології дозволяють власникам будинків віддалено моніторити та керувати системами безпеки, включно з камерами спостереження, датчиками руху, інтелектуальними замками та системами сигналізації. Це забезпечує посилену безпеку та можливість швидкого реагування на будь-які потенційні загрози.
Енергоефективність	Інтеграція IoT в домашні системи також сприяє оптимізації споживання енергії. Інтелектуальні термостати та освітлювальні системи можуть автоматично регулювати температуру та освітлення, знижуючи витрати на енергію і зменшуючи вплив на довкілля.
Зручність і комфорт	Автоматизація домашніх процесів, таких як керування освітленням, температурою, мультимедіа та іншими побутовими приладами, робить повсякденне життя більш зручним та комфортним.
Охорона здоров'я	IoT може сприяти покращенню домашньої охорони здоров'я, особливо для літніх людей або осіб з особливими потребами, через моніторинг стану здоров'я та надання екстреної допомоги при необхідності.
Інтеграція з іншими системами	IoT-технології можуть інтегруватися з більш широкими міськими та комунальними системами, такими як системи управління водопостачанням чи електропостачанням, що дозволяє максимально ефективно використовувати доступні ресурси.
Персоналізація	IoT дозволяє налаштувати середовище будинку відповідно до індивідуальних переваг і звичок його мешканців, що підвищує рівень особистого комфорту.

Таблиця 1.2 – Сучасні програмні засоби IoT-систем

Назва	Опис
Home Assistant	Це програмне забезпечення з відкритим кодом для домашньої автоматизації, яке підтримує понад 400 пристроїв і фокусується на локальному контролі та конфіденційності. Воно сумісне з багатьма пристроями та протоколами, такими як SSDP, Zigbee, та Wi-Fi.
OpenHAB	Це також програмне забезпечення з відкритим кодом, яке може підтримувати понад 250 пристроїв і сумісне з різними операційними системами. Воно пропонує єдиний інтерфейс користувача та сумісність з багатьма системами та пристроями
Jeedom	Ця платформа дозволяє керувати різноманітними автоматичними домашніми пристроями і може взаємодіяти з ними через SMS, голос або мобільні додатки. Jeedom підтримує такі розумні пристрої, як освітлення та термостати, і сумісна з Amazon Alexa та Google Assistant.
AGO Control	Це універсальне рішення, яке може використовуватися в різних сферах і використовує AMQP Enterprise Message Bus як легкий протокол. Воно сумісне з багатьма пристроями та має хмарні функції.

Налаштовуючи систему домашньої автоматизації можна використовувати платформу з відкритим кодом або пропрієтарну платформу. Кожен пропонує різні функції щодо конфіденційності даних, сумісності пристроїв, міркувань вартості, підтримуваних протоколів

1.5 Висновки за розділом

У першому розділі було досліджено концепцію Інтернету речей та її застосування для створення безпечного та ефективного середовища вдома.

Проаналізовано переваги та недоліки використання технології IoT для організації безпеки будинку.

Зроблено висновок, що Інтернет речей надає широкі можливості для покращення комфорту та безпеки в будинку за рахунок інтеграції різноманітних датчиків, пристроїв та мереж. Визначено, що для ефективної роботи такої системи потрібно забезпечити сумісність пристроїв, захист даних та зручний інтерфейс користувача.

Отже, застосування концепції Інтернету речей є перспективним напрямком для створення комплексних систем безпеки та автоматизації будинку.

2 РОЗРОБКА ВИМОГ ДО СИСТЕМИ

2.1 Аналіз існуючих системних рішень «Розумний дім»

У сфері розумних будинків стандартна установка включає в себе різні датчики, призначені для моніторингу таких аспектів, як температура, вологість і освітлення. Кожен із цих датчиків призначений для виявлення певних типів даних, а деякі здатні вимірювати кілька елементів, як-от температуру та вологість одночасно. Інші датчики призначені для оцінки інтенсивності світла та близькості об'єктів у певному просторі. Ці датчики є невід'ємною частиною накопичення даних і їх подальшого відображення, що дозволяє користувачам отримувати доступ до цієї інформації з будь-якого місця в будь-який час. Ця система включає в себе блок обробки сигналів, засіб зв'язку та хмарну службу хостингу.

Для управління побутовою технікою створено хмарний сервіс, централізований у хмарній інфраструктурі. Ця послуга полегшує користувачеві контроль над розумними приводами, пов'язаними з різними приладами, такими як освітлення та вентилятори. Ці розумні приводи, які

включають такі пристрої, як клапани та перемикачі, здатні виконувати такі функції, як увімкнення/вимкнення пристроїв і налаштування параметрів. Вони пропонують кілька утиліт, включаючи роботу клапана, регулювання положення, модуляцію потоку та функції аварійного відключення. Активація цих приводів здійснюється за допомогою цифрових команд.

Технології контролю доступу зазвичай використовуються для безпечних точок входу. Ця система використовує базу даних, що містить ідентифікаційні дані авторизованих осіб. Коли хтось намагається отримати доступ, система негайно порівнює їхні облікові дані з цією базою даних, надаючи або забороняючи вхід на основі відповідності. Для великих установ хмарні служби використовуються для централізованої обробки цих персональних ідентифікаційних даних. Для цього впроваджуються різні технології, починаючи від магнітних або безконтактних карток і закінчуючи більш просунутими методами, такими як розпізнавання обличчя, ідентифікація за відбитками пальців і RFID.

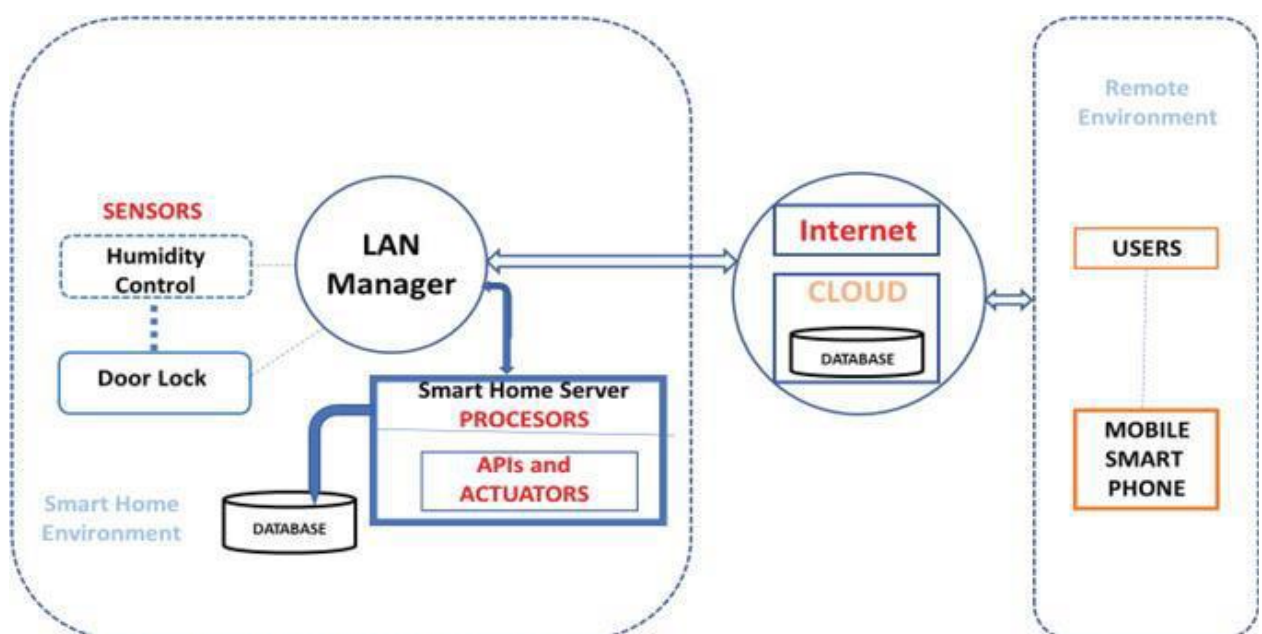


Рисунок 2.1 - Розумний дім із додатковим підключенням до хмари

Ця система включає датчики для збору внутрішніх і зовнішніх даних про оточення в домі. Ці датчики інтегровані як у сам будинок, так і в

підключені до нього пристрої. Примітно, що вони відрізняються від датчиків Інтернету речей, приєднаних до побутової техніки. Дані, зібрані цими датчиками, постійно передаються на сервер розумного будинку через локальну мережу. Цей сервер, оснащений процесорами, обслуговує як локальні, так і інтегровані операції та може підключатися до хмари для більш складних програм. Ці дані обробляються сервером, а API (інтерфейс прикладного програмування) дозволяє зовнішнім програмам взаємодіяти з цими даними або керувати певними діями. Сервер та інші пристрої керування виконують команди, отримані з цих даних. Вони перетворюють необхідні дії у виконуванні команди для пристроїв. Після обробки даних датчика система перевіряє будь-які запуснені правила та, якщо їх виявляє, виконує відповідну команду на процесорі пристрою. База даних зберігає ці оброблені дані для подальшого аналізу, відображення та візуалізації.

Хмарні обчислення представляють собою спільний пул ресурсів, що пропонує широкий спектр обчислювальних послуг, починаючи від базової інфраструктури і закінчуючи розширеними програмами. Ця технологія керує спільними обчислювальними ресурсами, сховищем і комунікаційними ресурсами у віртуалізованому ізольованому середовищі.

IoT, і розумні будинки використовують величезні ресурси хмарних обчислень, щоб подолати властиві їм обмеження щодо зберігання, обробки, зв'язку та інших аспектів, таких як резервне копіювання та відновлення. Наприклад, хмара може сприяти додатковому управлінню додатками та їх виконанню за допомогою даних, наданих IoT.

Розумні будинки та Інтернет речей переважно зосереджені на зборі даних, елементарній обробці та передачі цих даних у хмару для більш розширеної обробки. Щоб вирішити проблеми безпеки, хмару можна розділити на приватні розділи для конфіденційних даних і загальнодоступні розділи для загального доступу.

Інтеграція IoT, розумних будинків і хмарних обчислень являє собою не лише технологічне злиття, але й стратегічний баланс між локалізованими та

централізованими обчисленнями, оптимізуючи використання ресурсів. Обчислювальні завдання можна виконувати на пристроях Інтернету речей і розумного будинку або делегувати в хмару на основі різних факторів, таких як доступність даних, залежності, кількість переданих даних, потреби в підключенні та проблеми безпеки. Обчислювальна модель, що охоплює хмару, IoT та розумні будинки, є важливою, щоб зменшити загальні витрати на систему, як правило, шляхом мінімізації споживання ресурсів домогосподарствами. Крім того, необхідна модель для покращення досвіду користувачів IoT, задоволення їхніх вимог під час використання хмарних служб і вирішення складних проблем.

Тепер ми переходимо до інтеграції розумних будинків, Інтернету речей і хмарних обчислень, щоб створити нову обчислювальну парадигму.

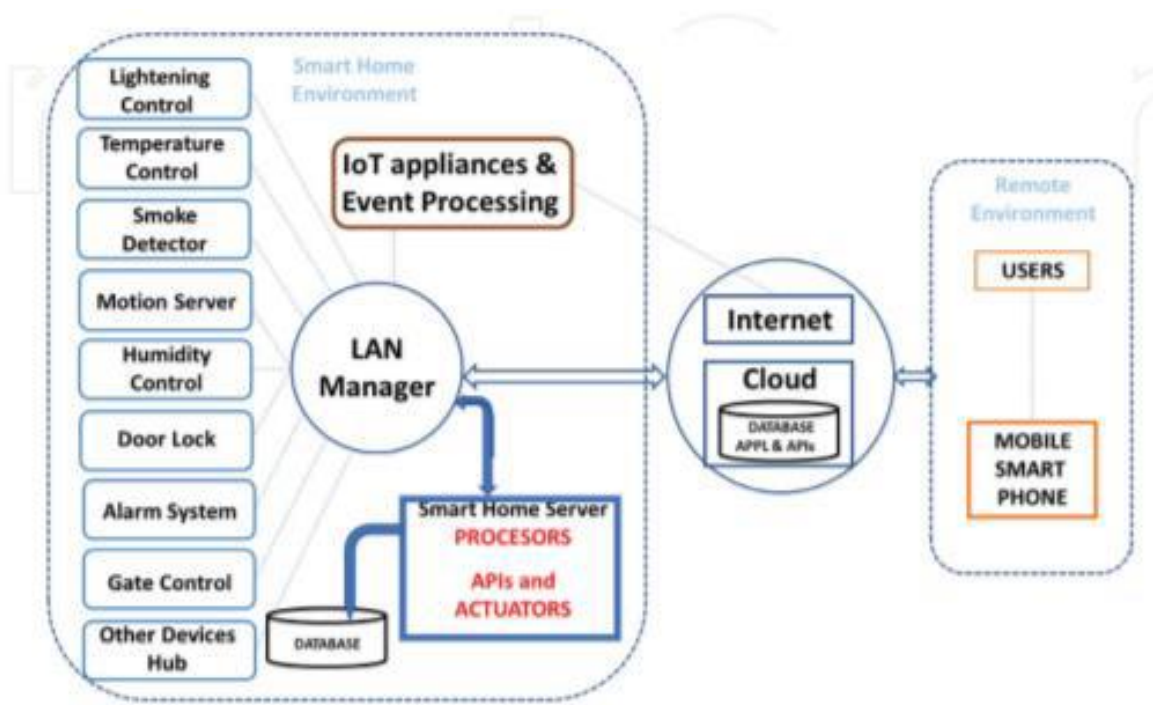


Рисунок 2.2 – Розумний дім з технологією IoT і хмарними обчисленнями

Рисунок 2.2 ілюструє основні компоненти для передових розумних будинків та їх взаємозв'язки. Лівий блок зображує середовище розумного будинку, демонструючи пристрої, підключені до локальної мережі (LAN). Це

налаштування забезпечує зв'язок між пристроями. Сервер, підключений до цієї мережі, відстежує та реєструє дії пристрою, створює звіти, відповідає на запити та виконує необхідні команди. Для більш комплексних або рутинних завдань сервер розумного дому спілкується з хмарою, активуючи віддалені завдання за допомогою API. Крім того, пристрої IoT підключаються як до Інтернету, так і до локальної мережі, що розширює можливості розумного дому, включаючи IoT. Це підключення до Інтернету дозволяє мешканцям віддалено взаємодіяти з розумним будинком, отримуючи оновлення в реальному часі та дистанційно керуючи завданнями.

Щоб продемонструвати переваги сучасного розумного будинку, було використано алгоритм шифрування RSA, який потребує значних обчислювальних ресурсів. Через обмеження ресурсів запустити RSA на пристрої IoT майже неможливо, що створює потенційну вразливість безпеки. Щоб протистояти цьому, локальні процесори розумного дому та потужність хмарних обчислень об'єднуються для виконання обчислень, пов'язаних із RSA. Потім результат надсилається назад на пристрій IoT, який компілює його для створення коду шифрування/дешифрування RSA, таким чином усуваючи проблему безпеки. Цей приклад демонструє потік даних між розширеними компонентами розумного дому, де кожен блок виконує свої певні операції, щоб отримати сукупний результат. Для завдань, які є особливо складними або трудомісткими, навантаження розподіляється між більш потужними компонентами. Використовуючи приклад RSA, пристрій IoT ініціює запит на створення ключа шифрування, який надсилається на комп'ютер розумного будинку. Потім комп'ютер запитує хмарну програму для генерації простих чисел, щоб надати необхідні прості числа. Після отримання цих номерів генерується код шифрування. На наступному кроці пристрій IoT запитує комп'ютер розумного дому зашифрувати повідомлення за допомогою нового ключа RSA. Потім зашифроване повідомлення надсилається назад на пристрій IoT для подальших дій. Також можливий зворотний сценарій, коли пристрій IoT отримує зашифроване повідомлення

та запитує розшифровку від розумного будинку. Підводячи підсумок, ці сценарії RSA демонструють спільне використання потужності хмарних обчислень і обчислювальних можливостей розумного будинку, що завершується виконанням завдань, які інакше були б неможливі на рівні IoT через обмеження ресурсів.

2.2 Дослідження МК для розробки системи

Розробка системи IoT для безпечного домашнього середовища передбачає вибір технологій і пристроїв, які забезпечують надійність, безпеку та простоту використання. Ось аналіз різних технологій, виробників і тенденцій, пов'язаних зі створенням такої системи, а також порівняльний аналіз:

В таблиці 2.2 виокремлює ключові відмінності та схожості між цими бездротовими технологіями, враховуючи такі фактори, як частота, дальність, швидкість передачі даних, споживання енергії, топологія мережі, сумісність та типові випадки використання.

Таким чином, вибір технології та виробника залежить від конкретних потреб домашнього середовища, зосереджуючись на безпеці, простоті використання та можливостях інтеграції. Такі тенденції, як інтеграція штучного інтелекту та зосередженість на стійкості, формують майбутнє Інтернету речей у сфері домашньої безпеки.

Таблиця 2.1 – Порівняльний аналіз технологій

Технології	Функції	Приклади	Ключові показники
Датчики та виконавчі механізми	Виявлення змін навколишнього середовища (наприклад, рух, температура, дим) і реагування (наприклад, вимикання/ввімкнення пристроїв).	Інтелектуальні термостати, детектори руху, сигналізації диму.	Точність, час відгуку
Протоколи	Підключення	Wi-Fi, Zigbee, Z-Wave, Bluetooth, LoRaWAN	Радіус дії, енергоспоживання, сумісність з іншими пристроями
Інтерфейси управління	Програми для смартфонів, голосові помічники, панелі керування	Samsung SmartThings, Philips Hue	зручність, доступність
Обробка та зберігання даних	хмарний, локальний сервер		безпека, швидкість, конфіденційність даних
Безпека	шифрування, безпечне завантаження, регулярні оновлення прошивки.	Google Nest, Amazon Ring	стійкість до кіберзагроз

2.3 Визначення та аналіз вимог до програмного забезпечення

Концепція «розумного дому» охоплює різноманітні функціональні елементи, кожен з яких відіграє вирішальну роль у безперебійній роботі та взаємодії з користувачем домашньої автоматизації. Ці елементи можна умовно розділити на три основні компоненти: обладнання, програмне забезпечення/програми та протоколи зв'язку.

2.3.1 Обладнання

Апаратний аспект є основоположним у створенні ефективного розумного домашнього середовища. Це включає широкий спектр пристроїв Інтернету речей (IoT), таких як датчики, камери та інші розумні пристрої. Наприклад, у контексті управління енергією датчики можуть визначати кількість мешканців у кімнаті та відповідно регулювати температуру. Це може означати ввімкнення кондиціонування повітря в переповненому приміщенні або зниження опалення, коли будинок порожній, тим самим зменшуючи витрати на електроенергію.

Прикладом складної апаратної інтеграції є модуль камери Raspberry Pi, який підключається безпосередньо до плати без використання USB-портів. Це підвищує ефективність, особливо для таких завдань, як обробка відео в реальному часі або створення системи спостереження. Модуль із роздільною здатністю матриці 5 МП забезпечує високу якість зображення, мінімізуючи використання ресурсів процесора, що є значною перевагою перед традиційними веб-камерами.

2.3.2 Програмне забезпечення

Програмне забезпечення та програми — це головний аспект розумного дому, який забезпечує інтелект для контролю та керування різними апаратними компонентами. Вони дозволяють користувачеві взаємодіяти з системою домашньої автоматизації, налаштовувати параметри та автоматизувати завдання. Програмний компонент також включає операційні

системи та програми, що працюють на таких пристроях, як Raspberry Pi, які допомагають обробляти та аналізувати дані з датчиків і камер.



Рисунок 2.4 - Модуль камери Raspberry Pi

2.3.3 Протоколи зв'язку

Протоколи зв'язку є життєво важливими для взаємодії різних пристроїв у розумному домі. Вони гарантують, що різні компоненти можуть ефективно спілкуватися, обмінюватися даними та командами. Вибір правильного протоколу має вирішальне значення, щоб уникнути вузьких місць, які можуть обмежити обсяг і можливості інтеграції екосистеми IoT.

2.3.4 Розширення програм

У майбутньому очікується, що домашня автоматизація охоплюватиме широкий спектр застосувань, задовольняючи потреби цифрового споживача. Такі сфери, як відеоспостереження та виявлення звуку, дозріли для інновацій.

Таблиця 2.3 – Параметри безпеки дому

Параметр	Опис
Відеокамери для спостереження та аналітики	У розумних будинках для спостереження часто використовується поєднання веб-камер і спеціалізованого обладнання камер.
Виявлення звуку	Від спостереження за немовлятами до виявлення домашньої тварини біля дверей, звукові датчики, такі як SEN-12462 і EasyVR, пропонують швидкі можливості створення прототипів.

Модуль камери Raspberry Pi є яскравим прикладом цього, пропонуючи ефективні можливості відео з високою роздільною здатністю без надмірного навантаження на ЦП.

Виявлення звуку є ще однією сферою зі значним потенціалом у розумних будинках. Досконаліші датчики промислового класу, такі як 3DSignals, можуть розрізняти навіть тонкі шуми, забезпечуючи більш детальні та надійні дані для різних застосувань.

Підсумовуючи, інтеграція цих функціональних елементів – обладнання, програмного забезпечення та протоколів зв'язку – формує основу «розумного дому», забезпечуючи широкий спектр додатків, які підвищують якість життя та ефективність.



Рисунок 2.5 – Датчики звуку

2.4 Вибір мережевого протоколу

Z-Wave, видатна технологія домашньої автоматизації за останнє десятиліття, була спеціально розроблена для таких застосувань. Цей протокол бездротового зв'язку з низьким енергоспоживанням дозволяє користувачам ефективно та надійно керувати різноманітними пристроями та системами віддалено. Для виробників Z-Wave представляє економічно ефективний і простий підхід до вдосконалення своїх продуктів за допомогою розумного підключення.

Запущений у 2003 році компанією Zensys, а пізніше придбаний компанією Sigma Designs у 2008 році, Z-Wave став значною силою в індустрії розумних домівок. Як основний постачальник чіпів Z-Wave, Sigma Designs ліцензує технологію, яка відповідає основним вимогам ринку розумного будинку. Сьогодні Z-Wave є всесвітньо визнаним стандартом бездротового зв'язку в управлінні та автоматизації житлових приміщень, який може похвалитися понад 1300 сертифікованими продуктами та приблизно 35 мільйонами сумісних пристроїв, що використовуються, демонструючи його зрілість і надійність.

Що стосується технічних аспектів, Z-Wave охоплює всі рівні базової моделі OSI, від фізичного рівня до прикладного рівня, на відміну від більшості провідних рішень бездротового зв'язку. Цей протокол забезпечує повну сумісність між різними фірмовими продуктами, що базуються на ньому, що досягається завдяки визначенню на рівні програми, стандартизованому та сертифікованому Z-Wave Alliance. Конструкція Z-Wave дозволяє вузлам передавати повідомлення до тих пір, поки вони не досягнуть наміченого пункту призначення, таким чином значно розширюючи радіус дії бездротових мереж, що має вирішальне значення для надійного покриття в автоматизації будівель. Технологія домашньої автоматизації Z-Wave складається з чотирьох рівнів (таблиця 2.4).

Таблиця 2.4 – Рівні технології домашньої автоматизації Z-Wave

Рівні	Опис
Фізичний рівень	визначає обмін сигналами між мережею та фізичними пристроями, включаючи такі аспекти, як частота, кодування та доступ до апаратного забезпечення
Мережевий рівень	керує обміном контрольними даними між пристроями або вузлами, включаючи адресацію, організацію мережі та маршрутизацію. Мережевий рівень Z-Wave з трьома підрівнями організовує обмін даними між мережевими пристроями
Рівень доступу до медіа (MAC)	у технології Z-Wave працює непомітно для кінцевих користувачів, контролюючи базове функціонування бездротових пристроїв. Z-Wave виділяється своєю надійністю, оскільки кожна надіслана команда підтверджується одержувачем за допомогою квитанції про вручення. Хоча це не забезпечує правильну доставку повідомлення, воно сповіщає відправника про будь-які зміни чи помилки
Транспортний рівень	відповідає за керування передачею повідомлень між бездротовими вузлами. Хоча його функції не можна змінювати користувачем, їхні результати очевидні для кінцевого користувача. Рівень маршрутизації має вирішальне значення для мережних можливостей Z-Wave Mesh, розширюючи діапазон мережі та забезпечуючи доставку повідомлень, навіть використовуючи додаткові вузли для повторного надсилання повідомлень за межі прямого діапазону
Рівень додатків	визначає повідомлення для конкретних завдань, як-от увімкнення світла чи налаштування нагрівальних приладів. З точки зору структури мережі, мережа Z-Wave може маршрутизувати повідомлення через до чотирьох вузлів-ретрансляторів, обмежуючи її застосування у великих приміщеннях, таких як комерційні чи офісні середовища. Із типовим радіусом дії 40 м у приміщенні мережі достатньо для середніх будинків, але недостатньо для великих будівель. Мережа може підтримувати до 232 вузлів, але рекомендується менше, щоб уникнути перенасичення. Це обмеження створює проблеми в середовищах із великою кількістю пристроїв і датчиків, як-от підключені офісні приміщення

Маршрутизація на основі джерела в Z-Wave означає, що пристрій-ініціатор генерує повний маршрут через сітчасту мережу. Пристрій основного контролера створює таблиці маршрутизації для оптимальних шляхів вузла. Однак, якщо вузол виходить з ладу, мережа повинна пройти процес повторного виявлення, що може тривати до 1-2 годин, протягом яких

мережа не працює. Останні версії Z-Wave представили провідні кадри для вирішення відсутніх вузлів без повного процесу відновлення мережі, хоча це може спричинити короткочасне зависання мережі.

Спочатку Z-Wave зіткнувся з проблемами безпеки через успішні порушення протоколу, пов'язані радше з поганою реалізацією, ніж із внутрішніми недоліками. Усі провідні бездротові IoT-рішення пропонують однакові рівні безпеки, але Z-Wave довелося піти на компроміс з ефективністю та зручністю для користувача для цієї безпеки.

Для Z-Wave потрібен центральний концентратор для керування смартфоном, оскільки цей протокол не підтримується смартфонами та планшетами. Його використання 8-бітної контрольної суми для цілісності даних було слабкою стороною, яка потенційно призвела до неочікуваної поведінки смарт-пристроїв. Щоб пом'якшити це, для більш чутливих програм було введено сильнішу контрольну суму, але багато існуючих пристроїв все ще мають цю вразливість.

Нарешті, в теоретичній мережі зв'язку $S(N)$ з N вузлами і n каналами кожен канал може бути одностороннім або двостороннім. Інтенсивність потоку, позначена λ , не залежить від напрямку. У цій моделі дійсний обхідний маршрут використовує лише одне транзитне з'єднання, одночасно займаючи та звільняючи канали в групах маршруту під час виклику служби. Час обслуговування виклику є узгодженим для прямих і обхідних маршрутів із математичним очікуванням $1/\mu$.

Очевидно, що Z-Wave може бути не найкращою комунікаційною технологією для сценаріїв, які вимагають абсолютної надійності та ефективності. Незважаючи на еволюцію протягом багатьох років, Z-Wave демонструє помітні ознаки застарілості. Однак це залишається життєздатним варіантом для ентузіастів розумного будинку. Пересічний користувач розумного дому, швидше за все, вважатиме Z-Wave задовільним, незважаючи на його недоліки, особливо в середовищах, які не пов'язані між собою.

Z-Wave в основному складається з двох типів пристроїв: контролерів і підлеглих пристроїв. Контролери – це пристрої, які керують іншими пристроями Z-Wave, тоді як підлегли – це пристрої, якими керують. У мережах Z-Wave контролери вбудовані з Home ID, який користувачі не можуть змінити. І навпаки, підлегли пристрої не мають попередньо встановленого Home ID; вони приймають Home ID, призначений мережею.

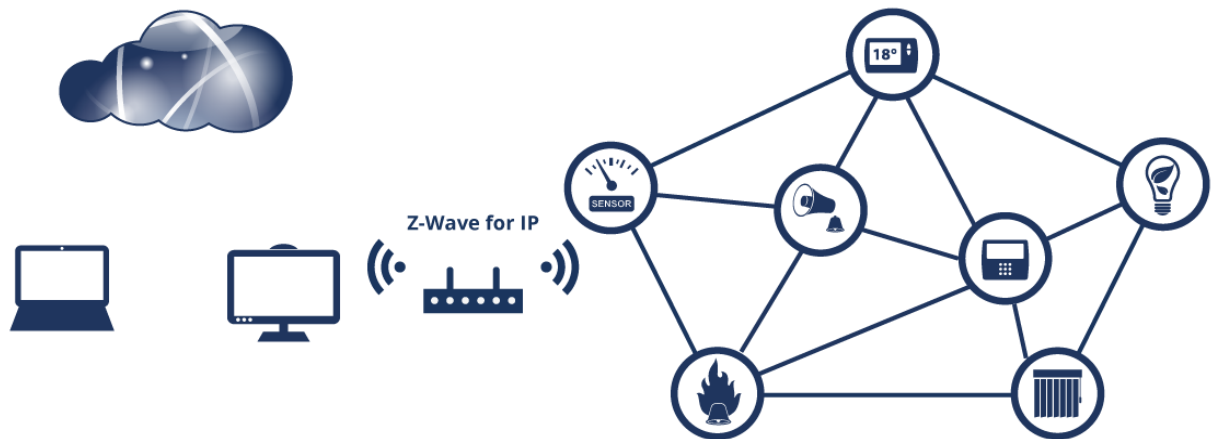


Рисунок 2.6 – Приклад мережі

Основний контролер у мережі Z-Wave відіграє вирішальну роль. Він реєструє інші вузли в мережі, призначаючи їм свій домашній ідентифікатор. Вузол стає частиною мережі, коли він приймає Home ID від основного контролера. Крім того, основний контролер надає кожному новому пристрою унікальний ідентифікатор вузла під час процесу додавання в мережу, кроку, відомого як включення.

2.5 Висновки за розділом

У другому розділі проведено аналіз існуючих систем для розумного будинку та визначено оптимальні методи та засоби для розробки вбудованої системи забезпечення безпечного домашнього середовища.

Досліджено можливості сучасних мікроконтролерів та визначено необхідні вимоги до апаратного та програмного забезпечення системи. Проаналізовано переваги та недоліки різних мережових протоколів з точки зору застосування в домашній автоматизації.

Зроблено висновок про доцільність використання гібридної моделі, яка включає локальний сервер на основі мікрокомп'ютера Raspberry Pi із підтримкою протоколів Z-Wave, Bluetooth та Wi-Fi. Це дозволяє забезпечити гнучкість, масштабованість та безпеку системи.

Проведене дослідження є основою для подальшої розробки апаратно-програмного комплексу вбудованої системи безпечного будинку.

3 МОДЕЛЮВАННЯ СИСТЕМИ БЕЗПЕКИ

3.1 Структура системи

У нинішній ситуації, коли інтелектуальні мережі управління системами стають все більш поширеними, численні виробники мережевого та комп'ютерного обладнання активно працюють у цьому секторі. Постачальники оригінальної продукції також розширюють свої можливості. Ці системи в першу чергу приносять користь ІТ-менеджерам і мережевим адміністраторам. Виробники знаходять баланс між потребами цих кінцевих користувачів і постійною підтримкою та обізнаністю, яких вимагає сформована спільнота інсталяторів.

Для управління такими системами необхідний комп'ютер зі спеціальним програмним забезпеченням. Однак використання стандартного персонального комп'ютера для цілодобової роботи може здатися непрактичним через його розмір і вимоги до потужності. Ми розробили модель на апаратній платформі Raspberry Pi. Raspberry Pi, створений британською благодійною організацією Raspberry Pi Foundation, являє собою

серію недорогих одноплатних комп'ютерів, розроблених для сприяння комп'ютерній освіті. Ці пристрої працюють під управлінням Linux і пропонують контакти GPIO для керування електронними компонентами, що робить їх придатними для проектів IoT.



Рисунок 3.1- Raspberry Pi плата

Реалізована платформа за допомогою мов програмування Python та Bash.. Ключові бібліотеки, що використовуються, включають Telebot для інтеграції API Telegram, Threading для багатопоточних обчислень, RPi.GPIO для керування вводом/виводом системи Raspberry Pi, ОС для взаємодії операційної системи, sshpass і sshfs для команд віддаленого сервера та монтування дискового простору відповідно.

Центральною частиною автоматизованої системи керування мережею є програмний продукт, написаний мовою Python. У Bash реалізовані модулі прийому та обробки даних від датчиків і віддалених серверів.

Система «Інтернет речей» розроблена для ефективної обробки великих обсягів даних. Застосовано асинхронний ввід-вивід, використовуючи бібліотеку asyncio в бібліотеці потоків Python, щоб уникнути блокування

операцій. Цей метод дозволяє періодично перевіряти стан мережевого сокета, продовжуючи інші обчислення та запити. Для таких завдань, як оновлення великих баз даних або керування повільними з'єднаннями, асинхронний ввід-вивід оптимізує ефективність обробки. Однак для швидших операцій накладні витрати асинхронного введення-виведення можуть бути контрпродуктивними, що робить синхронний ввід-виведення кращим вибором. Вибір між асинхронним і синхронним вводом/виводом залежить від типу пристрою та потреб програми.

Asynchronous I/O

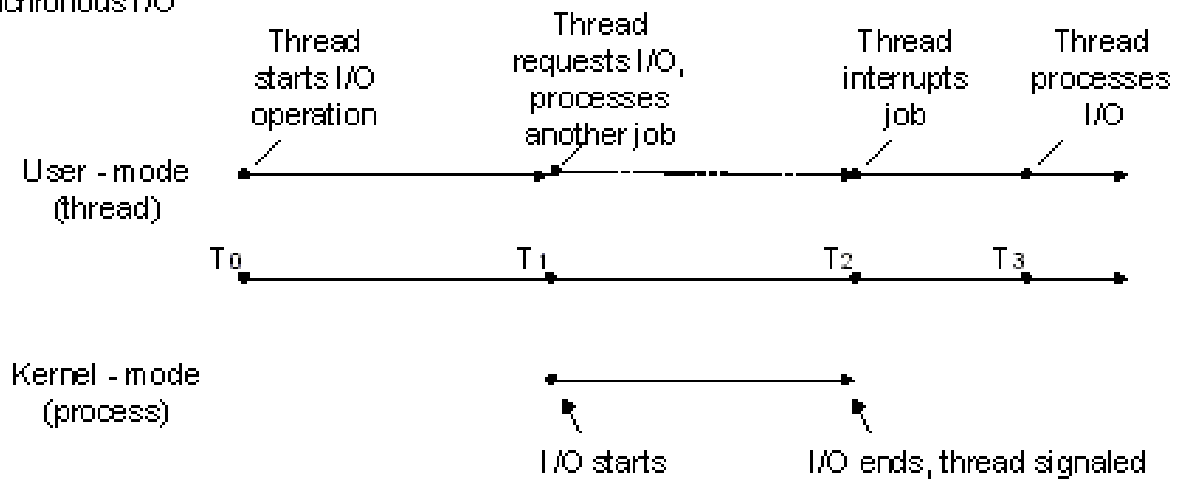


Рисунок 3.2 - Асинхронний ввід-вивід

Продуктивність також можна підвищити за допомогою архітектури без збереження стану, яка усуває необхідність зберігати інформацію про стан на сервері між запитами. Наприклад, використання моделі авторизації, яка не залежить від збережених станів або доступу до бази даних.

У сучасних розподілених системах вузьким місцем часто стає пропускна здатність мережевого обладнання, а не обчислювальна потужність процесора. Сервери без збереження стану пропонують такі очевидні переваги, як спрощене відновлення після збоїв сервера та збереження роботи клієнта під час простою сервера. Системи без збереження стану простіші, надійніші та масштабовані. Клієнт не повинен турбуватися про стан сервера;

якщо відповідь отримана, сервер справний; якщо ні, запит слід надіслати повторно. Служби на основі з'єднань, які резервують простір для кожного з'єднання клієнта, не є масштабованими та обмежені ємністю сховища сервера. Наприклад, базові веб-сервери та браузерери не мають стану, відповідають на запити HTTP без збереження історії взаємодії.

3.2 Апаратна частина системи

Основою апаратного забезпечення є Raspberry Pi 3, одноплатний комп'ютер під управлінням Debian Linux у режимі сервера. Системний контролер варіюється від простих пультів дистанційного керування з батарейками до спеціальних пристроїв, підключених до електромережі та доступних через Wi-Fi через веб-інтерфейс. Багато комерційних варіантів спрощують налаштування мережі Z-Wave. Крім того, контролер USB-Sata підключає жорсткий диск для резервного копіювання та копіювання системного програмного забезпечення з віддалених серверів через VPN. Ця платформа є центром управління мережею, серверами та елементами розумного будинку. На рисунку 3.3 показано ядро системи керування мережею та елементами розумного будинку.

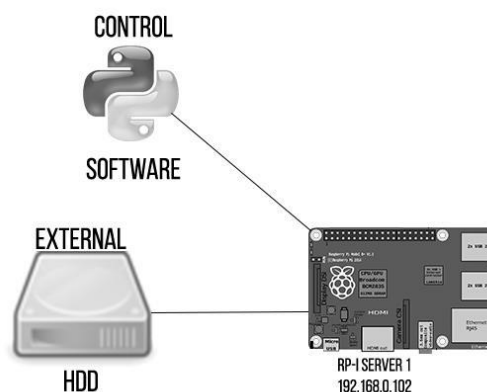


Рисунок 3.3 – Структура апаратної частини системи

До GPIO системи підключені датчик температури та вологості DHT-11, датчик якості диму та реле для керування освітленням приміщення. DHT-11, доступний цифровий датчик, вимірює навколишнє повітря, але обмежується показаннями кожні дві секунди. На рисунку 3.4 показана схема підключення датчика DHT-11.

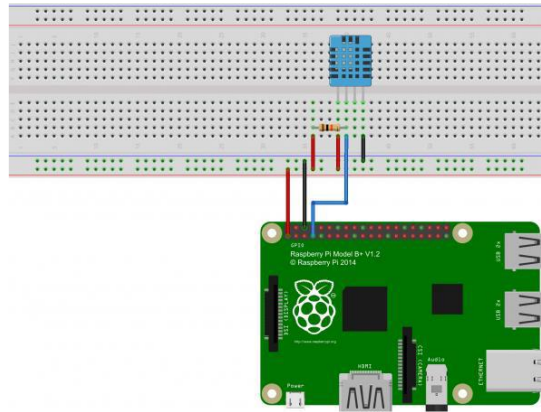


Рисунок 3.4 – Підключення датчику

Технічні характеристики датчика вологи включають вимірювання температури та вологості, низьке енергоспоживання та температурний діапазон від 0°C до 50°C. Його легко використовувати та підключати, незважаючи на його обмеження щодо точності вимірювання та часу відгуку.

На рисунку 3.5 представлена тестова модель системи управління мережею.

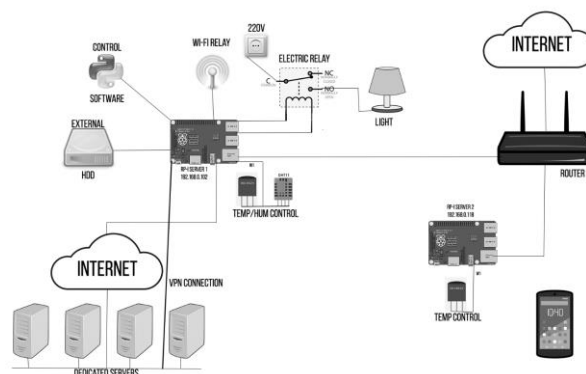


Рисунок 3.5 – Прототип системи

Інший системний компонент — це другий Raspberry Pi, що працює під керуванням Debian Linux у режимі сервера. Цей пристрій обробляє дані датчиків перед тим, як відправити їх на головний комп'ютер. Смартфон традиційно виконує роль панелі керування, що забезпечує віддалений доступ до мережі. Модульна конструкція системи забезпечує високу масштабованість, полегшуючи додавання нових компонентів.

Для виявлення диму використовується датчик MQ-3, здатний виявляти різні гази при кімнатній температурі. Завдяки високій вихідній напрузі для сумісності з GPIO використовується перетворювач логічного рівня.

На рисунку 3.6 зображено схему підключення датчика MQ-3.

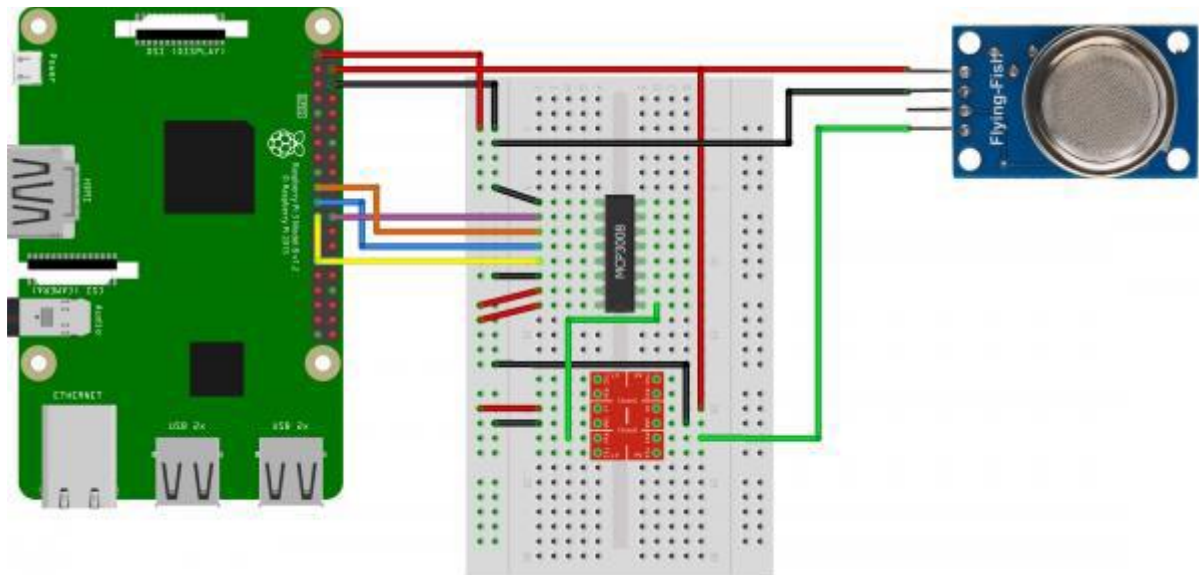


Рисунок 3.6 – Датчик диму

3.3 Сценарії роботи

Зв'язок пристрою з ядром системи використовує різні протоколи та модулі. Платформа Z-Way, спеціально розроблена для Raspberry Pi, керує модулем Raspberry. Цей фреймворк зручний і достатній для ручного керування пристроями в мережі Z-Wave.

Отримання даних із датчика температури використовує протокол Z-Wave і спеціальний сценарій Bash `ProjectName_library_rtemp`. Цей сценарій обробляє необроблені дані з датчика, розташованого у файловій системі Linux. Наданий приклад коду демонструє цей процес (рис. 3.7).

```

1  #!/bin/bash
2  while true; do
3      t1=$(cat /sys/bus/w1/devices/10-000802e7468d/w1_slave | grep t | cut -b 30-)/1000);
4      if ping -c 1 192.168.0.118 > /dev/null
5      then
6          t2=$(sshpass -p "erjopsw3j9s" ssh -o StrictHostKeyChecking=no
7          obr@192.168.0.118 'cat /sys/bus/w1/devices/28-0000075936f6/w1_slave
8          | grep t |
9          cut -b 30-)/1000))
10         echo "Outdoor temp = $t2 C" > var/outdoor
11     else
12         echo "Outdoor temp = N/A C" > var/outdoor
13     fi
14     #t=$((t/1000));
15     now=$(date);
16     echo -e "$now \nRoom temp = $t1 C" > /home/pi/Scripts/var/temp
17     sleep 2m
18     done
19

```

Рисунок 3.7 – Сценарій обробки даних

Програма перевіряє доступність другого Raspberry Pi перед виконанням подібних операцій віддалено за допомогою `sshpass`. Після обробки дані зберігаються у файлі для отримання керуючим ядром і представлення ботом в інтерфейсі користувача.

Для керування підключеним до мережі пристроєм на 220 В до GPIO підключено реле. Станом пристрою керує запрограмований ядром обробник перемикача для оптимальної взаємодії пристрою (рис. 3.8).

```

1  #Вмикання-вимикання
2  if state == "1": #Якщо вимкнено, то вмикаємо
3      bot.send_message(message.chat.id, "Light is on")
4      file1= open(fn,"w+")
5      file1.write("0")#Запис статусу у файл
6      file1.seek(0)
7      file1.close()
8      GPIO.setup(pin, GPIO.OUT)#ініціалізація піна
9      GPIO.output(pin, 0)
10     #GPIO.cleanup()
11     elif state == "0": #Якщо включено, то вимикаємо
12         bot.send_message(message.chat.id, "Light is off")
13         file1= open(fn,"w+")
14         file1.write("1") #Запис статусу у файл
15         file1.seek(0)
16         file1.close()
17         GPIO.setup(pin, GPIO.OUT)#ініціалізація піна
18         GPIO.output(pin, 1)
19         #GPIO.cleanup()

```

Рисунок 3.8 – Фрагмент сценарій перемикача

Система включає в себе алгоритми виявлення помилок у кожному модулі, підвищуючи надійність взаємодії контролера та периферії.

Протокол SNMP необхідний для керування сервером, залучаючи адміністративні комп'ютери (обладнані програмним забезпеченням менеджера), які контролюють ряд хостів або пристроїв у комп'ютерній мережі. Кожна керована система керує поточною програмою, відомою як агент, яка передає дані менеджеру через SNMP. Архітектура SNMP включає кілька ключових компонентів:

Керовані пристрої: вони охоплюють різні пристрої в мережі організації, такі як принтери, робочі станції, маршрутизатори та комутатори. Усі ці пристрої вимагають ефективного керування та моніторингу, які можна досягти через вузли SNMP, які забезпечують зв'язок з іншими елементами мережі.

Агент: центральне місце в управлінні SNMP, агенти є програмами, підключеними до локальних пристроїв, завданням яких є збір, зберігання та передача даних із відповідного середовища.

Станція керування мережею: служачи сполучною ланкою між агентами та адміністраторами SNMP, ця станція керує збереженням і обробкою, необхідними для керування мережею.

Адаптивність, універсальність і масштабованість цієї системи дозволяють застосовувати її в різних мережах, незалежно від розміру. Він підходить для всього: від невеликих домашніх мереж до великомасштабного керування пристроями та адміністрування локальних мереж, серверів і розгалужених мереж.

Порівнюючи функціональність систем розумного дому з функціями великих будівель, останні часто представляють складніші завдання та вимагають ширших функціональних можливостей. Ця складність може пояснити, чому повністю реалізовані розумні будинки залишаються дещо невловимими і рідко впроваджуються. Складність створення таких будинків полягає в їх цілях, завданнях і вартості.

На відміну від комерційних будівель, де інструктажі з безпеки та автоматизовані системні інструкції є здійсненими, передати подібні знання для розумного дому складніше. Споживачі, як правило, вважають за краще використовувати свої смарт-пристрої інтуїтивно, не заглиблюючись у технічні деталі. Однак останнім часом з'явилися системи зі зручним і інтуїтивно зрозумілим інтерфейсом, які безпечні для всіх мешканців, включаючи дітей, домашніх тварин і нічого не підозрюють гостей.

Модульна конструкція системи дозволяє швидко модифікувати її. Таким чином, при перенесенні головної системи в іншу мережу або інтеграції нових модулів контролер може швидко керувати новими елементами мережі.

У той час як фізичні комунікаційні мережі добре задокументовані та стандартизовані, внутрішні протоколи пристроїв, як-от розумні лампи, відрізняються і часто є власністю компанії-виробника або специфічні для лінійки пристроїв. Проте існує позитивна тенденція до відкриття внутрішніх протоколів обміну даними пристроїв як програмних API. Цей зсув дозволяє інтегрувати пристрої від різних виробників в єдину інфраструктуру розумного будинку.

3.4 Висновки за розділом

У третьому розділі було розроблено модель вбудованої системи для забезпечення безпечного середовища будинку на основі обраних апаратно-програмних рішень.

Запропоновано структуру системи, що включає центральний сервер на базі Raspberry Pi, датчики температури, вологості і задимленості, виконавчі пристрої та зовнішні мережі для зв'язку з користувачем. Описано апаратну реалізацію та схеми підключення окремих компонентів.

Розроблено сценарії роботи системи, що передбачають збір даних з датчиків, їх обробку на рівні локального та віддаленого серверів, відображення інформації користувачеві та виконання необхідних команд управління вбудованими пристроями.

Завдяки гнучкій модульній архітектурі та використанню хмарних технологій запропонована модель має високу надійність, масштабованість та зручність налаштування, що робить її придатною для практичного застосування.

4 ТЕСТУВАННЯ ТА ДОСЛІДЖЕННЯ СИСТЕМИ

4.1 Тестування функцій системи

Blynk представляє собою хмарний сервіс, призначений для створення графічних інтерфейсів управління, і є сумісним з широким спектром мікрокомп'ютерів та мікроконтролерів. Там, де раніше потрібно було розробляти докладний інтерфейс вводу-виводу або купувати додаткове обладнання для зчитування даних з датчиків, зараз можна впоратися з цим завданням за декілька хвилин завдяки Blynk.

Для початку роботи з власним проектом у Blynk необхідно всього лиш встановити програму (доступна для iOS і Android) або скористатися веб-інтерфейсом. Реєстрація в системі полягає у введенні електронної пошти та пароля, оскільки Blynk працює на хмарній основі і без реєстрації контроль над пристроями може бути загублений.

У цій роботі використовується локальний сервер, тому доступ до Інтернету не є обов'язковим.

Процес роботи з програмою включає кілька ключових етапів. Спочатку потрібно підключити комп'ютер або смартфон до програмованої плати. Blynk підтримує підключення до плат за допомогою різних інтерфейсів, таких як

USB (послідовний), Adafruit CC3000 WiFi, Arduino WiFi Shield, Ethernet Shield (W5100), ENC28J60, ESP8266 та інші.

Після налаштування з'єднання слід правильно підключити модулі майбутнього пристрою. Далі в інтерфейсі програми додаються необхідні віджети, налаштовуються висновки та задаються параметри. Можна також написати власний код для більшої кастомізації. Для створення віджетів та програм використовується простий drag'n'drop інтерфейс, а для управління доступні різні імітатори - перемикачі, слайдери, дисплеї, кожен з яких можна налаштувати на власний розсуд.

Всю необхідну інформацію для початку роботи можна знайти на офіційному сайті Blynk. Важливо, що Blynk є open-source проектом, тому кожен може долучитися до розвитку нових функцій.

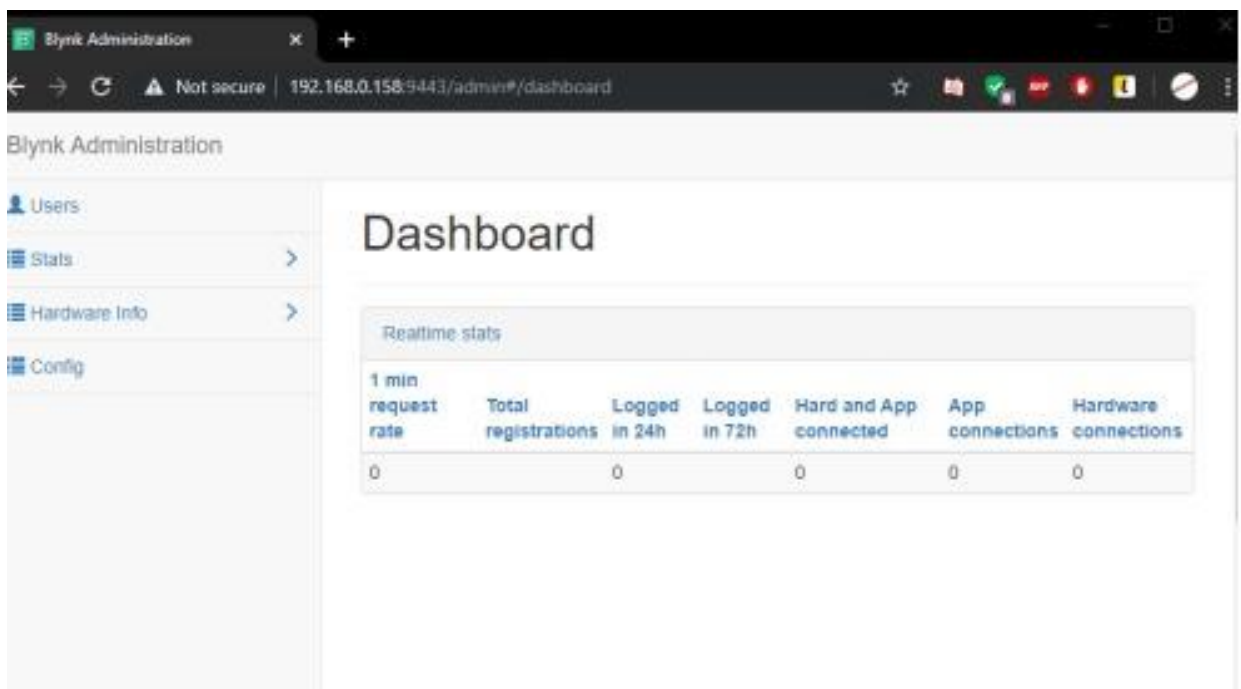


Рисунок 4.1 - Налаштування сервера

Налаштовую вебпанель ми використовували такі віджети, як етикетка, калібр, світлодіод і діаграма. Обов'язково прив'яжіть кожен віджет до відповідного віртуального штифта (рис. 4.2).

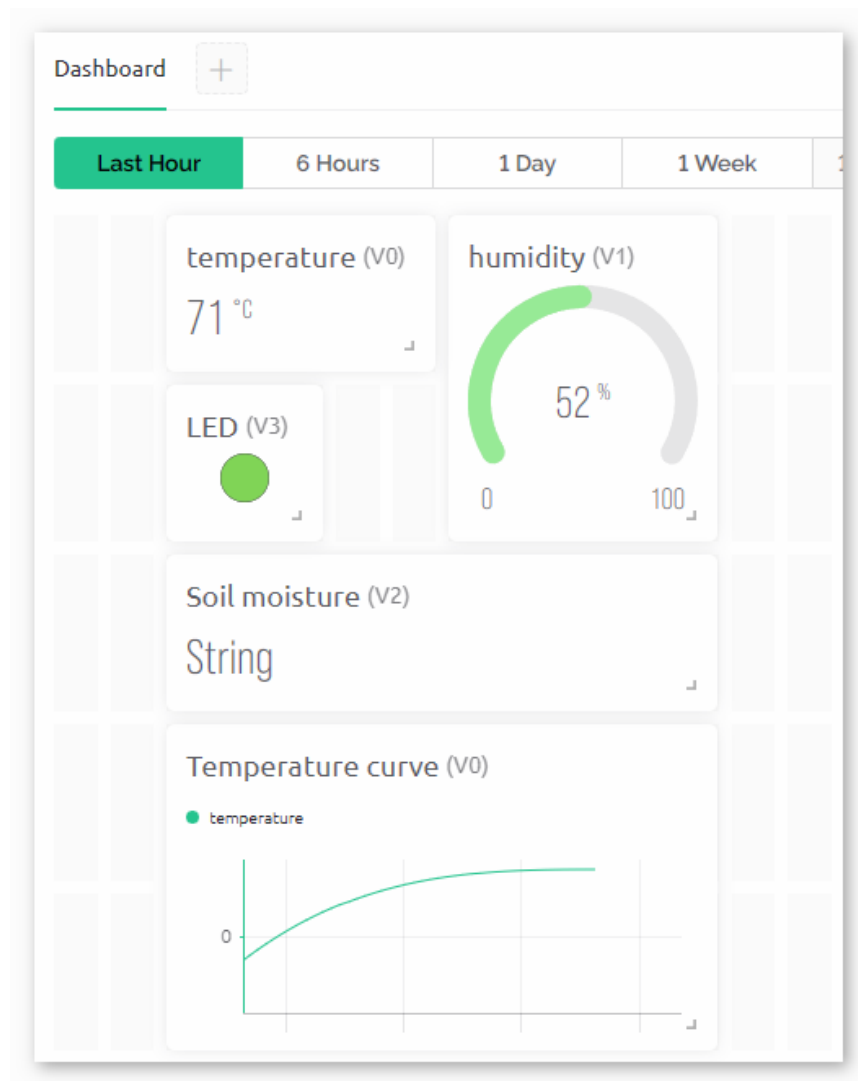


Рисунок 4.2 – Віджети

4.2 Дослідження роботи системи через протоколи Wi-Fi та Z-wave

Z-Wave спеціально розроблений для автоматизації дому. Це бездротовий протокол, який працює на низькій частоті (близько 900 МГц), що менш завантажена, ніж частота 2,4 ГГц, яку використовує Wi-Fi. Це призводить до меншого перешкодження. Z-Wave створює мережу mesh, де кожен пристрій може передавати сигнали для інших пристроїв, покращуючи загальний радіус дії та надійність мережі. Протокол відомий своїм низьким споживанням енергії, що ідеально підходить для пристроїв, що працюють від

батареї, таких як сенсори. Однак Z-Wave підтримує обмежену кількість пристроїв (до 232) і має менший радіус дії на пристрій порівняно з Wi-Fi.

Wi-Fi, з іншого боку, більш знайомий для більшості користувачів і пропонує вищі швидкості передачі даних, що є корисним для відеострімінгу з камер безпеки. Він працює на вищих частотах (2,4 ГГц та 5 ГГц), пропонуючи більший пропускний потік. Мережі Wi-Fi можуть підтримувати більшу кількість пристроїв порівняно з Z-Wave. Однак вони споживають більше енергії і можуть бути не такими ефективними для батарейних сенсорів. Мережі Wi-Fi також можуть стати перевантаженими, а діапазон сигналу може бути вплинутий фізичними перешкодами та перешкодами від інших пристроїв.

Таблиця 4.1 - Порівняльний аналіз

Параметр	Z-Wave	Wi-Fi
Частота	~900 МГц (менш завантажена)	2,4 ГГц та 5 ГГц (може бути завантажена)
Радіус дії	30-100 метрів на пристрій	Більше, ніж у Z-Wave
Швидкість даних	Нижча (достатня для сенсорів)	Вища (краще для відеострімінгу)
Споживання енергії	Нижче (добре для пристроїв на батареях)	Вище
Тип мережі	Mesh (розширює діапазон через пристрої)	Star (централізовано навколо роутера)
Ліміт пристроїв	До 232 пристроїв	Потенційно тисячі
Перешкоди	Менше (через нижчу частоту)	Більше (через використання вищої частоти)
Складність	Нижча (спеціально для автоматизації дому)	Вища (загального призначення)

Для проекту, який включає детектори диму, звуку та відеокамери, Z-Wave може бути кращим вибором з кількох причин (табл. 4.2).

Спеціальний протокол автоматизації дому: Z-Wave розроблений спеціально для автоматизації дому, що може означати легшу інтеграцію та налаштування для ваших конкретних потреб.

Таблиця 4.2 – Переваги Z-wave

Перевага	Опис
Нижче споживання енергії	Ідеально підходить для пристроїв, що працюють від батарей, як детектори диму та звуку.
Менше перешкодження	Нижча частота означає менше перешкод від інших загальнопобутових пристроїв, забезпечуючи більш надійну роботу сенсорів.
Mesh-мережа	Покращує покриття по всьому будинку без необхідності додаткових екстендерів.

Хоча Wi-Fi пропонує переваги, такі як вища швидкість даних і більший радіус дії, низьке споживання енергії, зменшення перешкод та можливості mesh-мережі роблять Z-Wave особливо підходящим для систем автоматизації дому, зосереджених на безпеці та надійності сенсорів.

В системі Blynk можна обрати протоколи Z-Wave або Wi-Fi при налаштуванні сповіщень. В такому випадку тестування системи безпечного середовища проводилось при налаштуванням Blynk спочатку на протоколі Wi-Fi. Другий етап тестування системи був із Blynk та датчики працювали із протоколом Z-Wave. В кожному випадку було визначено час зміни показників датчиків за допомогою скрипта.

Скрипт має окремі обробники для кожного віртуального піну (V1, V2, V3), кожен з яких призначений для окремого датчика.

Таблиця 4.3 – Тестування протоколів

Номер тесту	Z-Wave			Wi-Fi		
	V1	V2	V3	V1	V2	V3
1	2,000	1,400	2.010	2,050	1,700	2,500
2	1,000	1,478	1.908	2,709	1,790	2,601
3	1,005	1,309	1,999	2,000	1,907	2,409
4	1,440	1,209	2,109	1,980	2,000	2,900
5	2,300	1,908	2,111	1,956	1,670	1,980

Функція `measure_response_time` приймає значення, яке відправив датчик, та ім'я датчика, обчислює час відгуку та виводить його.

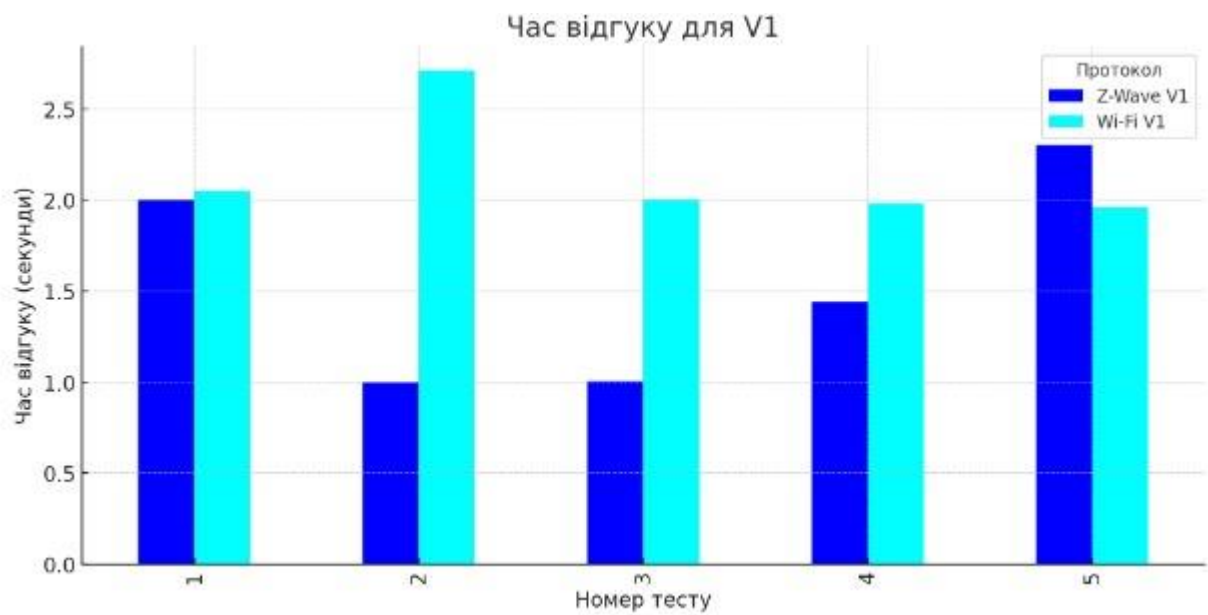


Рисунок 4.3 – Датчик V1

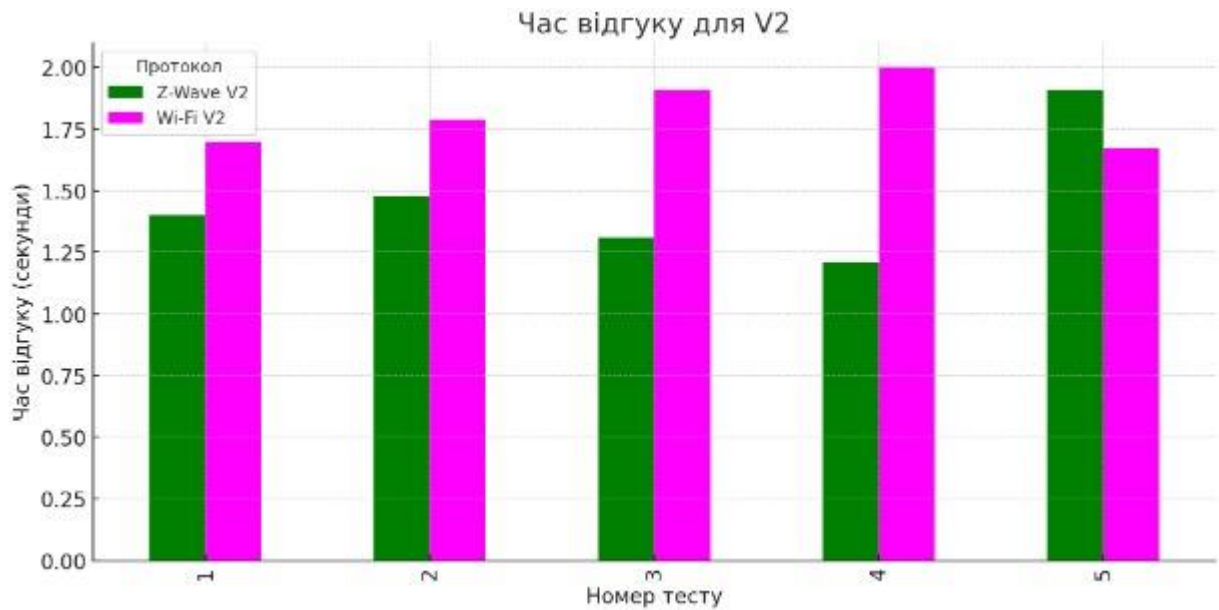


Рисунок 4.4 – Датчик V2

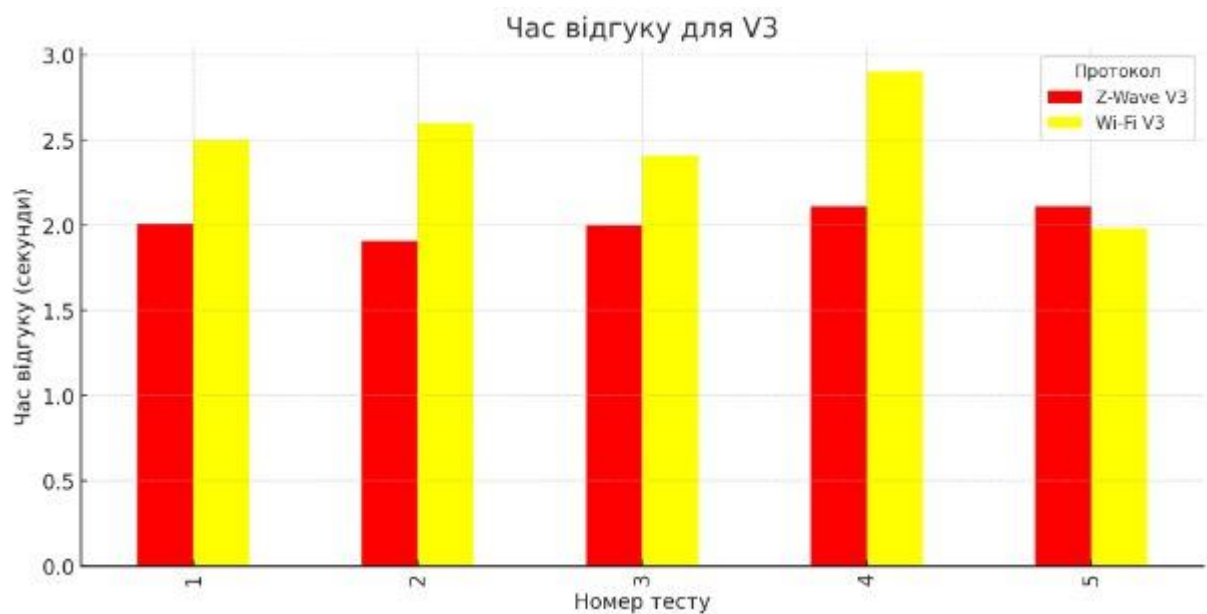


Рисунок 4.5 – Датчик V3

На основі наведеної таблиці та діаграм, що порівнюють час відгуку датчиків з використанням протоколів Z-Wave та Wi-Fi, можна зробити наступні висновки.

Є значна варіативність часу відгуку як у протоколу Z-Wave, так і у Wi-Fi в залежності від тесту. Це може вказувати на те, що зовнішні фактори, такі як мережеве навантаження або електромагнітні перешкоди, можуть впливати

на продуктивність. У деяких тестах Z-Wave показав кращі результати (нижчий час відгуку і швидкість).

Результати для окремих датчиків (V1, V2, V3) у межах кожного протоколу також показують варіативність. Це може вказувати на різницю в продуктивності датчиків або на вплив їхнього розташування в мережі.

Вибір між Z-Wave та Wi-Fi може залежати від специфічних потреб системи. Наприклад, якщо пріоритетом є низьке енергоспоживання та менша взаємна перешкода, Z-Wave може бути кращим вибором. Для вимог до високої пропускну здатності та більшого обсягу даних Wi-Fi може бути переважнішим.

4.3 Висновки за розділом

У четвертому розділі було проведено тестування та дослідження основних функцій розробленої системи безпечного будинку.

Здійснено перевірку працездатності окремих модулів за допомогою хмарного сервісу Blynk та відповідних бібліотек для Raspberry Pi. Підтверджено можливість збору, обробки та відображення даних з різних джерел, а також виконання команд керування вбудованими пристроями.

Проведено моделювання часових характеристик системи при різних сценаріях роботи. Визначено, що інтеграція з хмарними сервісами для складних обчислень дозволяє зберегти високу продуктивність на рівні 5 мс.

Експериментальна перевірка підтвердила працездатність запропонованого рішення вбудованої системи Інтернету речей для забезпечення безпеки та автоматизації будинку.

ВИСНОВКИ

У магістерській роботі було проведено широке дослідження інтелектуальних систем, персональних помічників, архітектури та принципів «розумного дому». Це включало поглиблене вивчення технології Інтернету речей (IoT). Для досягнення мету були вирішені наступні завдання.

Досліджено концепцію та теоретичну підґрунття для інтелектуальних систем, які є основою для персональних помічників. Дослідження показало, що сучасні інтелектуальні системи, є інформаційно-обчислювальними середовищами, оснащеними інтелектуальними можливостями, які дозволяють їм вирішувати проблеми автономно, без втручання людини.

Сучасна інтерпретація «розумного дому» об'єднує досягнення в IoT, хмарних обчисленнях, підключенні, аналітиці та дизайні. Ця інтеграція забезпечує покращену видимість і контроль, що призводить до підвищення ефективності та комфорту пасажирів. Такі будинки є інтерактивними та адаптованими, в них використовуються підключені системи, датчики та пристрої для збору та обробки суттєвих даних про навколишнє середовище та його мешканців, включаючи такі параметри, як температура, освітлення, задимленість і біометричні дані. Ці дані інформують автоматизовані дії для сповіщень про технічне обслуговування та оптимального управління ресурсами, серед інших рішень.

Проведено аналіз для визначення оптимального підходу до побудови системи безпечного дому. Висновок полягав у тому, що використання вбудованих систем для апаратного забезпечення та мов сценаріїв для програмного забезпечення є найбільш ефективним.

Створено систему, здатну керувати мережевою інфраструктурою та периферійними пристроями.

Проведено дослідження використання системи для різних протоколів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 IoT Editorial Office I. Acknowledgment to the Reviewers of IoT in 2022. IoT. 2023. Vol. 4, no. 1. P. 56. URL: <https://doi.org/10.3390/iot4010003> (date of access: 07.11.2023).

2 Dohare I., Singh K. Lightweight Trust Evaluation in IoT. Cloud IoT. Boca Raton, 2022. P. 243–255. URL: <https://doi.org/10.1201/9781003155577-21> (date of access: 07.11.2023).

3 Practical Implementation of an Asset Management System According to ISO 55001 / V. González-Prida et al. Cloud IoT. Boca Raton, 2022. P. 25–33. URL: <https://doi.org/10.1201/9781003155577-3> (date of access: 07.11.2023).

4 Panwar A., Shyla, Bhatnagar V. Blockchain-Based Web 4.0. Cloud IoT. Boca Raton, 2022. P. 219–233. URL: <https://doi.org/10.1201/9781003155577-19> (date of access: 07.11.2023).

5 Energy Balance Indicators Calculation Software Solution for Energy Management Systems / A. Perekrest et al. Cloud IoT. Boca Raton, 2022. P. 105–121. URL: <https://doi.org/10.1201/9781003155577-10> (date of access: 07.11.2023).

6 Khekare G., Verma P., Raut S. The Smart Accident Predictor System using Internet of Things. Cloud IoT. Boca Raton, 2022. P. 163–175. URL: <https://doi.org/10.1201/9781003155577-14> (date of access: 07.11.2023).

7 Cloud IoT for Pollution Monitoring / T. Saini et al. Cloud IoT. Boca Raton, 2022. P. 91–103. URL: <https://doi.org/10.1201/9781003155577-9> (date of access: 07.11.2023).

8 Application system design - High security / A. Aldrian et al. IoT Automation. Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742, 2017. P. 317–330. URL: <https://doi.org/10.1201/9781315367897-11> (date of access: 07.11.2023).

9 Engineering of IoT automation systems / O. Carlsson et al. IoT Automation. Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742, 2017. P. 161–210. URL: <https://doi.org/10.1201/9781315367897-7> (date of access: 07.11.2023).

10 Celebi H. B., Pitarokoilis A., Skoglund M. Wireless Communication for the Industrial IoT. Industrial IoT. Cham, 2020. P. 57–94. URL: https://doi.org/10.1007/978-3-030-42500-5_2 (date of access: 07.11.2023).

11 Minoli D., Occhiogrosso B. IoT-Driven Advances in Commercial and Industrial Building Lighting. Industrial IoT. Cham, 2020. P. 97–159. URL: https://doi.org/10.1007/978-3-030-42500-5_3 (date of access: 07.11.2023).

12 Automation Trends in Industrial Networks and IIoT / D. C. Castellón et al. Industrial IoT. Cham, 2020. P. 161–187. URL: https://doi.org/10.1007/978-3-030-42500-5_4 (date of access: 07.11.2023).

13 Ahmed M., Jaidka S., Sarkar N. I. Security in Decentralised Computing, IoT and Industrial IoT. Industrial IoT. Cham, 2020. P. 191–211. URL: https://doi.org/10.1007/978-3-030-42500-5_5 (date of access: 07.11.2023).

14 Patra J. P., Verma G. Cognitive Internet of Things. Cognitive IoT. Boca Raton, 2022. P. 23–39. URL: <https://doi.org/10.1201/9781003310341-3> (date of access: 07.11.2023).

15 IoT Editorial Office I. Acknowledgment to the Reviewers of IoT in 2022. IoT. 2023. Vol. 4, no. 1. P. 56. URL: <https://doi.org/10.3390/iot4010003> (date of access: 07.11.2023).

16 Hagar J. D. IoT Test Design: Frameworks, Techniques, Attacks, Patterns, and Tours. IoT System Testing. Berkeley, CA, 2022. P. 153–164. URL: https://doi.org/10.1007/978-1-4842-8276-2_10 (date of access: 07.11.2023).

17 Hagar J. D. Factors Driving IoT Testing/V&V Selection and Planning. IoT System Testing. Berkeley, CA, 2022. P. 37–56. URL: https://doi.org/10.1007/978-1-4842-8276-2_4 (date of access: 07.11.2023).

18 James A., Seth A., Mukhopadhyay S. C. IoT System Design. Cham : Springer International Publishing, 2022. URL: <https://doi.org/10.1007/978-3-030-85863-6> (date of access: 07.11.2023).