Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Метод забезпечення надійності та захищеності мультимедійних сервісів в системі Інтернету речей
(тема)

Виконав:

студент II курсу, групи СПм-22-6

Старов О.Є.
(прізвище, ініціали)

Спеціальність

123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: проф. Торба А.А.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-наукова
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Старову Олексію Євгеновичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод забезпечення надійності та захищеності мультимедійних сервісів в системі Інтернету речей

затверджена наказом по університету від " 01 " квітня 2024 р. № 257 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 червня 2024 р.

3. Вхідні дані до роботи 1) мережі IoT – дротові, бездротові, хмарні;
2) види мультимедійної інформації – відео та аудіо стандартних категорій якості;
3) використання оцінки QoS.

4. Перелік питань, що потрібно опрацювати у роботі
1) особливості обробки мультимедіа в IoT;
2) надійність і продуктивність IoT;
3) захищеність сервісів;
4) розробка моделі;
5) проведення експериментальних досліджень;
6) висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

Слайд-презентація – 12 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз особливостей обробки мультимедіа в	02.04.24-08.04.24	
	IoT		
2	Аналіз питань надійності і продуктивності	09.04.24-16.04.24	
3	Аналіз питань захищеності сервісів	17.04.24-22.04.24	
4	Розробка моделі системи	23.04.24-06.05.24	
5	Проведення експериментів	07.05.24-23.05.24	
6	Оформлення матеріалів кваліфікаційної роботи	24.05.24-03.06.24	
7	Подання кваліфікаційної роботи керівникові та	04.06.24-07.06.24	
	її попередній захист		
8	Подання кваліфікаційної роботи на рецензу-	08.06.24-12.06.24	
	вання		

Дата видачі завдання 01 квітня 2024 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Торба А.А.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 73 с., 16 рис., 13 табл., 1 дод., 50 джерел.

ІНТЕРНЕТ МУЛЬТИМЕДІЙНИ РЕЧЕЙ, КЕРУВАННЯ МЕРЕЖЕЮ, КЛАСТЕР ПРИСТРОЇВ, НАДІЙНІСТЬ, ОБЧИСЛЮВАЛЬНА ПОТУЖНІСТЬ, ЯКІСТЬ ОБСЛУГОВУВАННЯ.

Представлено підхід до об’єднання обчислювальної потужності пристроїв IoMT з метою забезпечення надійної обробки мультимедіа-даних. Запропонована структура дозволяє динамічно формувати коаліції пристроїв, які використовують свої резервні ресурси для надання послуги заданого рівня якості.

Інфраструктура повністю настроюється, а відповідно до сценарію застосування, налаштовуються параметри QoS. У майбутньому можна адаптувати потокові алгоритми для використання кластера IoMT, планувати використання функцій апаратного прискорення, а не виключно потужність, яку забезпечує центральний процесор.

ABSTRACT

Master’s thesis: 73 pages, 16 figures, 13 tables, 1 appendix, 50 sources.

COMPUTING POWER, DEVICE CLUSTER, INTERNET OF MULTIMEDIA THINGS, NETWORK MANAGEMENT, QUALITY OF SERVICE, RELIABILITY.

An approach to combining the computing power of IoMT devices in order to ensure reliable processing of multimedia data is presented. The proposed structure allows to dynamically form coalitions of devices that use their reserve resources to provide a service of a given quality level.

The infrastructure is fully configurable, and according to the application scenario, the QoS parameters are adjusted. In the future, it is possible to adapt the streaming algorithms to use the IoMT cluster, plan to use hardware acceleration functions, rather than exclusively the power provided by the CPU.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОП – оперативна пам’ять

ЦП – центральний процесор

IaaS – інфраструктура як послуга (англ., Infrastructure as a service)

IoMT – Інтернет мультимедійних речей (англ., Internet of multimedia things)

IoT – Інтернет речей (англ., Internet of things)

M2H – взаємодія машини з людиною (англ., Machine to human)

M2M – взаємодія машини з машиною (англ., Machine to Machine)

MTSA – архітектура захисту трафіку медіапрограми (англ., Mediaware traffic protection architecture)

PaaS – платформа як послуга (англ., Platform as a service)

PoF – фізикf відмови (англ., Physics of failure)

QoE – якість досвіду (англ., Quality of experience)

QoS – якість обслуговування (англ., Quality of service)

QoT – якість речей (англ., Quality of things)

SaaS – програмне забезпечення як послуга (англ., Software as a service)

SBC – одноплатний комп’ютер (англ., Single-board computer)

SDN – (англ., Software Defined Networking)

UWB – надширокосмуговий зв’язок (англ., Ultra-wide band)

VoIP – передача голосу через IP (англ., Voice over IP)

VSP – постачальник відеопослуг (англ., Video service provider)

WMSN – бездротова мультимедійна сенсорна мережа (англ., Wireless multimedia sensor network)

WSN – бездротова сенсорна мережа (англ., Wireless sensor network)

ВСТУП

Інтернет речей (IoT) – це сучасна концепція, яка перетворила звичайний спосіб життя на високотехнологічний. Розвиток інтелектуальних середовищ [1] означає, що технології стають все більш взаємопов'язаними, а Інтернет використовується все частіше. Інтернет речей (IoT) швидко розширюється, а можливість зв'язувати фізичну та віртуальну реальність відкриває нові двері для інновацій майже в кожній сфері життя. З іншого боку, Інтернет речей – це набір різнорідних об'єктів або пристроїв із різними обчислювальними можливостями та можливостями підключення, які можуть збирати дані з фізичного світу, пов'язаного через Інтернет. Вважають, що зв'язок між машинами (M2M) буде найпоширенішою технологією в концепціях IoT [2]. Датчики, виконавчі механізми, мобільні телефони, системи домашньої автоматизації та розумні електромережі – усі вони мають здатність справляти величезний вплив на життя людини та те, вона з ними спілкується. Також Інтернет речей можна розумыти як суміш інформаційних технологій, інформатики, електроніки, телекомунікацій та інших галузей. Концепція Інтернету речей була представлена Кевіном Ештоном у 1999 році.

Інтернет речей показав, що комп'ютери – не єдині пристрої з підключенням до Інтернету, і що різні пристрої та артефакти мають таку можливість. Це стало найважливішою темою дослідження за останні 20 років [3], мета якого базується на повсякденних об'єктах, які мають ідентифікацію, виявлення, взаємозв'язок і здатність обробки для спілкування один з одним і зі службами через Інтернет, щоб розгадати конкретну та корисну потребу людей. Інтернет речей є системою широкого спектру, яка включає багато інтегрованих систем. Бездротові датчики в Інтернеті речей спілкуються один з одним через бездротовий зв'язок малої дальності. Бездротова сенсорна мережа (WSN) – це набір датчиків, підключених до Інтернету через один або кілька шлюзів [2]. Для зв'язку між датчиками та шлюзами сенсорної мережі

можна використовувати бездротовий зв’язок з одним або кількома стрибками.

Інтернет мультимедійних речей (IoMT) – це нова парадигма, створена інтелектуальними різнорідними мультимедійними пристроями, які спілкуються та співпрацюють один з одним та з іншими пристроями через Інтернет речей. Розумні об’єкти в Інтернеті мультимедійних речей зазвичай [4] обмежені з точки зору енергії, ємності пам’яті та потужності обробки. Щоб зробити пристрої меншими, рентабельними та енергоефективними, датчики зазвичай розробляють для роботи від батареї або сонячної енергії з лише кількома кілобайтами пам’яті та обмеженою потужністю обробки (тактовою частотою).

Мультимедійні дані – це набір неструктурованих характеристик, який включає аудіо, зображення та відео. Передача таких великих неструктурованих даних через мережу з обмеженою пропускною здатністю та обчислювальною потужністю вимагає ефективної та інтелектуальної топології мережі. У режимі реального часу через обмеження пропускної здатності та втрату пакетів, додатки IoT можуть мати затримки та перевантаження мережі, що знижує якість переданого мультимедіа.

Щоб вирішити вищезазначені проблеми, в останні роки були запропоновані спеціальні мультимедійні комунікації в IoT. У більшості інтелектуальних систем IoMT інтелект, створений методами глибокого навчання, тісно пов’язаний із додатком, який його реалізує, обмежуючи надання [5] цього конкретного інтелектуального сервісу іншими додатками, також у тому ж системному домені. Наприклад, у сценарії університетського містечка, передбачається, що ту саму систему розпізнавання обличчя слід застосовувати для реєстрації присутності студентів і аспірантів в університетській аудиторії, а також для розблокування дверей лабораторії для дослідника.

Дана робота представляє вичерпний огляд сучасного стану IoMT. Мультимедійні бездротові сенсорні мережі, які обробляють величезний

мультимедійний трафік у додатках IoT в режимі реального часу, а саме моніторинг трафіку, віддалений моніторинг системи та моніторинг домашньої безпеки, моніторинг інтелектуальної мережі, потребують величезної пам’яті та обчислювальних ресурсів і споживають більше енергії, відрізняючись від традиційних бездротових сенсорних мереж, які збирають інформацію від фізичного середовища, наприклад температури, тиску та світла.

1 ІНТЕРНЕТ МУЛЬТИМЕДІЙНИХ РЕЧЕЙ (IOMT)

1.1 Загальні відомості

Інтернет речей – це термін, який використовується для опису системи взаємопов’язаних пристроїв, підключених до Інтернету, які можуть отримувати та передавати дані через бездротову мережу без участі людини. Пристрої з вбудованим підключенням до Інтернету, датчики та інше обладнання забезпечують зв’язок і контроль через Інтернет в Інтернеті речей [6]. IoT став однією з найважливіших технологій 21 століття. Тепер, коли можна підключати побутові предмети, кухонну техніку, автомобілі, термостати, радіоняні до Інтернету через вбудовані пристрої, можливий безперебійний зв’язок між людьми, процесами та речами. Системи Інтернету речей не можуть успішно реалізувати поняття повсюдного підключення всього, якщо вони не здатні справді включати «мультимедійні речі». Тому слід проаналізувати деякі особливості мультимедіа перед розглядом Інтернету мультимедійних речей (IoMT).

Мультимедіа – це поняття, яке об’єднує слова мульти та медіа. Термін носій (носій) має подвійне значення: він стосується пристрою, який зберігає дані на диску, компакт-диску, стрічці, напівпровідниковій пам’яті та інших пристроях. По-друге, це передача носіїв інформації, таких як цифри, текст, звук, графіка тощо. Отже, відповідний термін і мультимедіа є окремим медіа, буквально, медіа складається з одного медіа. Мультимедіа – це все, що людина дивиться і слухає. Це графіка, аудіо, звук, текст і багато іншого. Зазвичай це записується та відтворюється, відображається або доступ до нього здійснюється за допомогою пристроїв обробки інформаційного вмісту, таких як комп’ютеризовані та електронні пристрої.

Мультимедіа включає все, що можна бачити і чути у вигляді тексту, зображень, аудіо, відео та інших форматів [7]. Системи обробки

інформаційного вмісту, такі як комп’ютеризовані та електронні пристрої, зазвичай перекодують і відтворюють, переглядають або отримують до нього доступ. Можна використовувати мультимедіа на робочому місці, у школах, у помешканнях, у громадських місцях та у віртуальній реальності. Існує багато функцій, які дозволяють робити багато речей, і зробили їх більш мобільними. Мультимедіа покращила простий, текстовий інтерфейс комп’ютера та сфокусувала увагу на потрібних об’єктах. Одним словом, покращила використання інформації. Якщо правильно реалізувати, комп’ютер може стати глибокою та корисною мультимедійною розвагою. Мультимедіа можна використовувати різними способами: у бізнесі, школі, вдома, у громадських місцях і віртуальній реальності.

Інтернет мультимедійних речей можна описати як «мережу взаємопов’язаних об’єктів, здатних отримувати мультимедійний вміст із реального світу та подавати інформацію в мультимедійний спосіб» [8] шляхом включення мультимедійного контенту. Ідея поєднання мультимедіа та IoT відносно нова. Вираз «Інтернет мультимедійних речей» (IoMT) порівняно недавно був введений для опису мультимедійних комунікацій на основі IoT. Мультимедійні об’єкти, з іншого боку, можна описати як «об’єкти, здатні отримувати мультимедійний вміст із фізичного світу, будучи обладнаними мультимедійними пристроями». Обробка мультимедійних подій і середовища їх виконання є важливими в IoMT для аналізу величезної кількості неструктурованих даних, створених у «розумних містах».

IoMT додає специфіку до викликів IoT таких, як захист, маршрутизація, якість обслуговування (QoS) і якість досвіду (QoE), неоднорідність мультимедійних датчиків тощо [9]. Пристроям IoMT потрібна більша пропускна здатність, об’ємні ресурси пам’яті та більша обчислювальна потужність для аналізу та обробки отриманих мультимедійних даних. Традиційне мультимедійне застосування передбачає передачу даних багатоточкового зв’язку, наприклад, систему спостереження за цілим розумним міським районом і сценарії багатоточкового зв’язку. У таблиці 1.1

представлено порівняння технологій на основі IoMT та IoT.

Таблиця 1.1 – Порівняння технологій на основі IoMT та IoT

Властивості	IoMT	IoT
Розмір даних	мега- та гігабайти	байти та кілобайти
Ресурси	високе енергоспоживання	низьке енергоспоживання
Розгортання	аудіо та відео датчики	мітки RFID
Пропускна здатність	мегабайт/с	кілобайт/с
Якість обслуговування	висока пропускна здатність	низька пропускна здатність
Зберігання	гігабайти	кілобайти та мегабайти
Неоднорідність даних	різноманітні мультимедійні дані	обмежена неоднорідність
Чутливість затримки	висока	низька
Обробка сигналів	аналітика мультимедійних даних	аналітика структурованих даних
Обробка	МГц, ГГц	КГц, МГц
Сервісні композиції	спеціалізовані не доступні	на основі SOA
Пам’ять	мега- та гігабайти	кілобайти та мегабайти
Комунікаційні протоколи	не стандартизовані	стандартизовані

У всьому світі мультимедійні системи використовуються в широкому діапазоні застосувань, включаючи системи реагування на надзвичайні ситуації, моніторинг дорожнього руху, медичні програми (для моніторингу пацієнтів або дітей), інспекцію злочинів, розумні міста, розумні будинки, розумні лікарні, розумне сільське господарство. Пристрої

відеоспостереження можуть бути розгорнуті в різних сценаріях, наприклад, у системах управління громадським транспортом (керування автобусами, літаками або дорожнім рухом), Інтернет тіл (IoB), обробка зображень, мобільні комп'ютери, промисловий Інтернет речей (IIoT), інтелектуальні системи, захист особистих активів (у будинках або на будівельних майданчиках) і багато інших програм [10]. Мультимедійна комунікація в IoT стикається з величезними труднощами через динамічні мережі, гетерогенні пристрої та дані, суворий QoS і вимоги до чутливості та надійності затримок порівняно з IoMT з обмеженими ресурсами. Мета полягає в тому, щоб зробити ці пристрої розумними, дозволивши їм спілкуватися один з одним, фактично перетворюючи їх на розумні об'єкти.

1.2 Архітектура IoMT

Оркестровка Інтернету мультимедійних речей дозволяє інтегрувати системи, програми, хмару та розумні датчики в єдину платформу. IoMT працює як для скалярних, так і для мультимедійних даних. Своєчасна та ефективна доставка даних є найважливішою особливістю IoMT. У результаті встановлюються суворі стандарти якості обслуговування (QoS), а також ефективна архітектура мережі. Швидке зростання мультимедійного трафіку в IoT привело до інноваційних технологій для задоволення його вимог [11]. Тут представлені нові архітектури Інтернету мультимедійних речей (IoMT), як показано на рисунку 1.1.

За останні кілька років мультимедійний трафік різко зріс. Значне збільшення мультимедійного трафіку вимагає ефективної системи керування мережевим трафіком. Була зроблена пропозиція [12] інтелектуальної системи керування мережею для системи відеоспостереження IoT на основі SDN та штучного інтелекту. SDN (Software Defined Networking) з'явилася як техніка для підвищення функціональності мережі при зниженні витрат, спрощенні апаратного забезпечення та заохоченні до новаторських досліджень.

Програмно визначені мережі (SDN) розширюють можливості керування мережею. Штучний інтелект у поєднанні з SDN може надавати мережеві рішення на основі методів класифікації та оцінки. Штучний інтелект допомагає динамічно керувати ресурсами та мережевим трафіком. Використовуючи штучний інтелект для вивчення трафіку мережі, можна виявити різні типи потоку, що передається. Таким чином можна отримати шаблони трафіку, які потім застосовувати при прийнятті рішень SDN.

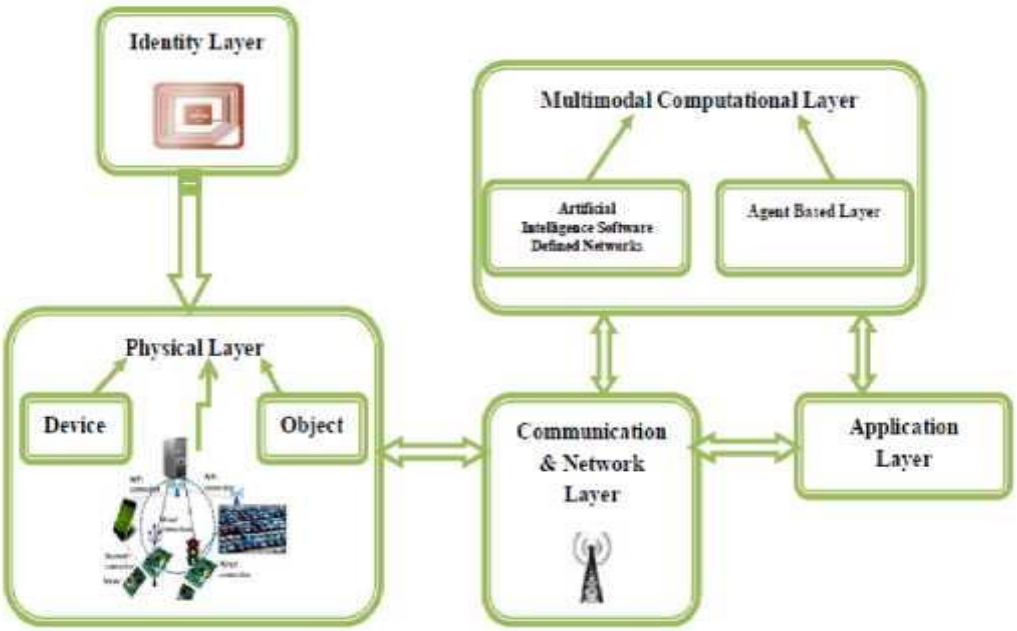


Рисунок 1.1 – Архітектура Інтернету мультимедійних речей (IoMT)

Інтеграція методів штучного інтелекту з SDN, адаптивна поведінка досягається для покращення продуктивності мережі. Мультиагентна архітектура на основі хмарних обчислень для мультимедіа спілкування в IoT має громіздкий і неструктурований характер мультимедійного контенту. Чотирма ключовими частинами цієї архітектури є:

- відстеження мультимедіа;
- моніторинг і адресність;
- мультимедійна хмара;
- багатоагентні системи.

Вдосконалення багатоагентної архітектури IoMT [13] робить її більш практичною, за рахунок реалізації п’ятирівневої архітектури. Інноваційна агентна архітектура для систем, що підтримують віддалену співпрацю, реалізується на основі підходу IoMT. У цих додатках використовуються базові елементи та інструменти IoT, такі як камери, мікрофони, датчики та мультимедійні лінії зв’язку. Ця архітектура розділена на п’ять рівнів:

- додатки;
- агенти виконання послуг;
- з’єднувачі ресурсів;
- служби та ресурси IoMT;
- пристрої та комунікації IoMT.

Кожен інтерфейс і зв’язок, наприклад сенсорні екрани, синхронні та асинхронні лінії зв’язку та хмарне сховище, представлені трьома нижніми рівнями. Паралельні канали вимагають одночасного використання кількох графічних інтерфейсів користувача та, що більш важливо, поверхні дисплея. Користувачі можуть динамічно включати ці канали в програми для підвищення можливостей розширення системи IoMT. Слід зазначити пропозицію [14] контекстно-залежної структури на основі гібридної туманної хмари, яка інтегрує просторово-часові мультимедійні дані з мобільних і стаціонарних вузлів Інтернету речей для великого натовпу ad-hoc. Представлена трирівнева архітектура, яка містить:

- рівень мобільного клієнта;
- рівень туманного вузла;
- рівень віддаленої хмари.

Автори прагнуть оптимізувати використання енергетичних ресурсів і зменшити затримку від кінця до кінця для великого натовпу в розумному місті. Рівень мобільного клієнта включає споживачів послуг. Рівень туманних вузлів включає туманні вузли смартфонів та інших IoT, розподілені в місті, щоб допомогти в обробці просторово-часових колективних або індивідуальних запитів у реальному часі. Для аналітичних обчислень,

зберігання та обробки офлайн-запитів хмарний рівень складається з архітектури масивних великих даних на основі IP. Модель стійкості та енергоефективності, а також величезна мультимедійна архітектура великих даних із геотегами включені в архітектуру зв'язку між мобільними користувачами та вузлами туману, а також між вузлами туману та хмарою.

Також можна зазначити пропозицію [15] шестирівневої архітектури IoMT, орієнтовану на агрегацію великих даних, обчислення та вилучення мультимедійного контенту. Замість слова медіа автори використали термін модальний, який пояснює, як дані сприймаються для передачі значення. Більше того, вони перерахували три основні проблеми, пов'язані з мультимодальним обчисленням великих даних, тобто обчислення величезної кількості даних, виявлення та витяг значущої інформації та поточні обмеження платформ обробки великих даних для мультимедіа. Крім того, у статті представлено унікальну та ефективну техніку, яка є аналізом головних компонентів «Розділяй і володарюй» (DC-PCA) для зменшення розмірів, поділу даних, обробки розділених даних паралельним способом і об'єднання остаточних паралельно оброблених даних для вилучення ознак.

Архітектура захисту трафіку медіапрограми (MTSA) для IoMT [16] складається з чотирьох ключових компонентів. Управління ключами, яке включає контроль послуг, контроль користувачів, контроль потоків, масштабовані та немасштабовані схеми, є одним із цих елементів. Водяні знаки використовуються для визначення походження мультимедійного вмісту, відстеження незаконного розповсюдження та блокування несанкціонованого доступу шляхом вбудовування унікального водяного знака в мультимедійний вміст. Безпека має вирішальне значення для різноманітних мультимедійних програм в IoT. Застосовується архітектура безпеки трафіку з урахуванням медіа (MTSA) для отримання задовільного управління трафіком на основі заданої класифікації та аналізу трафіку з урахуванням медіа. MTSA – це одна з перших стратегій керування трафіком із урахуванням безпеки для мультимедійних програм, що працюють через

IoT. Для сприяння різноманітним мультимедійним додаткам в Інтернеті речей автор запропонував ефективну систему безпеки з урахуванням медіа. Ця система класифікації та аналізу мультимедійного трафіку призначена для роботи з неоднорідністю різних програм. Для підтримки мультимедійного вмісту в різних додатках IoT необхідна стандартизована архітектура IoMT.

1.3 IoMT з використанням бездротового сенсору

IoMT є розширенням IoT, однією з основних цілей якого є підтримка потокового відео як частини реалізації IoT. В Інтернеті речей недорогі, малопотужні гетерогенні мультимедійні пристрої з обмеженими ресурсами можуть спілкуватися один з одним і бути глобально доступними через унікальні IP-адреси, так само, як комп'ютери та інші мережеві пристрої, підключені через Інтернет. IoMT стикається з тими ж проблемами, що й IoT, наприклад робота з великою кількістю даних, запитів і обчислень, а також деякі унікальні вимоги. Очікується, що мультимедійні пристрої в бездротових мультимедійних мережах на основі IoMT будуть невеликими артефактами з обмеженою кількістю ресурсів живлення, які вони повинні ефективно використовувати для продовження терміну служби мережі.

Мультимедійна комунікація в Інтернеті речей (IoT) потенційно може охопити величезну кількість сфер і глибоко та різними способами торкнутися життя людей. Наприклад, реальні уряди можуть дозволити своїм громадянам завантажувати мультимедійні дані в реальному часі за допомогою деяких програм для смартфонів, щоб повідомляти про стан доріг і дорожнього руху в містах. Потокова мультимедійна інформація в реальному часі може бути застосована до поточних служб реагування на надзвичайні ситуації. Це дозволить службі екстреного реагування надати точну інформацію про характер або серйозність інциденту, наприклад пограбування, нещасного випадку або домашнього насильства, якщо абонент може надіслати відео або фотографії інциденту або місця події. Поточна тенденція полягає в тому, що

пристрої та речі переходять із підтримки немультимедійних даних у бік потокового мультимедіа, особливо потокового відео. Тут важливо мати розуміння потокового передавання мультимедіа та датчика, вбудованого в ці пристрої, у цьому випадку вузли мультимедійного датчика.

Технологія IoT дозволяє масово збирати дані, що призводить до появи великої кількості сенсорних програм. Бездротові сенсорні мережі (WSN) стали найпоширенішими платформами збору даних на основі IoT. У бездротових сенсорних мережах (WSN) збір даних є однією з найважливіших операцій [17]. З огляду на характеристики цих даних, можна вважати, що дуже великомасштабні та неоднорідні WSN можуть бути дуже корисними для збору та обробки цих великих даних. За останнє десятиліття WSN набули популярності. У традиційних WMS і WMSN датчики є пристроями з обмеженими ресурсами з точки зору їх енергії, обробки та обчислювальних ресурсів. WMSN – це мережа взаємопов’язаних сенсорних вузлів, які сприймають навколишнє середовище та повсюдно отримують мультимедійні та звичайні дані з фізичного середовища, показаного на рисунку 1.2. Мультимедійні дані включають нерухомі зображення, аудіо та відео та навіть живі медіа-потоки, які підтримуються сенсорними вузлами із встановленими камерами та мікрофонами.

У мультимедійному блоці величезна кількість отриманих мультимедійних даних стискається за допомогою різних процедур обробки перед передачею, таких як перетворення, квантування, оцінка, ентропійне кодування тощо, щоб мінімізувати вимоги до пропускної здатності під час передачі [18]. Ці процеси є обчислювально складними та споживають значну кількість енергії. Пристрої IoMT мають обмежену пропускну здатність, але для забезпечення гарної якості відео потрібне високе стиснення, яке неможливо через високе енергоспоживання. Бездротові мультимедійні сенсорні мережі є особливим типом бездротових сенсорних мереж (WSN), де величезні обсяги мультимедійних даних передаються через мережі, що складаються з пристроїв малої потужності.

Передбачається, що більшість бездротових мультимедійних пристроїв працюють від батарейок. Оскільки пошук і обробка мультимедіа є енергоємними процесами, обробка мультимедійних даних є обчислювально інтенсивним завданням. Локальна мультимедійна обробка вимагає тимчасового зберігання даних під час зондування та маніпулювання. Обсяг даних у WMSN набагато більший порівняно з WSN, головним чином через використання потокового відео та аудіо. Мультимедійні пристрої на базі IoMT мають обмежену енергоємність і можливості обробки, тому складність слід перемістити в хмару. Інтелектуальні системи керування дорожнім рухом, військове програмне забезпечення, охоронні системи, моніторинг дикої природи – це лише деякі сфери, де WMSN знайшли застосування. Оскільки вони вимагають як немультимедійних, так і мультимедійних знань, усі ці програми неоднорідні за своєю природою [17].

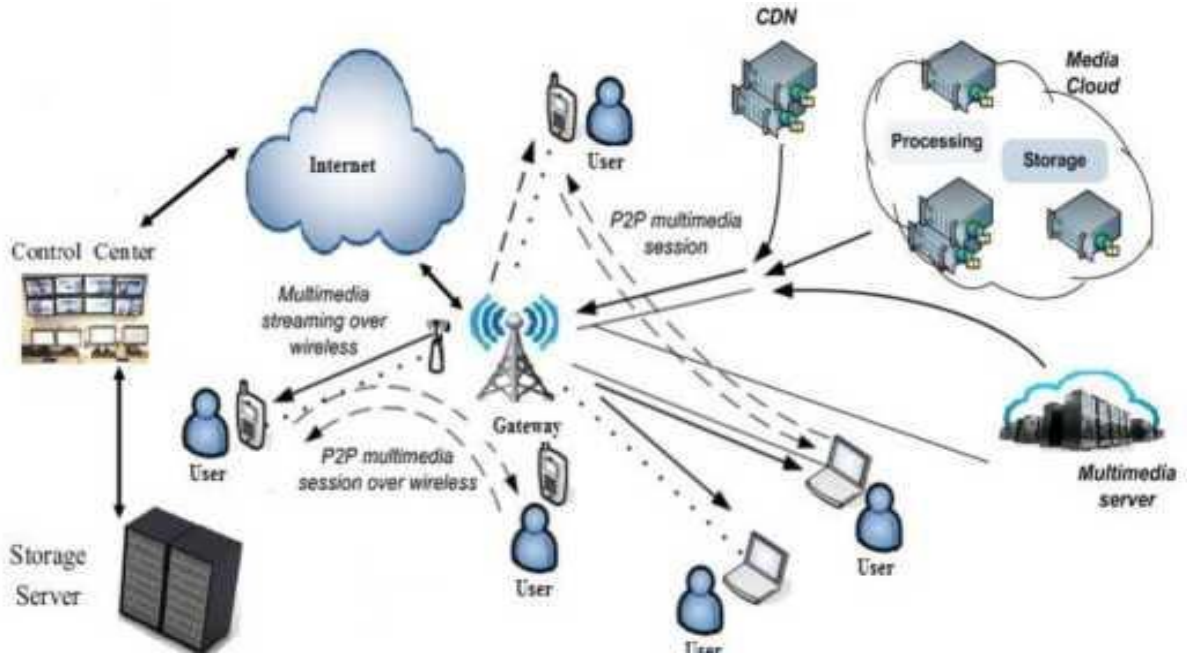


Рисунок 1.2 – Бездротовий зв’язок в IoMT

Надширокосмуговий зв’язок (UWB) зазвичай використовується як стандарт бездротового зв’язку малої дальності для надсилання та отримання мультимедійних інформаційних даних і працює через радіохвилі.

Надширокосмуговий діапазон використовується для смуги пропускання (BW), що перевищує або дорівнює 500 МГц, або для часткової смуги пропускання (FBW), що перевищує 20%, де FBW = BW/fc, де fc – центральна частота. Існують різні стандарти WPAN, такі як Zigbee, Bluetooth, IEEE 802:15:4. ZigBee був прийнятий для IoT через його енергоефективну роботу. Мультимедійне зондування вимагає високої обробки та постійного збору даних, що призводить до більшого споживання енергії. Оскільки очікується, що пристрої IoMT працюватимуть від батарей, які можуть не працювати довше через вимогливу природу мультимедійних даних. Таким чином, необхідно розробити ефективні процедури збору енергії для живлення датчиків і продовження терміну служби мережі.

1.4 IoMT у хмарних обчисленнях

Хмарні обчислення – це нова IT-технологія, яка сьогодні використовується в обчисленнях. Раніше дані користувачів зберігалися на жорстких дисках комп’ютерів. Технологію жорсткого диска замінили хмарні служби зберігання. Хмарні обчислення визначаються як доставка ресурсів, таких як сховище, бази даних, сервери, мережі та програмне забезпечення через Інтернет. Це зелена технологія, яка дозволяє користувачам отримувати доступ, обчислювати та зберігати ресурси через Інтернет без необхідності їх фізичного отримання [19]. Хмарні обчислення зазвичай включають інфраструктуру як послугу (IaaS), платформу як послугу (PaaS) і програмне забезпечення як послугу (SaaS).

Щоб скоротити час обчислень і подолати проблеми з дефіцитом місця для зберігання, більшість організацій сьогодні переходять на хмарні обчислення від традиційного процесу обчислень. Він зосереджений на розповсюдженні даних і обчислень через масштабовані центри обробки даних мережі. Сьогодні користувачі можуть легко отримати доступ до мультимедійного вмісту через Інтернет у будь-який час. Тут користувач

може ефективно зберігати без проблем в хмарі мультимедійний контент будь-якого типу і будь-якого розміру після підписки на нього.

Хмара забезпечує стабільне середовище, у якому реалізується доступ до даних, їх зберігання та обробка прозорим чином. Користувачі мають вищі очікування, коли йдеться про багатоекранні програми. Користувачі можуть отримувати доступ до хмарного мультимедійного вмісту за допомогою кількох пристроїв із широким набором відео- та аудіокодеків, пропорцій і розмірів екрану, які підтримуються на живій основі або на основі плати за використання. Крім того, хмарне мультимедіа має забезпечувати адаптацію QoS до програми та послуги з точки зору пропускної здатності та затримки під час виконання таких завдань, як зберігання, доставка, спільний доступ, подання та отримання, для величезної кількості різнорідних пристроїв кінцевого користувача [20].

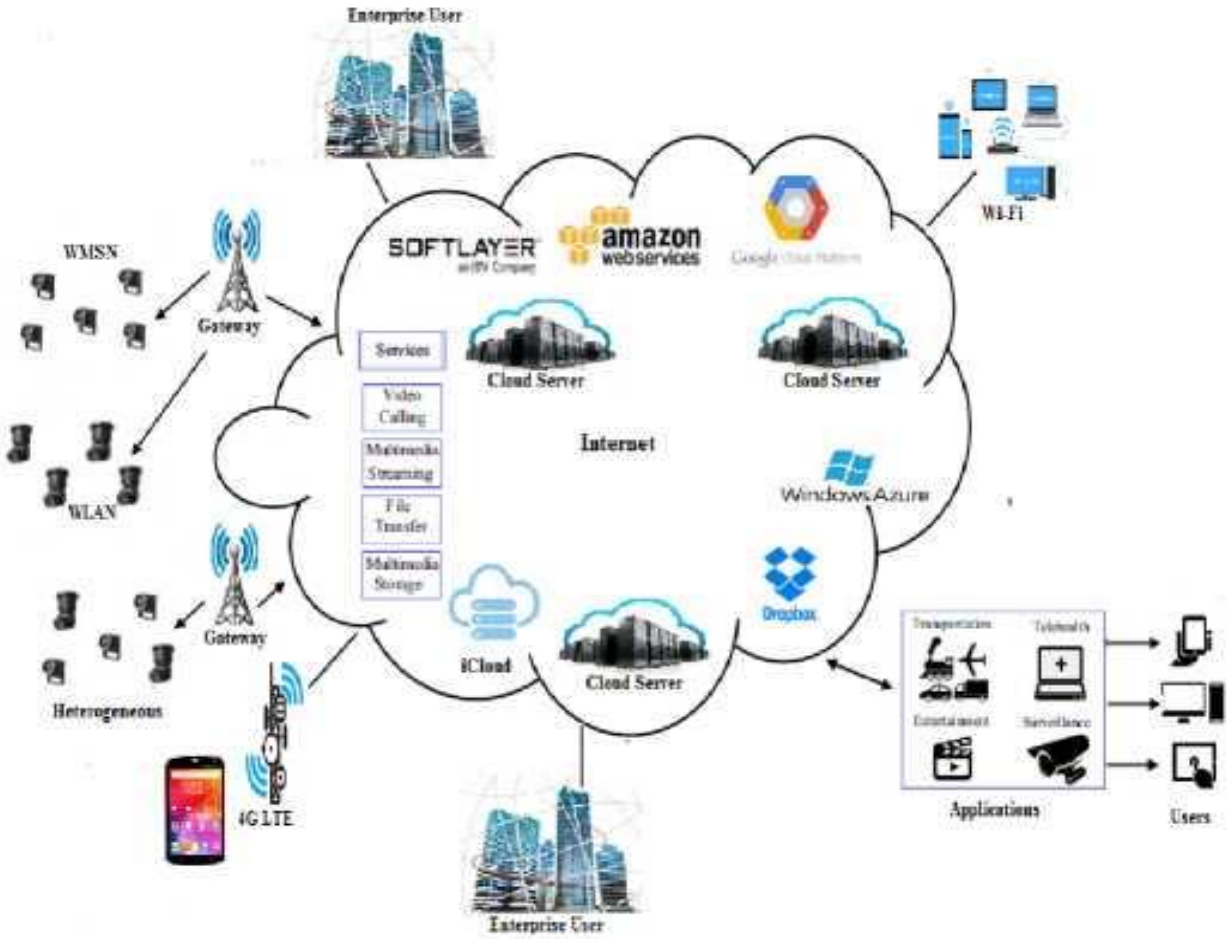


Рисунок 1.3 – IoMT у хмарі

Хмарні мультимедійні обчислення надають постачальникам послуг економічно ефективні послуги шляхом ефективного мультиплексування медіаконтенту, такого як аудіо, відео та зображення, пропонуючи загальну інфраструктуру, використовуючи сервер, оптимізацію, віртуалізацію, доступність та автоматичну обробку, як показано на рисунку 1.3. Використання технології Blockchain в IoMT може мати ряд переваг [21]. Блокчейн – це передова технологія, яка використовується для забезпечення безпеки за допомогою керування доступом до даних, захисту від несанкціонованого запису, прозорості, підтримки розумних контрактів і ненадійних консенсусних властивостей, що вказує на те, що її можна використовувати для захисту сервісів IoMT.

Однак інтеграція хмарної платформи в системи IoMT та IoT є складним завданням, яке пов’язане з численними проблемами, включаючи управління, синхронізацію, надійність і вдосконалення. Для мультимедійних послуг у реальному часі постачальники відеопослуг (VSP) переносять свою інфраструктуру на публічні хмари [22]. Інтеграція хмарних обчислень з IoMT та IoT дозволяє користувачеві отримувати доступ до бажаних даних будь-де та будь-коли. Якщо службами та додатками правильно керувати на хмарних платформах, користувачі зможуть не лише отримувати доступ до даних, а й контролювати свої системи. Наприклад, користувачам можна надати повсюдний доступ до даних датчиків із віддалених сенсорних пристроїв як зондування як послугу (SaaS), механізми правил можуть бути реалізовані для автоматичного керування роботою приводів із хмари як зондування та активація як послуга (SAaaS), яка забезпечує контроль над системами керування ідентифікацією та політикою. Керування ідентифікацією та політикою як послуга (IPMaaS) [23], що забезпечує доступ до аналізу відео та потокового відеоконтенту в хмарі відеоспостереження як сервіс (VSaaS). IoMT та IoT – це багаторівневі технології, які використовуються для

керування та автоматизації підключених пристроїв. Іншими словами, це допомагає отримувати фізичні об’єкти в Інтернеті. Ця платформа надає інструменти, необхідні для підключення пристроїв для міжмашинного зв’язку.

Таблиця 1.2 – Характеристики хмарних платформ IoMT та IoT

Platform	Шлюз	Забезпечення	Гарантії	Оплата	Протокол					
					DDS	REST	Z-Wave	CoAP	HIPP	MQTT
OpenRemore	+	-	+	-	-	-	+	-	-	-
Arkessa	-	+	+	-	+	+	-	-	-	+
Aseda	+	+	+	+	-	+	-	-	-	-
IRI Voracity	+	-	+	+	-	-	-	-	-	+
Ethenes	+	+	+	-	-	+	-	-	-	-
LittleBits	-	-	-	-	+	+	+	-	-	-
NanoSenice	+	+	+	-	-	+	-	+	-	-
Particle	+	-	+	+	-	+	-	+	-	-
Nimbks	-	-	-	-	+	+	+	-	+	-
Ninja Blocks	+	-	-	-	-	+	-	-	-	-
Togwiiig	+	-	-	+	+	+	-	+	-	-
OnePlatform	+	+	+	-	-	+	-	+	+	-
RealTimeao	+	+	-	-	+	+	-	-	-	-
SensorCloud	+	+	-	-	-	+	+	-	-	-
Altair SmartWorks	+	-	+	-	-	+	+	-	-	+
SmartTbings	+	+	-	-	-	+	-	-	-	-
TempoDB	-	-	-	-	-	+	-	-	-	-
SiteWre	+	-	+	+	-	+	-	+	-	+

Iliingvvoi’s	-	+	+	-	-	+	-	-	-	+
Watson bl	+	+	-	+	-	+	-	-	-	+
Xhely	+	+	+	+	-	+	-	-	-	+
ThingsBoaid	+	+	-	+	-	+	-	+	-	+

IoMT & IoT – це програмне забезпечення, яке з’єднує граничне обладнання, точки доступу та мережі передачі даних з іншою стороною, якою зазвичай є програма кінцевого користувача. Z-Wave продемонстрував прийнятну продуктивність, і, незважаючи на те, що він дещо дорожчий, ніж ZigBee, він широко використовується в програмах розумного будинку. Крім того, програми Z-Wave можуть скористатися гнучкістю та безпекою цього протоколу. Для комунікацій M2M у реальному часі служба розподілу даних (DDS) є опублікованим протоколом підписки. DDS має 23 політики QoS, які охоплюють широкий спектр критеріїв зв’язку, таких як безпека, терміновість, пріоритет, довговічність і надійність, серед інших. У цей час на ринку доступні численні хмарні платформи, і ці хмарні платформи розроблені для підтримки різних програм і організаційних вимог. У таблиці 1.2 наведено зведення хмарних платформ, доступних наразі для IoMT та IoT. Ці послуги включають підтримку WAN через шлюзи, підтримку конфігурації, доставку та виставлення рахунків за послуги, що надаються різними протоколами прикладного рівня, і в таблиці 1.2 «+» означає підтримку, а «-» означає відсутність підтримки.

1.5 «Якість речей» (QoT) для IoMT

Мультимедійні комунікації в додатках IoT в режимі реального часу можуть мати затримку мережі та перевантаження через обмеження пропускної здатності та втрату пакетів, що негативно впливає на якість доставленого мультимедіа.

Мільйони користувачів підключаються, зберігають, діляться,

редагують, обчислюють і передають мультимедійні дані через Інтернет, який має суворі специфікації QoS і QoE щодо пропускної здатності, затримки та тремтіння, що було б вузьким місцем для звичайних хмарних провайдерів [24]. Як наслідок, хмарні провайдери загального призначення стикаються з незадоволеними користувачами з точки зору якості обслуговування (QoS) і якості досвіду (QoE) медіа-трафіку. Щоб задовольнити ці потреби, хмарним провайдерам потрібна величезна ємність пам'яті, швидші графічні процесори (GPU), потужні засоби безпеки, високошвидкісне підключення до мережі та довший час роботи акумулятора.

Нефункціональні властивості об'єктів фіксуються моделлю QoT. Ці характеристики стосуються здатності речей виконувати такі завдання, як виявлення, активація та спілкування. Важливо розробити та побудувати якісну архітектуру IoT, щоб забезпечити якість мультимедійного вмісту, такого як аудіо, відео та зображення, які будуть отримані, оброблені та розповсюджені в додатках IoMT. Однак комунікації M2M будуть домінуючими додатками в IoT. Концепція QoT входить до уваги для комунікацій M2M в IoMT [25]. Загалом, QoT означає якість речей і означає безперебійну роботу пристрою IoT. У налаштуваннях IoT він зосереджується на якості мультимедійних даних, які мають бути записані, оброблені та передані між двома чи більше пристроями та об'єктами.

Мета QoT полягає в тому, щоб об'єкт IoT відповідав мінімальним вимогам до якості програми IoT. Він зосереджений на мінімальній якості мультимедійних даних, отриманих вузлом камери, які будуть оброблені та доставлені периферійними та хмарними вузлами. У результаті периферійні та хмарні вузли оброблятимуть і забезпечуватимуть відповідний QoE для мультимедійних даних. Показники Quality of Things мають вирішальне значення для покращення зв'язку між пристроями або між машинами. Для зв'язку між машиною та людиною, наприклад системи моніторингу електронної охорони здоров'я та системи навігації, він враховує показники QoE, такі як пристрої кінцевого користувача, уподобання, задоволеність і

фон. Основні фактори QoT для додатків IoMT, які можуть впливати на продуктивність послуг і додатків, включаючи моніторинг, збір даних, обробку та доставку є такими.

1. Вплив екосистеми. У цій ситуації можуть вплинути на специфікації QoT для екосистем, такі як фізичне розташування, температура та точність часу для програм IoT. Наприклад, інформація або дані, зібрані мультимедійними пристроями та надіслані на мережевий шлюз, мають бути достатньо точними, щоб використовувати їх для подальшої обробки, як-от фізичне місцезнаходження, час і температура.

2. Вплив пристрою. На платформі IoT моніторинг мультимедіа в реальному часі може призвести до високого споживання енергії. У результаті такі впливи системи, як тип пристрою, передача пристрою та батарея, можуть впливати на термін служби пристрою залежно від його поточного стану.

3. Вплив мережі. На ефективність мережі впливають такі впливи мережі, як втрата пакетів і тремтіння. Наприклад, втрата пакетів може призвести до втрати даних, погіршуючи якість передачі даних.

4. Вплив застосування. Щоб відповідати вимогам пристрою IoMT, орієнтовано вплив програми, наприклад типи програм і кодеків. Наприклад, замість H264 можна використовувати такий кодек, як H265, щоб зберегти пропускну здатність мережі, забезпечуючи при цьому високу якість передачі відео.

1.6 Технологій підтримки IoMT

IoMT підтримується декількома технологіями, включаючи бездротові сенсорні мережі, хмарні обчислення, протоколи зв’язку, «машина-машина» (M2M) і «машина-людина» (M2H). У цьому розділі аналізуються п’ять передових технологій для IoMT, показаних на рисунку 1.4.

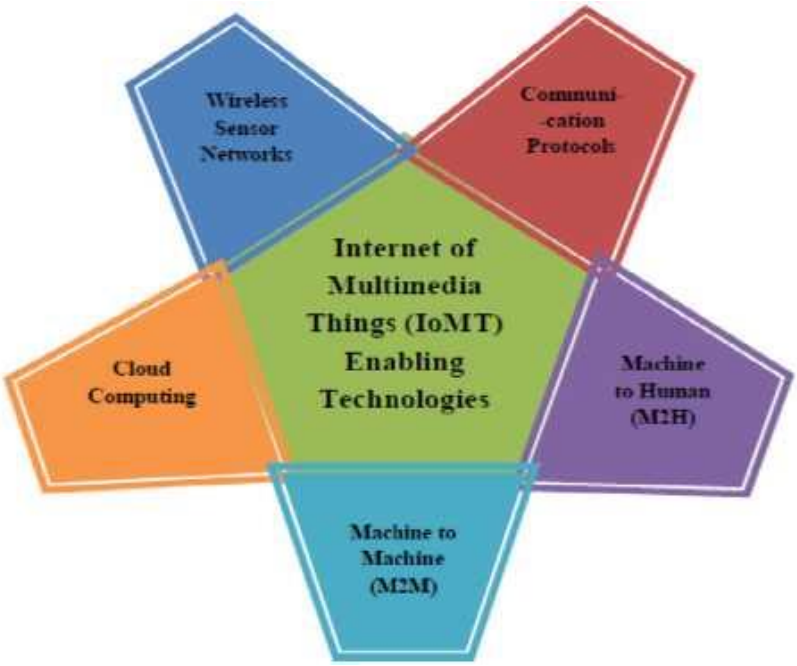


Рисунок 1.4 – Технології підтримки IoMT

1.6.1 Бездротові сенсорні мережі (WSN)

Бездротова сенсорна мережа складається з датчиків, які розподілені по всій мережі та використовуються для виявлення навколишніх і фізичних умов. WSN складається з кількох кінцевих вузлів, маршрутизаторів і координатора. Кінцеві вузли оснащені рядом датчиків, а також можуть служити маршрутизаторами. Пакети даних направляються через маршрутизатори від кінцевих вузлів до координатора. Координатор збирає дані з усіх вузлів [18]. Координатор також діє як шлюз, який підключає WSN до Інтернету. Розгортання WSN для додатків IoMT стає все привабливішим як для наукових кіл, так і для індустрії в таких сферах, як моніторинг енергії будинку та будівлі та моніторинг навколишнього середовища. Використання WSN, включаючи датчики камери та датчики приводу, які можуть сприймати скалярні дані, такі як температура, тиск, вологість і мультимедійну інформацію з навколишнього середовища, може підвищити ефективність, надійність і безпеку програми IoMT. Наприклад, бездротові мультимедійні

датчики здатні контролювати відновлювані джерела енергії, такі як інтенсивність і напрямок сонця та вітру, і прогнозувати інформацію. Також для моніторингу критичних аспектів можна використовувати систему мультимедійного моніторингу в реальному часі, таку як CCTV.

1.6.2 Хмарні обчислення

Хмарні обчислення – це трансформаційна обчислювальна парадигма, яка передбачає розповсюдження програмного забезпечення та послуг через Інтернет. Це включає в себе надання обчислювальних, мережевих і ресурсів зберігання на вимогу та пропонування цих ресурсів користувачам як послуги з виміром у моделі «оплата по ходу» [26]. Хмарні обчислення – це послуги, які є PaaS (платформа як послуга), IaaS (інфраструктура як послуга) і SaaS (програмне забезпечення як послуга). Хмарні обчислення надають різноманітні можливості, наприклад гнучкі обчислення та простір для зберігання. Пристрої можна контролювати та контролювати в будь-який час і з будь-якого місця. Туманні та росянисті обчислення нещодавно стали звичайним методом для роботи з чутливими до затримки додатками IoMT. Надання ресурсів є повністю автоматизованою операцією. Доступ до хмарних обчислювальних ресурсів можна отримати через мережу за допомогою стандартних механізмів доступу, які забезпечують незалежний від платформи доступ через використання різнорідних клієнтських платформ, таких як робочі станції, ноутбуки, планшети та смартфони.

1.6.3 Протоколи зв’язку

Комунікаційні протоколи є основою систем IoT та IoMT, забезпечуючи підключення до мережі та з’єднання пристроїв. Пристрої можуть обмінюватися даними через мережу за допомогою протоколів зв’язку [27]. Кілька протоколів іноді використовуються для позначення різних аспектів

одного зв’язку. Група протоколів, розроблених для спільної роботи, відома як набір протоколів, якщо вони реалізовані в програмному забезпеченні, вони є стеком протоколів. Голосові пакети та відеопакети передаються в існуючій інфраструктурі за допомогою протоколу передачі голосу через Інтернет (VoIP). VoIP (голос через IP, VoIP та IP-телефонія) став більш популярним в останні роки завдяки перевагам низьких цін на дзвінки порівняно з існуючою телефонною мережею загального користування.

1.6.4 Машина до машини (M2M)

Зв’язок M2M («машина-машина») є перспективною технологією для систем зв’язку нового покоління. M2M, або комунікація «машина-машина», це саме те, що це звучить: дві машини «спілкуються» або обмінюються даними без необхідності взаємодії людини [28]. Без будь-якого людського контакту це стосується мультимедійного зв’язку між двома чи більше пристроями. Наприклад, у системі керування дорожнім рухом є датчики камери, які використовуються для моніторингу таких змінних, як швидкість руху, аварії та затори на дорогах. Існує програмне забезпечення виявлення, яке використовується для надсилання всієї інформації через комп’ютери, які контролюють дорожній рух, показуючи світлофори та знаки.

1.6.5 Машина до людини (M2H)

Взаємодія між машинами та людьми – це форма спілкування, за якої люди співпрацюють із системами ШІ та іншими машинами, а не використовують їх як інструменти чи пристрої. Метою цього партнерства між людьми та машинами є використання сильних сторін, фізичних здібностей і недоліків один одного. Мультимедійний контакт між комп’ютерами та людьми називається так.

Найпопулярнішою програмою M2H є E-health monitoring, яка є

програмою та послугою, яка дозволяє лікарям віддалено контролювати пацієнтів. Розумні датчики фіксують дані пацієнта та відображають їх у мультимедійному форматі, щоб лікарі могли дізнатися більше про стан здоров’я пацієнта. Іншим застосуванням M2H є навігаційна система, яка є послугою, де дороги, обладнані датчиками камери, надають кінцевому користувачеві точну інформацію (наприклад, затримки в русі), щоб користувач міг вибрати кращий маршрут.

2 ВИКЛИКИ НАДІЙНОСТІ І ПРОДУКТИВНОСТІ СИСТЕМИ IOMT

2.1 Надійність системи IoMT

Впровадження багаторівневої системи безпеки є головною проблемою для різнорідних пристроїв, починаючи від невеликих систем малої потужності до систем високого діапазону. Завдяки цим різнорідним мережам підвищена сприйнятливість до загроз безпеки та передачі інформації про помилки. Таким чином, будь-яка система IoT буде оснащена стандартним механізмом для сигналізації про надмірність у разі збою або порушення безпеки [29]. Різноманітна багаторівнева інфраструктура системи IoT ускладнює збір достовірних даних, що в кінцевому підсумку призводить до неточних прогнозів терміну служби, що залишився. Аномальні дані генеруються та передаються через вразливість системи, і за найгірших обставин вони загрожують життю людини.

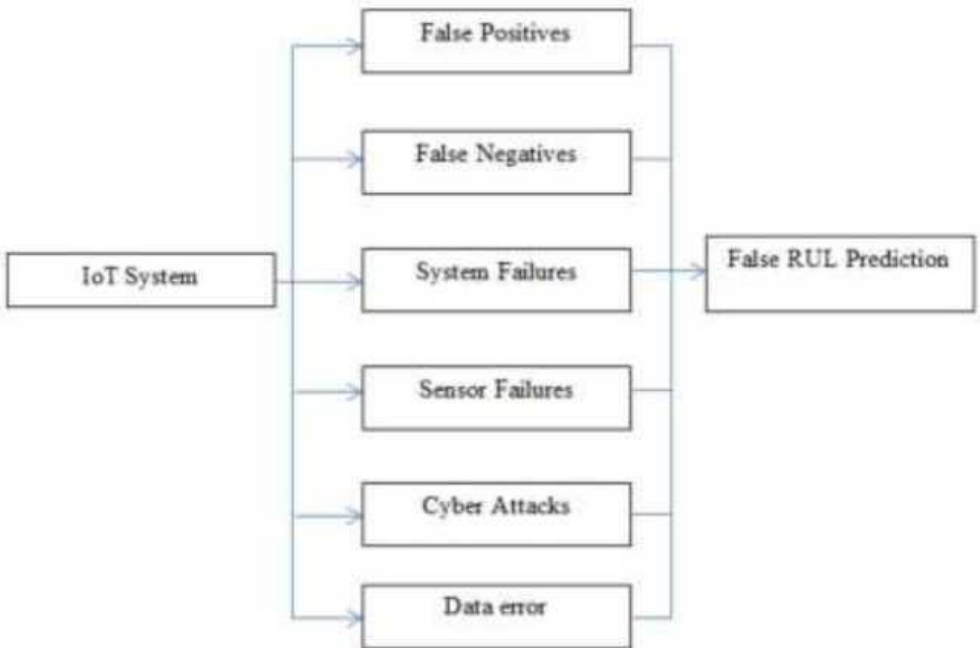


Рисунок 2.1 – Синдроми помилок IoT, що призводять до неправильного RUL

2.1.1 Проблеми у виявленні аномалій

Системи IoT, що працюють на гетерогенних платформах, повинні виробляти величезні обсяги даних, що вимагає великих обчислювальних ресурсів. Виявлення аномалій має вирішальне значення для визначення проблемних даних у звичайних наборах даних під час роботи з величезними обсягами даних за допомогою потужних обчислювальних систем [9]. Основні проблеми, що обмежують ідентифікацію аномалій, і їх потенційні джерела відображені в таблиці 2.1.

Таблиця 2.1 – Ключові проблеми та можливі причини виявлення аномалій

Ключові питання	Можливі причини
Неповнота даних	Неповні набори вхідних даних
Точки даних	Зовнішні дані із середовища
Зашифровані дані	Захист даних
Помилка датчика	Багатошарові сенсори
Шум даних	Збій системи передачі
Сплеск даних	Перевантаження даних

2.1.2 Проблеми з надійністю обладнання

Виправдати очікування розробників обладнання та обслуговуючого персоналу можливо завдяки надійності обладнання [30]. Завдяки управлінню великими обсягами даних обладнання та пристрої IoT стає складно оптимізувати. Ефективність апаратного забезпечення має вирішальне значення для математичних і комп’ютеризованих моделей, побудованих на основі згенерованих даних. Надійність таких пристроїв буде погіршена, що призведе до зниження якості даних і призведе до неточних оцінок залишкового терміну служби компонента.

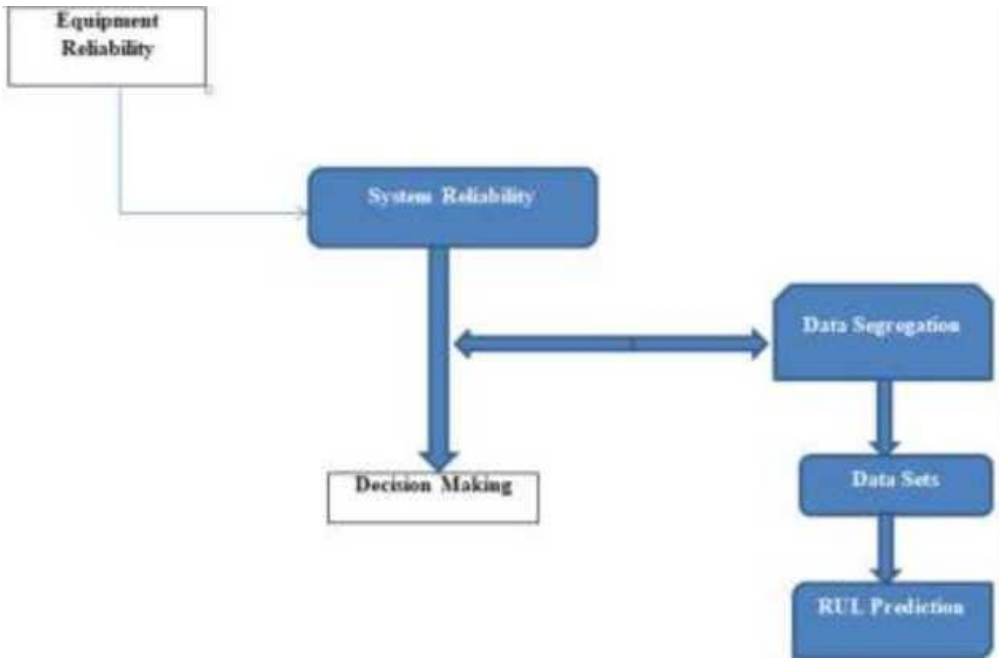


Рисунок 2.2 – Надійність обладнання (темні фігури розглядаються в цій роботі)

2.2 Виклики в архітектурі IoMT

Система IoT повинна забезпечувати надійний вихід протягом усього циклу своєї місії завдяки своїй багаторівневій архітектурі [31]. Під час обговорення архітектурних питань для самої системи IoT враховуються чотири основні рівні, щоб продемонструвати її надійність для отримання результату. Іншими словами, рівень обслуговування, рівень підтримки, рівень зв’язку та рівень сприйняття є частинами однієї багаторівневої архітектури IoT. Кожен рівень дизайну пропонує унікальний набір обставин функціональної відмови, що ставить під сумнів його надійність і створює оманливі прогнози [32]. Рівень підтримки призначений для роботи на FDEP (Functional Dependency), службових перемикачах, тригерних перемикачах і в режимах MTBF і MTTR, за допомогою яких вимірюється доступність системи, тоді як рівень обслуговування призначений працювати над розумними датчиками для вимірювання параметрів двигуна, таких як температура вихлопних газів (EGT) і швидкість компресора N1.

Рівень сприйняття створює труднощі в надійному моніторингу через збої сенсорного вузла для визначення таких вимірювань, як температура та вологість, які забезпечують помилковий вихід або відсутність вихідного сигналу. Рівні зв’язку також створюють проблеми з бездротовим зв’язком, зашумленими даними, ослабленням сигналів і збоями в рівні сприйняття. Рівні архітектури IoT і можливі механізми збоїв, які можуть призвести до неправильного прогнозу RuL, показані на рисунку 2.3.

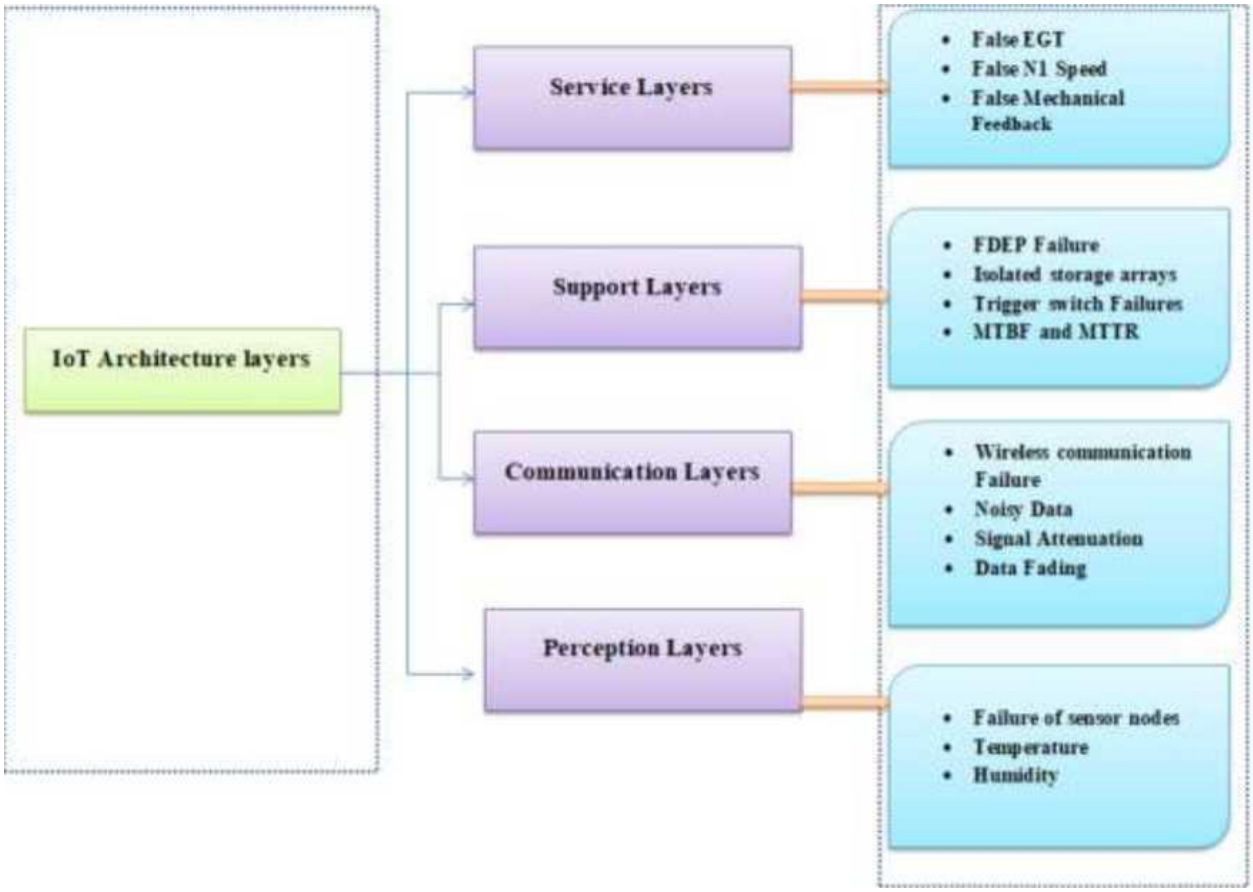


Рисунок 2.3 – Архітектура IoT і можливі збої

2.3 Проблеми продуктивності

Неоднорідність системи IoT матиме складність і обмеження на апаратне та програмне забезпечення, що вимагає масивної обчислювальної системи, що призводить до помітного погіршення параметрів продуктивності

з точки зору високого повного, затримки системи та точності даних [33]. Зокрема, висока вимога до точності в системі IoT може вплинути на аспекти керування у випадку безпілотного літального апарату, що впливає на затримки Ultra, Low і End to End. Крім того, вся система може забезпечувати унікальні комплексні завдання з точки зору датчиків. Таблиця 2.2 показує конкретні можливі причини, які впливають на продуктивність будь-якої багаторівневої системи IoT».

Таблиця 2.2 – Параметр, що впливає на продуктивність, і причини

Можливі причини	Параметри, що впливають на продуктивність
Нездійсненні вхідні дані	Висока пропускна здатність і кадри
Затримка зв’язку	Низькі затримки
Вимоги до високої точності	Збій управління

2.3.1 Проблеми з надійністю обладнання

Ненадійність обладнання в системі IoT дуже чутлива через відсутність кількісного визначення та оцінки фізичних матеріалів у підключеній системі. Таким чином, усі проблеми створюють необхідність у методологіях прогнозування для оцінки надійності апаратного забезпечення. Загальноприйнятими методами є прогнозування фізики відмови (PoF) [34].

Метод фізики відмов є широко використовуваним методом, який надає потенційні результати для точного прогнозування RuL і способу відмов. На рисунку 2.4 показані кроки, пов’язані з фізикою відмови (PoF).

2.3.2 Проблеми в надійності мережі

Основна проблема підтримки надійності мережі в системах Інтернету речей є дуже важливою, де важливо враховувати оцінку QoS (якість обслуговування) і безперервну кількісну оцінку. Тому для оцінки

ефективності мережі завжди слід призначати зручну для користувача техніку оцінювання та прогнозування [34]. Кількісна оцінка пропускної здатності затримки для метричного аналізу QoS виконується для надання достатньої інформації про надійність наскрізних систем IoT [35]. Для визначення затримки та пропускної здатності була запропонована генерація профілю QoS, яка пов’язана з різними компонентами в багаторівневій системі [33]. Підхід статистичного моделювання використовується для розрахунку таких показників QoS, як витрати часу, час відповіді та час ремонту [36]. Моделі резервування були досліджені інфраструктурою резервування шлюзу та ISP.

Рисунок 2.4 – Етапи передбачення PoF

Дослідниками були зроблені різні висновки щодо оцінки надійності мережі в системах IoT. Попередні роботи, проведені з оцінки надійності мережі, прокладуть майбутнім дослідникам шлях для вибору відповідного та прийнятного методу для багаторівневих систем.

2.3.3 Проблеми безпеки системи

Гетерогенна багаторівнева система IoT матиме більшу вразливість для атак на безпеку. Щоб вирішити цю проблему, дизайн системи IoT повинен бути оптимізований, щоб мати важливі фактори, які включають вимоги до ідеального фізичного зв’язку, зв’язку, безпеки, масштабованості та

конфіденційності [37]. Особливо різноманітні типи загроз були визначені попередніми дослідниками. У таблиці 2.3 наведено зведений огляд літератури, що показує внесок кожної роботи, пов’язаної з атаками безпеки на систему IoT.

Таблиця 2.3 – Узагальнений огляд літератури, пов’язаної з атаками на безпеку системи IoT

Напрямок	Висновки
Кібератаки [38-40]	Обговорювалося кілька потенційних кібератак, де активні та пасивні атаки створюють значні загрози на основі шпигунства, підслуховування та DoS
Атаки спуфінгу [41, 42]	Основною проблемою в системі IoT є сприйнятливість до атак спуфінгу, де спуфінг GPS відбувається через високоякісні неправильні сигнали, а спуфінг ARP – через помилкові повідомлення, пов’язані з MAC-адресою хакерів. Порушується протокол керування, що може ввести мережеві операційні системи в оману
Повторні атаки [43, 44]	Автентичність інформації сильно перехоплюється через атаки відтворення в системах IoT. Ця неправильна інформація може призвести до помилкового прогнозу RuL
Розумний лічильник DoS-атаки [45-47]	Атаки типу «Відмова в обслуговуванні» створюють велику кількість відповідей і пакетів запитів, що може призвести до повного збою системи. Коригувальна дія досягається шляхом інтеграції пристроїв IoT до Smart Grid
Атаки шкідливих програм [48, 49]	Шкідливе програмне забезпечення впроваджується в систему, що може спричинити перебої або відсутність обслуговування. Комунікаційний рівень системи IoT більш схильний до цих атак, які, можливо, доведеться інтегрувати для запобігання

3 МОДЕЛЬ СИСТЕМИ

3.1 Загальний опис

Використаний підхід полягає в кластері пристроїв IoMT, які надають певні послуги, гарантуючи попередньо визначені обмеження якості обслуговування. У цьому розділі описано за допомогою визначень і прикладів кілька компонентів системи та їх взаємодію.

Рисунок 3.1 надає високорівневий погляд на систему в цілому, де користувач визначає якість, необхідну для послуги, яка потім транслюється у властивостях програми і, нарешті, виконується кластером пристроїв, які використовують зарезервовану частину ресурсів для надання послуги з відповідним рівнем QoS для виконання запиту користувача.

Центральною особливістю цієї системи є розподіл коду. Пристрої IoMT із резервною ємністю пропонують свою доступність для участі в коаліції, щоб дозволити системі досягти глобального результату з точки зору надання послуг із заданою якістю. Через спеціальну природу цієї коаліції необхідно ретельно вивчити кілька деталей, а саме, як спілкуватися, поширювати дані та гарантувати глобальну якість обслуговування, а також як мати справу з динамічними змінами.

Важливу роль відіграє резервування ресурсів через встановлення точної резервної потужності, якою пристрій готовий поступитися коаліції, припускаючи, що така гарантія є центральною для належної роботи коаліції. Однак лише це не гарантує, що наданий QoS є стабільним, оскільки нові пристрої можна додавати та видаляти (через збої) у будь-який час. Таким чином, під час роботи система повинна гарантувати, що заданий рівень QoS все ще можливий, або буде обрано зміну на нову погіршену (якщо це прийнятно) версію сервісу. Якщо цей варіант неможливий, коаліція не зможе продовжувати надавати послуги. Далі наведено кілька визначень.

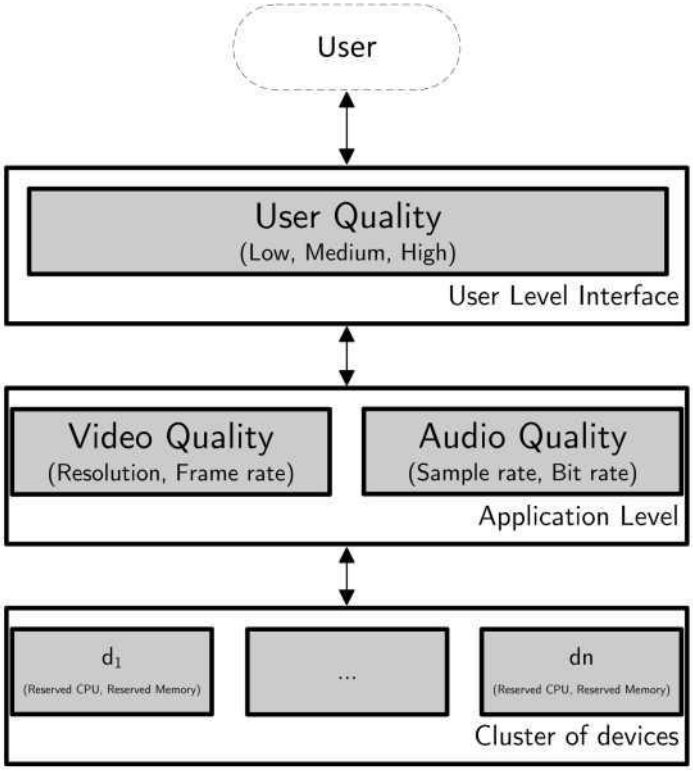


Рисунок 3.1 – Огляд системи на високому рівні

Визначення 1: кластер IoMT. Набір C = $\{d_1,...,d_n\}$ пристроїв IoMT d_i, які наразі надають спільне рішення для послуги.

Визначення 2: субкластер IoMT. Дано кластер IoMT C = $\{d_1,...,d_n\}$, субкластер SC – це набір $\{d_{i1},..., d_{in}\}$ пристроїв IoT, де кожен $d_{ik} \in C$.

Визначення 3: процесор. Блок обробки p визначається як{t, u}, де t – завдання коду, яке має виконуватися з вхідними даними u.

Визначення 4: служба. C = {P, Q} – множина P=$\{u_1,..., u_n\}$ блоків обробки разом з обмеженнями QoS, визначеними в Q.

Послуга може надаватися з різними рівнями QoS залежно від характеру послуги та вподобань користувача щодо якості.

Визначення 5: обмеження QoS. Нехай Q – це набір обмежень QoS користувача, пов’язаних із послугою S. Кожен Q_{kj} – це кінцевий набір варіантів якості для j-го атрибута розмірності k. Це може бути або дискретна, або неперервна множина, така що Q = {Dim, Attr, Val, DAr, AVr, Deps}, де

Dim – набір розмірів QoS, Attr – набір ідентифікаторів атрибутів, Val – набір ідентифікаторів значень атрибутів. Кожне значення представлено кортежем Val_i = {Type, Domain}, де Type = {integer, float, string} і Domain = {continuous, discrete}.

Набір зв'язків DA_r призначає кожному виміру в Dim набір атрибутів у Attr і визначається як DA_r: $Dim_i \rightarrow Atr$, $\forall_{Dim_i} \in Dim$.

Набір зв'язків AV_r призначає кожному атрибуту в Attr певне значення у Val і представлений як AV_r: $Atri \rightarrow Val_k$, $\forall_{Atr_i} \in Atr, \exists^1_{Val_k} \in Val$.

Deps визначає набір існуючих залежностей між значеннями існуючих атрибутів. Залежність між Atr_i і Atr_j представлена як $Dep_{ij} = f(Val_{ki}, Val_{kj})$, $\forall Attr_i, Attr_j \in Attr$.

Для певної послуги можна вибрати з набору значень параметрів QoS; наприклад, параметри, пов'язані зі звуком, такі як частота дискретизації (8, 16, 24, 44, 48 і 88 кГц), біти дискретизації (8, 16 і 32), наскрізна затримка (100, 75, 50 і 25 мс) і параметри, пов'язані з відео, такі як роздільна здатність зображення (SQCIF, QCIF, CIF, 4CIF, 16CIF), глибина кольору (1, 3, 8, 16,...) і частота кадрів (1,..., 60).

Користувачі надають специфікацію для мінімально бажаного QoS для послуги S з мінімальними прийнятними розмірами. Надання послуги може здійснюватися зі значеннями, які відповідають принаймні тим, які визначені користувачем.

Приклад 1. Використовуючи програму потокового відео як приклад, нижче наведено список параметрів якості, які можуть бути пов'язані з будь-якою конкретною програмою. Список наведено для ілюстрації запропонованої моделі і не є вичерпним.

Dim = {Video Quality, Audio Quality}

Attr = {compression index, color depth, frame size, frame rate, sampling rate, sample bits}

Val = {{1, integer, discrete},{3, integer, discrete}, . . . , {[1, 30], integer,

continuous}, . . . }

DA Video Quality = {image quality, color depth, frame size, frame rate}

DA Audio Quality = {sampling rate, sample bits}

AV compression index = {[0, 100]},

AV frame size = {SQCIF, QCIF, CIF, 4CIF, 16CIF}

AV color depth (bits) = {1, 3, 8, 16, 24, . . . }

AV frame rate (per second) = {[1, 30]}

AV sampling rate (kHz) = {8, 11, 32, 44, 88}

AV sample bits (bits) = {4, 8, 16, 24}

Маючи таку характеристику QoS конкретного домену програми, користувачі та постачальники послуг тепер можуть визначати вимоги до послуг і пропозиції для досягнення угоди щодо надання послуг. Оскільки QoS має багатовимірну природу, компроміси можуть бути зроблені через дефіцит ресурсів.

Подальші відомості про характеристику QoS для розподілених систем можна знайти, наприклад, у [36].

З прагматичної точки зору можна приховати деталі характеристики QoS в описах високого рівня, як представлено в наступному прикладі.

Приклад 2. З точки зору користувача та для практичності параметри QoS можна спростити. Наприклад, відео можна просто описати як SD, HD і FHD, як представлено в таблиці 3.1; звук як низький, середній і високий, як представлено в таблиці 3.2.

Слід зауважити, що це лише приклад, інші конфігурації можна легко реалізувати.

Таблиця 3.1 – Високорівнева чіткість відео

Опис	Загальне позначення	Роздільна здатність
SD (стандартна чіткість)	480 p	640 x 480
HD (висока чіткість)	720 p	1280 x 720
FHD (Full HD)	1080 p	1920 x 1080

Крім того, слід зауважити, що обмеження QoS визначаються як мінімально прийнятний набір властивостей для надання певної послуги. Це означає, що коаліція може дати більш якісний результат, але не нижчий. Таким чином, пристрої, що залишають коаліцію (через певний тип збою), повинні бути оброблені, а мінімальний QoS кластера IoMT повинен бути перерахований.

Таблиця 3.2 – Визначення звуку високого рівня

Роздільна здатність	Бітрейт (кбіт/с)	Частота дискретизації (кГц)
Низький	128	32
Середній	192	44,1
Високий	320	48

3.2 Алгоритми

Фреймворк розділений на два основні модулі: налаштування кластера та динамічна адаптація до нових сервісів. Кластери IoMT співпрацюють, щоб надати запитану послугу, обробляючи дані, оформлені за допомогою QoS, визначеного користувачем. Через неоднорідність послуг, що виконуються, переваги якості користувачів, базові операційні системи, мережі та пристрої, специфікація QoS повинна бути підтверджена всіма пристроями, або вони повинні мати можливість відображати свої індивідуальні специфікації на загальну.

Важливо зазначити, що хоча тут не досліджуються алгоритми потокової передачі, потрібно розуміти можливості різних пристроїв у кластері. Таким чином, було оцінено їх обчислювальну потужність, щоб зробити висновок, чи здатні вони впоратися з нав’язаним попитом.

3.3 Налаштування кластера

Перший крок до спільної мережі пристроїв IoMT, які працюють разом для надання мультимедійних послуг, – це знати, скільки пристроїв доступно та на що вони здатні, а отже, оцінити глобальну потужність. Формування кластера складається з реєстрації доступних пристроїв IoMT на головному пристрої (той, який запитує послугу) та оголошення вільної потужності для доставки. Оскільки метою є обробка аудіо та відео, кожен пристрій повідомляє про свою ємність у найгіршому випадку з наявними в нього запасними ресурсами. Потім це зіставляється з уподобаннями користувача, і, якщо це можливо, послуга надається. Кожен пристрій IoMT реєструється з пристроєм, який запитує запуск служби в моделі клієнт-сервер. В алгоритмі лістингу 3.1 описано, як реалізується цей процес.

Лістинг 3.1 – Налаштування кластеру

Let $\mathcal{N}$ be the node requesting the service S.
Let $\mathcal{A} := \{\}$ be a global variable that stores the set of available nodes in the cluster.
Take a service $S = \{P, Q\}$ with processing unit P and related QoS Q such that each Q_{kj} is a finite set of n quality choices for the j^{th} attribute, expressed in decreasing order of preference, for all k QoS dimensions.
Let $\mathcal{S} := \{\}$ be the set of nodes in the cluster capable of providing a given service.
Let $\mathcal{N}$ broadcast to the local network the request for nodes to register, adding them to $\mathcal{A}$.

1: **for** each $d_i \in \mathcal{A}$ **do**
2: Let Q_j be the QoS delivered by node d_i
3: **if** Q_j is higher (in all its dimensions) than Q **then**
4: $\mathcal{C} = \mathcal{C}\{(d_i, Q_j)\}$
5: **end if**
6: **end for**
7: **return** $\mathcal{C}$

3.4 Динамічна адаптація до нових послуг

Лістинг 3.2 демонструє погодження для прийому нових послуг.

Лістинг 3.2 – Динамічна адаптація до нових послуг

Let $\mathcal{N}$ be the node requesting the service S_{new}.
Given a new service $S_{new} = \{P_{new}, Q_{new}\}$ with processing unit P_{new} and related QoS Q_{new} such that each Q_{kj} is a finite set of n quality choices for the j^{th} attribute, expressed in decreasing order of preference, for all k QoS dimensions. Let $\mathcal{A}$ be a global variable that stores the set of available nodes in the cluster.
Let $S_{\mathcal{C}} = \{\}$ be the sub cluster that will provide the new service.
Let $\mathcal{N}$ broadcast to the local network the request for nodes to register adding them to $\mathcal{A}$.

```
while t < timeout do
    for each d_i ∈ A do
        Let Q_j be the QoS delivered by node d_i
        if Q_j is higher (in all its dimensions) than Q then
            if d_i can accommodate such service along existing ones then
                S_C = S_C ∪ {d_i}
            end if
        end if
    end for
end while
return S_C
```

Слід зауважити, що послуги можна додавати до номера, куди їх можна надавати. У разі відмови одного вузла служба скидається та визначається новий підкластер.

Приклад 3. На рисунку 3.2 можна побачити два підкластери, які були створені для надання двох різних послуг з різними QoS. пристрій N запитав першу послугу S_1, яку надали пристрої $\{d_1, d_2, d_5\}$, а після цього друга служба S_2, що забезпечувалося приладами $\{d_3, d_4, d_5\}$. Обидві служби базуються на доступних пристроях, які входять до основного кластера ($\{d_1, d_2, d_3, d_4, d_5\}$). Цей кластер є динамічним, оскільки він змінюється шляхом додавання та видалення пристроїв, що може статися в будь-який час.

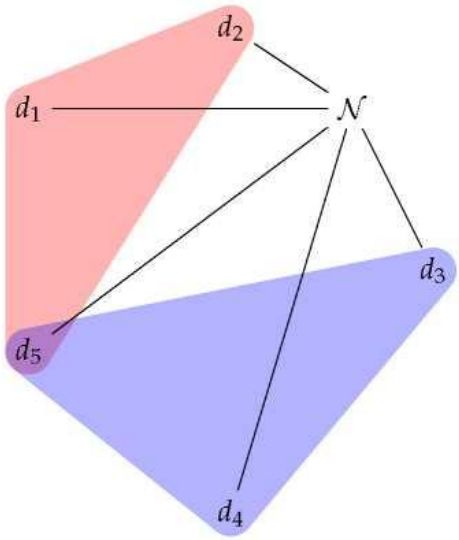


Рисунок 3.2 – Два підкластери, що надають різні послуги S_1 і S_2 з різними QoS

Усі наведені тут алгоритми є описом реалізації на високому рівні; багато дрібних деталей не описано. Далі буде детальніше розглянуто, як працює фактична структура, описуючи відповідні частини реалізації.

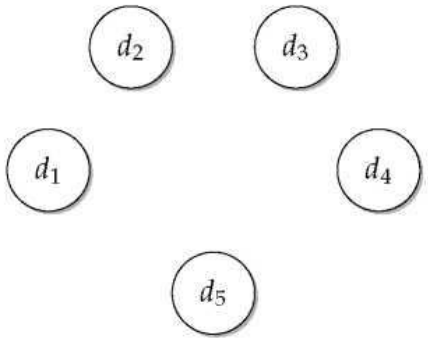
3.5 Результати та аналіз

Для реалізації фреймворку було використано мову програмування Elixir через легкість, яку він забезпечує для розподілу та виконання даних і коду пристроями в мережі. Для апаратного забезпечення використано Raspberry Pi, тип SBC (одноплатний комп’ютер), який можна використовувати як звичайний пристрій Інтернету речей і який користується величезною популярністю завдяки високій продуктивності для свого цінового діапазону та великій кількості сценаріїв, де він може бути використаним. Використання цього типу SBC також дозволяє використовувати Linux як операційну систему для реалізації політики резервування ресурсів і використання Elixir разом із віртуальною машиною Erlang у кожному з них, створюючи розподілений сценарій, яким простіше

керувати.

3.5.1 Формування кластерів

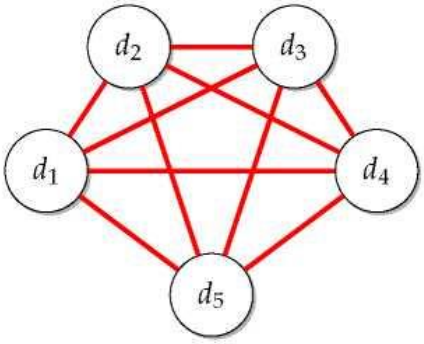
Усі пристрої IoMT запускали програму клієнт-сервер, яка дозволяла їм взаємодіяти з іншими та створювала кластер, який надавав би послугу. Будь-який IoMT-пристрій, коли він увімкнений, оголошує, що він доступний. Це робиться за допомогою вбудованих функцій виявлення Elixir, і кожен пристрій підтримує список усіх інших відомих пристроїв у мережі, як показано на рисунку 3.3.



Вузол	Зареєстровані вузли
d_1	$\{d_2, d_3, d_4, d_5\}$
d_2	$\{d_1, d_3, d_4, d_5\}$
d_3	$\{d_1, d_2, d_4, d_5\}$
d_4	$\{d_1, d_2, d_3, d_5\}$
d_5	$\{d_1, d_2, d_3, d_4\}$

Рисунок 3.3 – Відкриття вузла

Йдеться про те, що ці інші пристрої зареєстровані на пристрої, у списку якого вони є. Структура також надає функцію, за допомогою якої підтримується зв’язок між пристроями, як показано на рисунку 3.4. Далі виявляється будь-який збій (відключення пристрою), що дозволяє оновити список шляхом видалення відключеного пристрою, як показано на рисунку 3.5.



Вузол	Зареєстровані вузли
d_1	{d_2, d_3, d_4, d_5}
d_2	{d_1, d_3, d_4, d_5}
d_3	{d_1, d_2, d_4, d_5}
d_4	{d_1, d_2, d_3, d_5}
d_5	{d_1, d_2, d_3, d_4}

Рисунок 3.4 – Зв'язування вузлів

Коли одному з цих пристроїв потрібно запустити службу, він запитує кожен із пристроїв, які на ньому зареєстровані, отримуючи можливість QoS, яку кожен може надати. Пристрої, які забезпечують QoS вище мінімального, вибираються для співпраці. В лістингу 3.3 наведено невеликий приклад основної функції формування кластерів, написаний в Elixir.

Лістинг 3.3 – Основна функція формування кластерів

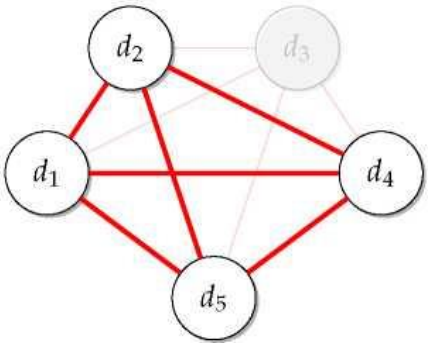
```
def create_cluster(RegistredNodes,QoSParametersList) do
    SubCluster = query_nodes(RegistredNodes,QoSParametersList)
end

def query_nodes([],[]) do
    []
end

def query_nodes([node|remainingnodes],qosparameterslist) do
    send(node, {:evaluate,qosparameterslist}
    receive do
        {node,:ok_capable} ->
            [node|query_nodes(remainingnodes,qosparameterslist)]
        {node,:not_capable} ->
            query_nodes(remainingnodes,qosparameterslist)
    end
end
```

3.5.2 Розрахунок локального QoS

Розрахунок локального QoS дозволяє дізнатися, чи може вузол співпрацювати в службі з урахуванням певних обмежень QoS. Щоб впоратися з динамічністю каркаса, це має реалізовуватися швидко. Запропоноване рішення для цієї конкретної проблеми полягає в тому, щоб порівняти пристрої та заздалегідь знати їхні можливості. Оскільки було використано SBC, є можливість профілювати ці пристрої, щоб знати, скільки ресурсів процесора та пам'яті потрібно для надання певної послуги за певних обставин. Було проведено порівняння всіх SBC, які використовуються у рамках, і отримано їхні потреби в ресурсах для обробки відео та аудіо за деякими типовими сценаріями, які були визначені. Знову ж таки, фреймворк можна моделювати за допомогою різних SBC і різних конфігурацій відео- та аудіопотоків, і це слід розглядати як приклад, який використовується конкретно в цьому рішенні, але його можна легко адаптувати до інших ситуацій.



Вузол	Зареєстровані вузли
d_1	{ d_2, ~~d_3~~, d_4, d_5}
d_2	{ d_1, ~~d_3~~, d_4, d_5}
d_4	{ d_1, d_2, ~~d_3~~, d_5}
d_5	{ d_1, d_2, ~~d_3~~, d_4}

Рисунок 3.5 – Збій вузла d_3

Було використано інструмент ffmpeg (https://ffmpeg.org/) та утиліта моніторингу використання ресурсів RPI-Monitor (https://github.com/ XavierBerger/RPi-Monitor), щоб протестувати та отримати статистичні дані щодо типових сценаріїв для розглянутих SBC, а саме Raspberry Pi 3 A+, 3 B+ і Zero W.

Проводилось вимірювання навантаження ЦП і пам’яті для декодування відео та аудіо в таких сценаріях:

- низьке навантаження – SD-відео та середня якість звуку: роздільна здатність відео 640 x 480 пікселів 24 кадри в секунду та аудіо з бітрейтом 128 Кбіт/с і частотою дискретизації 32 000 Гц;
- середнє навантаження – HD-відео та висока якість звуку: роздільна здатність відео 1280 x 720 пікселів 24 кадри в секунду та аудіо з бітрейтом 192 Кбіт/с і частотою дискретизації 44 100 Гц;
- високе навантаження – відео FHD і дуже висока якість аудіо: роздільна здатність відео 1920 x 1080 пікселів із частотою 30 кадрів на секунду та аудіо зі швидкістю передачі даних 320 Кбіт/с і частотою дискретизації 48 000 Гц.

Завантаження процесора представлено на рисунку 3.6, де видно, що серед моделей Raspberry Pi 3B+ і 3A+ майже не було різниці в навантаженні ЦП. Це було очікувано, оскільки вони покладаються на те саме апаратне забезпечення на рівні ЦП. У Raspberry Pi Zero W менш потужний процесор, і це добре помітно. Хоча ЦП був стабільним під час усіх тестів, слід зауважити, що це не стосується оперативної пам’яті, де кілька конфігурацій декодера призвели до досить різних вимог до оперативної пам’яті. У цьому випадку було помічено, що в середньому потрібно 27 МБ для декодування потоку найнижчої якості, 45 МБ для потоку середньої якості та 56 МБ у середньому для потоку найвищої якості; і це стосується всіх пристроїв, які було протестувано.

Слід звернути увагу на те, що в цих тестах не використовувалося апаратне прискорення H.264, оскільки не всі пристрої підтримують цю функцію. Тому було спрямувано підхід до типового пристрою IoMT, який покладається головним чином на здатність ЦП виконувати всю роботу. Тим не менш, можна сказати, що з увімкненим H.264 Raspberry Pi 3 мав постійне навантаження на ЦП 5% для всіх різних тестованих комбінацій відео/аудіо та постійний відбиток пам’яті 22 МБ, що робить його сильним кандидатом для

реалізації швидкої та ефективної обробки аудіо- та відеопотоків.

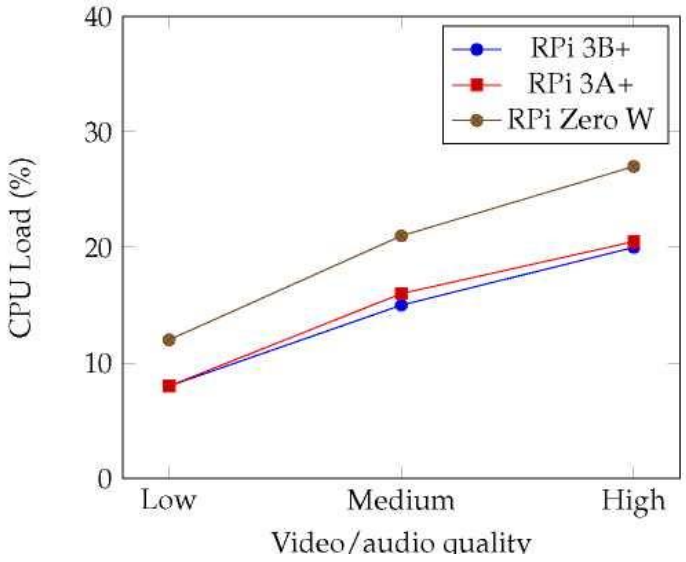


Рисунок 3.6 – Потрібна потужність процесора

Нарешті, можна підкреслити, що це етап конфігурації фреймворку, і будь-які інші значення та параметри можна враховувати під час етапу налаштування. Крім того, було протестувано кодування та транскодування потоків, але висновок можна зробити такий, що це набагато більш інтенсивне завдання, і що наявне обладнання не може впоратися з вимогами потоків досить низької якості.

3.5.3 Динамічна координація

Коли надходить нова послуга, запит QoS виконується для зареєстрованих пристроїв, а обчислення виконується, як було описано раніше. Якщо можливо надати послугу, то для неї створюється новий підкластер відповідно до процедури, продемонстрованої в лістингу 3.2. Вся координація покладається на систему повідомлень Elixir.

Коли один пристрій виходить з ладу, платформа негайно виявляє цю подію, як показано на рисунку 3.5. Після вивчення кількох підходів можна

дійти висновку, що найбільш адекватним є скидання кластера щоразу, коли виникає збій вузла. Це означає, що весь процес запиту зареєстрованих вузлів і формування коаліції, що надає послуги, виконується заново. Оскільки цей процес залежить від зв’язку в локальній мережі з дуже низькою затримкою, а дані, які використовуються для налаштування конфігурації, доступні статично, цей процес відбувається відносно швидко. Це означає, що у випадку, якщо все ще є можливість продовжити використання послуги, користувач буде лише на короткий час позбавлений її.

3.5.4 Перевірка

У цьому підрозділі аналізується ефективність запропонованого підходу з точки зору налаштування кластера та керування ресурсами. Було використано фізичний кластер для попередніх тестів, у якому запитувалися різні послуги та були зарезервовані необхідні ресурси. Потім було реалізовано симуляцію, яка уможливила тестування більшої кількості пристроїв і апаратних конфігурацій, і проаналізовано, як використовуються ресурси за нашим підходом.

3.5.5 Простий апаратний кластер

Для першого сценарію було використлано обладнання, описане в таблиці 3.3, з п’ятьма пристроями IoMT і відповідним доступним процесором і пам’яттю після застосування політики резервування ресурсів.

Було налаштувано кілька одночасних послуг. Один із прикладів представлений у таблиці 3.4.

Таблиця 3.3 – Налаштування кластера

Пристрій	Опис	Загальна оперативна пам’ять	Доступний ЦП (%)	Доступна пам’ять (МБ)
d_1	RPi 3 B+	1,0 ГБ	47	350
d_2	RPi 3 B+	1,0 ГБ	65	835
d_3	RPi Zero W	0,5 ГБ	34	126
d_4	RPi 3 A+	0,5 ГБ	53	277
d_5	RPi Zero W	0,5 ГБ	15	35

Таблиця 3.4 – Запитані послуги

Назва послуги	Запит пристрою	Опис послуги
S_1	d_1	Відео FHD і дуже висока якість звуку
S_2	d_2	SD відео та середня якість звуку
S_3	d_1	Відео FHD і дуже висока якість звуку

Пристрій d_1 містить усі інші (d_2, d_3, d_4, d_5) у своєму списку зареєстрованих вузлів, а пристрій d_2 має (d_1, d_3, d_4, d_5). У таблиці 3.5 можна побачити, що відбувається після додавання послуг S_1, S_2 і S_3 до кластера. Після запиту на обслуговування S_1 усі пристрої, крім d_5, можуть співпрацювати, розподіляючи ресурси, визначені у 3.5.2. Коли до кластера додається служба S_2, усі пристрої, крім d_3, можуть брати участь у пов’язаному підкластері. Слід зауважити, що оскільки необхідні ресурси менші, ніж ті, які потрібні S_1, тепер пристрій d_5 також може брати участь. Нарешті, додавання S_3 передбачає співпрацю d_2 і d_4. Під час тестування було помічено, що використання ЦП на межі його можливостей не є гарною ідеєю через незначні варіації навантаження на ЦП під час виконання, які в разі перевантаження ЦП можуть затримати виконання призначених служб; таким чином, можна вважати за гарну ідею залишати невелику частину ЦП завжди доступною (зазвичай принаймні 5%).

Таблиця 3.5 – Призначення послуг до пристроїв

Початковий стан			Додавання S_1		Додавання S_2		Додавання S_3	
Пристрій	ЦП	ОП	ЦП	ОП	ЦП	ОП	ЦП	ОП
d_1	47	350	27	294	19	267	–	–
d_2	65	835	45	779	37	752	17	696
d_3	34	126	7	70	–	–	–	–
d_4	53	277	33	221	25	194	5	138
d_5	15	35	–	–	3	8	–	–

3.5.6 Моделювання більших кластерів

Після проведення перших експериментів із реальним апаратним забезпеченням і після того, як за статистичними даними середня кількість підключених пристроїв на домогосподарство у 2023 році становила 13 у Північній Америці та 9 у Європі, було вирішено використати симулятор, щоб збільшити розмір кластера та провести тестування з різними конфігураціями. Ці симуляції були реалізовані в Elixir за допомогою процесів віртуальної машини Erlang. Пристрої моделюються процесами, у яких кожен з них підтримує список загальної та залишкової пам’яті та ЦП. Зв’язок імітується за допомогою функцій внутрішнього зв’язку процесу, а затримка ігнорується.

Типи служб, які можна прив’язати до пристроїв, відповідають описаним у попередніх розділах, і є профіль, який повідомляє, що вони споживають з точки зору процесора та пам’яті. Для цього моделювання було використано характеристику, описану в таблиці 3.6.

За допомогою цієї симуляції можна створити скільки завгодно процесів і послуг, враховуючи, що не перевищуються базові обмеження віртуальної машини. Однак ідея полягала в тому, щоб спробувати відповідати тому, що можна знайти в реальному сценарії. Наприклад, з 15 пристроями та кількома запущеними службами можна створити кластер, що включає пристрої,

описані в табл 3.7, де для кожного пристрою також докладно вказується доступна оперативна пам’ять у мегабайтах і доступний ресурс ЦП у відсотках. Також можна сформувати список послуг, описаних у табл 3.8.

Таблиця 3.6 – Характеристика пристроїв

Тип	Всього ОП	Низький		Середній		Високий	
		ЦП	ОП	ЦП	ОП	ЦП	ОП
1	1 ГБ	8	27	15	45	20	56
2	0,5 ГБ	8	27	16	45	20	56
3	0,5 ГБ	12	27	21	45	27	56

Таблиця 3.7 – Пристрої в симуляції

Пристрій	Тип	Доступна ОП, МБ	Доступний ЦП, %
d	1	652	56
d	1	375	85
d	2	458	47
d	3	216	61
d	2	127	36
d	3	89	15
d_7	3	127	26
d_8	1	450	64
d_9	1	784	82
d_{10}	2	318	63
d_{11}	2	287	41
d_{12}	2	299	76
d_{13}	3	30	13
d_{14}	1	128	24
d_{15}	3	280	53

Оптимізація ресурсів сильно залежить від порядку надходження послуг, але для попереднього сценарію можна відзначити значне збільшення використання ресурсів. На рисунку 3.7 можна побачити значення середньої потужності процесора, що використовується в кластері, коли вводяться послуги. На рисунку 3.8 можна побачити, скільки пристроїв можуть співпрацювати у наданні послуг. З впровадженням служб кількість пристроїв зменшується, оскільки деякі з них вичерпують ресурси (переважно потужність ЦП) і не можуть брати участь у спільній роботі.

Таблиця 3.8 – Опис послуги

опис	Тип
S_1	низький
S_2	високий
S_3	низький
S_4	середній
S_5	середній

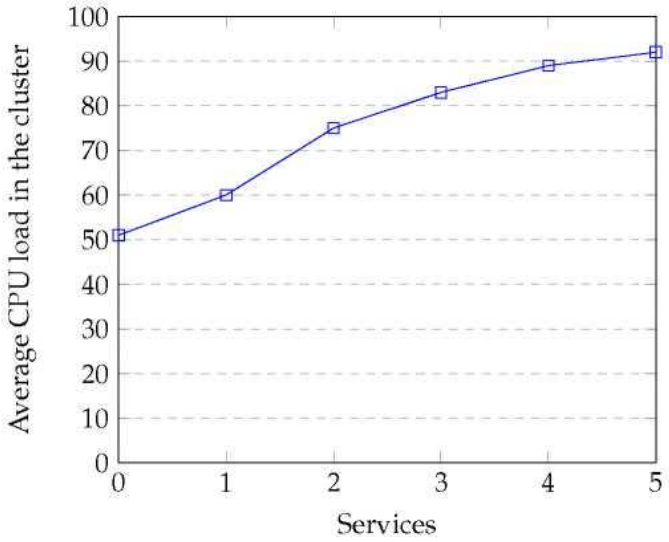


Рисунок 3.7 – Середнє навантаження на ЦП в кластері при введенні послуг

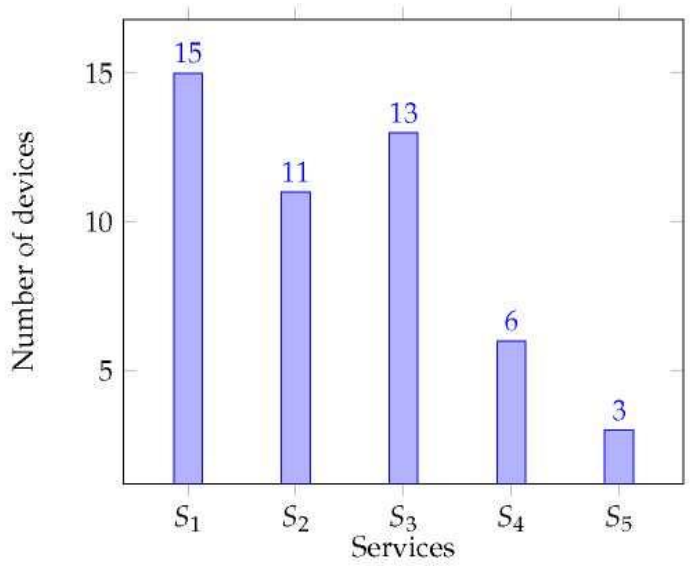


Рисунок 3.8 – Кількість пристроїв, що беруть участь у підкластерах

Слід зауважити, що тут не включені деталі споживання пам’яті, але вони дотримуються подібної моделі. Можна зробити висновок, що в усіх сценаріях існує певний ступінь оптимізації, досягнутий за рахунок використання резервних потужностей, які інакше не використовуються. Для дуже великих кластерів або невеликих проблем може бути цікавим обмеження кількості пристроїв, які беруть участь, шляхом упорядкування певної кількості за потужністю та використання лише достатньої кількості пристроїв.

ВИСНОВКИ

У цій роботі представлено підхід до збору обчислювальної потужності з різних пристроїв IoMT для надійної обробки даних мультимедійних програм. Було створено структуру, яка дозволяє динамічно формувати коаліції пристроїв, які використовують свої резервні ресурси в спільних зусиллях, щоб надавати послуги заданого рівня якості. Це означає, що пристрої готові об’єднати свої зусилля з іншими без шкоди для своїх початкових функціональних можливостей.

Завдяки застосуванню методів резервування ресурсів і гнучкості Elixir, вдалося створити структуру для досягнення заздалегідь визначеного результату. Інфраструктура повністю настроюється, а параметри QoS можна легко додавати або видаляти, враховуючи їх відповідність сценарію застосування. Накладні витрати, додані цією структурою, на нашу думку, низькі, а контрапунктом є багатообіцяюче збільшення обчислювальної потужності.

У майбутньому можна адаптувати потокові алгоритми для використання кластера IoMT, який розроблено прозорим і ефективним способом, і вивчати використання функцій апаратного прискорення, а не виключно потужність, яку забезпечує процесор.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Yusuf Perwej, Mahmoud Ahmed AbouGhaly, Bedine Kerim and Hani Ali Mahmoud Harb. “An Extended Review on Internet of Things (IoT) and its Promising Applications”, f Communications on Applied Electronics (CAE), New York, USA, Volume 9, Number 26, Pages 8 - 22, February 2019, DOI: 10.5120/cae2019652812

2. E. Park, Y. Cho, J. Han, and S. J. Kwon, "Comprehensive approaches to user acceptance of Internet of Things in a smart home environment," IEEE Internet Things J., vol. 4, no. 6, pp. 2342 - 2350, Dec. 2017

3. L. Atzori, A. Iera, and G. Morabito, “The Internet of Things: A survey", Comput. Netw., vol. 54, no. 15, pp. 2787 - 2805, 2010

4. A. Floris and L. Atzori, "Managing the quality of experience in the multimedia Internet of Things: A layered-based approach", Sensors, vol. 16, no. 12, pp. 2057, Dec. 2016

5. S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: Vision and challenges," Ad Hoc Netw., vol. 33, pp. 87_111, Oct. 2015

6. P. Hu, H. Ning, L. Chen and M. Daneshmand, "An open Internet of Things system architecture based on software-defined device", IEEE Internet Things J., vol. 6, no. 2, pp. 2583-2592, Apr. 2019

7. N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and robust digital image watermarking using coefficient differencing and chaotic encryption", IEEE Access, vol. 6, pp. 19876-19897, 2018

8. W. Zhu, P. Cui, Z. Wang, G. Hua, "Multimedia big data computing", IEEE Multi.Mag., vol. 22, no. 3, pp. 96-103, 2015

9. Alessandro Floris, Luigi Atzori, Quality of experience in the multimedia internet of things: Definition and practical use-cases, Communication Workshop (ICCW), IEEE International Conference on, IEEE, pp. 1747-1752, 2015

10. Aslam, A.; Curry, E. Towards a Generalized Approach for Deep Neural Network Based Event Processing for the Internet of Multimedia Things. IEEE Access, 2018

11. Qadri, Y.A.; Nauman, A.; Zikria, Y.B.; Vasilakos, A.V.; Kim, S.W. “The Future of Healthcare Internet of Things: A Survey of Emerging Technologies” IEEE Commun. Surv. Tutor, 2020

12. A. Rego, A. Canovas, J. M. Jimenez, and J. Lloret, "An intelligent system for video surveillance in loT environments," IEEE Access, vol. 6, pp. 31580-31598, 2018

13. Y. Kaeri, C. Moulin, K. Sugawara, and Y. Manabe, "Agent-based system architecture supporting remote collaboration via an Internet of Multimedia Things approach," IEEE Access, vol. 6, pp. 17067_17079, 2018

14. M. A. Rahman, M. S. Hossain, E. Hassanain, and G. Muhammad, "Semantic multimedia fog computing and IoT environment: Sustainability perspective," IEEE Commun. Mag., vol. 56, no. 5, pp. 80_87, May 2018

15. K. P. Seng and L.-M. Ang, "A big data layered architecture and functional units for the multimedia Internet of Things," IEEE Trans. Multi-Scale Comput. Syst., vol. 4, no. 4, pp. 500_512, Oct. 2018

16. L. Zhou and H.-C. Chao, "Multimedia traf_c security architecture for the Internet of Things," IEEE Netw., vol. 25, no. 3, pp. 35_40, May 2011

17. Hamidouche, R.; Aliouat, Z.; Gueroui, A.M.; Ari, A.A.A.; Louail, L. Classical and bio-inspired mobility in sensor networks for IoT applications. J. Netw. Comput. Appl., 121, pp. 70-88, 2018

18. F. Al-Turjman and A. Radwan, "Data delivery in wireless multimedia sensor networks: Challenging and defying in the IoT era", IEEE Wireless Commun., vol. 24, no. 5, pp. 126-131, Oct. 2017

19. K. S. Dar, A. Taherkordi and F. Eliassen, "Enhancing Dependability of Cloud-Based IoT Services through Virtualization", 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 106-116, 2016

20. Wenwu Zhu, Chong Luo, Jianfeng Wang, Shipeng Li, Multimedia cloud computing, IEEE Signal Process. Mag. 28 (3) (2011) 59-69

21. Xi Lin, Jianhua Li, Jun Wu, Haoran Liang, and Wu Yang,“ Making knowledge tradable in edge AI enabled IoT: A consortium blockchain-based efficient and incentive approach”, IEEE Trans. Industr. Info. No. 15, vol. 12, pp. 6367-6378, 2019

22. Z. Huang, C. Mei, L. E. Li, T.Woo, "CloudStream: Delivering highquality streaming videos through a cloud-based SVC proxy," in Proc. IEEE INFOCOM, Apr., pp. 201-205, 2011

23. Arkady Zaslavsky, Charith Perera, Dimitrios Georgakopoulos, Sensing as a Service and Big Data,.1301.0159, 2013

24. Q. Zhang, Z. Ji, W. Zhu, and Y.-Q. Zhang, “Power-minimized bit allocation for video communication over wireless channels,” IEEE Trans. Circuits Syst. Video Technol., Vol. 12, No. 6, pp. 398-410, June 2002

25. V. Gazis, “A survey of standards for machine to machine (m2m) and the internet of things (iot),” IEEE Communications Surveys & Tutorials, 2016

26. C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Cloud Computing Date of Publication, vol. 5, no. 2, April- June 2012

27. O Bello, S Zeadally and M Badra, Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT) [M], Elsevier Science Publishers B. V, 2017

28. V. Gazis, “A survey of standards for machine to machine (m2m) and the internet of things (iot),” IEEE Communications Surveys & Tutorials, 2016

29. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems. 2018;82:395-411.

30. Bianchini A, Pellegrini M, Rossi J. Maintenance scheduling optimization for industrial centrifugal pumps. International Journal of System Assurance Engineering and Management. 2019;10(4):848-860.

31. Palattella MR, Dohler M, Grieco A, Rizzo G, Torsner J, Engel T, et al.

Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications. 2016;34(3):510-527.

32. Xing L. Reliability in Internet of Things: Current status and future perspectives. IEEE Internet of Things Journal. 2020;7(8):6704-6721.

33. Bagchi S, Abdelzaher TF, Govindan R, Shenoy P, Atrey A, Ghosh P, et al. New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges. IEEE Internet of Things Journal. 2020;7(12):11330-11346.

34. Ahmad M. November. Reliability models for the internet of things: A paradigm shift. In 2014 IEEE International Symposium on Software Reliability Engineering Workshops. IEEE; c2014. p. 52-59.

35. Kamyod C. End-to-end reliability analysis of an IoT based smart agriculture. In 2018 International Conference on Digital Arts, Media and Technology (ICDAMT); c2018. p. 258- 261. IEEE.

36. Li S, Huang J. GSPN-based reliability-aware performance evaluation of IoT services. In 2017 IEEE International Conference on Services Computing (SCC)l; c2017. p. 483-486. IEEE.

37. Sha K, Wei W, Yang TA, Wang Z, Shi W. On security challenges and open issues in Internet of Things. Future Generation Computer Systems. 2018;83:326-337.

38. Goel S, Hong Y. Security challenges in smart grid implementation. In Smart grid security. Springer, London; c2015. p. 1-39.

39. McDaniel P, McLaughlin S. Security and privacy challenges in the smart grid. IEEE Security & Privacy. 2009;7(3):75-77

40. Ghansah I. Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks: Interim Project Report. California Energy Commission; c2012.

41. Pradhan P, Nagananda K, Venkitasubramaniam P, Kishore S, Blum RS. GPS spoofing attack characterization and detection in smart grids. In 2016 IEEE Conference on Communications and Network Security (CNS); c2016. p. 391-395. IEEE.

42. Risbud P, Gatsis N, Taha A. Vulnerability analysis of smart grids to GPS

spoofing. IEEE Transactions on Smart Grid. 2018;10(4):3535-3548.

43. Gao YL, An XH, Liu JM. A particle swarm optimization algorithm with logarithm decreasing inertia weight and chaos mutation. In 2008 international conference on computational intelligence and security. 2008;1:61-65. IEEE.

44. Tran TT, Shin OS, Lee JH. Detection of replay attacks in smart grid systems. In 2013 International Conference on Computing, Management and Telecommunications (ComManTel); c2013. p. 298-302. IEEE.

45. Yi P, Zhu T, Zhang Q, Wu Y, Li J. A denial of service attack in advanced metering infrastructure network. In 2014 IEEE International Conference on Communications (ICC); c2014. p. 1029-1034. IEEE.

46. Bekara C. Security issues and challenges for the IoT- based smart grid. Procedia Computer Science. 2014;34:532-537.

47. Guo Y, Ten CW, Hu S, Weaver WW. Modeling distributed denial of service attack in advanced metering infrastructure. In 2015 IEEE power & energy society innovative smart grid technologies conference (ISGT); c2015. p. 1-5. IEEE.

48. Dovom EM, Azmoodeh A, Dehghantanha A, Newton DE, Parizi RM, Karimipour H. Fuzzy pattern tree for edge malware detection and categorization in IoT. Journal of Systems Architecture. 2019;97:1-7.

49. Eder-Neuhauser P, Zseby T, Fabini J. Malware propagation in smart grid monocultures. e & I Elektrotechnik und Informationstechnik. 2018;135(3):264-269.

50. Торба А.А., Павлов О.С., Старов О.Є. Оптимізація продуктивності мережі на основі засобів машинного навчання // «Системи управління навігації та зв’язку», – Випуск 2 (76), – Полтава, Національний університет “Полтавська політехніка імені Юрія Кондратюка”, – 2024. – С. 107-111.