ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА СИСТЕМНОГО АНАЛІЗУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Аналіз використання технологій інтернету речей у виробничому секторі»

на здобуття освітнього ступеня бакалавра
зі спеціальності 124 Системний аналіз
(код, найменування спеціальності)
освітньо-професійної програми Системний аналіз
(назва)

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

_____ *Костянтин КОЛОСОВ*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувачка вищої освіти гр. САД-41
Костянтин КОЛОСОВ
Ім'я, ПРІЗВИЩЕ
Керівник: Олександр КОРЕЦЬКИЙ
ст викладач каф. СА. Ім'я, ПРІЗВИЩЕ

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

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут телекомунікацій

Кафедра Системного аналізу

Ступінь вищої освіти бакалавр

Спеціальність 124 Системний аналіз

Освітньо-професійна програма Системний аналіз

ЗАТВЕРДЖУЮ
Завідувач кафедрою Ровіл НАФЄЄВ
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Колосов Костянтин Анатолійович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Аналіз використання технологій інтернету речей у виробничому секторі
керівник кваліфікаційної роботи ст. викладач каф. СА Корецький Олександр Валерійович
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «__ _____» _____2024р. № _____
2. Строк подання кваліфікаційної роботи «_____» _____ 2024р.
3. Вихідні дані до кваліфікаційної роботи: Інформаційно-аналітичний метод, використання орієнтовних протоколів в мережі інтернету речей, архітектура та методи побудови IoT.

Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз технології інтернету речей
2. Аналіз моделей інтернету речей
3. Методи організації інфраструктури інтернету речей
4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання «_____» _____ 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних		Виконано
2	Обробка матеріалу		Виконано
3	Аналіз технології інтернету речей		Виконано
4	Аналіз моделей інтернету речей		Виконано
5	Методи організації інфраструктури інтернету речей		Виконано
6	Висновки за результатами аналізу		Виконано
7	Розробка презентації		Виконано
8	Передзахист		Виконано
9	Здача в деканат		Виконано

Здобувачка вищої освіти _____ Костянтин КОЛОСОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Олександр КОРЕЦЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут телекомунікацій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувачка Колосов К.А. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 124 Системний аналіз
(код, найменування спеціальності)
освітньо-професійної програми Системний аналіз
(назва)
на тему: «Аналіз використання технологій інтернету речей у виробничому секторі».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка Колосов Костянтин Анатолійович під час написання кваліфікаційної роботи показала гарну теоретичну підготовку, володіння необхідними знаннями з системного аналізу, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які доручались керівником, проявила ініціативність, сумлінність та хист до інженерної роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувачки Колосов К.А. на оцінку «відмінно» та присвоїти їй кваліфікацію **«***Бакалавр з системного аналізу».*

Керівник кваліфікаційної роботи _____ Олександр КОРЕЦЬКИЙ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____»_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Колосов К.А. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою Системний аналіз _____ Ровіл НАФЄЄВ
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачка вищої освіти Колосов Костянтин Анатолійович
(прізвище, ім'я, по батькові)
на тему «Аналіз використання технологій інтернету речей у виробничому секторі»

Актуальність.

IoT створить величезну мережу мільярдів або трильйонів "Речей", що спілкуються між собою. IoT не є диверсійною революцією над існуючими технологіями, вона є всеосяжним використання існуючих технологій, і це створює нові режими спілкування. IoT поєднує віртуальний світ і фізичний світ, приводячи різні концепції і технічні компоненти разом: всепроникні мережі, мініатюризація пристроїв, мобільний зв'язок та нова екосистема. У IoT додатки, послуги, компоненти проміжного програмного забезпечення, мережі, а кінцеві вузли будуть структурно організовані та використовуватися зовсім по-новому. IoT пропонує засоби для вивчення складних процесів.

Позитивні сторони.

1. Проаналізовано мережі IoT та методи організації інфраструктури. Представлено можливі методи збору та збереження даних в пристроях IoT, розглянуто такі підходи як, платформовий, цільовий та стратегії, що мотивовані точністю, критичністю часу, потребами в енергії, проблемами конфіденційності.
2. Представлено організацію інфраструктури з семи ключових компонентів. Описана передача та зберігання даних у динамічній мережі, проблематика створення мережі IoT.

Недоліки.

1. В роботі мають місце деякі неточності в перекладі технічних термінів.
2. В текстовій частині пояснювальної записки дипломної роботи надано не всі посилання на джерела інформації.

Висновок: *кваліфікаційна бакалаврська робота заслуговує оцінку "відмінно", а здобувач* Колосов Костянтин Анатолійович *заслуговує присвоєння кваліфікації: «Бакалавр з системного аналізу».*

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

РЕФЕРАТ

Робота містить 80 сторінок, 16 рисунків. Було використано 23 джерела.

Актуальність роботи: Технічна революція, яка з кожним днем еволюціонує та стрімкий розвиток мобільних технологій сприяє розвитку Інтернету Речей. Зростання кількості фізичних пристроїв, що взаємодіють з інтернетом, підштовхує до реалізації Інтернету Речей. На сьогодні застосування систем IoT, можна знайти в безлічі галузях промисловості, в тому числі в телеукомунікаціях. Пристрої, що подключені до Інтернету, є основою для розвитку проектування розумних міст. Застосування систем Інтернету Речей, звісно має переваги, але і недоліки у вигляді загрози їх неправомірного використання, такі як вторгнення у приватне життя людини, загроза збору та використання персональних даних в особистих цілях, кібернетична загроза, тощо.

Метою роботи є удосконалення методів організації інфраструктури IoT на основі запропонованої архітектури

Задачі дослідження:

- провести аналіз технологій IoT
- провести аналіз сучасного розвитку IoT
- проаналізувати існуючі моделі IoT
- удосконалити методи організації інфраструктури IoT на основі запропонованої архітектури.

Об’єкт дослідження: методи організації інфраструктури Інтернету Речей

Предмет дослідження: протоколи методів збору та передачі інформації.

Ключові слова: Інтернет Речей, Internet of Things, архітектура IoT, MQTT, XMPP.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВЧ	Високочастотний
ІСУ	Індустріальна Система Управління
ІТ	Інформаційні технології
МСЕ	Міжнародний Союз Електрозв'язку
ОТ	Операційні Технології
API	(Application Programming Interface) – Інтерфейс Прикладного Програмування
DDS	(Data Distribution Service) – Служба Розподілу Даних
ERP	(Enterprise Resource Planning) – Планування Песурсів Підприємства
GPS	(Global Positioning System) – Глобальна Система Позиціонування
HTTPS	(HyperText Transfer Protocol Secure) – Протокол Передачі Гіпертексту Захищений
IIC	(Industrial Internet Consortium) – Індустріальний Інтернет Консорціум
IIoT	(Industrial Internet of Things) – Індустріальний Інтернет Речей
IoT	(Internet of Things) – Інтернет Речей
IP	(Internet Protocol) – Інтернет Протокол
ITU	(International Telecommunication Union) – Міжнародний Союз Телекомунікацій
JSON	(JavaScript Object Notation) – Позначення Об'єкта JavaScript

ВСТУП

Інтернет речей (IoT) став важливою технологією сучасності, що використовує програми в багатьох сферах. IoT сягає корінням у кілька попередніх технологій: поширену інформацію системи, сенсорні мережі та вбудовані обчислення. Термін IoT система більш точно описує використання цієї технології, ніж Інтернет речей. Більшість пристроїв IoT з'єднані між собою, щоб утворити цільові системи; їх не часто використовують як пристрої загального доступу у всесвітній мережі. IoT виходить за рамки поширених обчислювальних та інформаційних систем, які зосереджуються на даних. Розумні холодильники - один із прикладів поширених обчислень пристроїв. Деякі продукти включали вбудовані ПК і дозволяли користувачам вводити інформацію про вміст свого холодильника для планування меню. Концептуальні пристрої автоматично сканує вміст холодильника, щоб подбати про введення даних. Випадки використання, передбачені для цих холодильників, не настільки віддалені від планування меню програми для окремих персональних комп’ютерів.

Дослідження сенсорної мережі охопило цілий ряд конфігурацій. Багато з них були призначений для збору даних при дуже низьких швидкостях передачі даних. Тоді зібрані дані будуть відправлятися на сервери для обробки. Традиційні дослідження сенсорних мереж не наголошували на обробці даних у мережі.

Вбудовані обчислення зосереджені або на окремих пристроях, або на тісно пов'язаних мережах, таких як ті, що використовуються в транспортних засобах. Споживча електроніка та кіберфізичні системи були двома основними областями застосування вбудованих обчислень; обидва наголошували на спроектованих системах з чітко визначеними цілями.

З огляду на широкий спектр прихильників технологій IoT, немає єдиного чіткого визначення терміну їх появи всюди. Ми можемо виділити кілька можливостей:

• Фізичні пристрої з підтримкою Інтернету, хоча багато пристроїв не використовують Інтернет Протокол

• М'які сенсорні мережі в режимі реального часу

• Динамічні та розвиваються мережі вбудованих обчислювальних пристроїв

По-перше, система IoT розрахована, скоріше, на один додаток або набір додатків ніж агломерація пристроїв з підтримкою Інтернету. По-друге, система IoT враховує динаміку фізичних систем. Система IoT може складатися насамперед з датчиків; в деяких випадках вона може включати значну кількість виконавчих механізмів. В обох випадках метою є обробка сигналів та даних часових рядів.

Розвиток мікроелектромеханічних датчиків (MEMS) дав поштовх у розвитку Інтернету речей. Вбудовані акселерометри, гіроскопи, хімічні датчики та інші форми датчиків зараз широко доступні. Низька вартість і енергоспоживання цих датчиків дає можливість нових застосувань значно перевершуючи традиційне лабораторне або промислове вимірювальне обладнання. Ці сенсорні програми підштовхують системи IoT до обробки сигналів.

РОЗДІЛ 1
АНАЛІЗ ТЕХНОЛОГІЇ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Сучасний стан IoT

IoT забезпечується дуже низькою вартістю цифрової та аналогової електроніки VLSI. Як ми побачимо, вузли IoT не покладаються на найсучасніші виробничі процеси VLSI. Насправді вони недорогі, оскільки вони можуть скористатися старшими виробничими лініями; нижча кількість пристроїв, доступна в цих старих технологіях є більш ніж достатніми для багатьох систем IoT.

Системи IoT повинні споживати дуже мало енергії. Енергоспоживання є ключовим фактором у загальній вартості володіння системами IoT. Досягнення необхідних рівнів потужності вимагає пильної уваги до проектування обладнання, програмного забезпечення та застосування алгоритмів.

Безпека - це ключова вимоги до проектування та експлуатації систем IoT. Злиття обчислювальної та фізичної систем вимагає об’єднання раніше відокремлених завдань безпечного проектування фізичної системи та проектування захищеної комп’ютерної системи.

IoT створить величезну мережу мільярдів або трильйонів “Речей”, що спілкуються між собою. IoT не є диверсійною революцією над існуючими технологіями, вона є всеосяжним використання існуючих технологій, і це створює нові режими спілкування. IoT поєднує віртуальний світ і фізичний світ, приводячи різні концепції і технічні компоненти разом: всепроникні мережі, мініатюризація пристроїв, мобільний зв’язок та нова екосистема. У IoT додатки, послуги, компоненти проміжного програмного забезпечення, мережі, а кінцеві вузли будуть структурно організовані та використовуватися зовсім по-новому. IoT пропонує засоби для вивчення складних процесів та стосунків. IoT передбачає симбіотичну взаємодію між реальним / фізичним та цифровим / віртуальним світами: фізична організація має цифрові аналоги та віртуальне

представництво; речі усвідомлюють контекст, і вони можуть відчувати, спілкуватися, взаємодіяти та обмінюватися даними, інформацією та знаннями.

Нові можливості будуть відповідати вимогам бізнесу, і нові послуги будуть створюватися на основі даних фізичного світу в режимі реального часу. Все, що стосується фізичного або віртуального світу, може бути підключеним IoT. Зв'язок між речами повинен бути доступним для всіх з низькою вартістю і може не належати приватним особам. Для IoT, інтелектуальне навчання, швидке розгортання, найкраще розуміння та тлумачення інформації, проти шахрайства та зловмисних атак, і захист конфіденційності є надзвичайно важливими вимоги.

IoT можна розглядати як продовження існуючої взаємодії між людьми та програмами через новий вимір “Речей” для спілкування та інтеграції. Процес розробки IoT є складним масштабним технологічним інноваційним процесом. IoT розвивається з вертикальним нанесенням на полімерне нанесення. На ранній стадії розгортання IoT основна стратегія розвитку - це керування додатками, що визначають домени. Додаткова програма може бути системою управління виробництвом зі своїми галузевими характеристиками. Додаток може надавати різні послуги з управління підприємством інтегровані з галузевим виробництвом та бізнес-процесами.

Полімерні додатки - це міжгалузеві додатки на платформах публічної інформаційної служби. Ці програми підтримують як домашніх, так і промислових користувачів. Додаток надається та просувається операторами зв'язку та постачальниками рішень з великими масштабами. Наприклад, транспортний засіб інтегрується з сенсорними мережами, глобальною системою позиціонування (GPS) та технологіями радіозв’язку можуть забезпечити всебічне виявлення, навігацію, розваги та інші інформаційні послуги. Зберігаючи таку інформацію через платформи комунального обслуговування, споживачів, оригінальному обладнанні виробників (OEM), постачальники технічного обслуговування та транспортних засобів

управлінських установ можуть ділитися цією інформацією та ділитися з ними послугами з вдосконалення транспортного засобу, конструкції компонентів та процесом виготовлення протягом життєвого циклу автоматичного управління.

1.2 Аналіз можливостей IoT

В даному розділі розглядаються програми IoT, які мають наступні можливості.

1) Зондування місцезнаходження та обмін інформацією про місцезнаходження: IoT система може збирати інформацію про місцезнаходження терміналів IoT і кінцеві вузли, а потім надавати послуги на основі зібраної інформації про місцезнаходження. Інформація про місцезнаходження включає інформацію про географічне положення, отримане від GPS, CellID, RFID тощо, а також абсолютну або відносну інформація про місцезнаходження між речами. Більш типові програми IoT включають принаймні наступне.

a) Відстеження мобільних активів: Ця програма може відстежувати і слідкувати за станом товару за допомогою пристрою, що контролює позицію, та функції зв'язку, встановленої на товар.

b) Управління флотом: ясла флоту можуть скласти графік транспортних засобів та водіїв на основі ділових вимог та зібраної інформації про положення в реальному часі транспортними засобами.

в) Система дорожньої інформації: Ця програма може отримати інформацію про дорожній рух, такі як умови дорожнього руху та перевантажені місця, відстежуючи інформацію про місцезнаходження великої кількості транспортних засобів. Таким чином, система допомагає водієві вибрати найбільш ефективний маршрут.

2) Зондування навколишнього середовища: система IoT може збирати і обробляти всі види параметрів фізичного або хімічного середовища через

локально або широко розгорнуті термінали. Типова екологічна інформація включає температуру, вологість, шум, видимість, інтенсивність світла, спектр, випромінювання, забруднення (CO, CO2 та ін.), зображення та показники тіла. Типові програми включають принаймні наступне.

a) Аналіз довкілля: системи IoT аналізують екологічний світ, такий як ліс та льодовик, моніторинг катастрофи, такі як вулкани та сейсмічні спостереження та заводський моніторинг. Всі вони мають автоматичну сигналізацію системи, що використовують екологічні параметри, зібрані у велику кількість датчиків.

b) Віддалений медичний моніторинг: IoT може аналізувати повторювані дані про показники, зібрані з пристрою, розміщеного на тілі пацієнтів та надавати користувачам тенденції щодо здоров'я та медичні поради.

3) Дистанційне управління: системи IoT можуть керувати IoT термінали та виконувати функції на основі команд додатків у поєднанні з інформацією, зібраною з речей та вимоги до обслуговування.

a) Контроль приладів: Люди можуть дистанційно контролювати робочий стан приладів за допомогою системи IoT.

b) Відновлення після катастрофи: користувачі можуть віддалено запускати катастрофи очисних споруд для мінімізації збитків, спричинених катастрофами, згідно з моніторингом, згаданим раніше.

4) Спеціальна мережа: система IoT повинна мати швидко самоорганізовану мережеву здатність і може взаємодіяти з мережевим/сервісним рівнем для надання супутніх послуг [1]. В транспортної мережі, для передачі даних, мережі між транспортними засобами та/або дорожньою інфраструктурою може бути швидко самоорганізована.

5) Безпечне спілкування: система IoT може надалі встановлюватись захищений канал передачі даних між додатком

Системи IoT корисні в широкому діапазоні програм:

• Промислові системи використовують датчики для контролю як самих промислових процесів - якості продукції, так і стану обладнання. Зростаюча кількість електродвигунів, наприклад, включає датчики, які збирають дані, що звикли передбачити майбутні несправності двигуна.

• Розумні будівлі використовують датчики для визначення місцезнаходження людей, а також штату будівлі. Ці дані можуть бути використані для управління системами опалення / вентиляції / кондиціонування та освітлення для зменшення експлуатаційних витрат. Розумні будівлі та конструкції також використовують датчики для моніторингу структурного стану.

• Розумні міста використовують датчики для контролю пішохідного та транспортного руху та можуть інтегрувати дані з розумних будівель.

• Транспортні засоби використовують мережеві датчики для контролю стану автомобіля та забезпечують покращення динаміки, зниження споживання палива та зниження викидів.

• Медичні системи з'єднують широкий спектр датчиків спостереження за пацієнтами, які можуть знаходитися вдома, в аварійних автомобілях, кабінеті лікаря або лікарні.

Розглянувши існуючі програми IoT можемо виділити основні вимоги до системи IoT.

Сенсорна мережа. Система може діяти суворо як система збору даних для набору датчики.

Система оповіщення. Дані датчиків можуть збиратися та аналізуватися. Сповіщення генеруються, коли дотримуються певні критерії.

Система аналізу. Дані датчиків збираються та аналізуються, але в цьому випадку аналіз триває. Звіти про аналітичні результати можуть створюватися періодично - щогодини, щодня тощо - або можуть постійно оновлюватися.

Реактивна система. Аналіз даних датчиків може спричинити спрацьовування приводів. Ми залишити термін реактивним для систем, які не застосовують типових законів управління.

Система управління. Дані датчика подаються в алгоритми управління, які генерують вихідні дані для виконавчі механізми. Ми можемо визначити клас нефункціональних вимог, які застосовуються до багатьох IoT системи. Нефункціональні вимоги до системи накладають нефункціональні вимоги до компонентів. Затримка події Затримка від захоплення події до місця призначення не може бути важливий для пакетних програм, але стає важливим для Інтернет-аналізу.

Пропускна здатність події. Швидкість, з якою події можна фіксувати, транспортувати та обробляти, залежить від пропускної здатності вузлів, пропускної здатності мережі та хмари пропускна здатність.

Частота втрат події та ємність буфера. За відсутності суворої верхньої межі події виробничих показників, навколишнє середовище може спричинити більше подій в інтервалі, ніж система може виробляти. Частота втрат подій фіксує бажану можливість, поки буфер потужність - це більш прагматична вимога, яка може бути безпосередньо пов’язана з компонентом можливості.

Час затримки та пропускна спроможність. Зрештою, події будуть оброблятися службами. Ми також можемо вказати затримку та пропускну здатність послуг.

Надійність та доступність. Оскільки системи IoT розповсюджуються, надійність стає більше ймовірно, буде вказано для частин мережі, а не для надійності всієї мережі система. Доступність зазвичай використовується для опису розподілених систем.

Термін служби. Зазвичай IoT системи мають довший термін служби, ніж очікується для систем ПК. Термін служби системи або її підмножини може становити значно довший, ніж у компонента, особливо якщо система використовує надлишкові датчики та інші компоненти.

Ключовим аспектом IoT є дискретизація, керована подіями або аперіодична. Традиційний цифровий сигнал обробка та контроль припускають періодичні вибірки, що приводить до даних про часові ряди. Однак часові ряди споживають занадто багато енергії у вузлах і занадто велику пропускну здатність мережі. Не всі додатки піддаються аперіодичним даним придбання.

Обмеження щодо потужності та пропускної здатності також заохочують розподілені обчислення датчик подій. Порівняно невеликі процесори можуть виконувати корисну обробку для багатьох потоків даних. Розпізнавання цікавих подій за допомогою обробки країв зменшує кількість споживаної пропускної здатності мережі; це також зменшує споживання енергії з бездротовий зв'язок вимагає великої кількості енергії. Хмарні обчислення- (централізовані сервери) або обчислення туману (сервери ближче до краю) можуть бути використані виконати подальшу обробку цих вилучених подій.

Бездротові мережі є невід'ємною частиною систем IoT. Підключення до бездротової мережі спрощує встановлення та експлуатацію бездротових мереж.

Однак бездротові мережі створюють деякі важливі проблеми та обмеження. Радіозв'язок вимагає більше енергії, ніж дротовий. Деякі бездротові мережі, що використовуються в сучасних пристроях IoT, були розроблені для інших

цілі, такі як телефонія та мультимедіа. Як результат, вони не оптимізовані для

керування подіями та споживання значної кількості енергії в протоколі зв'язку.

Однією з іроній IoT є те, що багато крайових пристроїв та їх бездротових мереж не працюватимуть з Інтернет-протоколом (IP). IP вводить значні накладні витрати з додатковим рівнем пакетування та пов'язаної з ним обробки. Багато пристроїв IoT уникають IP та покладаються на висхідні вузли, щоб забезпечити їм присутність в Інтернеті. Мережами IoT, як правило, керують

некомп'ютерні експерти. IoT бездротові мережі повинен бути простим у розгортанні та відносно самокерованим.

Характеристики керованих подіями систем дозволяють вузлам IoT бути відносно простими. Реалії роботи з низьким енергоспоживанням також штовхають вузли на відносно низький рівень інтеграція.

Технологія VLSI та закон Мура є ключовими факторами зростання систем IoT оскільки вони дозволяють виготовляти вузли надзвичайно дешево. Дуже маленькі мікросхеми можуть забезпечити достатньо обчислень, пам'яті та мереж для корисної функції вузла IoT. На відміну від традиційних мікропроцесорних та споживчих електронних додатків, де області мікросхем коливаються навколо або навіть вище, мікросхеми площею декілька квадратних міліметрів досить великі для багатьох пристроїв IoT-вузлів.

Безпека нарешті визнана важливою вимогою для всіх типів комп’ютерних систем, включаючи системи IoT. Однак у багатьох системах IoT безпека набагато менша, ніж у типових системах Windows / Mac / Linux. Проблеми безпеки IoT виникають з ряду причин: неадекватні функції безпеки в апаратному забезпеченні, погано розроблені програмне забезпечення з низкою вразливостей, паролів за замовчуванням та інших засобів безпеки помилки проектування. Небезпечні вузли IoT створюють проблеми для безпеки всієї системи IoT. Оскільки вузли, як правило, мають термін служби кілька років, велика встановлена база незахищені пристрої ще деякий час створюватимуть проблеми із безпекою. Небезпечні системи IoT також створюють проблеми з безпекою для решти Інтернету. IoT-пристроїв багато; небезпечні вузли IoT ідеально підходять для відмови в обслуговуванні атаки інтернет-інфраструктури.

Конфіденційність пов'язана з безпекою, але вимагає певних заходів щодо програми, мережі та рівні пристроїв. Дані користувачів не тільки повинні бути захищені від прямого викрадення, але мережа повинна бути спроектована

таким чином, щоб менш приватні дані не давали змогу використовувати більше приватних даних.

1.3 Перспективи та проблематика IoT

Тенденції IoT мають бути уніфікованими, цілісними та поширеними. Розгортання масштабних послуг повинно бути оформлено в рамках низки стандартів. Однак IoT залучає багатьох виробників, охоплює різні галузі, і він сильно відрізняється за сценаріями застосування та вимогами користувачів, що, відповідно, впливає на масштабне комерційне розгортання супутніх послуг. Розвиток IoT - це покроковий процес. Існує ще багато проблем, які потрібно вирішити, такі як вузли низької потужності та обчислювальна техніка, низька вартість та низька затримка зв'язку, технології ідентифікації та позиціонування, самоорганізування системних технологій та розподіленого інтелекту.

IoT надає багато нових можливостей для галузі та кінцевих користувачів у багатьох сферах застосування. В даний час, однак, самому IoT бракує теорії, архітектури технологій та стандартів, які б інтегрували віртуальний світ та реальний фізичний світ в єдину структуру [2]. Таким чином, перелічено наступні ключові проблеми.

1) Архітектурний виклик: IoT охоплює надзвичайно широкий спектр технологій. IoT передбачає збільшення кількості розумних взаємопов’язаних пристроїв та датчиків (наприклад, камер, біометричних, фізичних та хімічних датчиків), які часто не нав'язливі, прозорі та невидимі. Оскільки, як очікується, зв’язок між цими пристроями відбуватиметься будь-коли та в будь-якому місці для будь-яких супутніх служб, як правило, ці зв’язки здійснюються бездротовим, автономним та спеціальним способом. Крім того, послуги стають набагато мобільнішими, децентралізованими та складними. Таким чином, в IoT інтеграція даних у різних середовищах є жорсткою і буде підтримуватися модульними взаємодіючими компонентами. Інфраструктурні рішення

потребуватимуть систем, що поєднують обсяги даних з різних джерел та визначають відповідні особливості, інтерпретують дані та показати свої стосунки, порівняти дані з історично корисною інформацією та підтримати прийняття рішень. Отже, одна посилальна архітектура не може бути планом для всіх програм.

Неоднорідні еталонні архітектури повинні співіснувати в Інтернеті речей. Архітектури повинні бути відкритими, і, дотримуючись стандартів, вони не повинні обмежувати користувачів у використанні фіксованих наскрізних рішень. Архітектури IoT повинні бути гнучкими, щоб задовольнити такі випадки, як ідентифікація (RFID, мітки), інтелектуальні пристрої та розумні об'єкти (апаратні та програмні рішення).

2) Технічний виклик: технологія IoT може бути складною з різних причин. По-перше, у існуючих мережевих технологіях та додатках існують застарілі різнорідні архітектури, наприклад, різні програми та середовища потребують різних мережевих технологій, а діапазони, а також інші характеристики стільникової, бездротової локальної мережі та технології RFID значно відрізняються від кожної інші [3]. По друге, комунікаційні технології, включаючи системи фіксованого та мобільного зв'язку, лінії електропередачі, бездротовий зв'язок та технології бездротового зв'язку малого діапазону, як для стаціонарних, так і для мобільних пристроїв, як простих, так і складних, повинні мати низьку вартість і забезпечувати надійне підключення. Нарешті, існують тисячі різних додатків; цілком природно мати різні вимоги щодо того, яким сторонам потрібно спілкуватися між собою, які рішення безпеки є доречними тощо. Підсумовуючи, складність та альтернативні технології можуть створити проблеми; непотрібна конкуренція та бар'єри для розгортання на ринках також можуть створювати проблеми; системи та комунікаційні механізми з непотрібними залежностями можуть блокувати міграцію систем IoT на найбільш економічні та ефективні платформи. Все вищезазначене може заблокувати IoT, щоб підключити якомога більше «речей».

3) Апаратний виклик: розумні пристрої з розширеною взаємодією між пристроями призведуть до створення розумних систем з високим ступенем інтелекту. Його автономність дозволяє швидко розгортати програми IoT та створювати нові сервіси. Тому апаратні дослідження зосереджені на розробці бездротових ідентифікованих систем з низьким розміром, низькою вартістю, але достатньою функціональністю. Оскільки пропускна здатність терміналів IoT може варіюватися від kbps до mbps від простого значення до відеопотоку, вимоги до обладнання різняться. Однак дві вимоги, однак, були найважливішими: одна - надзвичайно низьке споживання енергії в режимі сну, а інша - надвисока вартість. Припустимо, що час сну протягом активного часу становить один мільйон, потужність витоку терміналу IoT повинна бути принаймні на мільйон разів менше, ніж активна. Поки що це неможливо, коли термінал IoT сплячий і приймає радіочастотні сигнали. Це буде навіть важко при використанні вдосконаленого КМОП-кремнію з відносно більшою потужністю витоків. Таким чином, апаратне забезпечення та кодова архітектура протоколу для сну стали першим апаратним завданням IoT. Будуть використані мільярди терміналів IoT; вартість терміналу IoT повинна бути надзвичайно низькою.

Однак поки що для IoT не існує дешевого рішення позиціонування, особливо точність позиціонування IoT-термінала короткого діапазону повинна бути високою. Низька активна потужність також є проблемою для недорогих терміналів [4]. Традиційно низька вартість дорівнює меншій продуктивності або більшій затримці процесу. Більша затримка обробки закінчується вищим енергоспоживанням. Оскільки ресурс спектра дуже обмежений в нижній частині діапазону L, IoT може використовувати більш високі ВЧ, такі як смуги частот, що перевищують 5 ГГц. Чим вище ВЧ, тим більше буде споживання енергії від РЧ ПА. Іншим чином, майбутнє IoT, можливо, доведеться використовувати ще не використовувану дуже вузьку смугу спектру між двома використовуваними смугами. Якщо використовувати дуже вузьку смугу з

потужними сусідами, вартість пасивного компонента не буде низькою, і це, безумовно, буде потенційною проблемою в майбутньому.

4) Проблема конфіденційності та безпеки: Порівняно з традиційними мережами, питання безпеки та конфіденційності IoT стають все більш помітними [5]. Багато інформації включає конфіденційність користувачів, тому захист конфіденційності стає важливою проблемою безпеки в Інтернеті речей. Через поєднання речей, послуг та мереж безпека IoT повинна охоплювати більше об’єктів та рівнів управління, ніж традиційна мережева безпека. Існуюча архітектура безпеки розроблена з точки зору людського спілкування, можливо, не підходить і безпосередньо застосовується до системи IoT. Використання існуючих механізмів безпеки заблокує логічні взаємозв'язки між речами в Інтернеті речей. IoT потребує недорогих технічних рішень, орієнтованих на M2M, щоб гарантувати конфіденційність та безпеку. У багатьох випадках використання безпека системи розглядалася як загальна характеристика. Супутні дослідження будуть зосереджені на контролі конфіденційності. Низька вартість, низька затримка та енергоефективні алгоритми криптографії та відповідне гнучке обладнання будуть важливими для датчика або пристрою.

5) Стандартизаційний виклик: стандарти відіграють важливу роль у формуванні IoT. Стандарт має важливе значення, щоб дозволити всім учасникам рівноправний доступ та використання. Розробка та узгодження стандартів та пропозицій сприятимуть ефективному розвитку інфраструктури IoT та додатків, послуг та пристроїв. Загалом стандарти, розроблені співпрацюючими багатосторонніми сторонами, а також інформаційні моделі та протоколи в стандартах повинні бути відкритими. Процес розробки стандартів також повинен бути відкритим для всіх учасників, а отримані стандарти повинні бути загальнодоступними та вільно доступними. У сучасному мережевому світі глобальні стандарти, як правило, актуальніші за будь-які місцеві угоди.

6) Виклик бізнесу: Для зрілої програми її бізнес-модель та сценарій застосування чіткі та легкі для відображення у технічних вимогах. Тож розробникам не потрібно витрачати багато часу на аспекти, пов’язані з бізнесом. Але для IoT у бізнес-моделях та сценаріях застосування занадто багато можливостей та невизначеностей. Таким чином, він неефективний з точки зору узгодження бізнес-технологій, і одне рішення не відповідає можливостям усіх. IoT є складною традиційною бізнес-моделлю. Незважаючи на те, що дрібномасштабні програми були вигідними в деяких галузях, це нестійко, якщо поширити їх на інші галузі. На ранній стадії розвитку IoT слід розглянути бізнес-аспекти, щоб зменшити ризик невдач.

Перспективи IoT. З розвитком та зрілістю розподілених інтелектуальних технологій обробки інформації системи IoT роблять інтелектуальне зондування широко доступним завдяки обміну інформацією та співпраці. Поступове встановлення та вдосконалення системи стандартів неминуче внесе IoT у наше повсякденне життя. IoT створює можливість для веб-сервісів, тим самим посилюючи комерційний та соціальний потенціал майбутнього IoT [6]. Розвиток IoT продовжує йти вперед у масштабі, спільному та інтелектуальному. Заохочувані технологіями, стандартизацією та досвідом застосування, додатки IoT розширять масштаби в різних галузях промисловості, і більше підприємств буде залучено до участі.

1) Взаємодія: Інформаційна сумісність матиме місце між різними речами, різними підприємствами, різними галузями та різними регіонами чи країнами; моделі застосування змінюватимуться із закритих на відкриті, і буде побудована глобалізація системи додатків IoT, що обслуговує різні галузі та галузі. Сумісність є важливою проблемою для перетину шарів фізичного, пристрою, зв'язку (утиліта протоколу та спектра), функції та застосування. Ці рівні традиційно будуються на різних мовах та протоколах. Тому потрібні прозорі мови та протоколи рівня та домену. Потрібен цілісний підхід у

вирішенні та вирішенні питань взаємодії пристроїв та послуг IoT на декількох рівнях.

2) Інтелектуальна система: IoT внесе в наше суспільство цілі ділові та соціальні мережі через швидкі надійні та безпечні мережі. Системний інтелект буде важливим для розвитку IoT, а ключовим моментом буде обізнаність щодо контексту та обмін інформацією між речами. Отже, збільшення та адаптація інтелекту на рівні пристрою буде зосереджена у фокусі досліджень, таких як інтеграція датчиків та виконавчих механізмів, висока ефективність, багатостандартні та адаптивні підсистеми зв'язку та адаптовані антени. Інтелектуальність може бути представлена за допомогою мікроконтролера (MCU) на верхніх шарах. Однак фізичний рівень поки що відставав від необхідного інтелектуального рівня, наприклад, для адаптації пристроїв IoT під різні радіоінфраструктури. Потрібно додатково розвивати чотири частини на фізичному рівні, щоб адаптуватись та / або сформувати інтелектуальний пристрій IoT, який є таким. Програмований процесор базової смуги буде використовуватися для адаптації до різних алгоритмів модуляції, різних алгоритмів виправлення помилок, різної смуги пропускання каналів та різних сценаріїв каналу. Програмне забезпечення контрольованої ВЧ-системи буде важливим для адаптера трансивера до місцевих вимог радіочастоти. Повністю цифровий РЧ-випромінювач буде необхідним пристроєм для споживання менш низької потужності та запропонує програмованість для ПА для адаптації вимог радіопередачі. Нарешті, керовані інтегровані пасивні компоненти стануть важливим клеєм для з'єднання інтелектуальних напівпровідникових компонентів у вузол датчика з низькою вартістю, низькими розмірами та малою потужністю.

3) Енергетична стійкість: У майбутньому енергоефективні та самостійкі системи будуть ключовими питаннями, що сприяють підвищенню рівня IoT. Потрібно розробити способи отримання енергії з навколишнього середовища. Ефективність обробки та зв'язку також повинна бути підвищена за допомогою

нових схем, нових парадигм програмування та подальшого розвитку енергоефективних протоколів та інтелектуальних антен. Розробка нових, ефективних та компактних акумуляторів, паливних елементів, а також нових пристроїв для виробництва енергії, що поєднують методи передачі енергії або збирання енергії, будуть ключовими факторами для впровадження автономних бездротових інтелектуальних систем. Зарядка глобальних терміналів IoT, енергоспоживання глобальних точок доступу та шлюзів IoT, а також енергоспоживання процесів обробки даних IoT в інфраструктурах IoT будуть одними з основних споживачів енергії в майбутньому світі. Механічного збору енергії буде достатньо для мережі тіла як частини IoT.

Висновки

В першому розділі було розглянуто сучасний стан IoT, програми та сфери використання. Проаналізовано можливості IoT, ключові аспекти, та перспективи. Виявлено основні проблеми IoT.

РОЗДІЛ 2

АНАЛІЗ МОДЕЛЕЙ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Орієнтовані протоколи IoT

В даному розділі розглянемо деякі протоколи, що використовуються для обслуговування даних у системах IoT.

Протоколи зв'язку можуть не забезпечувати достатню абстракцію для багатьох додатків. Системи IoT потребують мульти-стрибкового, наскрізного зв'язку. Вони також можуть виявляти складні взаємозв'язки між джерелами даних та раковинами. Протоколи вищого рівня можуть надавати послуги, які більш точно моделюють потреби систем IoT. Враховуючи неоднорідний і довговічний характер більшості систем IoT, часто використовують стандарти, а не власні протоколи. Запропоновано кілька різних протоколів, які в різній мірі використовуються для систем IoT [7]. Користувацький простір ще не сходився до єдиного стандарту для служб зв'язку IoT.

Враховуючи поширеність моделей, орієнтованих на події, в системах IoT, протокол повинен підтримувати спілкування у стилі подій.

Протокол HTTP використовує шаблон проектування запиту / відповіді. Клієнт видає запит на гіпертекстовий об'єкт; Потім сервер відповідає об'єктом у відповідь. Протокол публікації / передплати [8] вимагає меншого зв’язку між клієнтом та сервером, як показано на рис. 2.1.

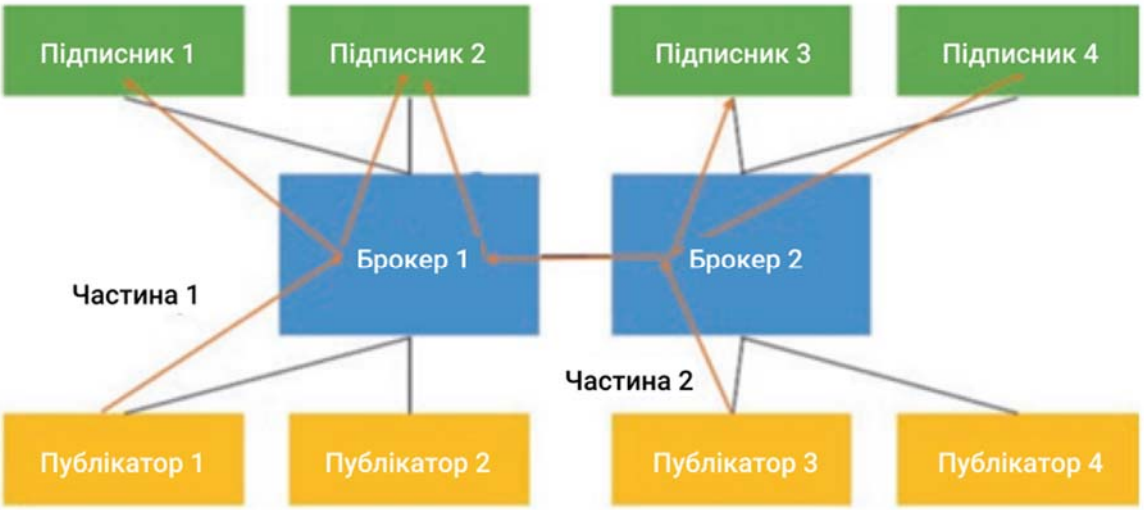


Рис. 2.1 Модель публікації / підписки

Сервер, відомий як видавець, класифікує повідомлення за категоріями. Клієнти підписуються на категорії, що їх цікавлять. Опублікувують повідомлення видавців та надсилають їх передплатникам. Повідомлення можуть бути упорядковані за темами; всі повідомлення з даної теми розповсюджуються брокерами передплатникам для цієї теми. Брокер знає особу передплатників, а видавець - ні. Брокери можуть взаємодіяти між собою, використовуючи мостовий протокол. Міст дозволяє побічно публікувати повідомлення, причому повідомлення надходить від видавця до першого брокера, потім до другого брокера і, нарешті, до абонентів, які не підключені до першого брокера.

Служба розподілу даних (DDS) [9] - це архітектура програмного забезпечення для публікації / підписки; використовується кілька реалізацій DDS. Домен DDS підтримує логічний глобальний простір даних; дані управляються набором місцевих магазинів. Видавці та передплатники динамічно виявляються в мережі. Видавці можуть вказати ряд параметрів якості обслуговування, які є примусовим застосуванням брокерами.

Протокол публікації / підписки в реальному часі (RTPS) [10] - це так званий дротовий протокол, який визначає протокол для зв'язку з DDS та

іншими системами публікації / підписки. RTPS забезпечує властивості QoS, стійкість до відмов і безпеку типу.

Було розроблено архітектуру чутливих до часу систем публікації / підписки, яка була б масштабованою до систем розміром до Інтернету. Визначилися три основні цілі проектування: передбачувана затримка, гарантована доставка при наявності кількох несправностей та продовження роботи при масштабуванні. Вони ідентифікували кілька типів моделей несправностей для систем публікації / підписки: аномалії мережі (втрата, упорядкування, пошкодження, затримка, перевантаження, розділення), збій посилання, збій вузла та відбій вузлів, які несподівано приєднуються та виходять із системи. Їх архітектура має три рівні абстракції: мережевий рівень складається з доменів, що складаються з вузлів; рівень вузлів складається з кластерів, причому члени кожного кластера належать до одного і того ж домену заглушки; і рівень координаторів. Рівень координації маршрутизує повідомлення за допомогою деревної топології, побудованої поверх розподіленої хеш-таблиці. Координатор є р-надлишковим, щоб забезпечити відмовостійку координацію.

Для забезпечення відмовостійких накладок формулюється модель різноманітності шляхів, яку можна обчислити з обмеженими знаннями про мережеві підключення.

Був використаний знайомий із семантикою механізм зв'язку для зменшення накладних витрат та підвищення надійності. Вони використовують оцінювачі простору станів як у видавця, так і в абонента, щоб підтримувати безперервність значень датчиків за наявності змін у мережі. Оцінювач їх стану має вигляд xk + 1 = Fk + 1xk. Архітектор системи встановлює модель точності δ для кожного датчика. Обмеження використовується для управління вимогами до пропускної здатності. Їх система також динамічно регулює межу точності моделі.

Поєднується DDS із програмно визначеним мережевим протоколом OpenFlow, щоб забезпечити можливість DDS реалізувати параметри QoS. Додаються два параметри QoS, які неможливо легко визначити зі стандартних параметрів DDS: MINIMUM_SEPARATION та E2E_LATENCY, визначені абонентами.

Протоколи можна розділити на дві великі категорії: ті, які прив'язані до певного фізичного рівня, і ті, які ні. Взагалі кажучи, протоколи, які покладаються на певний фізичний рівень, не використовують Інтернет-протокол, тоді як протоколи, які є агностичними на фізичному рівні, використовують IP.

Zigbee [11] - це сітчаста мережа, призначена для роботи з низьким енергоспоживанням. Різні стандарти похідних додатків спеціалізуються на протоколах для таких програм, як розумні будинки та комунальні послуги. Zigbee базується на стандартах IEEE 802.15.4 PHY та MAC. 802.15.4 працює в трьох діапазонах: 868 МГц, 915 МГц і 2,4 ГГц. Він забезпечує швидкість передачі даних від 20 до 250 кбіт / с, залежно від смуги частот.

Шар Zigbee NWK розміщений поверх рівня MAC 802.15.4 і надає послуги з управління даними та даними. Рівень APL включає три розділи: підшар підтримки додатків, рівень об'єктів пристрою Zigbee та фреймворк програми.

Zigbee пропонує два типи моделей мережевої безпеки: централізовану мережу безпеки може запустити лише координатор / центр довіри Zigbee; розподілені мережі безпеки не мають центрального центру довіри. Вузли можуть приєднуватися до будь-якого типу мережі та пристосовуватися до типу мережі, до якої вони приєдналися. Мережі формуються координаторами або маршрутизаторами після сканування для вибору доступного каналу. Координатори формують централізовані мережі безпеки, тоді як маршрутизатори - мережі розподіленої безпеки. Мережеве управління - це назва процесу, за допомогою якого вузол приєднується до мережі. Після

ідентифікації відкритої мережі вузол зв'язується з цією мережею і отримує мережевий ключ. Кластери визначають інтерфейси для функцій і

домени. Низький рівень енергії Bluetooth (BLE) [12] є частиною стандарту Bluetooth, призначеного для роботи з низьким енергоспоживанням, наприклад пристрої, що живляться від монетних батарей.

Пристрій BLE може працювати як передавач, приймач або як обидва. На исунку 2.2 зображено стек протоколів Bluetooth Classic.

Рис. 2.2 Bluetooth стек

Посилальний рівень забезпечує рекламну послугу; пристрої можуть сканувати, щоб ідентифікувати вузли та мережі. Пристрої можуть виступати в якості шлюзів до Інтернету на основі перекладу мережевих адрес. Протокол BLE є державним. BLE включає ряд оптимізацій для зменшення споживання

енергії. LoRa [13] призначений для великопрофільних програм IoT з базовою станцією, що охоплює сотні квадратних кілометрів. Він призначений для підтримки топології мережі із шлюзами для кінцевих пристроїв із шлюзами, організованими у власну зіркову мережу. Швидкість передачі даних коливається від 0,3 до 50 кбіт / с. MQTT [14] - орієнтований на IoT протокол із семантикою публікації / підписки. Протокол розроблений для низьких накладних витрат і є агностичним щодо корисного навантаження даних. MQTT забезпечує три рівні якості обслуговування: щонайменше один раз надає послуги з найкращими зусиллями, принаймні один раз забезпечує доставку, але може мати копії, і рівно один раз гарантує доставку повідомлення без дублювання.

MQTT базується на моделі публікації / підписки. Повідомленню при опублікуванні надається атрибут утримання; повідомлення з позначками QoS принаймні один раз або рівно один раз повинні встановлювати прапор збереження. Новий передплатник теми отримає останню публікацію на цю тему. Під час встановлення з'єднання клієнт може надати серверу заповіт, щоб вказати повідомлення, яке потрібно опублікувати, якщо клієнт несподівано від'єднаний.

Повідомлення класифікуються за допомогою рядків тем, подібних до ієрархічних назв файлів. Набір тем організований у дерево тем. Назви тем слідують за іменами вузлів у шляху до дерева тем, з іменами вузлів, розділеними знаком «/». Абоненти можуть використовувати символи підстановки у рядку теми: „+" позначає підстановочний знак на одному рівні дерева тем; "#" Позначає збіг на будь-якій кількості рівнів дерева тем.

XMPP - це протокол для потокового передавання XML. Він забезпечує безпеку, автентифікацію та інформацію про доступність мережі та реєстри клієнтів.

XMPP-IoT - це діалект XMPP, призначений для додатків IoT. REST [15] широко використовується для веб-служб і отримав певне використання як

модель обслуговування IoT. REST - це шаблон архітектури для передачі даних без протоколу HTTP. Він виставляє структуровані за каталогами показники ресурсних форм. REST можна використовувати для передачі даних XML або JSON. Клієнти отримують доступ до ресурсів методами GET, PUT, POST та DELETE.

CoAP [16] - це протокол веб-передачі на основі REST, призначений для пристроїв IoT. Він може використовуватися з декількома типами корисних даних, включаючи XML та JSON.

Google Cloud Pub / Sub [17] може використовуватися для надання послуг публікації / передплати IoT та інших систем.

Теми та підписки представлені як колекції REST. Система поділяється на площину даних для повідомлень та площину управління для розподілу до серверів, відомих як маршрутизатори; сервери даних площини відомі як експедитори. Маршрутизатори врівноважують узгодженість та однорідність даних за допомогою послідовного алгоритму хешування. Життєвий цикл повідомлення включає кілька етапів. Коли видавець надсилає повідомлення, воно записується на зберігання. Абоненти отримують повідомлення, а видавець отримує підтвердження. Абоненти підтверджують повідомлення до Google Cloud Pub / Sub. Повідомлення видаляється з пам’яті, як тільки принаймні один абонент на кожну підписку визнає повідомлення. Система контролює себе, щоб виявити та пом'якшити проблеми з обслуговуванням.

Amazon Web Services (AWS) IoT [18] - це керований хмарний сервіс для пристроїв IoT, які називаються речами. Тінь від речі - це хмарна модель речі. Механізм правил перетворює повідомлення на основі правил і направляє результати до служб AWS. Брокер повідомлень базується на MQTT. Реєстр речей присвоює речам унікальну ідентичність.

Microsoft Azure надає послуги, орієнтовані на IoT. Її Service Fabric - це система комунікації проміжного програмного забезпечення, яка підтримує мікросервіси, що працюють на кластері. Мікросервіс може бути як без

громадянства, так і з державним статусом. Він також надає модель контейнера для додатків; контейнер забезпечує ізольоване середовище, але покладається на операційну систему, на відміну від віртуальної машини, яка працює під операційною системою. Він забезпечує бази даних, використовуючи як структурований, так і неструктурований підхід. Він також надає API для служб штучного інтелекту.

2.2 Аналіз архітектури та моделі Індустріального IoT

Інтернет речей вже вніс революцію в наше розуміння застосувань у широкому діапазоні людської діяльності. Очікується, що ця тенденція посилиться найближчим часом.

Програми IoT поширюються в різних секторах, включаючи розумну енергетику, виробництво, сільське господарство, охорону здоров'я, безпеку та безпеку, розумні міста, розумні будівлі та розумне середовище. Усі ці сфери застосування повторюють одну і ту ж базову модель: велика кількість інтелектуальних пристроїв, пов’язаних між собою за допомогою дротових або бездротових носіїв, взаємодіють та координують для досягнення мети.

В промисловому середовищі розвиток у бік розумних фабрик [19], стратегія Industrie 4.0, Індустріальний Інтернет та Європейська ініціатива для фабрик майбутнього ініціювали впровадження IoT у промисловості з цілями збільшення гнучкості та продуктивності, одночасно знижуючи собівартість продукції.

Концепцією, що розвивається, є індустріальний IoT (IIoT). Індустріальний Інтернет речей є частиною загальної еволюції IoT. Однак він стикається з унікальними проблемами, які відрізняють його від інших систем та служб IoT через необхідність інтеграції програмованих логічних контролерів (PLC) та систем контролю та збору даних (SCADA). Системи PLC та SCADA разом із відповідними промисловими мережами, які їх взаємопов’язують, становлять інфраструктуру операційної технології (OT), яка традиційно еволюціонувала

незалежно від типової IT-технології, оскільки задовольняє потреби систем у цій галузі - об'єкти виробництва енергії, мережі розподілу енергії тощо - із суворими вимогами, такими як безперервна робота, безпека, робота в режимі реального часу тощо. Можливості, що пропонуються технологією IIoT, створюють проблеми для інтеграції цих систем OT із традиційними IT-системами підприємств на багатьох рівнях, від управління підприємством до кібербезпеки. Наприклад, системи планування ресурсів підприємства (ERP) потрібно розширити, включивши виробничі операції, якими в даний час керують системи виконання виробничих процесів (MES), які зросли самостійно та представляють значні проблеми сумісності для їх інтеграції. Очевидно, що інтегрована система, яка управляє повною ієрархією підприємства / заводу, починаючи від бізнес-процесів і закінчуючи датчиками, забезпечує значну гнучкість та представляє нові можливості для підприємств.

Інфраструктура виробництва та розподілу енергії включає системи OT, які є необхідною інфраструктурою, на якій будуються сучасні розумні мережі. Насправді енергетичний сектор є головним пріоритетом у розвитку IIoT не лише тому, що зростає потреба споживачів в енергії, особливо у тентенції приросту населення, а й тому, що енергоменеджмент є критичним фактором у промисловому секторі та бажане недороге виробництво товарів і послуг. Окрім енергетичного сектора, промислові системи широко поширені в багатьох інших секторах критичної інфраструктури, таких як управління водними ресурсами та транспорт.

Проблеми сумісності, пов’язані зі зближенням IT та OT, є лише частиною проблем, що виникають у IIoT. Потрібно розробити відповідні архітектури для побудови та управління ефективними системами IIoT, розробити технології для проектування та управління кіберфізичними системами, датчиками та мережами, і, що важливо, безпеку та конфіденційність потрібно вирішувати уніфіковано в контексті IIoT. Безпека та конфіденційність є серйозними викликами, оскільки традиційно безпека в IT-секторі була проблемою, в той час

як безпека була основною у секторі ОТ. Об'єднання двох призвело до усвідомлення того, що безпеку неможливо досягти без конфіденційності, в той же час безпека повинна включати технології, що поєднують надійність та відповідають суворим вимогам у режимі реального часу та низькій потужності у багатьох областях програм. Хоча питання безпеки промислових систем управління привертали увагу в останнє десятиліття, і стандарти розвивалися набагато швидше, ніж у минулому, наприклад, ISO / IEC 27000 та ISA / IEC 62443 сімейств стандартів [20], все ще існують значні проблеми на технологічному, архітектурному та управлінському фронтах для отримання рішень для уніфікованого IIoT.

У цьому розділі представлено концепції та еволюцію IIoT, починаючи від стратегії Industrie 4.0 і переходячи до Індустріального Інтернету. Описуються еталонні архітектури IIoT, коли вони еволюціонують від зусиль МСЕ до Індустріального Інтернет-консорціуму. Нарешті, описуються деякі репрезентативні проблеми в процесі розвитку та впровадження IIoT, зосереджуючи увагу на енергетичному секторі. Оскільки безпека та конфіденційність становлять значну проблему як у IIoT, так і в IoT.

Industrie 4.0 - це стратегічна ініціатива, яка спрямована на впровадження технологій IoT у виробничий та виробничий сектори [21]. Мета полягає у наданні можливості Німеччині зберегти провідну роль у виробництві, забезпечуючи ефективне та дешеве виробництво завдяки гнучким робочим процесам. Засобом досягнення цієї мети є широке включення кіберфізичних систем у виробничі та виробничі процеси, з метою включення інтелекту в системи та процеси, забезпечення їх високого рівня зв’язку та зв’язку та досягнення їх координації у більш складних, але гнучкі процеси, що призводять до отримання високоякісних, недорогих продуктів.

Industrie 4.0 бере свою назву від ідентифікації нової, що розвивається галузі як четвертої революції промислового виробництва. Загальновизнано, що на сьогоднішній день промислове виробництво пережило три революції. Перша

промислова революція, що відбулася у вісімнадцятому та дев’ятнадцятому столітті, - це та, коли у виробництво товарів та послуг були введені механізовані виробничі потужності, де необхідна енергія забезпечувалась водою та парою. Електрична енергія була введена під час другої революції, яка призвела до масового виробництва, оскільки електроенергія підвищила продуктивність. В епоху після Другої світової війни включення електроніки та програмного забезпечення, тобто промислових інформаційних технологій, до механічних та електричних компонентів призвело до третьої революції, яка дала можливість автоматизації на високих рівнях. В даний час багато зацікавлених сторін промисловості вважають, що ми перебуваємо на порозі наступної, четвертої, промислової революції, завдяки широкому впровадженню та використанню кіберфізичних систем, що призводить не тільки до ще більш високих рівнів автоматизації, але дає можливість масового виробництва та виробництва товарів та послуг завдяки гнучкості, що пропонується легко програмованими, налаштовуваними та керованими виробничими лініями.

Зусилля Industrie 4.0 засновані на широкому розгортанні та використанні обчислювальних та комунікаційних ресурсів. Останні два десятиліття характеризуються значним прогресом у високопродуктивних процесорах із низьким енергоспоживанням, пам'яті та комунікаційних компонентах, які забезпечують ефективну обробку та мережеві зв'язки. Ці досягнення забезпечили значні можливості обробки великої кількості пристроїв, які розгортаються серед споживачів або на місцях. Розумні споживчі пристрої стали нормою. Смартфони надають сотні додатків і надають послуги, починаючи від визначення маршрутів подорожей і транспорту до мобільного банкінгу та моніторингу стану здоров’я. Розумні телевізори поєднують і надають різні види розваг та мережевих послуг, починаючи від індивідуального управління та управління телевізійними каналами, до ігор в Інтернеті та управління домашніми пристроями. Розумні побутові прилади відстежують параметри, починаючи від температури навколишнього середовища і

закінчуючи споживанням води та енергії, що дозволяє громадянам ефективно та ефективно управляти своїми будинками, приводячи до необхідної якості життя, одночасно знижуючи експлуатаційні витрати на різних фронтах.

Велика основа обчислювальних ресурсів та підключення стає очевидною завдяки опублікованій кількості вбудованих процесорів та компонентів, які випускаються в даний час. Згідно з [22], переважна більшість вироблених процесорів, приблизно 98%, розгортаються у вбудованих системах. Розгорнута напівпровідникова пам’ять також зростає, і очікується, що вона зросте на 40% у порівнянні з минулим роком [23]. Крім того, значний прогрес дротових та бездротових мереж за останні два десятиліття призвів до повсюдного зв’язку, який наближається до міст та селищ. Наявна основа обробки та комунікації веде до зміни ієрархії вбудованих систем та послуг аж до рівня Інтернету речей, даних та послуг.

Приклади цієї еволюції можна виявити в декількох областях застосування. Наприклад, у транспорті вбудовані системи широко розповсюджених функцій управління від розважальних систем автомобіля до управління автокріслами. На цьому рівні вбудовані процесори запрограмовані для управління конкретними, індивідуальними параметрами, наприклад, висотою та переміщенням в автокріслах, на основі команд користувача. Однак вбудовані системи в автомобілях також пов'язані між собою, або всередині автомобільної системи, або з навколишнім середовищем, забезпечуючи вбудовані вбудовані послуги; автоматична плата за проїзд - це одна з них, коли вбудовані системи у вагоні та каси зв’язку взаємодіють між собою, щоб завершити електронну платіжну транзакцію проїзду. Наприклад, такі платіжні системи з декількох платних доріг можна додатково поєднувати в розподіленій системі, яка забезпечує більш широке управління дорожнім рухом та дорожнім збором, що призводить до більш ефективної транспортної інфраструктури, що забезпечує нижчі терміни очікування та витрати на пальне для мандрівників, а також нижчі експлуатаційні вартість і, отже, більший дохід органам управління

транспортом. Можна навіть передбачити ще вищий рівень зв’язку таких складних транспортних систем із розумними містами, які поєднують управління перевезеннями з додатковими послугами, такими як розподіл енергії, цивільні служби, аварійні служби тощо, як це потрібно в різний час, місця та протягом спеціальні заходи.

Досягнення сенсорних технологій, крім розвитку вбудованих систем та мереж зв'язку, роблять усі ці сценарії реалістичними. Важливо, що датчики заповнюють розрив між фізичним світом та цифровим світом, забезпечуючи все більшу інформацію цифровими системами та забезпечуючи інтелектуальне управління системами та процесами. У цьому відношенні виробнича та промислова автоматизація традиційно використовує ІТ-технології з датчиками та електромеханічними системами, що очолює розробку та впровадження технологій та концепцій інтелектуального управління, систем та послуг. Таким чином, розробка стратегії Industrie 4.0 та пов'язаних з нею ініціатив є природним кроком еволюції промислових технологій, що впливають і перебувають під впливом прогресу споживчих технологій Інтернету речей.

Розумна концепція заводу значною мірою втілює цілі стратегії Industrie 4.0. Концепція базується на згаданій вище ієрархії кіберфізичних систем, де інтелектуальні виробничі системи взаємопов’язані в багаторівневу ієрархію для досягнення високого ступеня автоматизації, націленої на гнучкість, ефективність, автономність, стійкість, безпеку та низьку вартість. Розумні машини будуть взаємопов’язані для створення розумних заводів, які, в свою чергу, будуть об’єднані для забезпечення розумних заводів. Беручи до уваги типові компоненти виробничого процесу, розумні фабрики націлені на ефективну автоматизацію всіх компонентів та стадій. Матеріали та ресурси будуть ефективно керовані та впроваджені в процес; переробка виробництва буде здійснюватися в режимі реального часу, мінімізуючи витрачені ресурси на продукцію та операції, тоді як реконфігурація та реорганізація виробничих процесів та налаштування продукції будуть здійсненними в режимі реального

часу та з безпекою для інфраструктури та операторів, мінімізуючи вплив на навколишнє середовище. Клієнти зможуть стежити за ходом розробки замовленої продукції, тоді як виробники будуть оптимізувати свої логістичні ланцюги.

Індустріальний Інтернет речей (IIoT) склався як загальна концепція застосування Інтернету речей до промислового сектору. Фактично, це узагальнення Industrie 4.0, яке, схоже, більше зосереджується на ефективності промислових процесів. Бачення IIoT включає всі аспекти промислових операцій, зосереджуючи увагу не тільки на ефективності процесів, але й на управлінні активами, обслуговуванні тощо.

Враховуючи, що IIoT є фактично IoT у промисловому секторі та що концепції Industrie 4.0 є фактично підмножиною IIot, як показано на рис. 2.3, потрібно виявити різницю між IoT та IIoT.

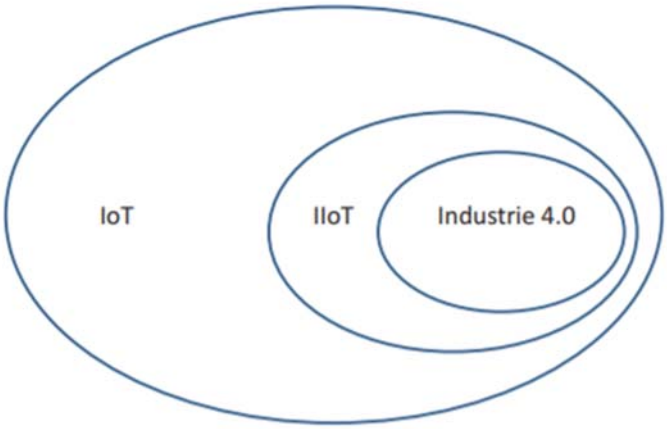


Рис. 2.3 IoT, IIoT та відносини Industrie 4.0

Хоча основні концепції однакові, тобто взаємопов'язані інтелектуальні пристрої, що дозволяють дистанційне зондування, збір даних, обробку, моніторинг та управління, параметри, що ідентифікують підмножину Ioo IIoT, є суворими вимогами до безперервної роботи та безпеки, а також операційні технології, що використовуються у промисловому секторі. Як приклад можна розглянути різницю між побутовою послугою, такою як програма контролю здоров'я на смарт-годиннику, та промисловою послугою, такою як моніторинг

парового насоса. Незважаючи на те, що обидва додатки збирають дані в режимі реального часу, наприклад, кроки або температуру тіла у справі, що стосується охорони здоров'я, і тиск або об'єм пари в корпусі парового насоса, передають дані, визначають події та надають зворотний зв'язок або команди операторам / споживачам та підсистемам, очевидно, що безперервна робота та безпека пред’являють більш суворі вимоги до випадку парового насоса, коли потенційний ефект поломки значно катастрофічніший і може призвести до дорогого часу простою та навіть травм людей чи людських втрат.

Ці характеристики промислового сектору - технологія та вимоги - ведуть до спеціалізованих, вимогливих рішень щодо технологій та послуг, що виправдовує спрямованість промислового сектору на спеціалізовану концепцію IoT. Це призвело до сильної зацікавленості промислового сектору у розробці спеціалізованих концепцій, від стратегії до застосування та технологій. Звичайні моделі розвитку бізнесу, які включають численні взаємозалежності між зацікавленими сторонами, від ланцюгів поставок до просування послуг, також призводять до гострої потреби в сумісних рішеннях на багатьох рівнях, від рівня пристроїв до послуг. Таким чином, існує потреба у скоординованій діяльності в процесі еволюції до IIoT, до якої звертаються консорціуми, такі як Індустріальний Інтернет-консорціум [24], який забезпечує значне керівництво у цій новій галузі.

Компанія General Electric представила термін "Індустріальний Інтернет" ще в 2012 році як лідер "Індустріального Інтернету Речей", визначивши також технології міжмеханічного зв'язку, SCADA, HMI, аналіз промислових даних та кібербезпеку як основні складові Бачення IIoT. Цікаво, що вони також розраховують вплив індустріального Інтернету на 46% світової економіки, тоді як в енергетичному секторі вони розраховують вплив 100% на виробництво енергії та 44% на споживання енергії у всьому світі [25].

Розробка та розгортання систем і служб IIoT вимагає розробки архітектур, що забезпечують ефективні та ефективні операції, а також

сумісність з урахуванням передбачуваних наскрізних послуг та великої кількості зацікавлених сторін, що стосуються пристроїв, кіберфізичних систем, систем зв'язку. мереж, постачальників послуг та розробників бізнесу. Таким чином, значні зусилля витрачаються на розробку стандартів та еталонних архітектур, які будуть прийняті та прийняті різними зацікавленими сторонами. Міжнародний союз електрозв'язку (МСЕ) вирішив цю проблему, опублікувавши в 2012 р. Рекомендацію ITU-T Y.2060, яка запроваджує довідкову архітектуру для Інтернету речей загалом, включаючи явно програми, що потрапляють у контекст IIoT, такі як інтелектуальна мережа , інтелектуальні транспортні системи, електронне охорону здоров'я тощо [26]. Індустріальний Інтернет-консорціум (IIC) також працює над еталонною архітектурою для IIoT і в даний час опублікував Версію 1.7 Довідкової архітектури Індустріального Інтернету. Ця архітектура є детально розробленою довідковою архітектурою, значно детальнішою, ніж МСЕ, що стосується всіх важливих аспектів усіх категорій зацікавлених сторін. Беручи до уваги деталі обох еталонних моделей, можна розглядати модель IIC як спеціалізовану еволюцію моделі МСЕ, розглядаючи більш докладно важливі питання IIoT щодо більш загальної еталонної моделі МСЕ, яка містить вимоги до загальної IoT .

Зусилля МСЕ розширили бачення комунікацій, включивши передачу "чого завгодно" до понять зв'язку "будь-який час" і "будь-яке місце". Важливо те, що він включає всі очікувані програми, включаючи промислові, зокрема згадаючи інтелектуальні мережі та інтелектуальні транспортні системи серед інших. Як "речі" МСЕ розглядає фізичні та віртуальні об'єкти, які можна ідентифікувати та здатні з'єднуватися з мережами зв'язку, тоді як вони мають відповідну інформацію, яка є статичною або динамічною. Важливо, що оскільки комунікація є критичною частиною всієї концепції IoT, фізичні речі потрібно приєднувати до “пристроїв”, які підключені до мереж, щоб будь-яка аналогова інформація могла бути перетворена в цифрову та передана через мережі. Пристроями можуть бути просто дані, що передають дані та зберігають

дані, фіксують дані, взаємодіючи з фізичними об’єктами за допомогою зчитувача та запису, пристроями контролю та керування, або пристроями загального призначення із вбудованими ресурсами обробки та зв’язку, такими як машини, прилади та споживчі електронні продуктів.

Важливою проблемою в довідковій моделі МСЕ є модель зв'язку між пристроями. Як вказує рис. 2.4, модель розглядає три методи зв'язку, засновані на використанні шлюзів (G) та використанні мережі зв'язку (CN).

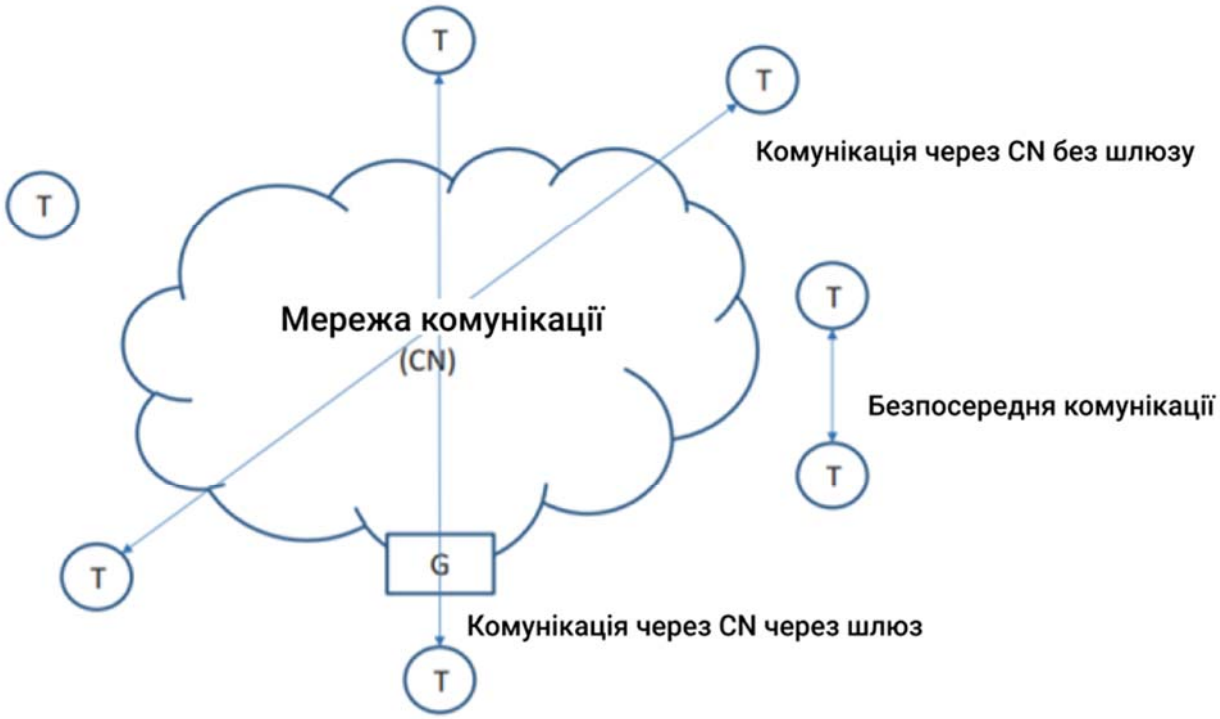


Рис. 2.4 Методи зв'язку для пристроїв IoT

Пристрої можуть спілкуватися без використання шлюзів, безпосередньо, через локальні мережі та / або через мережу зв'язку, або вони можуть спілкуватися через мережу зв'язку, що використовує шлюзи.

Модель МСЕ вміщує основні характеристики IoT, які визначені. Цими основними характеристиками є взаємозв’язок, масштабність, неоднорідність, послуги для речей та динамічний характер інформації про пристрій та зв’язок. Взаємозв'язок є важливою характеристикою, оскільки "все" може підключитися до глобальної мережі для будь-якої програми. Оскільки кількість підключених

пристроїв різко зростає, масштабування стає важливим параметром, який потрібно вирішити на всіх рівнях IoT та IIoT; проблема масштабування стосується не тільки кінцевих точок зв'язку та кількості пристроїв, але і розміру вироблених та переданих даних, а також управління ними з точки зору зберігання та обробки. Динамічний характер пристроїв, які динамічно вмикаються та вимикаються або підключаються та відключаються від мереж, зроблять пейзаж більш складним та вимогливим. Відкритий характер (I) IoT та велика кількість зацікавлених сторін, на додаток до гнучких та довгих ланцюгів поставок у звичайному наданні послуг, призводить до необхідності розміщення різнорідних "речей", пристроїв, платформ та послуг. Послуги щодо речей також повинні вирішуватися належним чином, не тільки через обмежені ресурси багатьох "речей", але й через вимоги ряду служб безпеки та безпеки, включаючи захист конфіденційності та безпечне спрацьовування, що дозволяє уникнути проблем та аварій.

Фундаментальні характеристики (I)IoT призводять до вимог, яким повинна відповідати еталонна архітектура. Основні вимоги, згадані MCE, включають сумісність, підключення на основі ідентифікації, автономність у роботі мереж та послуг, розміщення послуг, що базуються на розташуванні, безпеку та конфіденційність, а також можливості управління речами та послугами, включаючи plug and play. Рисунок 2.5 зображує еталонну модель ITU IoT, яка була введена для задоволення вищезазначених вимог.

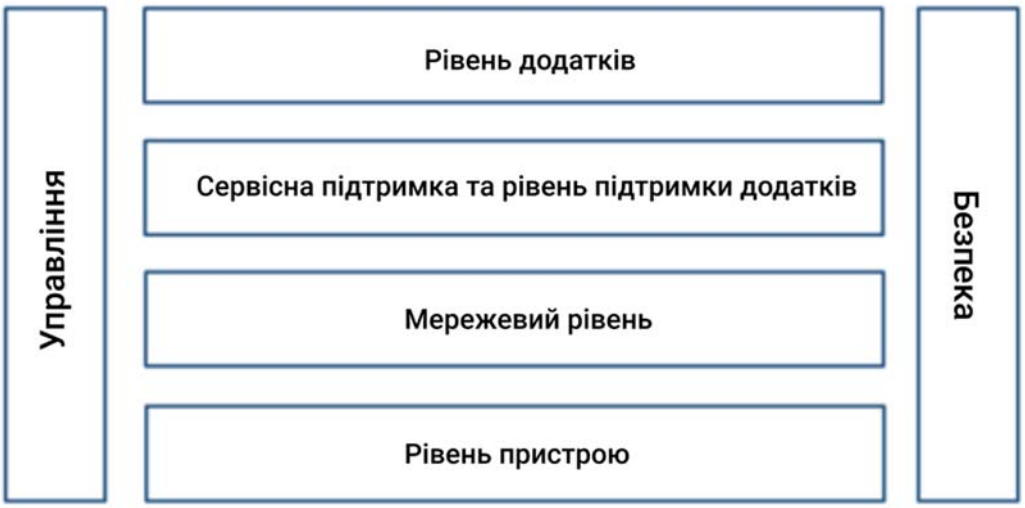


Рис. 2.5 Посилання на IoT модель ITU

Це типова багатошарова модель з чотирма ієрархічними рівнями, зокрема пристроєм, мережею, підтримкою додатків та послуг і, нарешті, прикладним рівнем, і двома вертикальними рівнями, які перетинають чотири ієрархічні рівні, визначаючи функції управління та захисту для всіх ієрархічних рівнів.

Рівень пристроїв, найнижчий в ієрархії, включає функціональність пристроїв та комунікаційних шлюзів. Враховуючи основний інтерес MCE у зв'язку, рівень описує орієнтовану на комунікацію функціональність пристроїв: (a) пристрої, які передають та приймають інформацію через мережу зв'язку безпосередньо, тобто, не використовуючи жодного шлюзу, (b) пристрої, які передають інформацію передачі та прийому) через шлюзи, (c) пристроїв, які здійснюють прямий зв’язок без використання комунікаційної мережі, але здатні здійснювати зв’язок через локальні мережі або формувати спеціальні мережі, та (d) пристрої, здатні вибірково вмикати та вимикати функціональність для економії робочої потужності. Що стосується шлюзів, рівень пристрою включає всі відповідні комунікаційні технології, дротові та бездротові, такі як шина CAN, Wi-Fi, Bluetooth, Zigbee тощо. Важливо, що рівень пристрою включає перетворення протоколів, оскільки пристрої можуть реалізовувати різні протоколи, і , отже, для взаємодії потрібне перетворення протоколів.

Мережевий рівень забезпечує інкапсуляцію даних пристрою та відповідного перетворення протоколів у протоколи мережевого рівня. Рівень включає функціональність мережевого та транспортного рівнів в еталонній моделі протоколу OSI. Для роботи в мережі вони включають функціонал управління мережевим підключенням, мобільністю, автентифікацією, авторизацією та обліком, тоді як для транспорту вони передбачають транспортний трафік користувача, а також передачу контрольної та управлінської інформації для (I) служби IoT та програм.

Рівень сервісної підтримки та підтримки додатків включає як загальну, так і функціональність (можливості), що стосується послуг / додатків, що дозволяють (I) додатки та послуги IoT. Беручи до уваги розподілений характер (I) послуг та додатків IoT, існує загальна функціональність, така як обробка та зберігання даних, а також спеціалізована функціональність для кожного додатка та послуги, оскільки нові послуги мають різні вимоги, наприклад, місця роботи інтелектуальної мережі інші вимоги до конфіденційності, ніж інтелектуальна система управління дорожнім рухом для транспортних послуг.

Нарешті, прикладний рівень, найвищий ієрархічний рівень, включає програми (I) IoT та послуги. Вертикальний наскрізний рівень управління включає як загальну, так і специфічну функціональність домену додатка. Загальний стосується типового управління конфігурацією, топологією, ресурсами, продуктивністю, помилками, безпекою та управлінням обліковими записами. Спеціальна програма стосується функцій, які відповідають вимогам програми, таких як інтелектуальний моніторинг лічильника в розумних мережах.

Аналогічно рівню управління, вертикальний рівень перехресного різання включає як загальну, так і специфічну функціональність домену додатка. Загальна функціональність зазвичай відноситься до функцій, пов’язаних з авторизацією, автентифікацією, цілісністю та конфіденційністю на всіх рівнях, конфіденційністю на рівні програми, захищеною маршрутизацією на

мережевому рівні, контролем доступу на всіх рівнях тощо. вимоги. Документ довідкової моделі MCE також представляє набір бізнес-моделей IoT, враховуючи велику кількість зацікавлених сторін у цій галузі та їхні різні інтереси та цілі. Що важливо, ці бізнес-моделі розробляються на основі думки мережевих операторів.

Бізнес-моделі базуються на п’яти основних ділових ролях, які можуть мати зацікавлені сторони: (a) постачальник пристроїв, (b) постачальник мереж, (c) постачальник платформ, (d) постачальник додатків та (e) клієнт додатків. Як вказують терміни, постачальники пристроїв є зацікавленими сторонами, які надають пристрої для (I) IoT, а постачальники мереж забезпечують мережеві системи, шлюзи та підключення для (I) IoT. Постачальники платформ забезпечують уніфіковану розподілену IT-платформу з чітко визначеними інтерфейсами, через які додаток може обслуговуватися наскрізь, тоді як постачальники додатків надають послугу (I) IoT через платформу, мережі та пристрої, що надаються відповідними постачальників послуг. Очевидно, що замовник додатка є користувачем програми (I) IoT або послуги. На основі цих п’яти бізнес-ролей MCE визначає п’ять бізнес-моделей залежно від кількості операторів, які беруть участь у програмі, та їх конкретних ролей. На рисунку 2.6 показані ці п’ять моделей (Моделі 1–5), що представляють ділові ролі у вигляді складених ящиків - аналогічно моделі вертикального шару - і вказуючи операторів з різними шаблонами заповнення в полях; поля (ролі) з однаковим шаблоном заповнення у стеку вказують на те, що одна і та ж організація є оператором цих блоків.

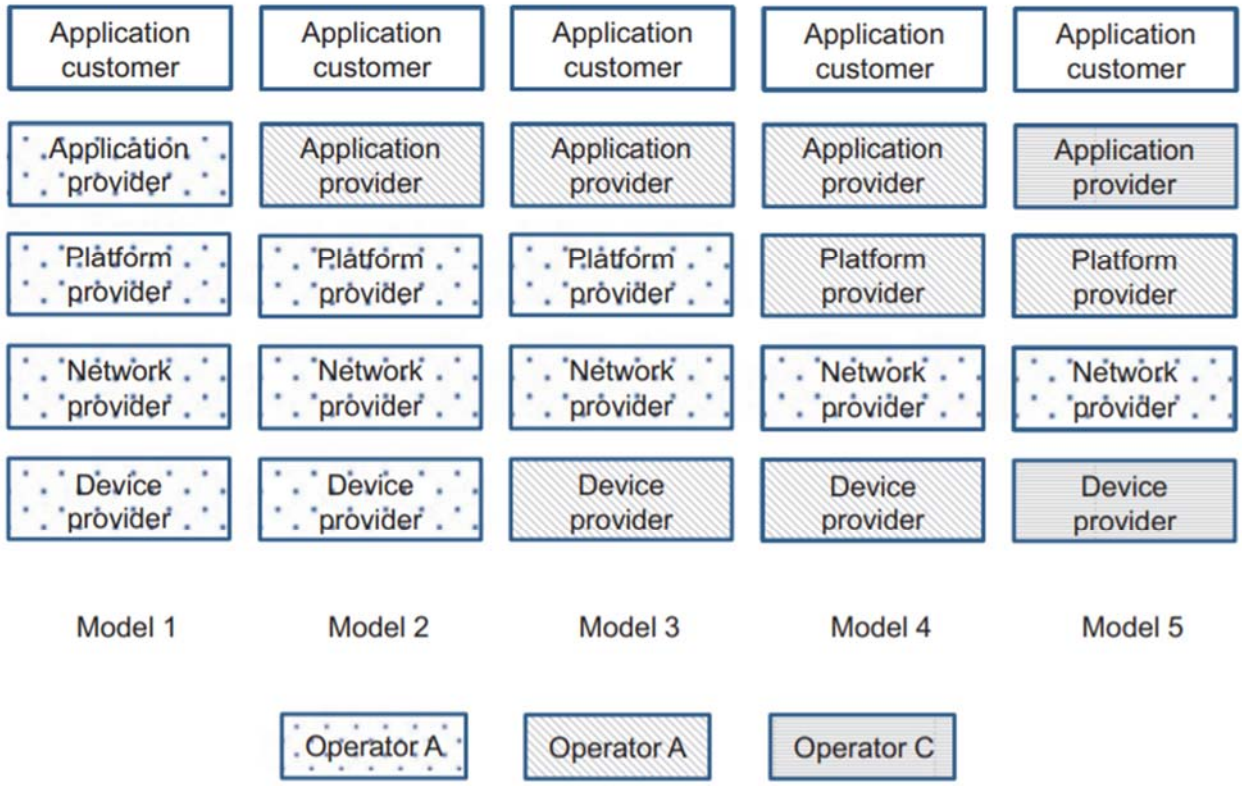


Рис. 2.6 Бізнес-моделі IoT, визначені MCE
(Application customer – замовник заявки; Application provider – провайдер додатків; Platform provider – провайдер платформи; Network provider – провайдер мережі; Device provider – провайдер пристроїв)

Наприклад, у Моделі 1 ця ж організація виконує ролі пристрою, мережевої платформи та постачальника додатків, тоді як у Моделі 2 одна зацікавлена сторона виконує ролі постачальника пристроїв, мережі та платформи, а інша - роль постачальник додатків.

Індустріальний Інтернет-консорціум (IIC) зосереджується на подібних концепціях та розробляє еталонну архітектуру IIoT, яка має кілька подібностей із підходом MCE та еталонною моделлю. Очевидно, що підхід IIC до розробки архітектури інтегровано враховує інтереси та проблеми всіх типів зацікавлених сторін, виходячи зі випадків використання та зосереджуючись на повних бізнес-моделях та додатках на всіх рівнях, від пристроїв до служб IIoT. IIC дотримується підходу, згідно з яким різні зацікавлені сторони, яким потрібно

приймати різні рішення, мають архітектурні точки зору, що знаходяться на різних рівнях абстракції. Ці точки зору дозволяють зацікавленим сторонам зосередитись на параметрах, що цікавлять, та розробити відповідні архітектури, які досягають своїх цілей та вирішують проблеми, які вони визначили. З цією метою IIC визначив чотири різні точки зору: (a) бізнес, (b) використання, (c) функціональний та (d) впровадження.

Бізнес-точка зору стосується проблем зацікавлених сторін у бізнесі, які визначають та визначають системи та послуги IIoT у своїх організаціях або для споживачів. Ці проблеми, такі як рентабельність інвестицій, витрати на технічне обслуговування тощо, вирішуються за допомогою моделі, яка дає змогу визначити бачення та цінності, які перекладаються на ключові цілі, а потім на специфікації бізнес-завдань високого рівня, названі фундаментальними можливостями. До зацікавлених сторін належать розробники бізнесу, а також системні інженери та менеджери продуктів. Точка зору використання описує, як використовується система, реалізуючи ключові цілі та можливості, які були визначені через точку зору бізнесу. Точка зору описується за допомогою моделі, яка ідентифікує систему та її діяльність, залучені сторони - людей чи машини - та їх ролі та, нарешті, завдання, тобто дії, які виконуються сторонами з певною роллю. Оскільки завдання є діями в системі, вони точно вказуються та описуються для кожної ролі за допомогою так званих функціональних карт та карт реалізації, що визначають точні функції та підсистеми реалізації, необхідні для повного виконання завдання. До зацікавлених сторін, залучених до точки зору використання, належать не тільки системні інженери та менеджери продуктів відповідних використовуваних продуктів, але й усі зацікавлені сторони, які беруть участь у специфікації системи та послуги IIoT, включаючи кінцевих споживачів.

Функціональна точка зору представляє функціональну архітектуру системи IIoT, описуючи її компоненти, залежності та координацію, відповідаючи вимогам і специфікаціям, розробленим з точки зору

використання. Зацікавлені сторони, залучені до цієї точки зору, є розробниками систем та підсистем, розробниками продуктів та менеджерами, а також системними інтеграторами. Беручи до уваги увагу ІІС на ІІоТ та все більш широке впровадження індустріальних систем управління (ІСУ) у галузях декількох секторів, а також в роботі та управлінні критичною інфраструктурою, еталонна модель ІІС фокусується на своїй функціональній архітектурі систем ІІоТ на інтеграції ІСУ із класичними інформаційними технологіями (ІТ) в уніфікованій, ефективній моделі, яка відповідає вимогам усіх зацікавлених сторін - як зазначено у точках зору бізнесу та використання - та дозволяє приймати ефективні рішення. Включення ІСУ та ІТ в уніфіковану модель представляє ряд проблем.

Промислові системи управління, Операційні технології (ОТ) були розроблені за іншим шляхом еволюції від типових ІТ-систем через їх цілі та вимоги, які, як правило, включають постійну роботу, безпеку та обмеження в режимі реального часу; Системи ОТ були в основному розроблені та належать інженерам з управління та експлуатації, вони використовують різні технології для обробки, зв’язку та інтерфейсів, оскільки вони взаємодіють безпосередньо з навколишнім середовищем за допомогою датчиків та виконавчих механізмів, і ними керують їх власники самостійно, оскільки вони, як правило, частина вимогливих систем та послуг з точки зору надійності, безперервної роботи, реального часу, безпеки. Як результат, їхні технології, практики та стандарти еволюціонували незалежно від ІТ-технологій. Однак розширені можливості, пропоновані вдосконаленими датчиками та виконавчими механізмами, процесорами та пам'яттю, дозволили ІСУ виконувати дуже складні операції, розроблені для складних ІТ-систем, такі як збір та аналіз великих обсягів даних, багатоваріантне моделювання та оптимізація тощо. Важливо, що в той же час збільшені можливості та зростаюча складність ІСУ призвели до того, що вони стали більш вразливими до збоїв та кібератак, що призвело до додаткових функціональних вимог до їх правильної та ефективної роботи.

Для вирішення питання інтеграції IT та OT в уніфікованій моделі підхід IIC до еталонної архітектури розділяє системи IIoT на п’ять доменів, кожен з яких групує функціональні можливості, необхідні для логічно виразної роботи системи на високому рівні. Ці п’ять доменів є (а) контролем, (б) операціями, (в) інформацією, (г) додатком та (е) бізнесом. Рисунок 2.7, [27], показує розкладання функціонального представлення системи IIoT на п’ять доменів та показує дані та потоки управління між доменами, як зазначено в IIC.

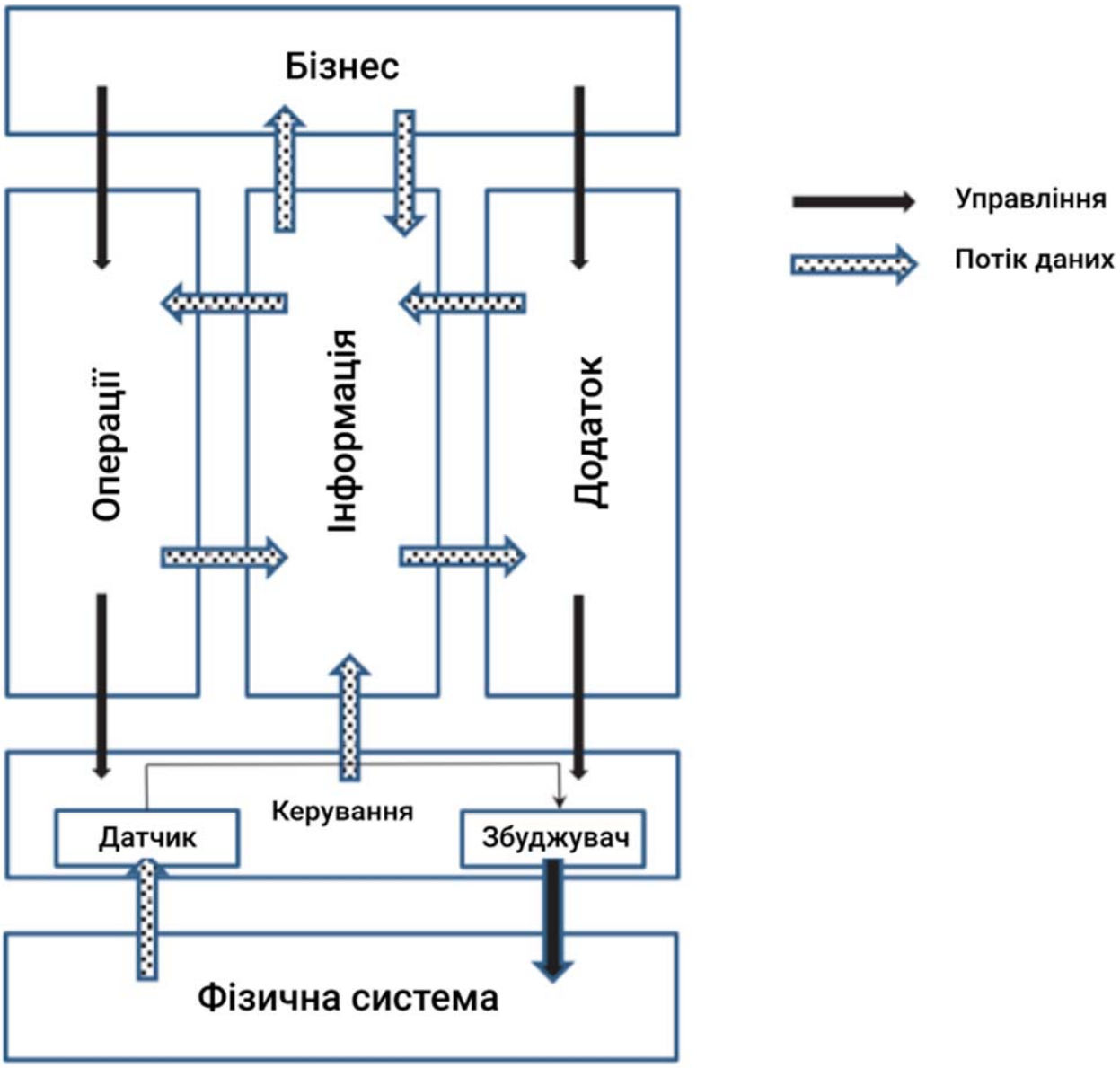


Рис. 2.7 Функціональні домени довідкової архітектури IIC

Домен управління ефективно представляє контур управління, реалізований промисловими системами управління, тобто він містить датчики, логіку та спрацьовування, які складають установку, реалізовану однією або кількома промисловими системами управління. Домен операцій включає функції, необхідні для роботи промислових систем управління в області управління; операція включає моніторинг та управління системою, а також оптимізацію ефективної роботи систем, особливо враховуючи вимоги декількох областей додатків до постійної роботи, задоволення вимог у режимі реального часу та досягнення цілей малої потужності.

Інформаційний домен відповідає за збір даних з усіх доменів та їх аналіз для прийняття рішень високого рівня для системи, наприклад, координація та оптимізація наскрізної роботи декількох промислових систем управління в домені управління. Домен програми включає в себе функціональність, яка залежить від програми та ефективно включає моделі та правила роботи відповідної програми; важливою частиною цього домену є набір API та користувальницьких інтерфейсів, щоб інші програми або користувачі могли ефективно використовувати програму. Нарешті, домен бізнесу включає системи та функції, які дозволяють керувати та приймати рішення на бізнес-рівні, наприклад, із системами планування ресурсів підприємства (ERP), системами виконання виробництва (MES) тощо.

Важливо відзначити, що підхід IIC зосереджений навколо концепції контрольної установки, тобто він розглядає всі точки зору навколо циклу управління, який реалізує установку. Оскільки цикли управління можуть бути простими, з однією системою, або складними з декількома системами, як правило, організованими в ієрархію, функціональне розкладання домену IIC може застосовуватися на всіх рівнях ієрархії. Таким чином, декомпозиція системи IIoT у доменах не являє собою шаруватий підхід як підхід ITU, а скоріше логічне функціональне декомпозицію всередині шару або між шарами в ієрархії. Через це посилальна архітектура IIC ідентифікує “перехресні

функції", які є фактично ієрархічними (або багаторівневими) функціями IT-інфраструктури, необхідними для розробки повного додатка IIoT. Ці функції включають підключення, розподілене управління даними, аналітику, інтелектуальне та еластичне управління та будь-яку іншу функцію програми, необхідну для конкретного домену програми або випадку використання. Наприклад, підключення має реалізовуватися в ієрархічному порядку, дотримуючись стандартів і практик, взаємопов'язуючи компоненти в рамках промислової системи управління або кількох таких систем, де кожна система може розглядатися як сукупність функцій з усіх п'яти визначених доменів. Спостерігаючи згадані перехресні функції, можна усвідомити, що вони фактично становлять шарувату архітектуру, аналогічну тій, що виконується MCE. У цьому відношенні можна розглядати підхід IIC та підхід MCE як доповнюючий, при цьому еталонна архітектура IIC є узагальненням до MCE, оскільки вона включає перехресні функції, аналогічні рівням MCE, в той час як це дозволяє розробляти більш детальні функціональні можливості моделі на рівень, що стосуються повних циклів управління та забезпечують підтримку всіх типів зацікавлених сторін - від розробників пристроїв до розробників бізнесу - для ефективного прийняття рішень.

Ця аналогія та взаємодоповнюваність стає більш очевидною з точки зору реалізації, яка розглядає деталі реалізації функціональної точки зору, розробленої для системи IIoT. Точка зору реалізації включає всі необхідні технічні та технологічні деталі, необхідні для реалізації повної системи IIoT та її застосування, включаючи функціональність системи, технологічні вимоги, комунікаційні та мережеві протоколи, всі типи інтерфейсів та відображення функціональних блоків які вказані у функціональній точці зору на типові архітектури реалізації, такі як трирівнева архітектура (де трьома рівнями є край, платформа та підприємство) та архітектура багатошарової шини даних.

2.3 Моделювання мережі IoT, що взаємодіє з навколишнім середовищем

Розглянемо модель мережі IoT, яка орієнтована на аналізі поведінки подій у системі. Оскільки події мають довге життя, пам’ять у формі черг на часових колесах відіграє вирішальну роль у моделі.

Модель обчислення базується на довгоживучих подіях. Подія генерується у вузлі та зберігається доти, поки вона не буде готова до завершення, і в цей час вона споживається вузлом.

Подія має 5 кортежів:

$$\langle \text{key, value, dest, gen\_time, release\_time} \rangle$$

Семантика події задається парою ключ-значення. Призначенням події є пристрій, який повинен обробити дану пару ключ-значення. Методи моделювання, описані в цій роботі, не стосуються семантики пар ключ-значення. Також необхідно знати часову поведінку події, яка задається двома значеннями. Час генерації ϑ - це час створення події. Час генерації корисний для нашого аналізу; реалізація може відстежувати це значення або не відстежувати це значення. Час випуску ρ події дозволяє системі IoT виконувати затримані дії - одна подія в середовищі може викликати не негайну реакцію, а скоріше таку, що трапляється через деякий час. Посилаючись на різницю між часом генерації та випуску, оскільки тривалість події становить $\lambda = \rho - \vartheta$. Події можуть генеруватися періодично або аперіодично. Час активації або випуску може бути періодичним або апериодичним.

Мережа складається з вузлів та посилань. Модулюються комунікаційні зв'язки односпрямовані. Більшість фізичних хабів є повнодуплексними, але в розлянутому випадку посилання як односпрямовані для просування нашого аналізу.

Можна виділити три методи моделювання взаємодії системи IoT із навколишнім середовищем, кожен зі своїм ступенем точності та деталізації.

Найпростіша модель розглядає і пристрій, і користувача як приурочені кінцеві автомати. Отримавши шлях через машину користувача, яка визначає даний випадок використання, ми можемо сформувати добуток машини пристрою та шлях машини користувача. Отриманий FSM разом із режимом хронометражу, який визначається випадком використання, повідомляє нам, коли події генеруються пристроєм. Це можна використовувати для побудови трасування сукупності подій.

Удосконалена модель розглядає користувача як процес прийняття рішення Маркова (MDP) із фіксованим терміном. Процес прийняття рішення Маркова - це стохастична модель, яка використовується для оптимізації. ПДР визначається набором станів та можливими діями з кожного стану. Кожній дії присвоюється винагорода R. Для переходів із дії у наступний стан присвоюються ймовірності. Ми можемо використовувати будь-який з декількох різних алгоритмів (динамічне програмування, лінійна алгебра), щоб знайти шлях, який максимізує винагороду. У цьому сценарії ми вирішуємо оптимальний шлях винагороди та формуємо його продукт із моделлю пристрою, використовуючи фіксовану часову модель. На рисунку 2.8 наведено приклад простої моделі пристрою та моделі користувача.

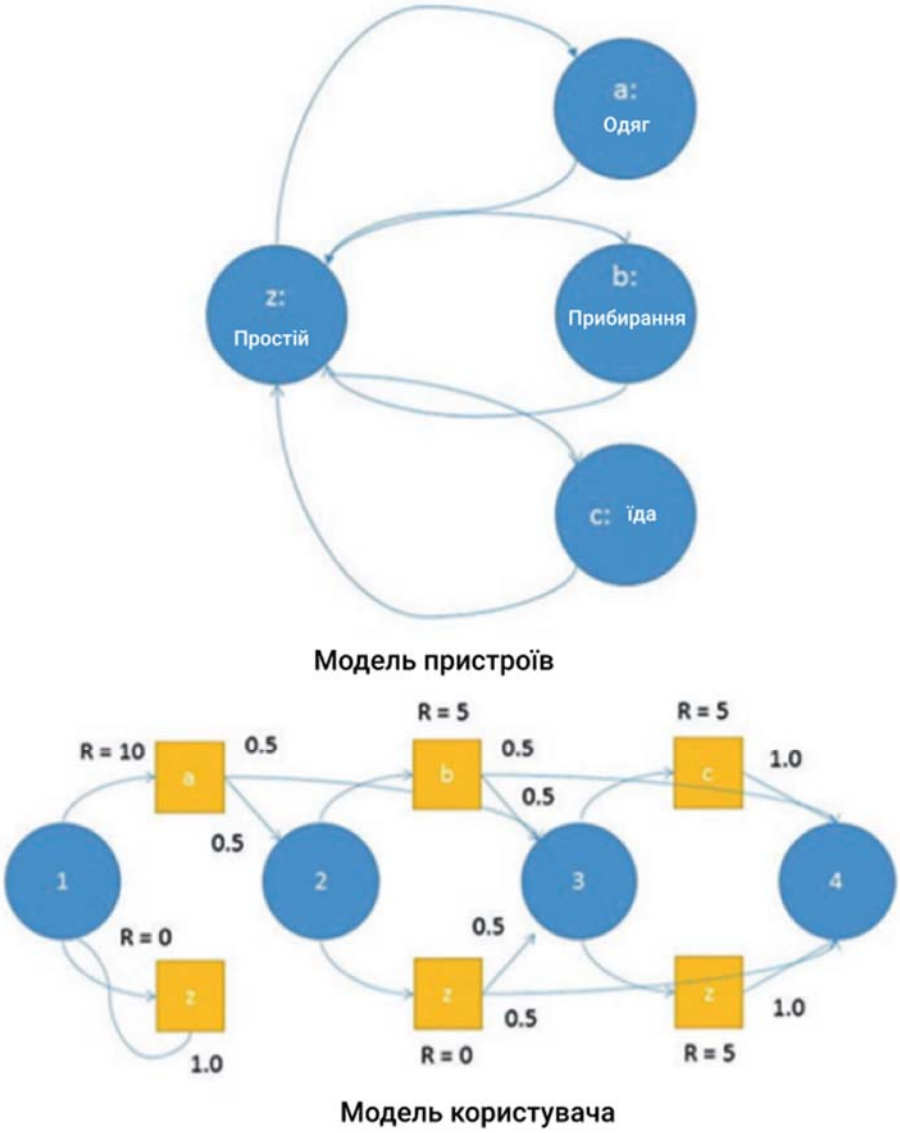


Рис. 2.8 Моделі ранкового режиму для пристроїв та мешканців

Модель пристрою поєднує дії всіх компонентних пристроїв, пов’язаних із рутиною, в єдиний автомат для простоти. Дії в користувацькій моделі MDP відповідають станам у моделі пристрою.

Ще більш складна модель використовує безперервний процес прийняття рішень Маркова (CTMDP). Найбільш поширеною математичною формою цієї моделі є MDP із термінами переходів стану, змодельованими як процес Пуассона [28]. Стандартні підходи MDP можуть бути використані для вирішення оптимального шляху із термінами, заданими процесом Пуассона.

Подія не обов'язково повинна зберігатися у концентраторі, який володіє джерелом або призначенням події. У системі з кількома концентраторами ми можемо розміщувати події на нелокальних концентраторах, щоб уникнути переповнення місткості черги концентратора або збільшити час його автономної роботи. Якщо подія знаходиться в черзі нелокально, ми повинні врахувати час передачі для її випуску, щоб переконатися, що вона досягає пристрою призначення в належний час.

Для простоти розглянемо випадок, коли витрати енергії на транспортування подій через мережу відсутні. Нехай Pe - це енергоспоживання для збереження однієї події в пам'яті протягом одиниці часу. Враховуючи сукупність подій П, енергія, необхідна для зберігання всіх подій у популяції до часу їх випуску, становить

$$E_{\text{pop}} = \sum_{e \epsilon \Pi} \left[\rho(e) - \vartheta(e) \right] P_{\text{e}}$$

Є набір концентраторів H, кожен з доступною енергією батареї Eh (i). Ми хочемо знайти такий розподіл подій для концентраторів

$$\forall i \epsilon H : E_{\text{pop}}(i) \leq E_{\text{h}}(i)$$

Це класична проблема упаковки, яку вирішуємо як розподілену проблему без централізованого переліку подій. На практиці енергія передачі зменшує набір правдоподібних розподілів подій.

Пропонується евристичний алгоритм міграції подій:

• Знаходиться часткове впорядкування концентраторів таким чином, щоб два сусідні концентратори не знаходились в одному наборі, а всі концентратори були покриті.

• Концентратори рухаються по порядку, щоб жодні суміжні концентратори не вивантажились одночасно.

• Кожен концентратор розвантажує достатньо подій, щоб задовольнити вимоги до акумулятора. Події переміщуються у сусідні концентратори з найбільшою доступною ємністю акумулятора.

Висновки

Розглянуті орієнтовані протоколи IoT, виявлені недоліки та переваги даних протоколів, розглянуто програми, що використовуються для функціонування IoT систем. Проведено обширний аналіз архітектури Індустріальної IoT системи, її рівнів та методів. Представлено моделі IoT та промодельовано мережу IoT, що взаємодіє з навколишнім середовищем.

РОЗДІЛ 3

МЕТОДИ ОРГАНІЗАЦІЇ ІНФРАСТРУКТУРИ ІНТЕРНЕТУ РЕЧЕЙ

3.1 Методи збору та аналізу даних пристроїв IoT

Потокове передавання даних IoT. В IoT кожна подія створює дані. Надсилання даних включає стандартні протоколи, такі як MQTT, WAMP, HTTP, CoAP або Sigfox. Кожен із них має свої сильні сторони та суміжні випадки використання. Ці протоколи підтримують отримання оновлень або іншої інформації з пристрою IoT для надсилання її до певного централізованого місця для фактичної обробки.

На цьому етапі вирішується, як дані агрегуються та зберігаються для подальшого використання. Як діяти відтепер, залежить від того, як будуть використовуватися дані IoT. Тут ви обираєте підхід і визначаєте, чи слід передавати дані в режимі реального часу або групами. Крім того, ви визначаєте, в якому порядку слід створювати точки даних для максимально точного аналізу.

Зберігання даних IoT. Використання даних у реальному часі гарантує максимальну точність. Цей підхід гарантує доступ до всіх даних, що генеруються кожним пристроєм IoT. Однак це зазвичай означає величезні обсяги вхідних даних. Поставити правильну позначку часу для сортування даних, що надходять з декількох пристроїв IoT, стає проблемою. Слід розглянути системи, які здатні врахувати швидкість та обсяг цих вхідних даних IoT.

Вибір методу збору всіх наявних даних IoT у режимі реального часу та їх аналіз повинен підтверджуватися чіткими обґрунтуваннями. В іншому випадку величезний обсяг даних може мати надмірно сильний вплив на хмарні системи - тобто мережеві ресурси та обчислювальні ресурси, необхідні для збереження надходження даних IoT.

Слід також розглянути конкретні програми IoT. Вони мають унікальні вимоги щодо затримки, енергоспоживання та точності. Деякі програми можуть допускати затримки. Інші, такі як програми безпеки, скоріше вважаються критично важливими для часу і не можуть мати місця для затримок.

Багато випадків використання можуть не вимагати високої точності та дозволяти надсилати дані групами. Якщо дані надсилаються пакетами або мікро-пакетами, ви все одно отримуєте запис усіх даних. Це відбувається не в реальному часі, а лише через задані заздалегідь встановлені інтервали. Вибір конкретного випадку використання залежить від вимог. У деяких сценаріях вам знадобляться точні дані в режимі реального часу для вашого аналізу. В інших сценаріях історичні дані будуть робити так само добре.

Платформовий підхід. Якщо ви плануєте безпосередньо аналізувати вхідні дані, на цьому етапі вам потрібна платформа, здатна передавати дані, що надходять з великої кількості пристроїв IoT, що передають дані в режимі реального часу. Одна з таких платформ повинна мати можливість реагувати на тимчасові проблеми з підключенням. Сюди можуть входити втрачені зв’язки, перебої в роботі або збій сервера. Платформа допомагає уникнути втрати даних. Таким чином, ви не ризикуєте погіршити точність результатів, які будуть створені на основі цих даних. На платформі дані зберігаються у готовій формі для моделювання та аналізу даних.

Цільові підходи до збору даних. У широких мазках, знову ж таки, підхід, обраний при збиранні та зберіганні даних IoT, сильно залежить від цільових потреб конкретного випадку використання. Вони передбачають, але не обмежуються ними, процедури збору даних, мотивовані такими різноманітними потребами, як точність даних, споживання енергії, час відгуку та захист конфіденційності. Перевіреними підходами до зменшення обсягів зібраних даних IoT є агрегування даних, фільтрація, інтерпретація та стиснення на рівні датчика або IoT, як можна ближче до джерела даних.

Далі ми підсумовуємо деякі ключові підходи до збору даних на основі передбачуваного застосування, як викладено в цьому дослідженні.

Стратегії, мотивовані точністю. Ця стратегія збору даних IoT враховує компроміс між частотою запитів на вимірювання та точністю даних. Тут частота адаптується з огляду на точність цільових даних. Може бути так, що даний випадок використання вимагає лише певного рівня точності даних. Більш високий рівень точності не приносить додаткових значень зусиллям. В рамках цієї стратегії потрібно зменшити частоту вимірювань даних. Це зменшує ресурси, необхідні для збору даних IoT, зберігаючи при цьому цільову точність, яка була розрахована як оптимальна для цього випадку використання.

Стратегії, мотивовані критичністю часу. При такому підході до збору даних IoT заздалегідь встановлюється максимальне значення затримки. Час, що минув з часу позначки часу останнього вимірювання, повинен залишатися нижче максимального значення затримки. У сценаріях збору даних IoT, мотивованих вимогами, пов'язаними з часом, кожне нове вимірювання, яке отримується за мінусом позначки часу останнього вимірювання, має бути нижче максимальної затримки. Таким чином, минулий час відповідає “свіжості” вимірювань даних.

Стратегії збору даних IoT, мотивовані потребами енергії. Вибираючи такий підхід, споживання енергії є ключовим фактором. Зусилля полягає в тому, щоб досягти цільової точності при оптимізації споживання енергії. Енергетична стратегія збору даних IoT націлена на максимальну ефективність. Перевага тут вимірюється як різниця між корисністю, досягнутою для певної цільової точності даних мінус енергоспоживання для вимірювань, необхідних для досягнення цієї точності даних. Подібно до сценарію, керованого точністю, тут передбачається, що залежно від програми застосовуватиметься конкретна цільова точність, знаючи, що більш висока точність не принесе жодної додаткової вигоди.

Стратегії збору даних IoT, мотивовані проблемами конфіденційності. Якщо конфіденційність кінцевих користувачів має переважне значення, можна застосувати такий підхід. Згідно з дослідженням, тут буде докладено зусиль, щоб мінімізувати кількість запитів датчика про дані та додати шум до результатів за допомогою методів конфіденційності. Мета полягає в захисті конфіденційності кінцевих користувачів шляхом зміни точності окремих вимірювань, одночасно підтримуючи певний рівень "адекватної точності" для результатів в цілому.

Додавання “шуму” до результату досягається за допомогою “різної конфіденційності”. Згідно з дослідженням, це дозволяє отримувати дані, що стосуються сукупності користувачів, не розкриваючи жодної інформації про осіб. Це завдяки додаванню «шуму» під час самого процесу вилучення даних без істотних змін статистичного результату. Цей підхід рекомендує додавати шум на етапі збору даних IoT, а не на етапі обробки даних. Супутні експерименти показують, що втручання такого роду має незначний вплив на підсумкову статистику.

Налаштування за допомогою платформи Record Evolution. Це було лише смаком різних підходів до збору даних та тенденцій збору даних IoT прямо зараз. На платформі Record Evolution студія обробки даних дозволяє підключатись до джерела даних IoT та передавати дані IoT безпосередньо в компактне полегшене сховище даних. Платформа дає змогу точно налаштувати спосіб збирання даних, а також постійно контролювати та контролювати потоки даних.

3.2 Методи організації інфраструктури IoT

Інфраструктура IoT. Організаціям слід зосередитись на семи ключових компонентах інфраструктури IoT. Якщо вони розроблять та стандартизують кожну, вони можуть максимально використати свої інвестиції в IoT.

На рисунку 3.1 можна побачити архітектуру IoT

Рис. 3.1. Компоненти архітектури безпеки IoT

Мережі IoT. Мережі підключаються до датчиків і приводів IoT. Датчики - це пристрої, які вимірюють такі фактори, як вологість, рух, температура та тиск, тоді як виконавчі механізми - це пристрої, які контролюють або вживають дії, такі як контролери, роботизовані озброєння або безпілотники. Організації зазвичай використовують бездротову мережу. Датчики та виконавчі механізми можуть покладатися на різні мережі або працювати в одній і тій же мережі, залежно від випадку використання IoT. Мережеві технології включають Wi-Fi, Bluetooth, 4G або 5G бездротові мережі. Точне проектування мережі та вибір технології є критично важливими для успішного розгортання IoT.

Шина зв'язку IoT. Часто інфраструктура IoT включає в себе шину для підключення мереж до першого набору платформ аналітики та агрегування даних. Шина спрощує зв'язок. Замість безлічі розрізнених з'єднань із платформами агрегації організації використовують загальну шину для управління та захисту всього трафіку IoT.

Платформа аналітики та агрегації. Дані датчиків і виконавчих механізмів концентруються і іноді аналізуються на крайньому обчислювальному пристрої або хмарній платформі. У деяких випадках розгортання IoT також вимагає окремих платформ для датчиків і виконавчих механізмів.

Мережа платформ IoT. Це мережа, що з'єднує платформи аналітики та агрегації з іншими платформами аналітики та візуалізації, які є ймовірними, але не виключно хмарними. Ці мережі платформ часто базуються на послугах дротового підключення з низькою затримкою та таких технологіях, як програмно-визначена глобальна мережа, оператор обміну WAN та прямі хмарні з'єднання.

Платформа для агрегації та візуалізації. Це платформа, де перебувають озера даних та аналітика. Він, як правило, заснований на хмарі і включає в себе ряд інструментів візуалізації, управління даними та аналізу даних.

Система управління та контролю. Ця інформаційна панель надає корпоративним технологам наскрізний огляд компонентів IoT та їх взаємодії з мереж та платформ.

Кібербезпека. Усі компоненти інфраструктури Інтернету речей повинні інтегруватися в платформу та структуру кібербезпеки, яка відповідає всім випадкам використання Інтернету речей та включає в себе загальну систему кібербезпеки організації.

Інші ключові компоненти, які зазвичай виконуються на платформах агрегації, аналітики та візуалізації, включають програмне забезпечення для бази даних IoT та програмне забезпечення для аналізу даних; інтеграційне програмне забезпечення, яке пов'язує інфраструктуру IoT із існуючими ERP та системами виконання виробництва; а також будь-які додатки, які застосовуються до всіх або більшості ініціатив IoT організації.

IoT система представляє гібридну архітектуру, що означає, що вона може містити різні архітектури підсистем. У більшості випадків системи IoT формуються двома архітектурами управління: керуванням подіями та часом.

Сенсори архітектури, керовані подіями, передають дані, коли вони відчувають активність у зовнішньому середовищі, наприклад, спрацьовує сигнал тривоги, якщо двері відкриваються вночі. В архітектурі, заснованій на часі, її компоненти безперервно передають дані протягом певного інтервалу (наприклад, датчики системи клімат-контролю один раз на секунду зчитують кімнатну температуру). Останні зазвичай працюють неодноразово після паузи, яку можна налаштувати окремо для кожного пристрою або налаштувати в центральній системі управління, яка через певний проміжок часу надсилатиме запити до пристроїв кінцевих точок та датчиків [29]. Одне з таких системних рішень пропонує корпорація Intel

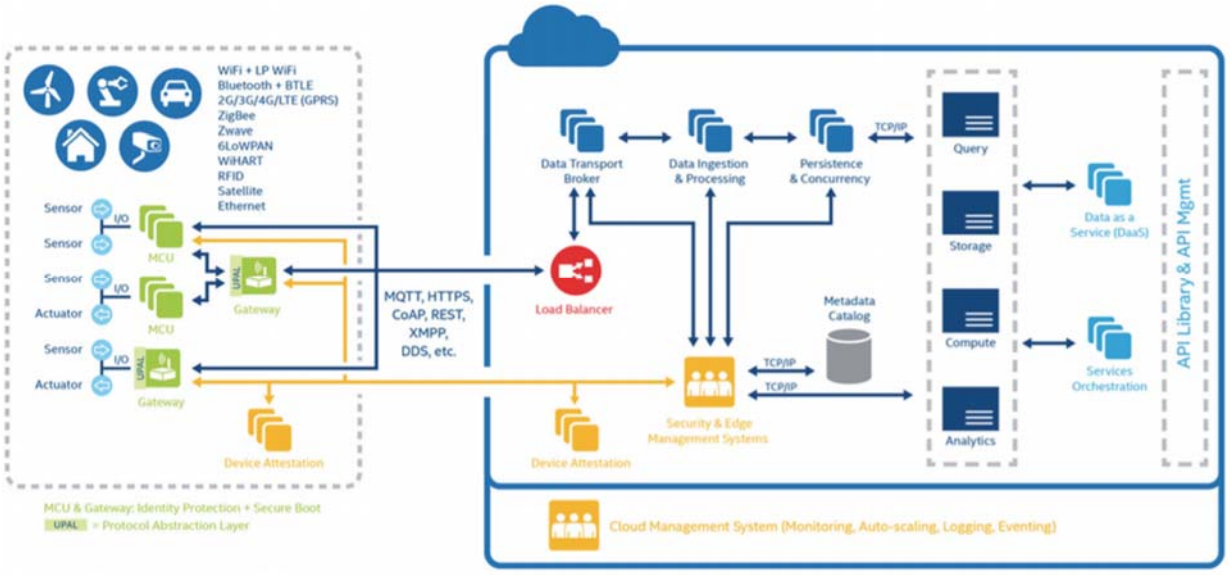


Рис. 3.2. Архітектура центральної системи управління IoT.

Архітектуру мережі можна розділити на три топології: з'єднання точка-точка, зірка та сітка. Топологія мережі точка-точка встановлює з'єднання для передачі даних між двома станціями [30].

Простота з’єднання «точка точка» - це перевага і, в той же час, обмеження поточної технології, що гарантує низьку вартість, але також позбавляє можливості дістатися до пристроїв поза мережею.

Топологія зірок складається з безлічі кінцевих вузлів і лише одного центрального концентратора. Всі вузли можуть взаємодіяти між собою, але лише передаючи або отримуючи дані через центральний концентратор. Така структура дозволяє досягти низької затримки, високої пропускної здатності і певним чином захищає систему від збоїв, коли один з вузлів перестає працювати. У порівнянні з діапазоном з'єднання «точка-точка», мережа зіркового типу все ще обмежена центральним хабом, який відключається від глобального середовища, якщо він падає.

Меш - це мережева топологія, яка використовує одну з двох децентралізованих схем підключення: топологію повної мережі або часткову топологію сітки. У топології з повною сіткою кожен вузол мережі (робоча станція чи інші пристрої) підключений до кожного з інших. У частковій топології сітки деякі вузли з'єднані з усіма, тоді інші з'єднані лише з тими вузлами, з якими вони обмінюються найбільше даних [31]. Меш мережа використовується для багатьох додатків, що вимагають великого діапазону та широкого покриття, що дозволяє створити мережу майже необмеженого розміру. Недоліком цієї топології є її складність у порівнянні з мережами типу «точка-точка» та «зірка», що може призвести до великої затримки, збільшення витрат та технічних проблем у мережі.

Передача та зберігання даних у динамічній мережі є важливими та складними проблемами. IoT може складатися з необмеженої кількості пристроїв, які інтегровані в локальні або глобальні, фізичні та бездротові мережі. Пул цих автоматизованих пристроїв та датчиків генерує та передає великі обсяги даних у режимі реального часу, що не має ніякої користі без відповідної фільтрації та обробки даних.

Мережеві протоколи. Передача даних можлива завдяки різним мережевим протоколам - набору семантичних та синтаксичних правил, що визначає активність функціональних блоків комп’ютерної мережі в процесі передачі даних. У комп'ютеризованих мережах, які побудовані відповідно до

вимог архітектури відкритої системи, протокол визначає поведінку сутності одного рівня під час передачі даних [32].

Створення мережі IoT, безумовно, не є простим завданням, особливо якщо є датчики, які не можуть бути включені в глобальну схему адрес, що заважає можливості створити повноцінний вузол датчика. Тому традиційні протоколи IP не підходять для обміну даними. Більше того, вузли IoT тісно залежать від постійних джерел енергії, пропускної здатності мережевих каналів та параметрів зберігання, що вимагає складного управління ресурсами [33]. У випадку бездротових датчиків виникає необхідність додавання радіосигналу до мережі. Вся зібрана інформація спочатку зберігатиметься у раковині та згодом надходитиме до інших вузлів мережі. Правильно підібрана стратегія передачі даних між датчиками кінцевих точок та поглиначами, їх розташування та конфігурація можуть покращити пропускну здатність мережі IoT, значно зменшити енергетичні витрати та перешкодити майже розташованим датчикам надсилати ту саму інформацію на пристрої аналізу даних [34], [35].

Передача даних у IoT - це складний процес, який може споживати велику кількість мережевих ресурсів для своїх цілей. Інформація може відрізнятися залежно від типу пристрою та протоколів передачі. Наприклад, стандарт ISO 8583, на основі якого складаються повідомлення платіжного терміналу, генерує рядок даних, що представляє платіжну транзакцію замовника (рис. 3.3).

```
0200420004000000000216123456789012345606091730301234
56789ABC1000123456789012345678901234567890123456789012
3456789012345678901234567890123456789012345678901234567
89
```

Рис. 3.3. Приклад тіла повідомлення ISO 8583.

Коротке повідомлення містить всю необхідну інформацію про платіжну картку, термінал та фінансову частину покупки. На жаль, ні людина, ні комп'ютер не можуть використовувати цю інформацію без інструкції щодо декодування. Власники системи повинні вибирати між компактними

повідомленнями в середовищі IoT, витрачаючи більше обчислювальних ресурсів на дешифрування даних або просто надсилаючи повнорозмірні повідомлення, які можуть перевантажити мережевий трафік. Зашифроване повідомлення, про яке згадувалося раніше, може виглядати твердим, але інформація, яку він містить, ніколи не може зберігатися або використовуватися для аналізу даних у вихідному вигляді. Варто продумати ефективну політику передачі даних, яка працює з готовою до використання інформацією, як новий стандарт платіжного терміналу ISO 20022 на основі розширюваної мови розмітки (XML). Створений для мережевих документів, він робить інформацію більш зручною та полегшує аналіз даних. Рисунок 3.4 містить приклад повідомлення ISO 20022.

```
<CdtTrfTxInf>
  <IntrBkSttlmAmt Ccy='USD'>12500</IntrBkSttlmAmt>
  <IntrBkSttlmDt>2009-10-29</IntrBkSttlmDt>
  <Dbtr>
    <Nm>ACME NV.</Nm>
    <PstlAdr>
      <StrtNm>Amstel</StrtNm>
      <BldgNb>344</BldgNb>
      <TwnNm>Amsterdam</TwnNm>
      <Ctry>NL</Ctry>
    </PstlAdr>
  </Dbtr>
  <DbtrAcct>
    <Id>
      <Othr>
        <Id>8754219990</Id>
      </Othr>
    </Id>
  </DbtrAcct>
  <DbtrAgt>
    <FinInstnId>
      <BIC>EXABNL2U</BIC>
    </FinInstnId>
  </DbtrAgt>
</CdtTrfTxInf>
```

Рис. 3.4. Приклад тіла повідомлення ISO 20022.

Неоднорідність пристрою IoT є однією з відмінних характеристик IoT, а також його слабким місцем. Залежно від складності архітектура IoT може включати кілька рівнів пристроїв, кожен з яких орієнтований на певний тип

виконання функції. Різниця полягає не тільки в переданих протоколах, але в основному в хитросплетінні пристроїв, що безпосередньо відображає рівень використання обчислювальних ресурсів та обсяг даних, що передаються через них. Він розділив архітектуру IoT на кілька рівнів, де найнижчий рівень неоднорідності по вертикалі містить пристрої / датчики кінцевих точок, які працюють із зовнішнім середовищем, і, рухаючись вгору, можна досягти найскладніших маршрутизуючих та обчислювальних пристроїв (див. Рис. 3.5). В оптимізованих системних архітектурах кожен наступний рівень повинен містити менше пристроїв.

Рис. 3.5. Вісь неоднорідності IoT

Неоднорідність IoT передбачає різні пристрої: персональні апаратні засоби користувача, датчики, маршрутизатори, комутатори, концентратори,

бази даних, обчислювальні сервери тощо. У IoT кожен пристрій виконує певну роль і виконує лише необхідні функції, щоб не перевантажувати систему. З іншого боку, багато пристроїв виконують більше однієї функції, яка іноді може бути подібною або навіть перекриватися функціональністю інших пристроїв, що дозволяє їм замінювати одне одного у разі надзвичайної ситуації. Опускаючи деталі, всі пристрої можна розділити на три категорії: пристрої кінцевих точок, інструменти введення-виведення та обчислювальні машини. Пристрої кінцевих точок прослуховують команди виконання від зовнішніх подразників (наприклад, повідомлення від смартфона користувачів) або основного блоку (команда від Cron) і генерують дані залежно від отриманих параметрів. У більшості випадків пристрої кінцевих точок важко налаштувати, не кажучи вже про втручання на рівні програмування. Пристрої вводу-виводу обмежені з точки зору обчислювальних ресурсів, тому вони в основному виконують роль посередника між пристроями кінцевої точки та машинами вищого рівня. Остання категорія пристроїв відповідає за ресурсомістку фільтрацію та обробку даних. Варто згадати, що всі три типи можуть брати участь у мережі IoT як окремі фізичні пристрої, обидва вони виступають як внутрішні логічні вузли одного пристрою, але це залежить від складності системи IoT або ускладнення самого пристрою.

3.3 Види тестування Інтернету Речей

Щоб гарантувати якість продуктів і послуг Інтернету Речей необхідно розробити такі рішення для тестування, як:

1) Продумана стратегія тестування. Потрібно зосередитися на ефективних методах та практиках тестування. Чіткі вимоги, детальний план випробувань повинні бути частиною цієї стратегії, що дозволить в подальшому випустити якісний продукт або послугу.

2) Нові інструменти і платформи тестування. Нові платформи будуть необхідні для отримання корисної інформації з величезного кількості необроблених даних, забезпечуючи при цьому основу для систем технічної підтримки підтримки. Також знадобляться додаткові інструменти, утиліти та симулятори для тестування, так як в іншому випадку цей процес буде перешкодою.

3) Тестування методом «чорного ящика». Для розробки ефективних тестів потрібно вміти виявити архітектуру пристрою, тип операційної системи, протоколи взаємодії без знання внутрішніх механізмів тестувального об'єкта (рис. 3.6).

Рис. 3.6. Тестування методом «чорного ящика»

Аналіз методів і видів тестування Інтернет Речей. Рекомендація МСЕ-Т Q.3900 «Архітектура модельної мережі і методи тестування технічних засобів мереж зв'язку нового покоління (NGN) для використання в мережах зв'язку загального користування» ", випущена в 2006 р, стала основним стандартом для тестування NGN-мереж [36]. Дану концепцію можна використовувати і

щодо тестування Інтернету Речей, однак, рекомендаціях Q.3900 не визначає структуру IoT-тестування. Як вже було сказано, тестування Інтернет Речей так чи інакше відноситься до перевірки різних аспектів, що стосуються функціонування самих пристроїв, їх взаємодії з мережею і безпеки. Проблеми тестування виходять за рамки пристроїв і датчиків, так як включають в себе додаткові складності, пов'язані з концепцією великих даних, тобто великий обсяг і різноманітність інформації, що генерується. Окрім цього, на даний момент, не існує єдиного підходу до тестування пристроїв Інтернету речей, які існують для візлів мережі зв’язку наступного покоління. Таким чином, створення модельної мережі та різних методів тестування допоможе вирішити цю проблему.

На даний момент існує чотири основні області тестування IoT-пристроїв, які повинні враховуватися при розробці будь-якого продукту, який має можливість підключення до мережі Інтернет. Вони приведені на рисунку 3.7.

Рис. 3.7. Області тестування Інтернету Речей

Процес тестування вкрай важливий. Внаслідок цього необхідно використовувати спеціальні симулятори, які можуть імітувати роботу мережевих вузлів і пристроїв Інтернету Речей, що дозволить скоротити витрати на обладнання. В цілому, питання, що стосуються тестування охоплюють велику область, починаючи з самих пристроїв, всіляких датчиків і закінчуючи різними платформами, які збирають і аналізують дані Інтернету Речей. Крім тестування пристроїв фізичного світу, також є певні види тестування віртуальних Речей. Віртуальні Речі існують в інформаційному світі, їх можна зберігати, обробляти і отримувати до них доступ. Прикладом таких речей є прикладне ПО та мультимедійний контент.

Найбільш поширені методи для тестування ПО:

1) Модульне тестування. В даному методі з метою виявлення можливих помилок компоненти програми перевіряються окремо. При цьому необхідно добре знати склад програми, отже, цей вид тестування здійснюється програмістами, а не тестувальниками.

2) Інтеграційне тестування. В основному виявляє помилки інтерфейсу. Компоненти програми, які були перевірені в ході модульного тестування, інтегруються один з одним, а потім тестуються на наявність несправностей.

3) Системне тестування. На даному етапі аналізується робота всієї системи в цілому при взаємодії її апаратних і програмних складових.

Види тестування Інтернету Речей. В даному пункті будуть розглянуті деякі види тестування, котрі проводяться тестувальниками для забезпечення стабільної роботи IoT-систем (рис. 3.8).

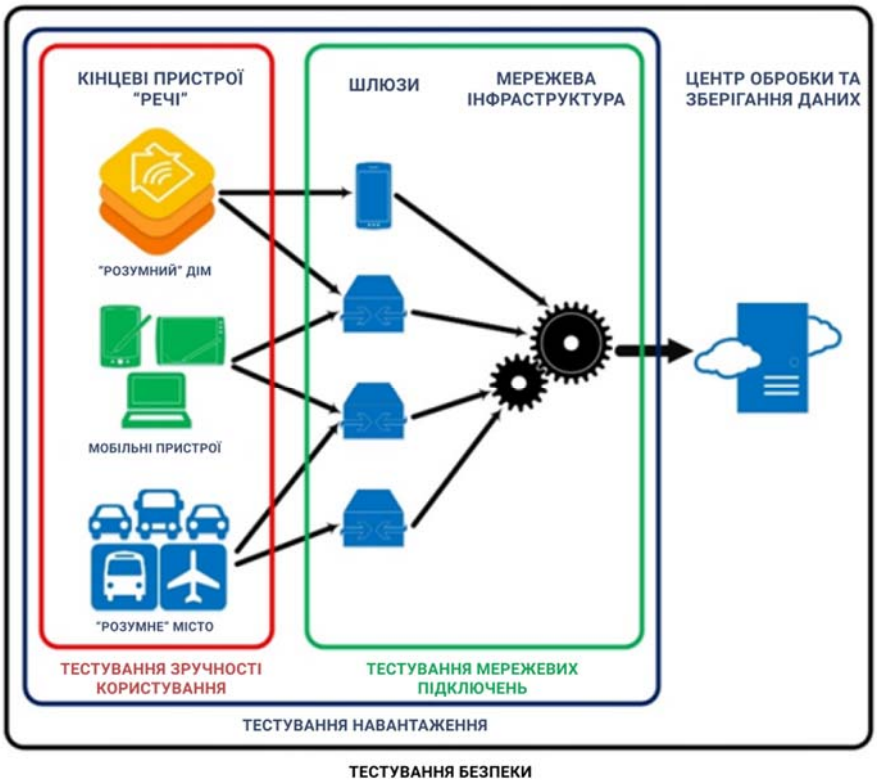


Рис. 3.8. Види тестування Інтернету Речей

Тестування зручності користування (Usability Testing). Перш за все, функціональні можливості Інтернету Речей повинні відповідати вимогам користувача. Найбільш важливим моментом є те, що споживач зміг би виявити

всі властивості і особливості продукту без будь-яких проблем. Цей метод тестування спрямований на встановлення ступеню зручності використання, навченості, зрозумілості та привабливості розробляємого продукту для користувачів. Для того, щоб провести таке тестування, потрібно відібрати групу людей, які відповідають певним критеріям (стать, вік, рід діяльності), і провести серед них невелике опитування. Це дозволить отримати оцінки та відгуки щодо використання будь-якого продукту, що в подальшому допоможе підвищити його якість.

Тестування мережевих підключень (Connectivity Testing). Інтернет Речі повинні взаємодіяти один з одним, тому необхідно звернути увагу на різні способи зв'язку, а також на обмін інформацією між пристроями і користувачами. В ході тестування мережевих підключень важливо враховувати середу, в якій буде використовуватися пристрій (тип мережі, потужність сигналу, погодні умови і т. д.), і перевіряти те, як вона функціонує при заданих умовах.

Висновки

Проаналізовано та представлено методи збору та аналізу даних пристроїв IoT. Представлено метод організації інфраструктури IoT. Представлено різні види тестування IoT.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У роботі проведено аналіз стану IoT систем, їх можливості, перспективи і проблематика. Висвітлено такі можливості: зондування місцезнаходження та обмін інформацією про місцезнаходження; відстеження мобільних активів; управління системами телекомунікацій та дорожньої інфраструктури; аналіз довкілля; віддалений медичний моніторинг, тощо. Було розібрано такі проблематики систем IoT, як архітектурна, технічна, апаратна, бізнесу, проблематика стандартизації, конфіденційності та безпеки. Проаналізовано існуючі рішення розгортоння IoT систем, архітектуру та протоколи, що використовуються в IoT. Висвітлено архітектуру програмного забезпечення для системи публікації/підписки, протоколи для цієї системи в реальному часі, архітектуру чутливих до часу систем, протоколи MQTT, XMPP, CoAP та низько енергозатратний Bluetooth (BLE) Представлено архітектуру та модель Індустріального IoT та його робота з навколишнім середовище, концепції та еволюцію Індустріального IoT, починаючи від стратегії Industrie 4.0 і переходячи до Індустріального Інтернету. Було проведено повний аналіз стратегічної ініціативи Industrie 4.0, приведено приклади еволюції цієї стратегії. Описані досягнення сенсорних технологій, розумні концепції IoT систем в промисловості. Представлено та описано методи зв'язку для пристроїв IoT, метод посилань на IoT модель ITU, бізнес моделі IoT, визначені MCE, функціональні домени довідкової архітектури IIC, моделі для пристроїв та мешканців розумного будинку. Проаналізовано мережі IoT та методи організації інфраструктури. Представлено можливі методи збору та збереження даних в пристроях IoT, розглянуто такі підходи як, платформовий, цільовий та стратегії, що мотивовані точністю, критичністю часу, потребами в енергії, проблемами конфіденційності. Представлено організацію інфраструктури з семи ключових компонентів. Описана передача та зберігання даних у динамічній мережі, проблематика створення мережі IoT, передача даних у IoT

та слабкі місця пристроїв IoT - їх неоднорідність. Проаналізовані та представлені види та методи тестування Інтернету Речей, такі як тестування методом «чорного ящика», модульне тестування, інтеграційне тестування, системне тестування, тестування зручності користування та тестування мережевих підключень, стратегії тестування, нові інструменти і платформи тестування

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Дж. А. Станкович, “Напрямки досліджень Інтернету речей”, IEEE Internet Things J., vol. 1, № 1, с. 3–9, лютий 2014 р.

2) “Умови повсюдної мережі”, Стандарт CCSA YDB 062-2011, бер. 2011 рік.

3) "Огляд IoT", стандарт MCE-T Y.2060, червень 2012 р.

4) I. M. Сміт та ін., “RFID та інклюзивна модель для IoT”, CASAGRAS Partnership Rep., West Yorkshire, UK, Final Rep., 2009, pp. 10–12.

5) G. M. Lee et al., “The IoT - Поняття та Постановка проблеми”, Стандартний проект IETF-lee-iot-problem-statement-05, 30 липня 2012 р.

6) Т. Лю та Д. Лу, “Застосування та розвиток IoT”, у Proc.Int. Симп. Інф. Технол. Мед. Освіт. (ITME), 2012, вип. 2, с. 991–994.

7) J. Huang et al., "Нова схема розгортання зеленого Інтернету речей", IEEE Internet Things J., vol. 1, № 2, с. 196–205, квітень 2014 р.

8) Міністерство промисловості та інформаційних технологій Китаю (2012, лютий). Національний 12-й п’ятирічний план, що включає розвиток IoT (2011–2015) [Інтернет]. Доступно: http://www.gov.cn/zwgk/2012-02/14/content 2065999.htm

9) Група управління об’єктами. (2014). Специфікація протоколу оперативної сумісності DDS протоколу публікації-передплати (RTPS), версія 2.2.

10) Група управління об’єктами. (2016). Що таке DDS? http://portals.omg.org/dds/what-isdds-3/, доступ 4 травня 2017 року.

11) Альянс Zigbee (2014, 2 грудня). ZigBee 3.0: відкритий глобальний стандарт Інтернету речей. http://www.zigbee.org/zigbee-for-developers/zigbee/

12) Дж. Губбі та ін., “IoT: бачення, архітектурні елементи та майбутні напрямки”, Future Gener. Обчислення. Сист., Вип. 29, ні. 7, с. 1645–1660, вересень 2013 р.

13) К. Янг та З. Чжан, “Підсумок щодо Інтернету речей та дослідження в технічній системі”, в Proc. IEEE Symp. Робот. Заяв. (ISRA), 2012, с. 653–656.

14) А. М. Ортіс та ін., “Кластер між Інтернетом речей та соціальними мережами: огляд та наукові завдання”, IEEE Internet Things J., vol. 1, № 3, с. 206–215, червень 2014 р.

15) А. Занелла та ін., “Інтернет речей для розумних міст”, IEEE Internet Things J., vol. 1, № 1, с. 22–32, лютий 2014 р.

16) П. Влачеас та ін., “Сприяння розумним містам через систему когнітивного управління Інтернетом речей”, IEEE Commun. Маг., Вип. 51, ні. 6, с. 102 111, червень 2013.

17) Т. Чжан та ін., “Захист підключених транспортних засобів від шкідливих програм: виклики та рамки рішень”, IEEE Internet Things J., vol. 1, № 1, с. 10–21, лютий 2014 р.

18) Дж. Ян та З. Фей, “Мовлення з прогнозуванням та вибірковим переадресацією в транспортних мережах”, Міжнар. Дж. Розподілити. Датчик мережі, вип. 2013, с. 1–9, 2013.

19) Р. Краненбург та А. Бассі, “Проблеми IoT”, Commun. Mobile Comput., Vol. 1, № 1, с. 1–5, 2012.

20) Ю. Чень та співавт., “Безпроводова парадигма із зворотною зміною часу для зеленого Інтернету

Речі: огляд, ”IEEE Internet Things J., vol. 1, № 1, с. 81–98, лютий 2014 р.

21) S. Lanzisera et al., "Комунікаційні джерела живлення: підведення Інтернету до повсюдних енергетичних шлюзів електронних пристроїв", IEEE Internet Things J., vol. 1, № 2, с. 153–160, квітень 2014 р.

22) Х. Нін та ін., "Безпека кібернетичності в Інтернеті речей", Комп'ютер, вип. 46, ні. 4, с. 46–53, квітень 2013 р.

23) Х. Нін і З. Ван, “Майбутня архітектура IoT: як нейронна система людства або система соціальної організації”, IEEE Commun. Lett., Vol. 15, № 4, с. 461–463, квітень 2011 р.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Аналіз використання технологій інтернету речей у виробничому секторі

ВИКОНАВ - КОЛОСОВ КОСТЯНТИН АНАТОЛІЙОВИЧ
КЕРІВНИК РОБОТИ - СТ. ВИКЛАДАЧ КАФ. СА
КОРЕЦЬКИЙ ОЛЕКСАНДР ВАЛЕРІЙОВИЧ

Актуальність роботи

Технічна революція, яка з кожним днем еволюціонує та стрімкий розвиток мобільних технологій сприяє розвитку Інтернету Речей. Зростання кількості фізичних пристроїв, що взаємодіють з інтернетом, підштовхує до реалізації Інтернету Речей. На сьогодні застосування систем IoT, можна знайти в безлічі галузях промисловості Пристрої, що підключені до Інтернету, є основою для розвитку проектування розумних міст. Застосування систем Інтернету Речей, звісно має переваги, але і недоліки у вигляді загрози їх неправомірного використання, такі як вторгнення у приватне життя людини, загроза збору та використання персональних даних в особистих цілях, кібернетична загроза, тощо.

Мета, об'єкт, предмет дослідження

Метою роботи є удосконалення методів організації інфраструктури IoT

Задачі дослідження:

- провести аналіз технологій IoT

- провести аналіз сучасного розвитку IoT

- проаналізувати існуючі моделі IoT

- удосконалити методи організації інфраструктури IoT

Об’єкт дослідження: методи організації інфраструктури Інтернету Речей

Предмет дослідження протоколи методів збору та передачі інформації.

Аналіз можливостей IoT

1) Зондування місцезнаходження та обмін інформацією про місцезнаходження: IoT система може збирати інформацію про місцезнаходження терміналів IoT і кінцеві вузли, а потім надавати послуги на основі зібраної інформації про місцезнаходження. Інформація про місцезнаходження включає інформацію про географічне положення, отримане від GPS, RFID тощо, а також абсолютну або відносну інформацію про місцезнаходження між речами.

2) Зондування навколишнього середовища: система IoT може збирати і обробляти всі види параметрів фізичного або хімічного середовища через локально або широко розгорнуті термінали. Типова екологічна інформація включає температуру, вологість, шум, видимість, інтенсивність світла, спектр, випромінювання, забруднення (CO, CO2 та ін.), зображення та показники тіла.

3) Дистанційне управління: системи IoT можуть керувати IoT терміналами та виконувати функції на основі команд додатків у поєднанні з інформацією, зібраною з речей та вимоги до обслуговування.

4) Спеціальна мережа: система IoT повинна мати швидко самоорганізовану мережеву здатність і може взаємодіяти з мережевим/сервісним рівнем для надання супутніх послуг.

5) Безпечне спілкування: система IoT повинна встановлювати захищений канал передачі даних з додатком

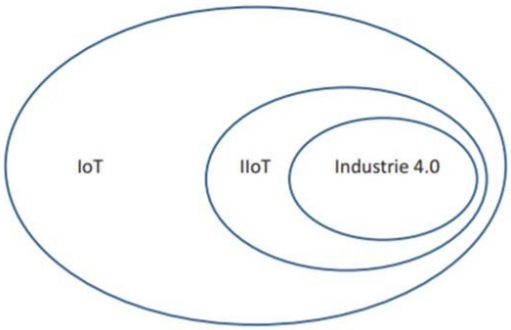
Перспективи IoT

Взаємодія: Інформаційна сумісність матиме місце між різними речами, різними підприємствами, різними галузями та різними регіонами чи країнами

Інтелектуальна система: Системний інтелект буде важливим для розвитку IoT, а ключовим моментом буде обізнаність щодо контексту та обмін інформацією між речами

Енергетична стійкість: У майбутньому енергоефективні та самостійні системи будуть ключовими питаннями, що сприяють підвищенню рівня IoT

Аналіз архітектури та моделі Індустріального IoT



Індустріальний Інтернет речей (IIoT) склався як загальна концепція застосування Інтернету речей до промислового сектору. Фактично, це узагальнення Industrie 4.0, яке більше зосереджується на ефективності промислових процесів .

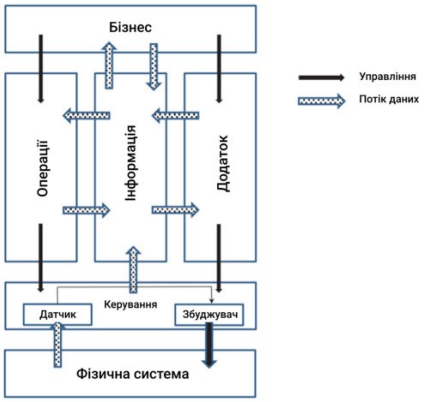
IIoT включає всі аспекти промислових операцій, зосереджуючи увагу не тільки на ефективності процесів, але й на управлінні активами, обслуговуванні тощо.

Методи зв'язку для пристроїв IoT

Модель зв'язку між пристроями розглядає три методи зв'язку, засновані на використанні шлюзів (G) та використанні мережі зв'язку (CN).

Пристрої можуть взаємодіяти:
1) без використання шлюзів, безпосередньо,
2) через локальні мережі та / або через мережу зв'язку,
3) через мережу зв'язку, що використовує шлюзи.

Розкладання функціонального представлення системи IIoT на п’ять доменів

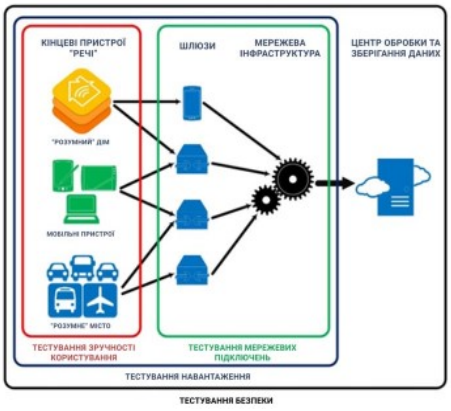


Для вирішення питання інтеграції Інформаційних Технологій та Операційних Технологій в уніфікованій моделі системи IIoT представлено п’ять доменів, кожен з яких групує функціональні можливості, необхідні для логічно виразної роботи системи на високому рівні.
Ці п’ять доменів є
(а) контролем,
(б) операціями,
(в) інформацією,
(г) додатком,
(е) бізнесом.

Організація інфраструктуриIoT

Залежно від складності архітектура IoT може включати кілька рівнів пристроїв, кожен з яких орієнтований на певний тип виконання функції. Різниця полягає не тільки в переданих протоколах, але в основному у взаємодії пристроїв, що безпосередньо відображає рівень використання обчислювальних ресурсів та обсяг даних, що передаються через них.

Області тестування Інтернету Речей



Висновки

У роботі проведено аналіз стану IoT систем, їх можливості, перспективи і проблематика

Висвітлено такі можливості: зондування місцезнаходження та обмін інформацією про місцезнаходження; відстеження мобільних активів; управління системами телекомунікацій та дорожньої інфраструктури; аналіз довкілля; віддалений медичний моніторинг, тощо.

Було розібрано такі проблематики систем IoT, як архітектурна, технічна, апаратна, бізнесу, проблематика стандартизації, конфіденційності та безпеки.

Проаналізовано існуючі рішення розгортання IoT систем, архітектуру та протоколи, що використовуються в IoT.

Висвітлено архітектуру програмного забезпечення для системи публікації/підписки, протоколи для цієї системи в реальному часі, архітектуру чутливих до часу систем, протоколи MQTT, XMPP, CoAP та низько енергозатратний Bluetooth (BLE).

Представлено архітектуру та модель Індустріального IoT та його робота з навколишнім середовищем, концепції та еволюцію Індустріального IoT, починаючи від стратегії Industrie4.0 і переходячи до Індустріального Інтернету. Було проведено повний аналіз стратегічної ініціативи Industrie4.0, приведено приклади еволюції цієї стратегії.

Описані досягнення сенсорних технологій, розумні концепції IoT систем в промисловості

Представлено та описано методи зв'язку для пристроїв IoT, метод посилань на IoT модель ITU, бізнес моделі IoT, визначені MCE, функціональні домени довідкової архітектури IIC, моделі для пристроїв та мешканців розумного будинку.

Проаналізовано мережі IoT та методи організації інфраструктури. Представлено можливі методи збору та збереження даних в пристроях IoT, розглянуто такі підходи як, платформовий, цільовий та стратегії, що мотивовані точністю, критичністю часу, потребами в енергії, проблемами конфіденційності. Представлено організацію інфраструктури з семи ключових компонентів. Описана передача та зберігання даних у динамічній мережі, проблематика створення мережі IoT, передача даних у IoT та слабкі місця пристроїв IoT - їх неоднорідність

Проаналізована та представлені види та методи тестування Інтернету Речей, такі як тестування методом «чорного ящика», модульне тестування, інтеграційне тестування, системне тестування, тестування зручності користування та тестування мережевих підключень, стратегії тестування, нові інструменти і платформи тестування