Тема 3. Стандарти сумісності IoT. Еталонні моделі IoT

Найближчим часом різнорідні «острівці» рішень, швидше за все, будуть випереджати в своєму розвитку розгортання IoT-рішень, заснованих на функціонально-сумісних стандартах. Так йдуть справи з будь-якою новою технологією на етапі її зародження.

Наприклад, Sutaria and Govindachari відзначають, що дві характеристики мережевих IoT-пристроїв, що викликають найбільші проблеми, - це наявність пристроїв з низьким енергоспоживанням (розрахованих на роботу місяцями і роками без підзарядки) і частий обмін даними по мережах з втратою пакетів.

Нинішні стандартні протоколи Інтернету в цих умовах неоптимальні.

У більш широкому сенсі має місце дисбаланс між величезною кількістю пристроїв, що генерують дані з шаленою швидкістю в різних місцях, і використанням мережевих технологій і хмарних систем, які зберігають величезні обсяги даних в невеликій кількості локацій при відносно низькій швидкості оновлення даних.

Інтеграція цих двох класів систем для задоволення потреб користувачів вимагає певних можливостей від мережевих протоколів у всій архітектурі мережі і протоколів, від фізичного рівня до прикладного.

Над вирішенням цих питань працює кілька організацій і стандартизаційних форумів, прагнучі розширити або адаптувати протоколи Інтернету для пристроїв IoT. Основники організаціями є:

– Міжнародний союз електрозв’язку (International Telecommunication Union, ITU): 193 країни і понад 700 членів по секторам і асоціаціям (науково-промислових підприємств, державних і приватних операторів зв'язку, радіомовних компаній, регіональних і міжнародних організацій).

– Всесвітній форум IoT (IoT World Forum, IWF): IBM, Intel, Cisco, Samsung.

– Національний інститут стандартів і технології Міністерства торгівлі США.

– Консорціум індустріального Інтернету (Industrial Internet Consortium,IIC): SAP, IBM, Intel, Fujitsu, General Electric, Oracle.

Для створення єдиної структури і класифікації необхідних функцій за їх місцем в стеку протоколів ряд цих груп також займається питанням формальної архітектури для IoT. У той час як існуючі стандарти та Інтернет зробили IoT можливим, в найближчому майбутньому навряд чи можлива поява стека нових стандартів, які доповнять або модифікують існуючі для сфери IoT.

Як і багато інших досягнень, що стали можливими завдяки Інтернету, IoT буде якийсь час стихійно розвиватися і проходити через процеси природного відбору, поки поступово не виявили життєздатні технології та механізми протоколів.

Але з урахуванням складності IoT має сенс створення архітектури, яка б специфікувала основні компоненти і їх взаємозв'язок. Архітектура IoT може надати такі переваги:

– дати адміністраторам мережі або IT-менеджеру корисний контрольний список для оцінки функціональності і повноти пропозицій від різних постачальників;

– служити орієнтиром для розробників в плані того, які функції потрібні в IoT і як вони взаємодіють;

– служити основою для стандартизації, стимулюючи сумісність і скорочення витрат.

Еталонна модель IoT від MCE-T

Еталонна модель IoT від Міжнародного союзу електрозв’язку (MCE-T) описана в Рекомендації Y.2060. На відміну від більшості інших еталонних моделей і архітектурних моделей, описаних в літературі, модель MCE-T деталізує фактичні фізичні компоненти екосистеми IoT. Це корисно, тому що це зосереджує увагу на елементах екосистеми IoT, які повинні бути з'єднані, інтегровані, керовані і надані додаткам. Детальна специфікація екосистеми описує вимоги до можливостей IoT.

Один з важливих аспектів, який загострює модель, є той факт, що IoT на ділі не є мережею фізичних речей. Це скоріше мережа пристроїв, які з'єднано фізичними речами, разом з прикладними платформами - такими як комп'ютери, планшети і смартфони, які взаємодіють з цими пристроями. Тому огляд моделі MCE-T необхідно почати з визначення пристроїв:

- Мережа зв'язку (Communication Network) – інфраструктурна мережа, що з'єднує пристрої та додатки, така як мережа на основі стека протоколів IP або Інтернет.
- Річ (Thing) – предмет фізичного світу (фізичні речі) або інформаційного світу (віртуальні речі), який може бути ідентифікований та інтегрований в мережі зв'язку.
- Пристрій (Device) – елемент обладнання, який володіє обов'язковими можливостями зв'язку та додатковими можливостями вимірювання, спрацьовування, а також введення, зберігання і обробки даних.
- Пристрій переносу даних (Data-carrying Device) – пристрій переносу даних підключається до фізичної речі і непрямим чином з'єднує цю фізичну річ з мережами зв'язку. Прикладами можуть служити активні мітки RFID.
- Пристрій збору даних (Data-capturing Device) – під пристроєм збору даних розуміється пристрій, що зчитує / записуючий пристрій, що має можливість взаємодії з фізичними речами. Взаємодія може здійснюватися непрямим чином за допомогою пристроїв перенесення даних або безпосередньо за допомогою носіїв даних, підключених до фізичних речей.
- Носій даних (Data Carrier) – безбатарейний об'єкт перенесення даних, підключений до фізичної речі і має можливість надавати інформацію придатному для цього пристрою збору даних. Ця категорія включає штрих-коди і QR-коди, наклеєні на фізичні речі.

– Сенсорний пристрій (Sensing Device) – пристрій, який може виявляти або вимірювати інформацію, що відноситься до навколишнього середовища, і перетворювати її в цифрові електричні сигнали.
– Виконавчий пристрій (Actuating Device) – пристрій, який може перетворювати цифрові електричні сигнали, що надходять від інформаційних мереж, в дії.
– Пристрій загального призначення (General Device) – пристрій загального призначення володіє вбудованими можливостями обробки і зв'язку і може обмінюватися даними з мережами зв'язку з використанням дротових або бездротових технологій. Пристрої загального призначення включають обладнання та прилади, які стосуються різних галузей застосування IoT, наприклад, верстати, побутові електроприлади і смартфони.
– Шлюз (Gateway) – елемент IoT, що з'єднує пристрої з мережами зв'язку.

Він виконує необхідну трансляцію між протоколами, що використовуються в мережах зв'язку і в пристроях.

Унікальним аспектом IoT, в порівнянні з іншими мережевими системами, очевидно є наявність безлічі фізичних речей і пристроїв, відмінних від обчислювальних пристроїв і пристроїв обробки даних.

На рис. 3.1, адаптованому з Рекомендації Y.2060, зображені типи пристроїв в моделі MCE-T. Модель розглядає IoT як мережу пристроїв, тісно пов'язаних з речами. Сенсорні і виконавчі пристрої взаємодіють з фізичними речами в навколишньому середовищі. Пристрої збору даних зчитують дані з фізичних речей або записують дані на фізичні речі шляхом взаємодії з пристроями перенесення даних або носіями даних, підключеними або пов'язаними з фізичним об'єктом тим чи іншим чином.

Ця модель показує відмінність між пристроями перенесення даних і носіями даних. Пристрій переносу даних є пристроєм в сенсі Рекомендації Y.2060. Як мінімум, пристрій завжди має можливості зв'язку і може мати інші електронні можливості. Прикладом пристрою перенесення даних є RFID-мітка.

У той же час носій даних – це елемент, приєднаний до фізичної речі з метою ідентифікації або інформування.

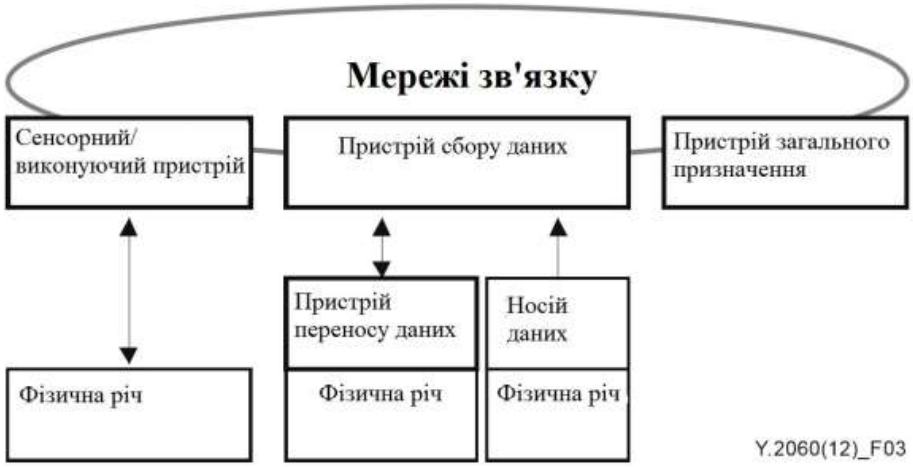

Рисунок 3.1 – Типи пристроїв та їх взаємозв’язок із фізичними речами

В рекомендації Y.2060 відзначається, що технології, які використовуються для взаємодії між пристроями збору даних і пристроями перенесення даних або носіями даних, включають радіочастотне, інфрачервоне, оптичне і гальванічне збудження. Приклади кожної з них:

– Радіочастотні: радіочастотні ідентифікаційні (RFID) - бірки, або радіопозначки.
– Оптичні: штрих-коди і QR-коди можуть служити прикладами ідентифікаційних носіїв даних, які зчитуються оптично.
– Інфрачервоні: інфрачервоні мітки, що можна використовувати в Збройних Силах, лікарнях та інших середовищах, де потрібно відстежувати розташування і переміщення персоналу. Це можуть нашивки на військовій формі, що відбивають світло, і такі, що працюють від батарейок та випромінюють ідентифікуючу інформацію.

Останні можуть мати кнопку, при натисканні якої бейдж може використовуватись для проходу через автоматичні контрольні пункти, або ж бейджи, що автоматично повторюють сигнал для контролю за переміщеннями персоналу.

Пульти дистанційного керування, що використовуються в побуті або в інших середовищах для управління електронними пристроями, теж можна легко інтегрувати в IoT.

Гальванічне збудження: прикладом можуть служити медичні імпланти, які використовують електропровідні властивості людського тіла. В ході комунікації між імплантом і поверхнею гальванічна пара передає сигнали з імпланта на електроди, виведені на шкіру. Ця схема використовує дуже мало енергії, що дозволяє знизити розмір і складність імплантованого пристрою.

Останнім типом пристроїв з рисунку є пристрої загального призначення.

Вони володіють можливостями обробки даних і зв'язку, які можуть бути інтегровані в IoT. Хорошим прикладом є технологія «розумного будинку», яка може інтегрувати практично будь-який пристрій в будинку в мережу для централізованого або дистанційного керування.

В Рекомендації Y.2060 наведено огляд елементів, задіяних в IoT. Розглядаються різні способи зв'язку з фізичними пристроями. Передбачається, що одна або кілька мереж підтримують зв'язок між пристроями.

В рекомендації особливу увагу приділено такому простою, пов'язаному з IoT: шлюзу. Як мінімум шлюз працює транслятором між протоколами. Шлюзи вирішують одну з головних проблем при проектуванні IoT, а саме проблему сумісності, як між різними пристроями, так і між пристроями та Інтернетом або корпоративною мережею.

«Розумні» пристрої підтримують широкий спектр бездротових і дротових технологій передачі даних і мережевих протоколів. Крім того, можливості обробки даних у таких пристроїв, як правило, обмежені.

Рекомендація Y.2067 закріплює вимоги до шлюзів IoT, які зазвичай розпадаються на три категорії:

– Шлюз підтримує різні технології доступу до пристроїв, дозволяючи пристроїв обмінюватися даними один з одним і з мережею Інтернет або корпоративною мережею, що містить додатки IoT. Такі схеми доступу можуть, наприклад, включати ZigBee, Bluetooth і Wi-Fi.

– Шлюз підтримує необхідні мережеві технології як для локальних, так і для глобальних мереж. Ці технології можуть включати в себе Ethernet і Wi-Fi на території організації, а також стільниковий зв'язок, Ethernet, DSL і кабельний доступ до Інтернету і глобальним корпоративним мережам.
– Шлюз підтримує взаємодію з додатками, управління мережею і функції безпеки.

Дві перших вимоги включають в себе трансляцію протоколів між різними мережевими технологіями і стеками протоколів.

Третя вимога зазвичай називається функцією IoT-агента. По суті, IoT-агент надає функціональність високого рівня від імені IoT-пристроїв, таку як організація або резюмування даних з декількох пристроїв для передачі в IoT-додатки, забезпечення протоколів і функцій безпеки і взаємодія з системами управління мережею.

Термін «мережа зв'язку» прямо не визначається в серії IoT-стандартів Y.206x. Мережа (або мережі) зв'язку підтримує зв'язок між пристроями і може безпосередньо підтримувати прикладні платформи. Вона може мати розміри невеликого IoT, такого як домашня мережа «розумних» пристроїв. У більш загальному сенсі мережу (або мережі) пристроїв з'єднується з корпоративними мережами або Інтернетом для зв'язку з системами додатків і серверами, на яких розташовані бази даних, пов'язані з IoT.

В рекомендації розглядаються також можливості зв'язку пристроїв між собою.

– Перша можливість - зв'язок між пристроями через шлюз. Наприклад, за допомогою шлюзу сенсорне або виконавчий пристрій з підтримкою Bluetooth може здійснювати зв'язок з пристроєм збору даних або пристроєм загального призначення, що використовують Wi-Fi.
– Друга можливість - зв'язок по мережі зв'язку без шлюзу. Наприклад, якщо всі пристрої в мережі «розумного будинку» підтримують

Bluetooth, вони можуть управлятися з комп'ютера, планшета або смартфона з підтримкою Bluetooth.

– Третя можливість - прямий зв'язок пристроїв між собою за окремою локальної мережі, в той час як зв'язок із зовнішньою мережею (на малюнку не показана) здійснюється через шлюз LAN.

Кожна фізична річ в Інтернеті речей може бути представлена в інформаційному світі однією або декількома віртуальними речами, але при цьому віртуальна річ може існувати без відповідної фізичної речі. Фізичні речі зіставлені віртуальним речам, що зберігаються в БД і інших структурах даних. Додатки обробляють віртуальні речі і працюють з ними.

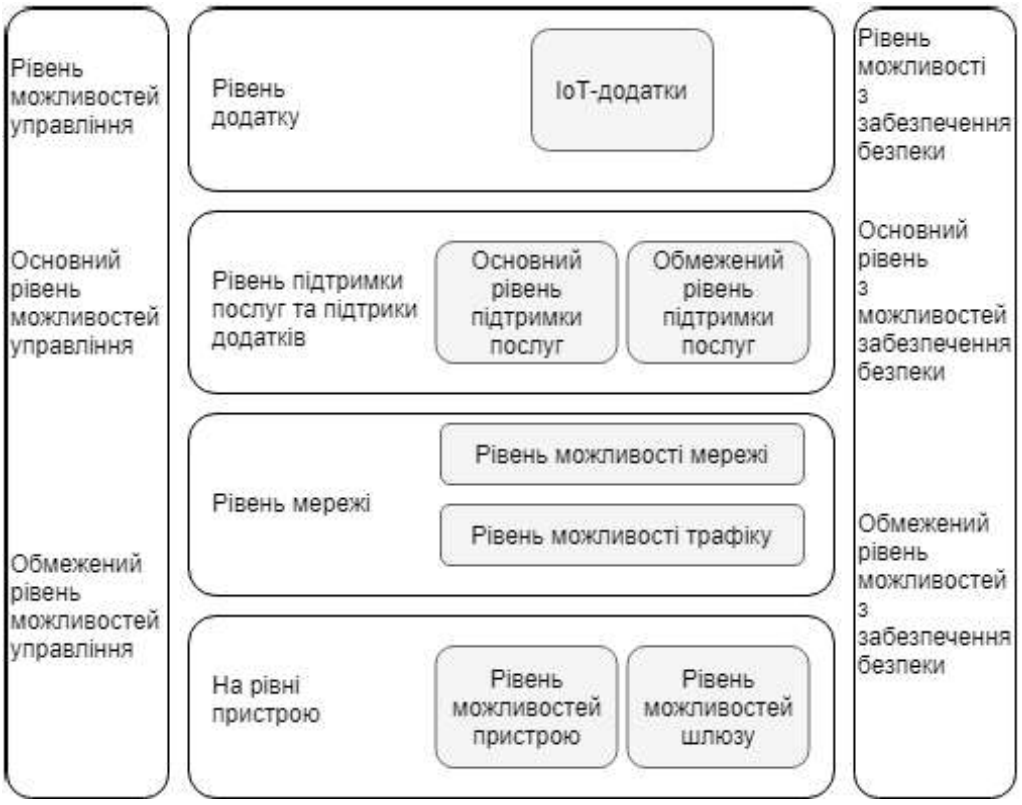

Рисунок 3.2 – Еталона модель IoT за рекомендацією Y.2060

Еталонна модель IoT від MCE-T складається з чотирьох рівнів плюс можливості управління і безпеки, що діють між рівнями. До сих пір ми говорили про рівень пристрою. У термінах функціональності зв'язку рівень пристрою включає в себе, грубо кажучи, фізичний і канальний рівні OSI.

Рівень мережі виконує дві базові функції. Можливості мережі відносяться до взаємодії пристроїв і шлюзів. Транспортні можливості відносяться до транспорту інформації служб і додатків IoT, а також інформацією управління і контролю IoT.

Грубо кажучи, ці можливості відповідають мережевому і транспортному рівням OSI.

Рівень підтримки послуг і підтримки додатків надає можливості, які використовуються додатками. Багато різноманітних додатків можуть використовувати загальні можливості підтримки. До прикладів належать спільне опрацювання даних і управління БД. Спеціалізовані можливості підтримки – це конкретні можливості, які призначені для задоволення потреб конкретного підмножини додатків IoT.

Рівень додатку складається з усіх додатків, взаємодіючих з IoT-пристроями. Рівень можливостей управління охоплює традиційні функції управління мережею, тобто управління несправностями, управління конфігурацією, управління обліком, управління показниками роботи і управління безпекою.

В Рекомендації Y.2060 як приклади загальних можливостей управління перераховані:

- управління пристроями: приклади включають виявлення пристроїв, автентифікацію, дистанційну активацію і дезактивацію пристроїв, конфігурацію, діагностику, оновлення прошивки і / або ПЗ, управління робочим статусом пристрою;
- управління топологією локальної мережі: прикладом є управління конфігурацією мережі;
- управління трафіком і перевантаженнями: наприклад, виявлення умов перевантаженості мережі і реалізація резервування ресурсів для термінових і / або життєво важливих потоків трафіку.

Спеціалізовані можливості управління тісно пов'язані з вимогами додатків, наприклад, вимогами з контролю лінії передачі електроенергії в «розумній» електромережі.

Рівень можливостей забезпечення безпеки включає загальні можливості забезпечення безпеки, які не залежать від додатків. В Рекомендації Y.2060 приклади загальних можливостей забезпечення безпеки включають:

- на рівні програми: авторизацію, автентифікацію, захист конфіденційності і цілісності даних програми, захист недоторканності приватного життя, аудит безпеки і антивірусний захист;
- на рівні мережі: авторизацію, автентифікацію, конфіденційність даних про використання та даних сигналізації, а також захист цілісності даних сигналізації;
- на рівні пристрою: автентифікацію, авторизацію, перевірку цілісності пристрою, управління доступом, захист конфіденційності і цілісності даних.

Спеціалізовані можливості забезпечення безпеки тісно пов'язані з вимогами додатків, наприклад, вимогами безпеки мобільних платежів.

Еталонна модель від Всесвітнього форуму IoT

Всесвітній форум IoT (IoT World Forum, IWF) - щорічна подія, що спонсорується галуззю та об'єднує представників бізнесу, державних структур та вузівської науки з метою просування IoT на ринок.

Комітет з архітектури Всесвітнього форуму IoT, складений з лідерів індустрії, включаючи IBM, Intel та Cisco, в жовтні 2014 опублікував еталонну модель IoT. Ця модель є загальною структурою, покликаною допомогти галузі прискорити розгортання IoT.

Модель призначена для того, щоб стимулювати співпрацю та сприяти створенню повторюваних моделей впровадження.

Ця еталонна модель є корисним доповненням до моделі МСЕ-Т. Документи МСЕ-Т роблять упор на рівнях пристрою та шлюзу, описуючи верхні

рівні лише в загальних рисах. І дійсно, в Рекомендації Y.2060 увесь опис рівня додатку вмістився в одну фразу. Найбільше уваги рекомендації серії Y.206x приділяють визначенню концепції для підтримки розробки стандартів взаємодії з пристроями IoT.

IWF стурбований більш масштабним питанням розробки додатків, проміжного програмного забезпечення і функцій підтримки для корпоративного Інтернету речей. Запропонована семирівнева модель зображена на рисунку 3.3.

Рисунок 3.3 – Еталонна модель від Всесвітнього форуму IoT

Документальний опис моделі IWF, опублікований Cisco, вказує, що розроблена модель відрізняється наступними характеристиками:

- спрощує: допомагає розбити складні системи на частини так, щоб кожна з цих частин стала більш зрозумілою;
- прояснює: надає додаткові відомості для точної ідентифікації рівнів IoT і вироблення загальної термінології;
- ідентифікує: ідентифікує аспекти, в яких ті чи інші типи обробки оптимізовані в різних частинах системи;
- стандартизує: є першим кроком до того, щоб постачальники могли створювати продукти IoT, здатні взаємодіяти один з одним;
- організовує: робить IoT реальним і доступним, а не просто абстрактною концепцією.

Рівень 1 утворюють фізичні пристрої та контролери, які можуть керувати кількома пристроями.

Рівень 1 моделі IWF приблизно відповідає рівню пристрою в моделі MCE-T . Як і в моделі MCE-T, елементи на цьому рівні – не фізичні речі як такі, а пристрої, які взаємодіють з фізичними речами, такі як сенсорні і виконавчі пристрої. Серед інших можливостей ці пристрої можуть вміти здійснювати аналого-цифрове і цифро-аналогове перетворення, генерацію даних, а також підтримувати дистанційний опитування і / або дистанційне керування.

Рівень 2 моделі IWF приблизно відповідає рівню мережі в моделі MCE-T. Основна відмінність в тому, що модель IWF відносить шлюзи до рівня 2, в той час як в моделі MCE-T вони відносяться до рівня 1. Оскільки шлюз є мережевим пристроєм і пристроєм зв'язку, віднесення його до рівня 2 має більше сенсу.

З логічної точки зору цей рівень реалізує зв'язок пристроїв між собою і між пристроями і низькорівневою обробкою на рівні 3. З фізичної точки зору цей рівень складається з мережевих пристроїв, таких як маршрутизатори, комутатори, шлюзи і брандмауери, що використовуються для створення локальних і глобальних мереж і підключення до Інтернету.

Цей рівень дозволяє пристроям здійснювати зв'язок один з одним і за допомогою більш високих логічних рівнів обмінюватися даними з прикладними платформами, такими як комп'ютери, пристрої дистанційного управління і смартфони.

У багатьох впроваджуваних системах IoT розподілена мережа датчиків може генерувати великі обсяги даних. Наприклад, офшорні нафтові родовища і нафтопереробні заводи можуть генерувати до терабайта даних щодня. Літак може генерувати кілька терабайт даних на годину. Замість того, щоб зберігати всі ці дані постійно (або хоча б довгий час) в централізованому сховищі, доступному для додатків IoT, часто більш доцільно виконувати якомога більшу частину обробки даних якомога ближче до датчиків. Тому завданням рівня периферійних обчислень (edge computing level) (рівень 3) є перетворення мережевих потоків даних в інформацію, придатну для зберігання і більш високорівневої обробки. Елементи обробки на цьому рівні можуть мати справу з

великими обсягами даних і виконувати операції перетворення даних, в результаті яких зберігати доводиться вже набагато менший обсяг.

Опублікований Cisco документ по моделі IWF містить такі приклади операцій на рівні периферійних обчислень:

- аналіз: аналіз даних по критеріях того, чи підлягають вони обробці на більш високому рівні;
- форматування: переформатування даних для однакової високорівневої обробки;
- розархівування / декодування: обробка криптографічних даних з додатковим контекстом (таким як походження);
- дистиляція / скорочення: скорочення і / або резюмування даних для того, щоб мінімізувати обсяг даних, трафік в мережі і в високорівневих системах обробки;
- оцінка: визначення того, чи становлять дані порогове значення або аварійний сигнал; цей процес повинен включати перенаправлення даних додатковим одержувачам.

Елементи обробки на цьому рівні відповідають пристроїв загального призначення в моделі MCE-T. Як правило, вони розгортаються фізично на краю мережі IoT, тобто поруч з сенсорами і іншими пристроями генерації даних.

Таким чином, частина базової обробки великих обсягів генеруються даних знімається з прикладних програм IoT, розташованих центрально.

Обробка на рівні периферійних обчислень іноді називається туманними обчисленнями (Fog Computing). Туманні обчислення і туманні служби, як очікується, стануть відмінною характеристикою IoT. Цей принцип проілюстрований на рис. 3.4.

Туманні обчислення представляють в сучасних мережевих технологіях тренд, протилежний хмарних обчислень. У хмарні обчислення великий обсяг централізованих ресурсів зберігання і обробки даних доступний розподіленим споживачам за допомогою хмарних мережевих структур для відносно невеликого числа користувачів.

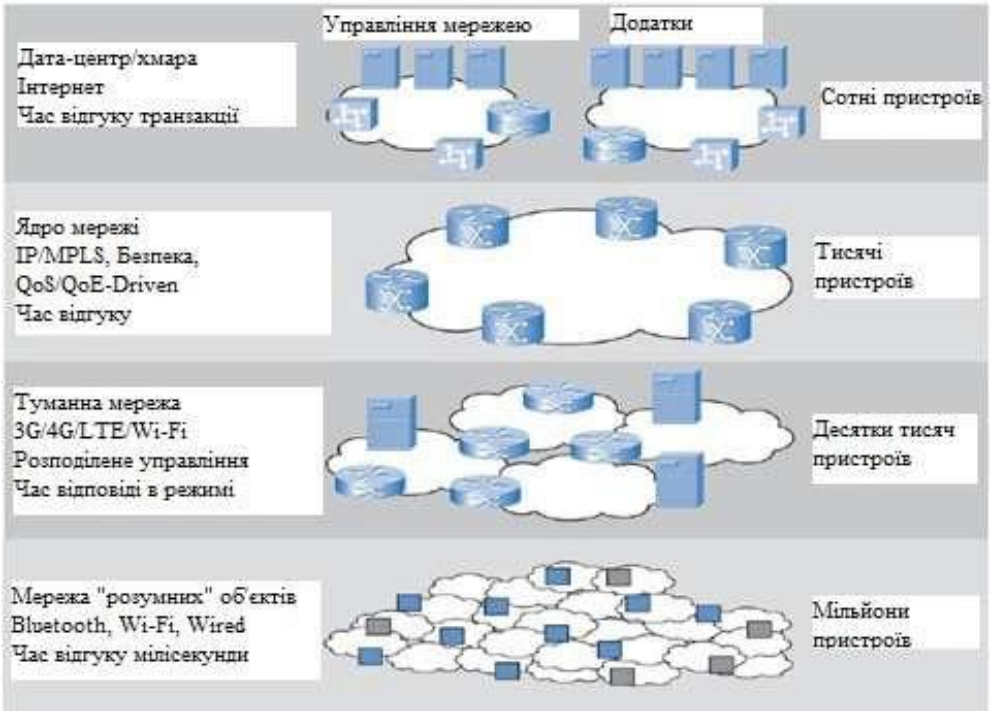

Рисунок 3.4 – Туманні обчислення

В туманних обчисленнях велике число окремих інтелектуальних об'єктів здійснюють зв'язок з туманними мережевими структурами, які здійснюють обчислення і зберігають ресурси поруч з периферійними пристроями в IoT.

Туманні обчислення вирішують проблеми, що виникли внаслідок діяльності тисяч або мільйонів «розумних» пристроїв, включаючи проблеми безпеки, конфіденційності, обмежених можливостей мережі і затримки. Термін «туманні обчислення» обраний тому, що туман стелиться по землі, в той час як хмари знаходяться високо в небі.

На рівні 4, рівні накопичення даних, дані, що надійшли з різних пристроїв, профільтровані і оброблені рівнем периферійних обчислень, поміщаються в сховище, де будуть доступні для більш високих рівнів. Цей рівень разюче відрізняється і від низькорівневих (туманних), і від високорівневих (хмарних) обчислень за особливостями конструкції, вимогам і методам обробки.

Дані, що проходять крізь мережу, називаються «даними в русі». Швидкість і організація даних в русі визначається пристроями, що генерують дані. Генерація даних відбувається по подіям, або періодично, або по виникненні якої-небудь події в середовищі.

Для збору даних та їх обробки необхідно реагувати на їх появу в реальному часі. Навпаки, багатьом додаткам не потрібно обробляти дані зі швидкістю мережевої передачі. На практиці ні хмарна мережу, ні прикладні платформи не змогли б встигати за обсягами даних, що генеруються величезною кількістю IoT-пристроїв. Замість цього додатки мають справу з «даними в спокої», тобто даними в тому чи іншому легкодоступному сховище. Додатки можуть звертатися до даних у міру необхідності або поза режимом реального часу. Таким чином, високі рівні функціонують за принципом транзакцій, в той час як три нижніх рівні працюють по подіях.

Таблиця 3.1 – Порівняння хмарних та туманних обчислень

	Хмара	**Туман**
Розташування ресурсів, зберігання / обробки	Центр	Край
Затримка	Від низької до високої	Низька
Доступ	Фіксований або бездротовий	Головним чином безпровідний
Підтримка мобільності	Не застосовується	Так
Контроль	Централізований /ієрархічний (повний контроль)	Розподілений / ієрархічний (частковий контроль)
Доступ до служб	Через ядро	На краю / з портативного пристрою (смартфон і т.д.)
Доступність	99,99%	Висока нестабільність /високий рівень резервування
Число користувачів / пристроїв	Десятки і сотні мільйонів	Десятки мільярдів
Основний генератор контенту	Люди і пристрої	Пристрої / сенсори
Генерація контенту	У центральному розташуванні	Скрізь
Споживання контенту	На кінцевих пристроях	Скрізь
Віртуальна програмна інфраструктура	Центральні корпоративні сервери	Призначені для користувача пристрої

Нижче перераховані операції, що виконуються на рівні накопичення даних:

- перетворення «даних в русі» в «дані в спокої»;
- перетворення формату з мережевих пакетів в реляційні таблиці БД;
- перехід від обчислень щодо подій до обчислень за запитом;
- значне зниження обсягу даних за рахунок фільтрації і вибіркового зберігання.

Ще один погляд на рівень накопичення даних полягає в тому, що він являє собою кордон між інформаційними технологіями (IT), під якими розуміється цілий спектр технологій обробки інформації, включаючи ПЗ, обладнання, технології зв'язку і супутні служби, і операційними технологіями (Operational Technology, OT), що представляють собою обладнання і ПЗ, які виявляють або викликають зміни шляхом прямого моніторингу та / або контролю фізичних пристроїв, процесів і подій на підприємстві.

Рівень накопичення даних вбирає велику кількість даних і поміщає їх в сховище, практично не пристосовуючи до потреб конкретних програм або груп додатків. З рівня периферійних обчислень в сховище може надходити безліч різних видів даних в різних форматах і від різнорідних оброблювачів. Рівень абстракції (рівень 5) даних може агрегувати і форматувати такі дані способами, які роблять доступ додатків більш керованим і ефективним. У числі пов'язаних завдань можуть бути наступні:

- Комбінування даних з різних джерел, включаючи вивірку кількох форматів даних.
- Виконання необхідних перетворень для забезпечення однакової семантики даних з різних джерел.
- Приміщення відформатованих даних у відповідну базу даних, наприклад, великі обсяги повторюваних даних поміщаються в систему великих даних, таку як Hadoop. Дані подій направляються в реляційну СУБД, що відрізняється більш швидким часом реакції і адекватним інтерфейсом для таких типів даних.

- Оповіщення додатків більш високого рівня про те, що дані заповнені або досягнутий певний рівень даних.
- Консолідація даних в одному місці (за допомогою ETL (extract, transform, load), ELT (extract, load, transform) або реплікації даних) або надання доступу до декількох джерел даних шляхом віртуалізації даних.
- Захист даних шляхом відповідної автентифікації і авторизації.
- Нормалізація / денормалізація і індексація даних для швидкого доступу додатків.

Рівень 6 (рівень додатку) містить додатки будь-якого типу, що використовують дані IoT на вході або керуючі IoT-пристроями. Як правило, додатки взаємодіють з рівнем 5 і з даними в спокої, тому їм не обов'язково функціонувати на швидкостях мережі.

Слід передбачити спрощений режим роботи, який дозволить додаткам минути проміжні рівні і безпосередньо взаємодіяти з рівнем 3 або навіть рівнем 2. Модель IWF не визначає додатки по всій строгості, вважаючи цей аспект виходять за рамки дискусії про модель IWF.

Рівень взаємодії і процесу (рівень 7) з'явився в результаті визнання того, що IoT буде корисний лише тоді, коли з ним зможуть взаємодіяти люди. Цей рівень може включати кілька додатків і обмін даними і / або керуючої інформацією по Інтернету або корпоративної мережі.

IWF вважає еталонну модель IoT прийнятої в галузі базовою структурою, спрямованої на стандартизацію концепцій і термінології, пов'язаних з IoT.

Що ще більш важливо, модель IWF визначає необхідний функціонал і проблеми, які потрібно вирішити до того, як галузь зможе реалізувати цінність IoT.

Ця модель корисна як для постачальників, що розробляють функціональні елементи всередині моделі, так і для замовників, допомагаючи їм виробити свої вимоги і оцінювати пропозиції постачальників.

Модель NIST Special Publication 800-183

Публікація «Networks of Things» Національного інституту стандартів і технології Міністерства торгівлі США вийшла в розділі COMPUTER SECURITY в липні 2016 року.

Основними пунктами публікації є:

- Введено поняття «Network of« Things » - вид розподілених систем.
- IoT, мережі соц. медіа, мережі сенсорів, промисловий Інтернет розглядаються як види NoT.
- «Речами» може бути програмне забезпечення, «залізо», їх комбінація і людина.
- Виділено та описано характеристики п'яти ключових примітивів: сенсор, агрегатор (шлюз), канал зв'язку, зовнішня утиліта і тригер рішення.
- У модель також внесені шість елементів: середа, витрати, місце розташування, власник (оператор), Device_ID (для будь-якого прімітива), і момент часу (снепшот).

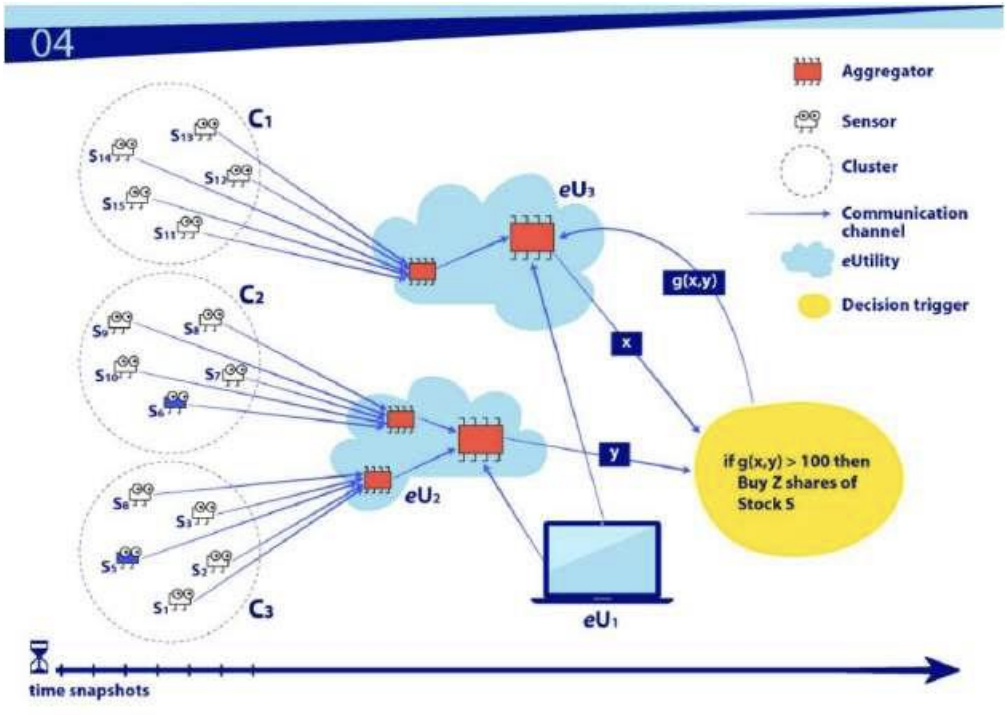

Рисунок 3.5 – Архітектура моделі за публікацією NIST Special Publication 800-183

Додаткові міркування:

- Система може бути відкритою, закритою або мати проміжний стан.
- Необхідність використання шаблонів проектування для побудови великих систем.
- Рівень довіри до системи в деякий момент часу - функція від реалізації примітивів з урахуванням основних елементів.
- Низька вірогідність виявлення помилок в системі під час тестування.
- Облік механізмів і особливостей впливу на зовнішнє середовище.

У публікації зачіпаються питання безпеки і надійності.

Як можна побачити з рисунку для шлюзів (агрегаторів) тут виділяється більша роль аніж у архітектурах міжнародного IoT форуму та Міжнародного союзу електрозв’язку.

Агрегатор не просто виконує функцію «перепакування» з одного стеку протоколів у інший, а ще й агрегує, аналізує та зберігає дані.