ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра комп'ютерних наук

Пояснювальна записка

до бакалаврської роботи
на ступінь вищої освіти бакалавр

на тему: «Дослідження застосування хмарних технологій для ефективного функціонування IoT- мереж»

Виконав: студент 4 курсу, групи КНД–41
спеціальності 122 Комп'ютерні науки
Дерновий Я. Ю
(прізвище та ініціали)

Керівник Каргаполов Ю. В.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтроль

Київ – 2021

ВСТУП

Я хотів би почати своє дослідження з повного розуміння про ці дві глобальні технології. Хмарні обчислення та IoT часто поєднуються, але як саме взаємодіють ці сутності? Хоча підключення IoT могло б існувати і без хмари, можна з упевненістю сказати, що хмарні обчислення дозволяють багатьом пристроям IoT працювати з набагато більшою потужністю та ефективністю. Важливо вивчити загальні риси технологій, задіяні в галузі обчислювальноїтехніки. Справді, це так безумовно, справа у хмарних обчисленнях та Інтернеті Речей - дві парадигми, які мають багато спільних особливостей. Інтеграція цих численних концепцій може сприяти та вдосконалювати ці технології. Загально визнано, що Хмарні обчислення можуть бути використані для комунальних послуг у майбутньому. За рахунок хмарних технологій надаються послуги, які роблять можливим обмін обчислювальними ресурсами через Інтернет. З іншого боку, IoT можна розглянути як динамічну, так і глобальну мережеву інфраструктуру, яка керує об'єктами, що само конфігуруються. Властивість здатності до само конфігурації об'єктів є невід'ємною частиною інтелектуальних систем. IoT рухається до фази, коли всі елементи навколо нас підключені до Інтернету і мають можливість взаємодіяти з мінімальними зусиллями людини.

IoT зазвичай включає ряд об'єктів з обмеженим зберіганням і обчислювальною здатністю. Деякими дослідними центрами передбачається, що хмарні технології і IoTскладуть основу майбутнім технологіям наступного покоління інтернету. Однак, об'єднання цих технологій є не простим завданням, оскільки, наприклад хмарні сервіси є залежними від постачальників послуг і вимагають вирішення завдань технологічної сумісності баз даних, тоді як для сучасного стану технологій IoTбільш властива різноманітність протоколів, а не сумісність форматів представлення даних. При цьому треба відзначити, що обидві технології потребують надійних рішень для задач забезпечення безпечного

доступу з точки зору ідентифікації та управління доступом до даних.В цій роботі подано огляд інтеграції Хмарних технологій та IoT.

1 ДОСЛІДЖЕННЯ ХМАРНИХ ОБЧИСЛЮВАНЬ ТА IOT

1.1Хмарні обчислення

Хмарні обчислення - це доступ до інтернету за запитом до обчислювальних ресурсів - додатків, серверів (фізичних серверів та віртуальних серверів), зберігання даних, засобів розробки, можливостей мереж та іншого - розміщених у віддаленому центрі обробки даних, керованому хмарними службами. провайдера (або CSP). CSP надає ці ресурси доступними за щомісячну абонентську плату або виставляє їм рахунки відповідно до використання.

Порівняно із традиційними локальними IT та залежно від обраних хмарних служб, хмарні обчислення допомагають зробити наступне:

Зниження IT-витрат: Cloud дозволяє вам розвантажити частину або більшу частину витрат та зусиль на придбання, встановлення, налаштування та управління власною локальною інфраструктурою.

Покращення спритності та часу до вартості: за допомогою хмари ваша організація може почати використовувати корпоративні програми за лічені хвилини, а не чекати тижнів чи місяців, поки IT відповість на запит, придбає та налаштує допоміжне обладнання та встановить програмне забезпечення. Хмара також дозволяє розширити можливості певних користувачів - зокрема розробників та науковців даних - допомагати собі в розробці програмного забезпечення та підтримці інфраструктури.

Масштабуйте простіше та економічніше: хмара забезпечує еластичність - замість того, щоб купувати надмірну потужність, яка залишається невикористаною протягом повільних періодів, ви можете масштабувати ємність вгору та вниз у відповідь на стрибки та провали трафіку. Ви також можете скористатися перевагами глобальної мережі вашого хмарного провайдера, щоб поширити свої програми ближче до користувачів по всьому світу.

Термін «хмарні обчислення» також відноситься до технології, яка змушує хмарні роботи. Сюди входить певна форма віртуалізованої IT-інфраструктури - сервери, програмне забезпечення операційної системи, мережа та інша інфраструктура, яка абстрагована за допомогою спеціального програмного забезпечення, так що її можна об’єднати та розділити незалежно від фізичних меж апаратного забезпечення. Наприклад, один апаратний сервер можна розділити на кілька віртуальних серверів.

Віртуалізація дозволяє хмарним провайдерам максимально використовувати ресурси своїх центрів обробки даних. Не дивно, що багато корпорацій застосували модель хмарної доставки для своєї локальної інфраструктури, щоб вони могли реалізувати максимальне використання та економію витрат порівняно з традиційною IT-інфраструктурою та пропонувати такі ж самообслуговування та спритність своїм кінцевим споживачам.

Якщо ви використовуєте комп’ютер або мобільний пристрій вдома чи на роботі, ви майже напевно використовуєте якусь форму хмарних обчислень щодня, будь то хмарні програми, такі як GoogleGmail або Salesforce, потокові медіа, такі як Netflix, або хмарне сховище файлів, як Dropbox. Згідно з недавнім опитуванням, сьогодні 92% організацій використовують хмару (посилання знаходиться за межами IBM), і більшість з них планують використовувати її більше протягом наступного року.

Послуги хмарних обчислень:

IaaS (Infrastructure-as-a-a-Service), PaaS (Platform-as-a-a-Service) та SaaS (Software-as-a-a-Service) - це три найпоширеніші моделі хмарних служб, і це не рідкість для організації використовувати всі три. Однак часто існує плутанина серед трьох і того, що входить до кожного.

SaaS (програмне забезпечення як послуга):

SaaS - також відоме як хмарне програмне забезпечення або хмарні

додатки - це прикладне програмне забезпечення, яке розміщується в хмарі, і до якого ви отримуєте доступ та користуєтесь через веб-браузер, спеціальний

настільний клієнт або API, який інтегрується з вашою робочою або мобільною операційною системою. У більшості випадків користувачі SaaS платять щомісячну або річну плату за підписку; деякі можуть пропонувати ціноутворення "на виплату" залежно від вашого фактичного використання.

На додаток до економії витрат, витрат часу та вартості хмарності, SaaS пропонує наступне:

Автоматичне оновлення: за допомогою SaaS ви користуєтеся перевагами нових функцій, як тільки їх додає постачальник, без необхідності організовувати локальне оновлення.

Захист від втрати даних. Оскільки дані програми знаходяться в хмарі, ви не втрачаєте дані, якщо ваш пристрій виходить з ладу чи ламається.

SaaS є основною моделлю доставки для більшості комерційних програм сьогодні - доступні сотні тисяч рішень SaaS, від найбільш цілеспрямованих галузевих та відомчих програм, до потужної бази даних корпоративного програмного забезпечення та програмного забезпечення AI (штучного інтелекту).

PaaS (Платформа як послуга):

PaaS надає розробникам програмного забезпечення платформу на вимогу - апаратне забезпечення, повний стек програмного забезпечення, інфраструктуру та навіть засоби розробки - для запуску, розробки та управління програмами без витрат, складності та гнучкості утримання цієї платформи на місці.

За допомогою PaaS хмарний провайдер розміщує все - сервери, мережі, сховища, програмне забезпечення операційної системи, проміжне програмне забезпечення, бази даних - у своєму центрі обробки даних. Розробники просто обирають меню, щоб «розкрутити» сервери та середовища, необхідні для запуску, побудови, тестування, розгортання, обслуговування, оновлення та масштабування додатків.

Сьогодні PaaS часто будується навколо контейнерів - віртуалізованої обчислювальної моделі, яка на один крок видаляється з віртуальних серверів. Контейнери віртуалізують операційну систему, дозволяючи розробникам упаковувати додаток лише з послугами операційної системи, необхідними для

запуску на будь-якій платформі, без змін і без необхідності проміжного програмного забезпечення.

Red Hat Open Shift - це популярний PaaS, побудований навколо контейнерів Docker та Kubernetes, рішення для оркестрації контейнерів з відкритим кодом, яке автоматизує розгортання, масштабування, балансування навантаження тощо для додатків на основі контейнерів.

IaaS (Інфраструктура як послуга):

IaaS забезпечує доступ до Інтернету до основних обчислювальних ресурсів - фізичних та віртуальних серверів, мереж та сховищ - через Інтернет на основі оплати, як потрібно. IaaS дозволяє кінцевим споживачам масштабувати та скорочувати ресурси за необхідності, зменшуючи потребу у великих, попередніх капітальних видатках або непотрібних локальних або «власних» інфраструктурах, а також у перекупленні ресурсів, щоб забезпечити періодичні стрибки у використанні.

На відміну від SaaS та PaaS (і навіть новіших обчислювальних моделей PaaS, таких як контейнери та безсерверні), IaaS надає користувачам найнижчий рівень управління обчислювальними ресурсами в хмарі.

IaaS була найпопулярнішою моделлю хмарних обчислень, коли вона з’явилася на початку 2010-х. Хоча вона залишається хмарною моделлю для багатьох типів робочих навантажень, використання SaaS та PaaS зростає набагато швидше.

Безсерверні обчислення:

Безсерверні обчислення (їх також називають просто безсерверними) - це модель хмарних обчислень, яка розвантажує всі завдання управління внутрішньою інфраструктурою - забезпечення, масштабування, планування, виправлення - для хмарного провайдера, що дозволяє розробникам зосередити весь свій час та зусилля на коді та бізнес-логіці. специфічні для їх додатків.

Більше того, безсерверний запуск коду програми виконується лише на основі кожного запиту та автоматично масштабує допоміжну інфраструктуру вгору та вниз у відповідь на кількість запитів. Безсерверні клієнти платять лише за

ресурси, що використовуються під час запуску програми - вони ніколи не платять за простої.

FaaS або Function-as-a-Service часто плутають з безсерверними обчисленнями, коли насправді це підмножина безсерверних. FaaS дозволяє розробникам виконувати частини коду програми (так звані функції) у відповідь на конкретні події. Все, крім коду - фізичне обладнання, операційна система віртуальних машин та управління програмним забезпеченням веб-сервера - автоматично надається постачальником хмарних послуг у режимі реального часу під час виконання коду та повертається назад після завершення виконання. Виставлення рахунків починається, коли виконання починається, і припиняється, коли виконання зупиняється.

На мал.1.1. детально зображено сервіси хмарних обчислень і хто чим керує.

мал.1.1 - Сервіси хмарних обчислень

Види хмарних обчислень:

Публічна хмара - це тип хмарних обчислень, при якому постачальник хмарних послуг робить доступними для користувачів обчислювальні ресурси - що завгодно, від додатків SaaS до окремих віртуальних машин (ВМ), до простого

обчислювального обладнання, до інфраструктури корпоративного рівня та платформ розробки через загальнодоступний Інтернет. Ці ресурси можуть бути доступними безкоштовно, або доступ може бути проданий відповідно до моделей ціноутворення на основі підписки або оплати за використання.

Публічний хмарний постачальник володіє, управляє та бере на себе всю відповідальність за центри обробки даних, апаратне забезпечення та інфраструктуру, на яких виконуються робочі навантаження своїх клієнтів, і, як правило, забезпечує мережеве підключення з високою пропускною здатністю для забезпечення високої продуктивності та швидкого доступу до програм та даних.

Публічна хмара - це середовище для кількох орендарів - інфраструктура центру обробки даних хмарного провайдера є спільною для всіх клієнтів загальнодоступних хмар. У провідних публічних хмарах - Amazon Web Services (AWS), Google Cloud, IBM Cloud, Microsoft Azure та Oracle Cloud - ці клієнти можуть нараховувати мільйони.

Світовий ринок публічних хмарних обчислень швидко зростав за останні кілька років, і аналітики прогнозують, що ця тенденція збережеться; Промисловий аналітик Gartner прогнозує, що доходи від загальнодоступних хмарних технологій до кінця 2022 року перевищать 330 млрд. доларів США (посилання знаходиться за межами IBM).

Багато підприємств переносять частину своєї обчислювальної інфраструктури в загальнодоступну хмару, оскільки публічні хмарні служби є еластичними та легко масштабованими, гнучко пристосовуючись до мінливих вимог до робочого навантаження. Інших приваблює обіцянка більшої ефективності та меншої витрати ресурсів, оскільки клієнти платять лише за те, що вони використовують. Треті намагаються зменшити витрати на обладнання та локальну інфраструктуру.

Приватна хмара - це хмарне середовище, в якому вся хмарна інфраструктура та обчислювальні ресурси присвячені і доступні лише одному клієнту. Приватна хмара поєднує в собі багато переваг хмарних обчислень - включаючи еластичність, масштабованість та простоту надання послуг - з

контролем доступу, безпекою та налаштуванням ресурсів локальної інфраструктури.

Приватна хмара, як правило, розміщується локально в центрі обробки даних замовника. Але приватна хмара також може розміщуватися в незалежній інфраструктурі постачальника хмарних послуг або будуватися на орендованій інфраструктурі, розміщеній в зовнішньому центрі обробки даних.

Багато компаній вибирають приватну хмару над державною, оскільки приватна хмара - це простіший спосіб (або єдиний спосіб) задовольнити їх вимоги щодо дотримання нормативних вимог. Інші обирають приватну хмару, оскільки їх робоче навантаження стосується конфіденційних документів, інтелектуальної власності, інформації, що ідентифікує особу (ІПО), медичних записів, фінансових даних чи інших конфіденційних даних.

Побудувавши приватну хмарну архітектуру відповідно до власних принципів хмарності, організація надає собі гнучкість для легкого переміщення робочих навантажень у загальнодоступну хмару або запуску їх у гібридному хмарному середовищі (див. Нижче), коли вони будуть готові.

Гібридна хмара - це саме те, як це звучить - поєднання публічного та приватного хмарного середовища. Зокрема, і в ідеалі, гібридна хмара пов'язує приватні хмарні служби організації та загальнодоступні хмари в єдину гнучку інфраструктуру для запуску програм та робочих навантажень організації.

Метою гібридної хмари є створення поєднання загальнодоступних та приватних хмарних ресурсів - і з рівнем оркестрації між ними - що надає організації гнучкість у виборі оптимальної хмари для кожного додатка чи робочого навантаження та вільного переміщення робочих навантажень між двома хмари в міру зміни обставин. Це дозволяє організації досягти своїх технічних та бізнес-цілей ефективніше та економічніше, ніж це могло б зробити лише за допомогою державної або приватної хмари.

Multicloud та гібридний multicloud -це використання двох або більше хмар від двох або більше різних постачальників хмар. Наявність мультиоблачного середовища може бути настільки ж простим, як використання електронної пошти

SaaS одного постачальника та редагування зображень SaaS іншого. Але коли підприємства говорять про мультиклас, вони, як правило, говорять про використання декількох хмарних сервісів - включаючи послуги SaaS, PaaS та IaaS - від двох або більше провідних державних хмарних постачальників. В одному з опитувань 85% організацій повідомили, що використовують мультиоблачне середовище.

Гібридна мультиоблачність - це використання двох або більше публічних хмар разом із приватним хмарним середовищем.

Організації вибирають мультиголос, щоб уникнути блокування постачальників, мати більше послуг на вибір та отримати доступ до більшої кількості інновацій. Але чим більше хмар ви використовуєте - кожна зі своїм набором інструментів управління, швидкістю передачі даних та протоколами безпеки, тим складніше може бути управління своїм середовищем. Платформи управління мультикладом забезпечують видимість між хмарами багатьох постачальників через центральну інформаційну панель, де команди розробників можуть бачити свої проекти та розгортання, операційні групи можуть стежити за кластерами та вузлами, а співробітники кібербезпеки можуть контролювати наявність загроз.

Хмарна безпека:

Традиційно проблеми безпеки були основною перешкодою для організацій, які розглядають хмарні сервіси, особливо державні хмарні служби. Однак у відповідь на попит безпека, яку пропонують постачальники хмарних послуг, стабільно перевершує локальні рішення безпеки.

За словами постачальника програмного забезпечення для захисту даних McAfee, сьогодні 52% компаній відчувають кращий рівень безпеки в хмарі, ніж локальний (посилання знаходиться поза межами IBM). І Gartner передбачив, що до цього року (2020) хмарні робочі навантаження інфраструктури як послуги (IaaS) зазнають на 60% менше інцидентів безпеки, ніж у традиційних центрах обробки даних (посилання знаходиться поза IBM).

Протепідтримкахмарноїбезпекивимагаєіншихпроцедуртанаборунавичокспів робітників, ніжузастарілихІТ-середовищах. Деякі найкращі практики хмарної безпеки включають наступне:

1. **Спільна відповідальність за безпеку:** Як правило, хмарний постачальник відповідає за захист хмарної інфраструктури, а замовник відповідає за захист своїх даних у хмарі, але також важливо чітко визначити право власності на дані між приватними та державними третіми сторонами.

2. **Шифрування даних:** Дані слід шифрувати, перебуваючи в стані спокою, під час транспортування та використання. Клієнти повинні підтримувати повний контроль над ключами безпеки та апаратним модулем безпеки.

3. **Ідентифікація користувача та управління доступом:** Клієнтам та ІТ-командам потрібне повне розуміння та доступність мережі, пристрою, програми та доступу до даних.

4. **Спільне управління:** належний зв’язок та чіткі, зрозумілі процеси між ІТ, операціями та службами безпеки забезпечать безперебійну інтеграцію хмарних технологій, що є безпечною та стійкою.

5. **Моніторинг безпеки та відповідності:** це починається з розуміння всіх стандартів відповідності нормативним актам, що застосовуються у вашій галузі, та налаштування активного моніторингу всіх підключених систем та хмарних служб для підтримання видимості всього обміну даними між загальнодоступним, приватним та гібридним хмарним середовищем.

Взагалі хмарна безпека - це набір стратегій та практик для захисту даних та програм, розміщених у хмарі. Як і кібербезпека, хмарна безпека є дуже широкою сферою, і ніколи неможливо запобігти всіляким атакам. Однак добре розроблена стратегія хмарної безпеки значно зменшує ризик кібератак.

Навіть з урахуванням цих ризиків, хмарні обчислення часто є більш безпечними, ніж локальні обчислення. Більшість хмарних провайдерів мають більше ресурсів для захисту даних, ніж окремі компанії, що дозволяє хмарним провайдерам постійно оновлювати інфраструктуру та якомога швидше

виправлятивразливі місця. З іншого боку, у одного бізнесу може не вистачити ресурсів для послідовного виконання цих завдань.

Примітка: Хмарна безпека - це не те саме, що безпека як послуга (SECaaS або SaaS), що стосується продуктів безпеки, розміщених у хмарі.

Які основні ризики для хмарної безпеки?

Більшість ризиків безпеки в хмарі входять до однієї з таких загальних категорій:

1. Дані виявляються або просочуються

2. Неавторизований користувач із-за меж організації має доступ до внутрішніх даних

3. Внутрішній, уповноважений користувач має занадто великий доступ до внутрішніх даних

4. Шкідлива атака, така як атака DDoS або зараження шкідливим програмним забезпеченням, калічить або руйнує хмарну інфраструктуру

5. Метою хмарної стратегії безпеки є максимально зменшити загрозу, пов’язану з цими ризиками, захищаючи дані, керуючи автентифікацією та доступом користувачів та залишаючись працездатним перед атакою.

Які основні технології для хмарної безпеки?

Шифрування - це спосіб скремблювання даних, щоб лише уповноважені сторони могли зрозуміти інформацію. Якщо зловмисник зламає хмару компанії і знайде незашифровані дані, він може робити будь-яку кількість шкідливих дій з даними: витокувати їх, продавати, використовувати для подальших атак тощо. Однак, якщо дані компанії зашифрований, зловмисник знайде лише скрембовані дані, які не можна використовувати, якщо вони якимось чином не виявлять ключ розшифровки (що має бути майже неможливим). Таким чином, шифрування допомагає запобігти витоку даних та відкриттю даних, навіть коли інші заходи безпеки не вдаються.

Дані можуть шифруватися як у стані спокою (коли вони зберігаються), так і під час передачі (поки вони надсилаються з одного місця в інше). Хмарні дані слід шифрувати як у стані спокою, так і в дорозі, щоб зловмисники не могли їх

перехопити та прочитати. Шифрування даних при передачі повинно стосуватися як даних, що переміщуються між хмарою та користувачем, так і даних, що переміщуються з однієї хмари в іншу, як у багатохмарному або гібридному хмарному середовищі. Крім того, дані повинні шифруватися, коли вони зберігаються в базі даних або через хмарну службу зберігання.

Якщо хмари в багатохмарному або гібридному хмарному середовищі з'єднані на мережевому рівні, VPN може шифрувати трафік між ними. Якщо вони з'єднані на рівні програми, слід використовувати шифрування SSL / TLS. SSL / TLS також повинен шифрувати трафік між користувачем та хмарою (див. Що таке HTTPS?).

Управління ідентифікацією та доступом (IAM):

Продукти управління ідентифікацією та доступом (IAM) відстежують, хто є користувачем та що їм дозволено, а також дозволяють користувачам і за необхідності забороняють доступ неавторизованим користувачам. IAM надзвичайно важливий у хмарних обчисленнях, оскільки ідентифікація користувача та привілеї доступу визначають, чи можуть вони отримувати доступ до даних, а не до пристрою або місцезнаходження користувача.

IAM допомагає зменшити загрозу доступу несанкціонованих користувачів до внутрішніх ресурсів та авторизованих користувачів, які перевищують їхні привілеї. Правильне рішення IAM допоможе пом'якшити кілька видів атак, включаючи поглинання облікових записів та інсайдерські атаки (коли користувач або співробітник зловживає своїм доступом для викриття даних).

IAM може включати кілька різних служб, або це може бути одна послуга, яка поєднує в собі всі наступні можливості:

1. Постачальники ідентифікаційних даних (IdP) автентифікують ідентифікацію користувача

2. Послуги єдиного входу (SSO) допомагають автентифікувати ідентифікатори користувачів для декількох програм, завдяки чому користувачі мають лише один раз увійти, щоб отримати доступ до всіх своїх хмарних служб

3. Послуги багатофакторної автентифікації (MFA) посилюють процес

автентифікації користувачів

4. Служби контролю доступу дозволяють і обмежують доступ користувачів

Брандмауер: хмарний брандмауер забезпечує рівень захисту навколо хмарних ресурсів, блокуючи зловмисний веб-трафік. На відміну від традиційних брандмауерів, які розміщуються локально і захищають периметр мережі, хмарні брандмауери розміщуються в хмарі та утворюють віртуальний бар'єр безпеки навколо хмарної інфраструктури. Більшість брандмауерів веб-додатків належать до цієї категорії.

Хмарні брандмауери блокують DDoS-атаки, зловмисні дії ботів та використання вразливостей. Це зменшує ймовірність кібератаки, яка скалічує хмарну інфраструктуру організації.

Які ще практики важливі для захисту хмарних даних?

Впровадження вищезазначених технологій (а також будь-яких додаткових продуктів хмарної безпеки) само по собі недостатньо для захисту хмарних даних. Окрім стандартних передових практик кібербезпеки, організації, які використовують хмару, повинні дотримуватися таких практик хмарної безпеки:

Правильна конфігурація параметрів безпеки для хмарних серверів: Коли компанія не налаштовує належним чином свої параметри безпеки, це може призвести до порушення даних. Неправильно налаштовані хмарні сервери можуть передавати дані безпосередньо в ширший Інтернет. Щоб правильно налаштувати параметри безпеки в хмарі, потрібні члени команди, які є експертами в роботі з кожною хмарою, а також може знадобитися тісна співпраця з постачальником хмар.

Послідовна політика безпеки у всіх хмарах та центрах обробки даних: Заходи безпеки повинні застосовуватися до всієї інфраструктури компанії, включаючи загальнодоступні хмари, приватні хмари та локальну інфраструктуру. Якщо один із аспектів хмарної інфраструктури компанії - скажімо, їх загальнодоступна хмарна служба для обробки великих даних - не захищений шифруванням та надійною автентифікацією користувачів, зловмисники, швидше

за все, знайдуть та націлять слабке посилання.

Плани резервного копіювання: Як і для будь-якого іншого типу безпеки, повинен бути план, коли щось піде не так. Щоб дані не загубилися та не були підроблені, дані слід резервно копіювати в іншій хмарі або локально. Також повинен бути розроблений план відновлення після відмови, щоб бізнес-процеси не переривалися, якщо одна хмарна служба виходить з ладу. Однією з переваг багатохмарних та гібридних хмарних розгортань є те, що різні хмари можуть використовуватися як резервні копії - наприклад, зберігання даних у хмарі може створювати резервну копію локальної бази даних.

Освіта користувачів та працівників: великий відсоток порушень даних відбувається через те, що користувач став жертвою фішингової атаки, несвідомо встановив шкідливе програмне забезпечення, використовував застарілий і вразливий пристрій або погано виконував гігієну паролів (повторне використання того самого пароля, запис свого пароля видиме місце розташування тощо). Навчаючи своїх внутрішніх співробітників про безпеку, підприємства, які працюють у хмарі, можуть зменшити ризик таких випадків. (Навчальний центр Cloudflare - хороший ресурс для освіти з питань безпеки.)

Оскільки 25% організацій планують перенести всі свої програми в хмару протягом наступного року, здається, випадки використання хмарних обчислень безмежні. Але навіть для компаній, які не планують оптового переходу до хмари, певні ініціативи та хмарні обчислення відповідають IT-небесам.

Відновлення наслідків стихійних лих та безперервність бізнесу завжди були природними явищами для хмари, оскільки хмара забезпечує економічно ефективне резервування для захисту даних від збоїв системи та фізичної відстані, необхідної для відновлення даних та програм у разі локального відключення або катастрофи. Всі основні державні хмарні провайдери пропонують службу Disaster-Recovery-as-a-Service (DRaaS).

Все, що передбачає зберігання та обробку величезних обсягів даних на високих швидкостях - вимагає більшої ємності та обчислювальних потужностей, ніж більшість організацій може або хоче придбати та розгорнути локально - є

ціллю для хмарних обчислень. Приклади включають:

1. *Аналітика великих даних*
2. *Інтернет речей (IoT)*
3. *Штучний інтелект* - зокрема, машинне навчання та програми глибокого навчання

Для команд розробників, які застосовують Agile або DevOps (або DevSecOps) для впорядкування розробки, хмара пропонує самообслуговування кінцевого користувача на вимогу, яке не дозволяє операційним завданням, таким як обертання серверів розробки та тестування, стати вузькими місцями для розвитку.

1.2 Інтернет речей

Інтернет речей, або IoT, відноситься до мільярдів фізичних пристроїв у всьому світі, які зараз підключені до Інтернету, збираючи та передаючи дані. Завдяки надходженню наддешевих комп'ютерних чіпів і повсюдному бездротовому зв'язку можна перетворити все, що завгодно - від чогось такого маленького, як таблетка, до чогось такого великого, як літак, у частину IoT. Підключення всіх цих різних об’єктів та додавання до них датчиків додає рівень цифрового інтелекту пристроям, які в іншому випадку були б німими, дозволяючи їм передавати дані в режимі реального часу без участі людини. Інтернет речей робить тканину навколишнього світу розумнішою та чуйнішою, поєднуючи цифровий та фізичний всесвіт.

IoT представляє сучасний підхід, де межі між реальними та цифровими доменами поступово усуваються, які постійно змінюють кожен фізичний пристрій на розумний. Всі речі в IoT (розумні пристрої, датчики тощо) мають власну ідентичність. Вони поєднуються для формування комунікаційної мережі. Ці об'єкти включають не лише щоденно використовувані електронні пристрої, але й речі такі як: їжа, одяг, матеріали, деталі; товари та предмети розкоші; пам'ятники та пам’ятки; і різні форми комерції та культури. Крім того, ціоб'єкти здатні

створювати запити та змінювати свої стани. Таким чином,всі пристрої IoT можна контролювати, відстежувати та підраховувати, що значно зменшує витрати, втрати та вартість.

IoT вводить різноманітність можливостей та додатків. Однак з цим стикається багато проблем, які потенційно можуть перешкодити його успіху, реалізація, як зберігання даних, неоднорідні обмежені ресурси та масштабованість.

Приклад пристрою Інтернету речей

Практично будь-який фізичний об'єкт може бути перетворений на пристрій IoT, якщо його можна підключити до Інтернету для управління або передачі інформації.

Лампочка, яку можна ввімкнути за допомогою програми для смартфона, - це пристрій IoT, як і датчик руху або розумний термостат у вашому офісі або підключене ліхтар. Пристрій IoT може бути таким пухнастим, як дитяча іграшка, або таким серйозним, як вантажівка без водія. Деякі великі об'єкти самі можуть бути заповнені багатьма меншими компонентами IoT, наприклад, реактивний двигун, який зараз наповнений тисячами датчиків, що збирають і передають дані назад, щоб переконатися, що він працює ефективно. У ще більшому масштабі проекти розумних міст наповнюють цілі регіони датчиками, щоб допомогти нам зрозуміти та контролювати навколишнє середовище.

Термін IoT в основному використовується для пристроїв, від яких зазвичай не очікується підключення до Інтернету, і які можуть взаємодіяти з мережею незалежно від дії людини. З цієї причини ПК, як правило, не вважається пристроєм IoT, як і смартфоном, хоча останній переповнений датчиками. Однак розумний годинник, фітнес-ремінець чи інший пристрій, який можна носити, може вважатися пристроєм IoT.

Яка історія Інтернету речей

Ідея додавання датчиків та інтелекту до основних об’єктів обговорювалася протягом 1980-х і 1990-х (а є, можливо, і деякі набагато раніше предки), але крім деяких ранніх проектів - у тому числі підключеного до Інтернету торгового

автомата - прогрес був повільним просто тому, що технологія не була готова. Чіпси були занадто великими та громіздкими, і об’єкти не могли ефективно спілкуватися.

Процесори, які були досить дешевими та енергозберігаючими, щоб бути майже одноразовими, були потрібні, перш ніж нарешті стало економічно ефективним підключення мільярдів пристроїв. Прийняття RFID-міток - малопотужних мікросхем, які можуть обмінюватися бездротовим зв'язком - вирішило частину цієї проблеми разом із зростаючою доступністю широкосмугового Інтернету та стільникових та бездротових мереж. Прийняття протоколу IPv6 - який, крім усього іншого, повинен забезпечити достатню кількість IP-адрес для кожного пристрою, котрий коли-небудь буде потрібен світові (чи справді цій галактиці), також було необхідним кроком для масштабування IoT.

Кевін Ештон винайшов фразу "Інтернет речей" у 1999 році, хоча знадобилося ще принаймні десятиліття, щоб технологія наздогнала це бачення.Він заявив, що "Інтернет Речі можуть змінити світ, як це і зробив Інтернет".Можливо,навіть більше .

Пізніше IoT був офіційно представлений Міжнародним союзом електрозв'язку (ITU) у 2005 р. Дуже багато визначень IoT були висунуті численними організаціями та дослідниками.

Згідно з MCE (2012), IoT є «глобальною інфраструктурою для Інформаційного Суспільства, що дозволяє розвинути послуги шляхом взаємозв'язку (фізичного та віртуального) на основі речей.

"IoT інтегрує взаємозв’язок людської культури - наших" речей "- із взаємозв'язком нашої цифрової інформаційної системи -" Інтернету ".

Додавання тегів RFID до дорогих частин обладнання, щоб допомогти відстежувати їх розташування, було одним із перших додатків IoT. Але з тих пір витрати на додавання датчиків та підключення до Інтернету до об’єктів продовжують падати, і експерти прогнозують, що одного разу ця основна функціональність може коштувати лише 10 центів, що дозволяє підключити

майже все до Інтернету.

IoT спочатку був найцікавішим для бізнесу та виробництва, де його застосування іноді називають машиною-машиною (M2M), але зараз акцент робиться на наповненні наших будинків та офісів розумними пристроями, перетворюючи його на щось, що стосується майже всім. Ранні пропозиції щодо пристроїв, підключених до Інтернету, включали "об'єкти блогу" (об'єкти, які ведуть блог і записують дані про себе в Інтернет), всюдисущі обчислення (або "ubicomp"), невидимі обчислення та всеохоплюючі обчислення. Однак саме Інтернет речей та IoT застрягли.

Наскільки великий Інтернет речей

Компанія-аналітик IDC прогнозує, що загалом до 2025 року буде 41,6 мільярда підключених пристроїв IoT, або "речей". Він також припускає, що промислове та автомобільне обладнання представляють найбільшу можливість пов'язаних "речей", але в майбутньому також спостерігається сильне впровадження розумного будинку та носяться пристроїв.

Інший технічний аналітик, Gartner, прогнозує, що цього року на підприємства та автомобільний сектор припаде 5,8 мільярда пристроїв, що майже на чверть порівняно з 2019 роком. Утиліти стануть найвищим користувачем IoT завдяки постійному впровадженню розумних лічильників. Пристрої безпеки у вигляді виявлення зловмисників та веб-камер стануть другим за величиною використанням пристроїв IoT. Автоматизація будівель - як підключене освітлення - буде найбільш швидкозростаючим сектором, за яким слідують автомобільна (підключені автомобілі) та охорона здоров’я (моніторинг хронічних захворювань). На рис.1.2зображений IoT ринок кінцевих точок за сегментами 2018-2020 у всьому світі (встановлена база, мільярди одиниць):

Segment	2018	2019	2020
Utilities	0.98	1.17	1.37
Government	0.40	0.53	0.70
Building Automation	0.23	0.31	0.44
Physical Security	0.83	0.95	1.09
Manufacturing & Natural Resources	0.33	0.40	0.49
Automotive	0.27	0.36	0.47
Healthcare Providers	0.21	0.28	0.36
Retail & Wholesale Trade	0.29	0.36	0.44
Information	0.37	0.37	0.37
Transportation	0.06	0.07	0.08
Total	**3.96**	**4.81**	**5.81**

Source: Gartner (August 2019)

рис.1.2 - IoTринок кінцевих точок

Переваги Інтернету речей для бізнесу

Переваги IoT для бізнесу залежать від конкретного впровадження; спритність та ефективність, як правило, є головними міркуваннями. Ідея полягає в тому, що підприємства повинні мати доступ до більшої кількості даних про власну продукцію та власні внутрішні системи та більшу здатність вносити зміни в результаті.

Виробники додають датчики до компонентів своєї продукції, щоб вони могли передавати дані про те, як вони працюють. Це може допомогти компаніям визначити, коли компонент може вийти з ладу, і замінити його, перш ніж він заподіє шкоду. Компанії також можуть використовувати дані, що генеруються цими датчиками, щоб зробити свої системи та їх ланцюги постачання більш ефективними, оскільки вони матимуть набагато точніші дані про те, що насправді відбувається.

"Завдяки впровадженню всебічного збору та аналізу даних у режимі реального часу виробничі системи можуть стати значно гнучкішими", - кажуть консультанти МакКінсі.

Підприємницьке використання IoT можна розділити на два сегменти:

галузевіпропозиції, такі як датчики на генеруючій установці або пристрої визначення місцезнаходження в реальному часі для охорони здоров'я; та пристрої IoT, які можна використовувати у всіх галузях промисловості, наприклад, розумні системи кондиціонування або системи безпеки.

Хоча галузеві вироби будуть працювати на початку, до 2020 року Gartner прогнозує, що міжгалузеві пристрої досягнуть 4,4 млрд. Одиниць, тоді як вертикальні пристрої становитимуть 3,2 млрд. Одиниць. Споживачі купують більше пристроїв, але підприємства витрачають більше: аналітична група заявила, що, хоча витрати споживачів на пристрої IoT минулого року становили близько 725 млрд доларів, витрати підприємств на IoT сягнули 964 млрд доларів. До 2021 року витрати бізнесу та споживачів на обладнання IoT сягнуть майже $ 3 трлн.

Промисловий Інтернет речей:

Промисловий Інтернет речей (IIoT), або четверта промислова революція, або Індустрія 4.0 - все це назви використання технології IoT в бізнес-середовищі. Концепція така ж, як і для побутових пристроїв IoT вдома, але в цьому випадку метою є використання комбінації датчиків, бездротових мереж, великих даних, AI та аналітики для вимірювання та оптимізації промислових процесів.

Якщо його впровадити по всьому ланцюгу поставок, а не лише по окремих компаніях, вплив може бути ще більшим за умови своєчасної доставки матеріалів та управління виробництвом від початку до кінця. Підвищення продуктивності робочої сили або економії витрат - дві потенційні цілі, але IIoT може також створити нові потоки доходів для бізнесу; замість того, щоб просто продавати автономний продукт - наприклад, як двигун - виробники можуть також продавати прогнозне обслуговування двигуна.

Які переваги Інтернету речей для споживачів

IoT обіцяє зробити наше довкілля - наші будинки, офіси та транспортні засоби - розумнішими, більш вимірюваними та ... балакучими. Розумні колонки, такі як EchoAmazon і GoogleHome, полегшують відтворення музики, налаштування таймерів або отримання інформації. Системи домашньої безпеки полегшують відстеження того, що відбувається всередині та зовні, або бачення та

спілкування з відвідувачами. Тим часом, розумні термостати можуть допомогти нам обігріти наші будинки до того, як ми повернемося назад, а розумні лампочки можуть зробити так, щоби ми були вдома, навіть коли ми вийшли.

Дивлячись за межі дому, датчики можуть допомогти нам зрозуміти, наскільки галасливим або забрудненим може бути наше довкілля. Самохідні машини та розумні міста можуть змінити спосіб побудови та управління нашими громадськими просторами.

Інтернет речей та розумні будинки

Для споживачів розумний дім, ймовірно, там, де вони можуть зіткнутися з речами з підтримкою Інтернету, і це одна область, де великі технологічні компанії (зокрема Amazon, Google та Apple) жорстко конкурують.

Найбільш очевидні з них - це розумні колонки, такі як AmazonEcho, але є також розумні штекери, лампочки, камери, термостати та дуже глузливий розумний холодильник. Але не лише демонструючи свій ентузіазм до нових блискучих пристосувань, у розумних домашніх додатків є й більш серйозна сторона. Вони можуть допомогти тримати людей похилого віку незалежними і довше у своїх будинках, полегшуючи спілкування з ними сім'ї та опікунів та відстеження їхнього розвитку. Краще розуміння того, як працюють наші будинки, та можливість налаштування цих параметрів можуть допомогти заощадити енергію - наприклад, зменшивши витрати на опалення.

На рис.1.3. зображено будинок, який побудувала Alexa: вітрина Amazon у Лондоні в 2017 році.Зображення: Стів Рейнджер / ZDNet.

рис.1.3 - Розумний будинок(вітрина Amazon)

А як щодо безпеки Інтернету речей

Безпека - одна з найбільших проблем IoT. Ці датчики збирають у багатьох випадках надзвичайно конфіденційні дані - наприклад, про те, що ви говорите та робите у своєму будинку. Забезпечення такої безпеки є життєво важливим для довіри споживачів, але поки що послуга безпеки IoT була надзвичайно низькою. Занадто багато пристроїв IoT мало замислюються над основами безпеки, такими як шифрування даних під час передачі та відпочинку.

Недоліки програмного забезпечення - навіть старого та добре використовуваного коду - регулярно виявляються, але багато пристроїв IoT не мають можливості виправлення, що означає, що вони постійно ризикують. Зараз хакери активно націлюються на пристрої IoT, такі як маршрутизатори та веб-камери, оскільки властивий їм недостатній рівень безпеки робить їх легкими для компромісів і згортання у гігантські бот-мережі.

Недоліки залишили розумні домашні пристрої, такі як холодильники, духовки та посудомийні машини, відкритими для хакерів. Дослідники виявили 100 000 веб-камер, які можна було легко зламати, тоді як деякі підключені до Інтернету розумні годинники для дітей містять уразливі місця безпеки, які

дозволяють хакерам відстежувати місцезнаходження користувача, підслуховувати розмови або навіть спілкуватися з користувачем.

Уряди все більше стурбовані ризиками тут. Уряд Великобританії опублікував власні рекомендації щодо безпеки споживчих пристроїв IoT. Він очікує, що пристрої матимуть унікальні паролі, що компанії надаватимуть публічну контактну особу, щоб кожен міг повідомити про вразливість (і що вони будуть діяти), а виробники чітко зазначити, як довго пристрої отримуватимуть оновлення безпеки. Це скромний список, але початок.

Коли витрати на виготовлення розумних об'єктів стануть незначними, ці проблеми лише стануть більш поширеними та нерозв'язаними.

Все це стосується і бізнесу, але ставка ще більша. Підключення промислового обладнання до мереж IoT збільшує потенційний ризик хакерів виявити та атакувати ці пристрої. Промисловий шпигунство або руйнівний напад на критичну інфраструктуру - це потенційні ризики. Це означає, що компаніям потрібно буде переконатися, що ці мережі є ізольованими та захищеними, а необхідність шифрування даних із захистом датчиків, шлюзів та інших компонентів. Однак сучасний стан технологій IoT ускладнює це забезпечення, як і відсутність послідовного планування безпеки IoT в організаціях. Це дуже тривожно, враховуючи задокументовану готовність хакерів підробляти промислові системи, які були підключені до Інтернету, але залишились незахищеними.

IoT усуває розрив між цифровим та фізичним світом, а це означає, що злом пристроїв може мати небезпечні наслідки в реальному світі. Злом датчиків, що контролюють температуру на електростанції, може змусити операторів прийняти катастрофічне рішення; Управління автомобілем без водія також може закінчитися катастрофою.

Приватність Інтернету речей

Тепер, коли ми розібрали безпеку, що до приватності Інтернету речей.З усіма тими датчиками, які збирають дані про все, що ти робиш, IoT - це потенційно величезний головний біль щодо конфіденційності та безпеки. Візьміть розумний дім: він може визначити, коли ви прокидаєтесь (коли активується

розумна кавоварка) і наскільки добре ви чистите зуби (завдяки вашій розумній зубній щітці), яку радіостанцію ви слухаєте (завдяки вашому розумному динаміку), який тип їжі ви їсте (завдяки вашій розумній духовці або холодильнику), що думають ваші діти (завдяки їх розумним іграшкам) і хто відвідує вас і проходить повз ваш будинок (завдяки вашому розумному дзвінку). Хоча компанії зароблятимуть гроші, продаючи вам розумний об'єкт, насамперед, їхня бізнес-модель IoT, ймовірно, передбачає продаж принаймні деяких цих даних.

Те, що відбувається з цими даними, є життєво важливим питанням конфіденційності. Не всі компанії розумних будинків будують свою бізнес-модель навколо збору та продажу ваших даних, але деякі роблять це.

І варто пам'ятати, що дані IoT можна поєднувати з іншими бітами даних, щоб створити напрочуд детальну картину про вас. Напрочуд легко дізнатися багато про людину за кількома різними показаннями датчика. В одному з проектів дослідник виявив, що, проаналізувавши дані, що відображають лише споживання енергії в будинку, рівні окису вуглецю та вуглекислого газу, температуру та вологість протягом дня, вони могли визначити, що хтось вечеряв.

Також звертаючи увагу на конфедеційність ті бізнес IoT, споживачі повинні розуміти обмін, який вони проводять, і чи задоволені вони цим. Деякі з тих самих питань стосуються бізнесу: чи ваша команда виконавців із задоволенням обговорить питання злиття в залі для переговорів, обладнаній, наприклад, розумними колонками та камерами? Одне недавнє опитування показало, що чотири з п'яти компаній не зможуть ідентифікувати всі пристрої IoT у своїй мережі.

Погано встановлені продукти IoT можуть легко відкрити корпоративні мережі для атаки хакерів або просто витоку даних. Це може здатися тривіальною загрозою, але уявіть, якби розумні замки у вашому офісі одного разу відмовлялися відкриватись, або розумна метеостанція в офісі генерального директора використовувалася хакерами для створення бекдору у вашій мережі.

IoT та кібервійни:

IoT робить обчислення фізичними. Тож якщо з пристроями IoT все піде не так, це може мати серйозні наслідки в реальному світі - те, що зараз беруть до уваги країни, які планують свої стратегії кібервійни.

Брифінги британської розвідувальної спільноти попереджали, що супротивники країни вже мають можливість загрожувати її критичній інфраструктурі, а також "як ширшій екосистемі підключених споживчих та промислових пристроїв, відомій як Інтернет речей". Американська розвідка також попередила, що підключені термостати, камери та кухонні плити можуть використовуватися або для шпигунства за громадянами іншої країни, або для хаосу, якщо їх зламують. Додавання до IoT ключових елементів національної критичної інфраструктури (таких як дамби, мости та елементи електричної мережі) робить ще більш важливим, щоб безпека була якомога жорсткішою.

IoT та дані:

Пристрій IoT, швидше за все, міститиме один або кілька датчиків, які він використовуватиме для збору даних. Те, що збирають ці датчики, буде залежати від окремого пристрою та його завдання. Датчики всередині промислових машин можуть вимірювати температуру або тиск; камера безпеки може мати датчик наближення разом із звуком та відео, тоді як ваша домашня метеостанція, ймовірно, буде мати датчик вологості. Всі ці дані датчика - і багато, багато іншого - доведеться кудись відправити. Це означає, що пристроям IoT потрібно буде передавати дані і робитимуть це через Wi-Fi, 4G, 5G та інше.

Технічний аналітик IDC підрахував, що протягом п’яти років гаджети IoT створюватимуть 79,4 зеттабайта даних. Деякі з цих даних IoT будуть "дрібними і непомітними", говорить IDC - таке швидке оновлення, як зчитування температури з датчика або зчитування зі смарт-лічильника. Інші пристрої можуть створювати величезні обсяги трафіку даних, наприклад камера відеоспостереження за допомогою комп'ютерного зору.

IDC заявляє, що обсяг даних, створених пристроями IoT, буде швидко зростати в найближчі кілька років. За його словами, більшість даних генерується за допомогою відеоспостереження, але з часом інші промислові та медичні цілі

дадуть більше даних.

У ній сказано, що безпілотники також будуть важливим фактором створення даних за допомогою камер. Дивлячись далі, самокеровані машини також генеруватимуть величезну кількість багатих даних датчиків, включаючи аудіо та відео, а також більш спеціалізовані дані автомобільних датчиків.

Оскільки ціни на датчики та зв'язок продовжують падати, додавати більше пристроїв до Інтернету речей стає економічно вигідним - навіть якщо в деяких випадках очевидна користь для споживачів невелика. Розгортання перебувають на початковій стадії; більшість компаній, які працюють з IoT, зараз перебувають на стадії випробування, значною мірою тому, що необхідні технології - сенсорна технологія, 5G та аналітика, що працює на основі машинного навчання - все ще перебувають на досить ранній стадії розвитку. Існує багато конкуруючих платформ і стандартів, і багато різних постачальників, від виробників пристроїв до програмних компаній до мережевих операторів, хочуть отримати шматочок пирога. Досі незрозуміло, хто з них виграє. Але без стандартів і з постійною проблемою безпеки ми, найімовірніше, побачимо ще кілька великих випадків безпеки IoT у найближчі кілька років.

По мірі збільшення кількості підключених пристроїв наше життєве та робоче середовище буде наповнене розумними продуктами - припускаючи, що ми готові прийняти компроміси щодо безпеки та конфіденційності. Деякі вітатимуть нову еру розумних речей. Інші будуть хворіти в ті дні, коли стілець був просто стільцем.

1.3 Хмара на основі Інтернету речей

Величезний обсяг даних, який генерують додатки IoT, означає, що багато компаній вирішать обробляти дані в хмарі, а не створювати величезні обсяги власних потужностей. Гіганти хмарних обчислень вже сватаються до цих компаній: Microsoft має свій пакет Azure IoT, тоді як Amazon Web Services надає широкий спектр послуг IoT, як і Google Cloud.

IoT та хмарні обчислення швидко розвиваютьсята мають своїунікальні характеристики.Взагалі , підхід IoT базується на розумних пристроях, яківзаємодіють у глобальній мережі та динамічній інфраструктурі. IoT, як правило, характеризується широко розподіленими пристроямиз обмеженими можливостями обробки та зберігання. Ці пристроїстикаються з проблемами щодо продуктивності, надійності, конфіденційності, та безпеки. З іншого боку, хмарні обчислення складаються з масивної мережі з необмеженим сховищем.

Приклад хмарних обчислень та IoT в дії:

Ви прокидаєтесь лише в черговий понеділок вранці, починає лунати заспокійлива музика, ваша щоденна розчинна кава готова, укомплектована хлібним тостом, і вас інформують про останні новини, сповіщення та погодні звіти за день. У цьому сила поєднання хмарних обчислень та IoT. Це лише попередник тієї автоматизації, на яку люди роблять орієнтацію роками. Покращуючи технології передачі даних, все більше і більше пристроїв наближаються, щоб створити систему, яка кардинально змінює потенціал гаджетів завдяки включенню IoT та хмарних обчислень.

Ось ще один приклад - машина. Здійснивши довгу дорожню подорож, людина повернулася з рідного міста. Його машина попереджає його про деякі проблеми через сигнал на приладовій панелі. Тепер він бентежить, чи це незначна несправність, чи йому слід негайно повідомити про це механіка. Після базової діагностики він виявляє, що у гальмівної системи виникають певні проблеми.

Тепер, у цьому випадку, датчик розриву повідомив Маніш про несправність. Подібним чином існує безліч датчиків, які надсилають попереджувальні сигнали на головний контролер біля приладової панелі, який обробляє його та надсилає на екран у відповідний час. Отже, як ми бачили в цьому випадку, кілька маленьких пристроїв співпрацювали між собою, виконуючи дію, яка в іншому випадку виконувалась би окремо, що зажадало б великих зусиль.

Розуміння тісних відносин між хмарою та IoT

Мільйони розробників та компаній працюють над програмами Інтернету речей та хмарних обчислень. IoT також порушив різні сфери, включаючи ланцюги

поставок, освіту, архітектуру тощо. Від полегшення способу життя людей до забезпечення перевірок безпеки, розгляду нових несправностей, автоматичної передачі даних, автоматизації робототехніки та навіть виголошення тостів за людей, IoT все зробив.

У прикладі, який ми бачили вище, різні датчики або компоненти взаємодіяли в системі через фізичні зв’язки. З вдосконаленням бездротових режимів зв'язку IoT розширив різні можливості.

1. Зберігання даних:

Щоб зрозуміти роль хмарних обчислень в Інтернеті речей, давайте подумаємо про ситуацію, коли ми виймаємо деякі компоненти із системи та розміщуємо їх у хмарі, до яких можна отримати доступ через Інтернет. Зараз система не ламається, але вона забезпечує альтернативний спосіб зберігання та обробки даних у комбінованій системі IoT та хмарних обчислень. Наприклад, ви програмуєте свою Alexa, щоб щоранку інформувати вас про останні новини, погоду та дані про дорожній рух. Alexa, хмарний IoT, надсилає запити до хмарних додатків, таких як Карти Google тощо, щоб отримати інформацію та надати її вам.

2. Захист даних:

Окрім цього, безпечна інтеграція IoT та хмарних обчислень також допомагає уникнути витоку даних та атак. Зберігати дані (які можуть містити ключі та паролі) на локальному пристрої, як правило, не є гарною ідеєю. Для промислових додатків безпеку можна підвищити, шифруючи важливу інформацію в хмарі. Крім того, зберігання величезної кількості даних на локальних машинах може бути трудомістким та дорогим процесом. Обмеження обробки на локальних машинах також обмежені, і для складних операцій та програм хмара представляється життєздатним варіантом.

Інтеграція IoT та хмарних обчислень розширила численні можливості та відкрила двері для доменів, які працюють за для безпеки інтеграції IoT та Хмари та великого обсягу даних для обробки. У найближчі роки, коли з’являється все більше і більше постачальників IoT Cloud, ми можемо очікувати побачити нові захоплюючі програми IoT Cloud Computing. Корочекажучи, хмарні обчислення

мають велечезн іможливості та гігантську обчислювальну потужність. Крім того, сама хмара передбачає гнучке, надійне середовище, яке дозволяє отримувати динамічні даніз різних джерел. Хмарні обчислення мають частково вирішені питанння IoT. Справді, IoT та Хмара - це дві порівняно складні технології, і вони поєднуються для того, щоб змінити теперішнє та майбутнє середовище Інтернет-послуг.

Хмара Інтернету речей - це платформа, якадозволяє розумно використовувати програми, інформацію та інфраструктуру економічно вигідним способом.

Тоді як обчислення IoT та Хмари відрізняються один від одного, їх особливості є майже доповнюваними, як показано на Таблиці.1.1. Це взаємодоповнення є основною причиною того, чому багато дослідників запропонували інтеграцію IoT та Хмари.

Пункти	IoT	Хмарне обчислення
Характеристики	Iot є повсюдним (речі існують всюди).Це об’єкти реального світу.	Хмара являється повсюдною(ресурси доступні звідусіль). Ці ресурси є віртуальними.
Можливості обробки	Можливості обчислення обмежені.	Можливості віртуального обчислення необмежені.
Можливості зберігання	Обмежене зберігання, або взагалі не має можливості зберігання.	Можливості зберігання необмежені
З'єднання	Використовується інтернет, як точка збіжності.	Використовується інтернет для послуг доставки.
Великі дані	Це є джерелом великих даних.	Це засіб управліннями великими даними.

Таблиця.1.1 - Особливості IoTта хмари

Взагалі, на мою думку, хмарата IoT-це ідеальне поєднання.У типовому розгортанні IoT існує багато датчиків (десятки, сотні або тисячі), які збирають дані та відправляють їх у центральне місце для аналізу. У багатьох випадках

місцем збору є хмара. Хмарне управління дозволяє операторам мобільних мереж отримувати доступ до даних датчиків з будь-якої точки світу за допомогою Інтернет-порталу. За допомогою хмарного управління оператор може отримати доступ до даних з будь-якого місця за допомогою будь-яких пристроїв та підключення до Інтернету.

Наприклад, якщо морські датчики, прикріплені до буїв, розкидані по Мексиканській затоці, MNO може витягувати дані на планшет для оцінки проблем з технічним обслуговуванням або аналізу даних. Без хмари агрегування даних IoT на великих площах та на різних пристроях реалізується набагато складніше. Багато постачальників IoT також пропонують платформи IoT - програми SaaS, які допомагають менеджерам IoT перебирати свої підключені пристрої та дані здалеку. А хмарні провайдери дозволяють компаніям зберігати та обробляти великі обсяги даних з мінімальними витратами,відкриваючи двері для аналізу великих даних.

Незважаючи на те, що хмара є необхідною для більшості розгортань IoT, нещодавно відбулося повернення для обробки локальних даних для деяких функцій. Крайові обчислення утримують частину обробки даних на межі мережі, де розташовані датчики IoT та кінцеві пристрої. Це важливо в деяких додатках IoT, таких як автономні машини, де будь-яка затримка в аналізі даних та прийнятті рішень може призвести до аварії. У деяких випадках крайові обчислення можуть додати рівень безпеки. Наприклад, рішення IoT можуть використовувати крайові обчислювальні системи для передачі операційних даних технологій керівникам заводів, а не надсилати всі дані датчиків безпосередньо в хмару. Це мінімізує потенційний ризик безпеки передачі всього по повітрю. Але хоча передача даних через Інтернет завжди викликає певні проблеми з безпекою, профілактичні дії можуть значно покращити безпеку хмарних обчислень.

2 АРХІТЕКТУРА IOT НА ОСНОВІ ХМАРИТА ПЕРЕВАГИ ІНТЕГРАЦІЇ

Згідно з низкою попередніх досліджень, архітектура IoT зазвичай поділяється на три різні рівні:

1. *Застосування*
2. *Сприйняття*
3. *Мережевий рівень*

Більшість припускають, що мережевий рівень - це хмарний шар, який реалізує архітектуру IoT, базовану в хмарі, як показано на рисунку 2.1.

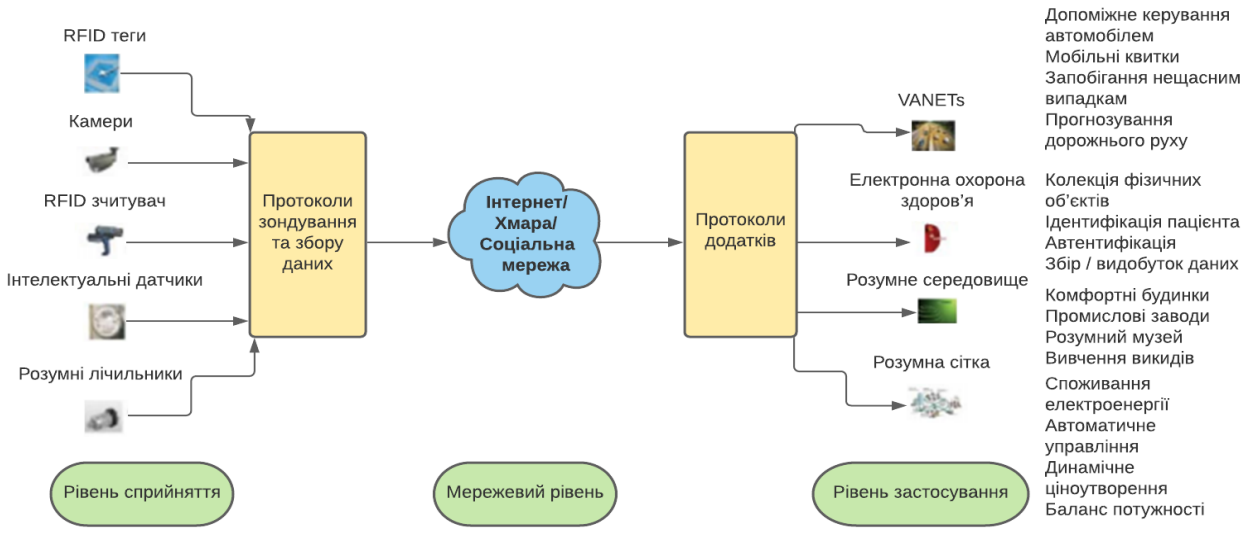

рис.2.1- Архітектура IoT

Шар сприйняття використовується для ідентифікації предметів та збирання даних, які збираються з навколишнього середовища. Основною метою мережевого рівня є передача зібраних даних в Інтернет / Хмару. Нарешті,рівень застосування забезпечує інтерфейс для різних служб.

2.1 Архітектура хмарних клієнтів для IoT

Інтернет речей (IoT) - одна із найбільш захоплюючих та найдинамічніших сфер IT на даний час. IoT передбачає зв'язок фізичних осіб ("речей") з IT-системами, які отримують інформацію про або з тих речей, які можуть бути використані для створення найрізноманітніших програм та послуг, які можуть бути прямо чи опосередковано пов’язані з цими речами. IoT охоплює дуже широкий спектр додатків, що охоплюють підприємства, уряди та споживачів та представляє інтеграцію системи традиційно різних спільнот: інформаційні технології та операційні технології.

Як результат, для систем IoT важливо мати архітектуру, принципи систем та операції , які можуть задовольнити цікаві вимоги до масштабу, безпеки, надійності та конфіденційності.

Деякі приклади застосування IoT включають:

Логістичні програми: телеметрія флоту та управління ланцюгами поставок; відстеження фізичного такі як об'єкти, як пакунки та контейнери;

Виробниче та промислове застосування, що включає контроль та експлуатацію промисловихобладнаннь та розумні виробничі лінії;

Управління активами та розумні стелажі. Підключені пристрої зберігання та продажу.

Автоматизація будівель або «розумні будівлі», де застосовуються системи моніторингу та управління, всі системи всередині будівлі, що полегшує безперебійну роботу будівлі та ініціативнууправління та обслуговування обладнання та обладнання;

Розумні транспортні системи, зокрема управління автомобільним та залізничним транспортом;

Підключені транспортні засоби, що включають такі можливості, як подача інформації водіям про стан дорогиабо використання «чорних ящиків», які динамічно оцінюють страхові ризики / премії;

Розумні міста, де моніторинг та контроль загальноміських систем обробляються автоматичнобільшої ефективності та кращого обслуговування громадян;

Розумні електромережі, що включають приладування електричної мережі в будь-якому масштабі для кращого управління та обслуговування обладнання для оптимізації використання електроенергії в електромережі таборотьба з переривчастими джерелами живлення, такими як вітер;

Споживчі програми, як правило, засновані на використанні смартфонів та носіїв;

Медичні програми, такі як дистанційне спостереження та лікування пацієнтів;

Роздрібна торгівля та «інтелектуальні покупки» - використання інформації про споживача для здійснення пропозиції та спрямувати споживача на предмети, що цікавлять;

Розумний дім - автономне управління домашніми приміщеннями, включаючи контроль опаленнясистем, експлуатації побутових приладів і поширюючись на автоматизацію технічного обслуговування замовлення витратних матеріалів (продуктів харчування тощо).

Основоположними для IoT є електронні пристрої, які взаємодіють з фізичним світом; датчики, які збирають інформація про предмети та діяльність людини; виконавчі механізми, які можуть діяти на предмети. Датчики можуть приймати багато форм. Такі пристрої, як термометри та акселерометри, вимірюють характеристики реального світу і генерують числову інформацію, тоді як камери та мікрофони створюють потоки відеота аудіоінформація, що містить більш складну інформацію про реальний світ. Маяки та вантаж датчики також входять до категорії IoT. Пускачі також приймають різні форми - наприклад, реле які можуть вмикати або вимикати обладнання, наприклад, обігрівач, деталь виробничого обладнання або ж дисплеї, які можна використовувати для інформування людей, таких як водії.

Існує кілька аспектів, які стосуються систем IoT, що впливають на їх архітектуру та здійснення, як показано нижче:

1. *Масштабованість:* шкала для системи IOT застосовується з точки зору кількості датчиків та виконавчих механізмів підключені до системи, з точки зору мереж, що з'єднують їх між собою, з точки зору обсягу даних, пов'язаних із системою, та швидкістю її руху, а також у умови необхідної обчислювальної потужності.

2. *Великі дані:* Багато вдосконалених систем IoT залежать від аналізу величезної кількостіданих. Існує потреба, наприклад, витягати зразки з історичних даних, які можна використовувати керуватися рішеннями щодо майбутніх дій. Вилучення корисної інформації зі складної такі дані, як відео, є ще одним прикладом аналізу, що вимагає обробки великих обсягів. Можливість видобування існуючих даних для отримання нових знань та необхідність поєднання різних наборів даних унові способи - це характеристики, які можуть бути частиною системи IoT. Таким чином, системи IoT часто єкласичні приклади обробки великих даних.

3. *Хмарні обчислення:* системи IoT часто передбачають використання хмарних обчислювальних платформ.Платформи хмарних обчислень дають можливість використовувати великі обсяги ресурсів, як вумови зберігання даних, а також здатність забезпечити гнучку та масштабовану обробку ресурсів для аналізу даних. Системи IoT, ймовірно, потребуватимуть використання різноманітних програмних забезпеченнь для обробки - і для адаптації хмарних сервісів, ймовірно, знадобиться порядоквирішувати нові вимоги, оновлення мікропрограми або системи та пропонувати нові можливості.

4. *Реальний час:* системи IoT часто функціонують у реальному часі; дані постійно надходять про події в прогресі, і може виникнути потреба в своєчасному реагуванні на цей потік подій. Цеможе передбачати обробку потоку; діючи на дані події в міру надходження, порівнюючи їх ізпопередні події, а також проти статичних даних, щоб реагувати найбільш відповідним чином.Існує паралельна необхідність гарантувати, що пошкоджені дані виявляються та не

використовуються - чи топредставлені несправними датчиками або зловмисними діями - оскількивикористання пошкоджених даних можезавдавати шкоди та шкоди людям, техніці та навколишньому середовищу.

5. *Високо розподілений:* системи IoT можуть охоплювати цілі будинки, цілі міста і навіть охоплюватиГлобус. Широке розповсюдження може також застосовуватися до даних - які можна зберігати на краюмережі або зберігаються централізовано. Поширення може стосуватися і обробки - деяка обробкавідбувається централізовано (у хмарних сервісах), але обробка може відбуватися на краюабо в шлюзах IoT, або навіть у межах (більш спроможних типів) датчиків і виконавчих механізмів. Сьогодні в світі офіційно більше мобільних пристроїв, ніж людей. Мобільні пристрої та мережі є одними з найвідоміших пристроїв та мереж IoT.

6. *Неоднорідні системи:* системи IoT часто будуються з використанням дуже різнорідного набору. Цезастосовується до датчиків та виконавчих механізмів, але також стосується типів задіяних мереж тарізноманітність обробних компонентів. Загальноприйнятим для датчиків є малопотужні пристрої,і часто буває так, що ці пристрої використовують спеціалізовані локальні мережі для зв'язку. Щоб увімкнути доступ до Інтернету до пристроїв такого роду, використовується шлюз IoT.

7. *Безпека та конфіденційність:* Питання про безпеку та надійність розподілених неоднорідних системи IoT - важка проблема, рішення якої мають масштабуватися та розвиватися. Необхідний захист даних, включаючи серйозні проблеми щодо конфіденційності даних, що стосуються фізичних осіб. Отримавши впевненість, що ці системи безпечні, надійні,стійкі та підтримувати очікування своїх зацікавлених сторін щодо конфіденційності є особливо складним завданням.

8. *Відповідність:*Необхідно забезпечити впевненість у роботі цих систем IoT, завдяки правилам конкретних галузей та вертикалей, так і нормамочікування зацікавлених сторін систем IoT.

9. *Інтеграція:* системи IoT не існують самі по собі, але їх потрібно

підключати до існуючих операційних технологічних систем, такі як заводські системи, системи управління будівлею та іншітипи систем фізичного управління, а також існуючі корпоративні системи, включаючикорпоративні програми та корпоративні бази даних.

Розуміння архітектур IoT ґрунтується на розумінні мобільних пристроїв, хостингу веб-додатків та великих даних та аналітичних можливостей. На рисунку 2.2 показані елементи, які можуть знадобитися для будь-якого рішення IoT у п’яти доменах: рівень користувача,наближені мережі, загальнодоступні мережі, хмари постачальників та корпоративні мережі.

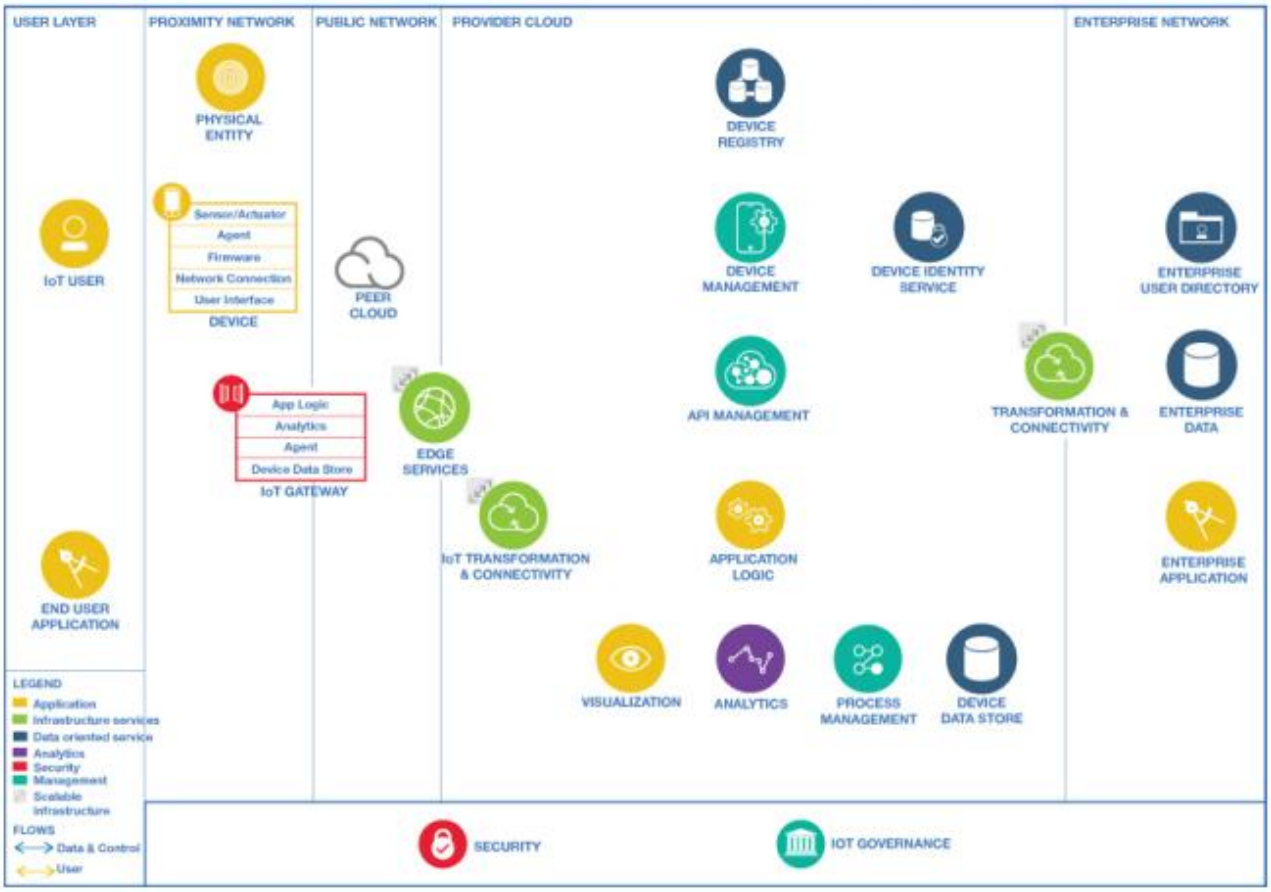

рис.2.2 - Елементи IoT рішеннь

Аспекти архітектури включають:

1. Рівень користувача не залежить від будь-якого конкретного домену мережі. Це може бути в будь-якому або поза ним конкретний домен.

2. Домен безконтактної мережі має мережеві можливості, які зазвичай

поширюють загальнодоступний доступ мережевий домен. Пристрої (включаючи датчик / привід, прошивку та агент управління) і фізична сутність є частиною домену близькості мережі. Пристрої спілкуються як для потоку даних, так і для управління потоком або через шлюз IoT, ічерез граничні служби, або безпосередньо через загально доступнумережу через крайові служби.

3. Домени загальнодоступної мережі та корпоративної мережі містять джерела даних, які живлятьціла архітектура. Джерела даних включають

традиційні системи запису від підприємства а також нові джерела зІнтернету речей (IoT). Публічна мережа включає спілкування з хмарами однолітків.

4. Хмара постачальника збирає дані з пристроїв, хмарних служб та інших джерел даних(наприклад, служби погоди). Він може використовувати технології інтеграції або обробку потоку длятрансформувати, фільтрувати та аналізувати ці дані в режимі реального часу, і він може зберігати дані у сховищахде можна проводити подальшу аналітику. Ця обробка, яку можна доповнитивикористанням когнітивної та передбачувальної аналітики використовується для створення активних статистичних даних. Цістатистичні дані використовуються користувачами та корпоративними додатками, а також можуть використовуватися для ініціювання дій та виконуватися виконавцями IoT. Все це потрібно робити в безпечному та керованомусередовищі.

5. Результати доставляються користувачам та додаткам із використанням трансформації та підключенними компонентами, що забезпечують безпечний обмін повідомленнями.

На рисунку 2.3 показані можливості та взаємозв'язки для підтримки IoT за допомогою хмарних обчислень.

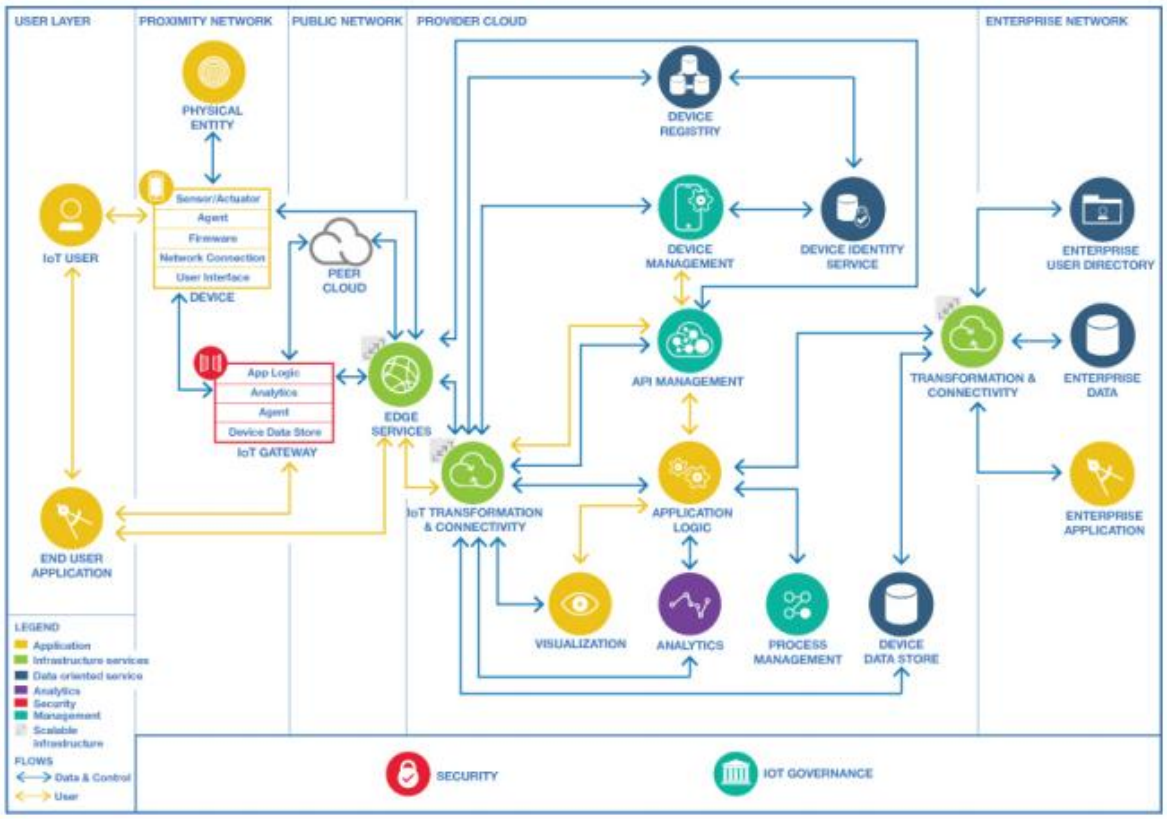

Рис.2.3 - Хмарні компоненти для IoT

Хмарні компоненти архітектури IoT розміщені в межах трирівневої архітектурної схемищо включає крайові, платформові та корпоративні рівні, як описано в Індустріальному Інтернет-консорціумі(довідкова архітектура).

1. **Крайній рівень** включає близькі мережі та загальнодоступні мережі, з яких збираються даніта передаються на пристрої. Дані протікають через шлюз IoT або, за бажанням, безпосередньовід / до пристрою, а потім через крайові служби до хмарного провайдера через перетворення IoTта підключення.

2. **Рівень платформи** - це хмара постачальника, яка приймає, обробляє та аналізує потоки даних, крайовий рівень і забезпечує управління та візуалізацію API. Це забезпечує можливістьініціювати команди управління з корпоративної мережі також у загальнодоступну мережу.

3. **Рівень підприємства** представлений мережею підприємств, що складається з даних підприємства, каталог корпоративних користувачів та корпоративні програми. Потік даних до і з підприємства, мережа відбувається за допомогою компонента «Трансформація та підключення». Дані, зібрані

зструктурованих та неструктурованих джерел даних, включаючи дані в режимі реального часу з потокових обчислень,можуть зберігатися в даних підприємства.

Однією з особливостей систем IoT є необхідність застосування логіки та логіки управління в ієрархії розташування, залежно від часових масштабів та наборів даних, які потрібно застосувати до рішення, які потрібно прийняти. Деякий код може виконуватися безпосередньо в пристроях на самому краю мережі, або в шлюзах IoT, поруч із пристроями. Інший код виконується централізовано в хмарних послугах провайдера або в корпоративній мережі. Іноді застосовується термін «обчислення краю» до випадку, коли код виконується в шлюзах IoT або на пристроях. Це іноді альтернативно називається "обчислення туману" на відміну від централізованих "хмарних обчислень", хоча обчислення туману також можуть містити один або кілька шарів під хмарою, кожен з яких потенційно може забезпечити можливості для різноманітних таких послуг, як аналітика. Ця конструкція забезпечує гнучкість у тому, як розраховано на зв’язок та послуги, оптимізацію та стійкість. Підсистеми управління та безпеки IoT охоплюють усі елементи архітектури для забезпечення контролю та політики для всіх даних та програм визначаються та вмикаються в системі. Відповідність відстежується щоб переконатися, що засоби контролю дають очікувані результати.

2.2 Детальне описання хмарних компонентів для IoT

Користувацький рівень - містить користувачів IoT та їх додатки для кінцевих користувачів.

1. Користувач IoT (люди / система) - особа, або ж автоматизована

система, яка використовує одну або кілька програм для кінцевих користувачів, яка досягає якоїсь мети.

2. Додаток для кінцевого користувача - додаток для конкретного домену чи пристрою.Користувач IoT може використовувати додатки для кінцевих користувачів, які працюють на інтелектуальній системітелефони, планшети, ПК або, як варіант, на спеціалізованих пристроях IoTвключаючи панелі управління.

Proximity Network- містить фізичні сутності, які є суттю системи IoT

з пристроями, які взаємодіють з фізичними сутностями та підключають їх до системи IoT.

Фізична сутність - фізична сутність є об’єктом реального світу, який представляє інтерес - вона підлягає датчикувимірювань або поведінки виконавчого механізму. Це «річ» в Інтернеті речей. Ця архітектурарозрізняє фізичні сутності та IT-пристрої, які їх відчувають або діють на них. Наприклад, річ може бути океаном, і прилад, який спостерігає, - це термометр температури води.Інший приклад - депо-відправлення посилок: посилки - це фізичні особи і є пристроїз датчиками, здатними спостерігати та ідентифікувати кожну посилку - напр. за допомогою тегів RFID або за допомогою зчитувачів штрих-коду. Зрозуміло, що зчитувач тегів RFID - це одне, а посилки - щось зовсім інше - ідентичність посилки - це фізична особа.

Пристрій - містить датчик (и) та / або привід (и), а також мережеве підключення, що забезпечує взаємодію з системоюIoT. Бувають випадки, коли пристрій є також фізичною суттю, за якою контролюютьсядатчики - наприклад, акселерометр у смартфоні.

1. Датчик / виконавчий механізм - відчуває і діє на фізичні сутності. Датчик є компонентом, який сприймає або вимірює певні характеристики в реальному світі і перетворює їх у цифрове представлення.

2. Агент - надає можливості віддаленого управління пристроєм,підтримка протоколу управління пристроєм, який може використовуватися службами керування пристроями або система управління IoT.

3. Прошивка - програмне забезпечення, що забезпечує управління, моніторинг. Прошивка, що міститься в таких пристроях, якпобутова електроніка забезпечує програму управління пристроями низького рівня.

4. Мережеве підключення - забезпечує підключення пристрою до системи IoT. Це часто є локальна мережа, яка з'єднує пристрій із шлюзом IoT - у багатьох низька потужність та низький діапазон для зменшення енерговитрат на пристрій. Однак бувають випадки, коли мережа підключенна безпосередньо до

загальнодоступної мережі, і шлюз IoT не потрібен. У системах IoT використовується широкий ряд альтернативних механізмів комунікації, які включають локальну мережуз використанням методів низького енергоспоживання та низького діапазону, таких як Bluetooth, BluetoothLowEnergy (BTLE) таінші. Це також може включати локальну мережу за допомогою Wi-Fi, широко масштабну мережу за допомогою 2G,3G та 4G, LTE.

Інтерфейс користувача - дозволяє користувачам взаємодіяти з програмами, агентами, датчиками та виконавчими механізмами (додатково -деякі пристрої не мають користувальницького інтерфейсу, і вся взаємодія відбувається із віддалених програм черезмережі).

IoTGateway - діє як засіб для підключення одного або декількох пристроїв до загальнодоступної мережі (як правило,Інтернет). Часто трапляється, що пристрої мають обмежене мережеве підключення - вони можуть бути не в змозідля прямого підключення до Інтернету. Це може бути з ряду причин, включаючи обмеження увімкніть пристрій, що може обмежити пристрій використанням малопотужної локальної мережі. Місцева мережа дозволяє пристроям обмінюватися даними з локальним шлюзом IoT, який потім зможеспілкуватися із загальнодоступною мережею. IoTGateway часто має інші можливості, включаючи можливостіфільтрувати та розумно реагувати на дані, можливість надсилати та отримувати дані або команди з Інтернету, можливість локального запуску логіки додатків або служб (обробка даних та виконання логіки управління без необхідності спілкуватися в центральному місці). Це також може забезпечити операційну ефективність шляхом, дозволяючи декільком пристроям спільно використовувати спільне з'єднання. IoTGateway містить наступні компоненти:

1. *Логіка додатків* - надає домен або рішення IoT, яка працює на шлюзі IoT. Для систем IoT, які мають виконавчі механізми, які діють на фізичних осіб, мають значні можливості логіки програм- це забезпечення логіки управління, яка робитьрішення про те, як повинні працювати приводи, враховуючи вхідні даніз датчиків та даних інших видів, які зберігаються локально або

зберігаютьсяцентралізовано.

2. *Analytics* - надає можливості аналізувати локально, а не в хмарі постачальника.

3. *Агент* - дозволяє керувати шлюзом IoT, а також може керувати сервером підключеного до пристроя, забезпечуючи з'єднання з керуванням пристроями хмарного рівня провайдерапослугу через протокол керування пристроєм.

4. *DeviceDataStore* - зберігає дані локально. Пристрої можуть генерувати велику кількість даних у режимі реального часуможливо, його потрібно буде зберігати локально, а не передавати в центральне місце. Дані всховище даних пристрою може використовуватися логікою програми та можливостями аналітики в IoTGateaway.

Громадська мережа - містить широкі мережі (як правило, Інтернет), однорангові хмарні системи, крайові послуги.

Peer Cloud - хмарна система сторонніх розробників, яка надає послуги з передачі даних та можливостей в IoT платформи. Хмари однолітків для IoT можуть сприяти передачі даних у системі IoT, а також можуть надавати деякі з нихможливості, визначені в цій архітектурі IoT. Наприклад, може використовуватися рішення IoT для страхування послуг від партнерів, такі як дані про погоду. Цілком ймовірно, що для більших систем IoT, таких як ті, що беруть участь у Smart Cities, насправді задіяніпоєднання низки менших систем IoT, кожна адресна частина рішення - ці "системи "передбачають зв'язок між кількома одноранговими хмарними системами, кожна з яких може мати пристрої IoTта пов'язані програми та послуги. Підключення цих окремих систем може дозволити більше комплексних рішенн.

Послуги Edge - послуги, необхідні для забезпечення безпечного надходження даних з Інтернету в хмару постачальникаі на підприємство. Послуги Edge також підтримують програми для кінцевих користувачів. Послуги Edge включають:

1. *Сервер системи доменних імен* - визначає URL-адресу певноговеб-

ресурсу на TCP-IP-адресу системи або служби, якаможе доставити цей ресурс.

2. *Мережі доставки вмісту (CDN)* - підтримують програми кінцевих користувачів забезпечуючи географічно розподілені системи серверів розгорнуто, щоб мінімізувати час відгуку для обслуговування ресурсівгеографічно розподілених користувачів, забезпечуючи високий вміст доступності та надаються користувачам із мінімальною затримкою. Які задіяні сервери залежатимуть від близькості сервера до користувача,і де вміст зберігається або кешується.

3. *Брандмауер* - керує комунікаційним доступом до системи. Брандмауери можутьбути реалізованим як окреме виділене обладнання або як компонент в інших мережах обладнання, таке як балансер навантаження або маршрутизатор, або як інтегральне програмне забезпечення для операційної системи.

4. *Балансери навантаження* - забезпечує розподіл мережевого або додаткового трафіку за багатьма ресурсами(таких як комп'ютери, процесори, сховище чи мережеві посилання), щоб максимізувати пропускну здатність, мінімізуватичас відгуку, збільшення потужності та підвищення надійності додатків. Навантажувачі можутьзбалансувати навантаження на місцевому та глобальному рівнях. Балансири навантаження повинні бути високодоступними без жодної точки відмови. Індикатори навантаження іноді інтегруються як частина аналітичної хмарної інформації провайдера, системні компоненти, такі як обробка потоків, інтеграція даних та сховища.

Провайдер Хмара - надає основні програми IoT та супутні послуги, включаючи зберігання пристроюдані; аналітика; управління процесами для системи IoT; створювати візуалізації даних. Елементи постачальника хмар включають:

Перетворення IoT та підключення

Логіка програми

Візуалізація

Аналітика

Управління процесами

Зберігання даних пристрою

API управління

Керування пристроями

Реєстр пристроїв

Служба ідентифікації пристрою

Трансформація та підключення

Середовище хмарних обчислень забезпечує масштабованість та еластичність, щоб впоратися з різним обсягом даних, швидкістю та відповідними вимогами до обробки. Експерименти та ітерації з використанням різних хмарконфігурації послуг - це хороший спосіб розвинути систему IoT без попередніх капіталовкладень.Трансформація та підключення IoT - забезпечує безпечне підключення з пристроїв IoT. Компонент повинен мати можливість обробляти та, можливо, перетворювати великі обсяги повідомлень і швидко маршрутизуватиїх до потрібних компонентів у рішенні IoT. Компонент трансформація та зв’язоквключає такі можливості:

1. *Безпечне з'єднання* - забезпечує захищене з'єднання, якеавтентифікує та авторизує доступ до хмари постачальника.

2. *Масштабованний обмін повідомленнями* - забезпечує обмін повідомленнями з пристроїв IoT.Для підтримки необхідна масштабованість компонента обміну повідомленнямипрограми з великим обсягом даних та програм з високою змінною швидкістю передачі даних.

3. *Масштабована трансформація* - забезпечує трансформацію IoT пристроюдані, перш ніж вони потраплять до хмарного шару провайдера, щоб надати форму більш придатну для обробки та аналізу. Це може включати декодуванняповідомлення, які зашифровані, перекладаючи стиснене відформатованеповідомлення та / або нормалізація повідомлень з різних пристроїв.

Логіка додатків - основні компоненти програми, які, як правило, координують роботу з IoT даними пристрою, виконання інших служб та

підтримка програм для кінцевих користувачів. Логіка програми може включати робочий процес. Логіка додатка може також включати логіку управління, якавизначає, як використовувати виконавчі механізми для впливу на фізичні сутності для тих систем IoT, які мають виконавчі механізми.

Візуалізація - дозволяє користувачам досліджувати та взаємодіяти з даними зі сховищ даних, що дієінсайт-додатки або корпоративні програми. До можливостей візуалізації належать інтерфейс кінцевого користувача та інтерфейс адміністратора, інформаційна панель як підкомпоненти.

Інтерфейс користувача кінцевого користувача - дозволяє користувачам спілкуватися та взаємодіятиз корпоративними програми, результати аналітики тощо. Сюди також входятьвнутрішні або мобільні користувальницькі інтерфейси, спрямовані на споживача.

Адміністративний інтерфейс - дозволяє адміністраторам отримувати доступ до показників, роботи з данними.

Інформаційна панель - дозволяє користувачам переглядати різні звіти. Інтерфейс адміністратора та інформаційна панель - це внутрішні інтерфейси користувача.

Аналітика - це виявлення та передача значущих зразків знайденої інформаціїв даних IoT, для опису, прогнозування та покращення ефективності бізнесу. Він охоплює наступні можливості для IoT:

1. *Сховище даних Analytics* - підтримує застарілі, нові та потокові передачіджерела, корпоративні програми, корпоративні дані, очищені даніта довідкові дані, а також результати потокової аналітики.Можливості включають: Дослідження та архівування (для зберігання, вивченняі збільшення великих наборів даних за допомогою різноманітних інструментів);Глибока аналітика та моделювання (застосування статистичних моделей дотримують інформацію з великих наборів даних, що складаються з обох неструктурованих та слабоструктурованих елементів); Інтерактивний аналіз та звітність (інструменти для відповіді на питання бізнесу та операційзапитання щодо наборів даних в масштабі Інтернету); Каталог даних.

2. *Когнітивна* - інтелектуальна система, яка навчається в масштабі, обґрунтовує свої цілі, аналізує, щоб передбачити,та щобпризначати та виявляти з масивних наборів даних взаємопов'язані фізичні, соціальні, підприємницькіта інших організацій, і замикає цикл з машинними порадами, допомогою та діями,таким чином, щоб самонавчатися та адаптуватися, щоб забезпечити розширений людський інтелект співпраця людини та машини.

3. *Дійовий аналіз* - розуміння, яке в кінцевому підсумку зумовлює дії, якими може скористатися бізнесдодатки з даних, зібраних, оброблених та збережених у сховищах даних. Можливостівключають: Управління рішеннями (засноване на аналітиці); Відкриття та дослідження(дослідження з різних джерел, щоб надати діловим користувачам нову інформацію прорезультати діяльності); Прогнозована аналітика (витягує інформацію з існуючих наборів даних, щоб визначати поточний стан, визначати закономірності та прогнозувати майбутні тенденції); Аналіз та звітність(звіти про оперативні та складські дані зацікавленим сторонам бізнесу та регуляторними органам, де вони зазвичай збільшують обсяг і глибину доступних даних); Контент аналіз (дозволяєбізнесу, отримати розуміння зі свого структурованого та неструктурованого змісту);Планування та прогнозування

(дозволяє швидше та ефективніше розробляти плани, бюджети тапрогнози шляхом створення, порівняння та оцінки бізнес-сценаріїв).

4. *Потокові обчислення* - приймає та обробляє в реальному часі великі обсяги високодинамічних, чутливихпотоків даних з різних входів, таких як сенсорніпристрої моніторингу, системи обміну повідомленнями та канали фінансового ринку. Можливості включають: аналітичну обробка часу (застосовуючи аналітичну обробку та прийняття рішень до руху перехідних даних з мінімальною затримкою).

Управління процесами - діяльність з планування, розробки, розгортання та моніторингувиконання бізнес-процесу. Система IoT може забезпечувати управління процесами в реальному часі.

Device Data Store - зберігає дані з пристроїв IoT, щоб можна було

інтегрувати дані процесів та програм, які є частиною системи IoT. Пристрої можуть генерувати велику кількість даних в реальному часі, які вимагають, щоб сховище даних пристрою було еластичним та масштабованим.

Управління API - публікує каталоги та оновлює API у широкому спектрі розгортання в середовищах. Це дозволяє розробникам та кінцевим користувачам швидко збирати рішення за допомогою відкриття та повторного використання наявних даних, аналітики та послуг.

Керування пристроями - забезпечує ефективний спосіб безпечного управління та підключення пристроївнадійно до хмарної платформи. Управління пристроєм містить надання пристроїв, віддалене адміністрування,оновлення програмного забезпечення, дистанційне керування пристроями, пристрої контролю.

Реєстр пристроїв - зберігає інформацію про пристрої, які система IoT може читати, спілкуватися з ними, контролювати, забезпечувати або управляти. Можливо, потрібно буде зареєструвати пристрої, перш ніж вони зможуть під'єднуватися і будуть управлятися системою IoT. Розгортання IoT може мати велику кількість пристроїв, отже, масштабованістьреєстру є важливим.

Служба ідентифікації пристрою - забезпечує надійну ідентифікацію пристроїв перед наданням доступу до системи та програми IoT. У системах IoT ідентифікація пристрою може допомогти вирішити такі загрози, які виникають із підроблених серверів або підроблених пристроїв.

Трансформація та підключення - забезпечує безпечне з'єднання з корпоративними системами та надає можливість фільтрувати, агрегувати або змінювати дані або їх формат під час переміщення між хмарними та IoT-системамикомпоненти та корпоративні системи (як правило, системи запису). В межах довідкової архітектури IoTкомпонент трансформації та зв'язку знаходиться між хмарним провайдером та підприємствоммережі. Однак у гібридній хмарній моделі ці лінії можуть стати розмитими. Трансформація іКомпонент підключення включає такі можливості:

1. *Безпечне підключення до підприємств* - інтегрується з даними

підприємства, системи безпеки для автентифікації та авторизації доступу докорпоративні системи.

2. *Трансформація* - трансформує дані, що надходять на підприємство та назад до системи.

3. *Підключення до корпоративних даних* - дозволяє хмарі провайдера надати компоненти для надійного підключення до корпоративних даних. Приклад(включають VPN і тунелі шлюзу).

Підприємницька мережа - розміщує ряд корпоративних програм для бізнесу, які забезпечують критичне значеннябізнес-рішенням разом із допоміжними елементами, включаючи дані підприємства. Як правило, додатки підприємства мають джерела даних, які витягуються та інтегруються із послугами, що надаються хмароюпровайдера. Аналіз виконується в середовищі хмарних обчислень, а вихідні дані споживаються корпоративними програмами.Системи даних записів, як правило, дозрівали з часом і їм дуже довіряють. Вони залишаються основнимиелементами у рішеннях звітності та прогнозної аналітики. Системи запису даних включають транзакційнідані про ділові взаємодії, які дотримуються послідовності пов'язаних процесів (фінансових або матеріально-технічного забезпечення). Ці дані можуть надходити з довідкових даних, сховищ основних даних та використовуваних даних програмфункціонально або оперативно або виробляються корпоративними додатками. Зазвичай дані буливдосконалені або доповнені для додавання вартості та стимулювання розуміння. Дані підприємства, в свою чергу, можуть бути введені впроцес аналізу шляхом інтеграції даних абобезпосередньо до сховищ даних, якщо це доречно.

Дані підприємства - включає метадані про дані, а також системи записів для підприємствадодатків. Дані підприємства можутьнадходити безпосередньо до інтеграції даних або сховищ даних, що надають цикл зворотного зв'язку в аналітичній системі для IoT. Системи IoT можуть зберігати необроблені, аналізовані або обробленіданіувідповіднихелементахEnterpriseData. Дані підприємствавключають:

1. *Довідкові дані* - надання контексту про зібрані дані.

2. *Основні сховища даних* - ці сховища можна оновлюватиз результатами аналітики, щоб допомогти з подальшими данимиперетворення, збагачення та кореляції.

3. *Транзакційні дані* - дані про ділові взаємодії та дотриманняпослідовності або пов'язаних із ними процесів (фінансових або логістичних).Ці дані можуть надходити з довідкових даних, основних даних сховища та розподіленого зберігання даних.

4. *Дані програми* - дані, що використовуються або виробляються підприємством, також додатки які функціонально або оперативно оброблюються.

5. *Дані журналу* - дані, агреговані з файлів журналів для підприємства, додатки, системи, інфраструктура, безпека, управління тощо.

6. *Дані про вміст підприємства* - дані для підтримки будь-якого підприємствадодатків.

7. *Історичні дані* - Дані попередньої аналітики та корпоративних додатків та систем.

Enterprise User Directory - зберігає інформацію про користувача для підтримки автентифікації, авторизації абодані профілю. Служби безпеки та граничні служби використовують це для контролю доступу до корпоративної мережі,корпоративні послуги або хмарні послуги провайдера.

Корпоративні програми - корпоративні програми використовують дані хмарних постачальників та дають аналітичні результати, що відповідають бізнес-цілям і завданням. Корпоративні програми можна оновлювати з корпоративними даними або програми IoT, або вони можуть забезпечити вхідні дані та вміст для корпоративних даних та програми IoT. Програми можуть включати:

1. *Досвід клієнта* - системи, спрямовані на споживача, можуть бути основною системою взаємодії, керує новим бізнесом та допомагає обслуговувати існуючих клієнтів за нижчою вартістю.

2. *Нові бізнес-моделі* - альтернативні бізнес-моделі, орієнтовані на низьку вартість, швидку реакцію тачудові взаємодії - це всі приклади

можливостей, заснованих на хмарних рішеннях.

3. *Фінансові показники* - фінансові програми можна зробити більш ефективними, як і дані які консолідуються та відповідають бистріше.

4. *Аналіз ризиків* - який може бути використаний для оцінки загроз бізнесу, таких як шахрайство або злом.Еластичне управління ресурсами означає, що більша обчислювальна потужність доступна у часи підвищення загроз.

5. *Економіка IT* - використовується для впорядкування IT-операцій, як і капітальні видатки які знижуються, в той час як продуктивність та функції покращуються за рахунок розгортання хмар.

6. *Операції та шахрайство* - хмарні рішення можуть забезпечити швидший доступ до більшої кількості даних, що дозволяє аналізувати більш точніше, яка вказує на підозрілу діяльність та пропонує своєчасне виправлення.

Безпека та конфіденційність

Безпека та конфіденційність у розгортаннях IoT повинні такожстосуватися як безпеки інформаційних технологій (IT) та елементів технології операцій (OT). Крім того, рівень уваги до безпеки, які потрібно розглянути, різняться залежно від середовища застосування, бізнес-структури та оцінки ризику. Оцінка ризику враховуватиме численні загрози та атаки разом із оцінкоюпотенційних витрат, пов’язаних з такими атаками.Окрім міркувань безпеки, підключення IT-систем до фізичних систем також приносить користь, разом з цим необхідність врахувати вплив системи безпеки IoT. Виходить, що процесиповинні бути проектовані, розгорнуті та керовані таким чином, що вони завжди можуть привести систему в безпечний робочий стан, навіть при відключенні від зв'язку з іншими системами, які є частиною розгортання.

Дійсно, відключення від зв’язку може бути частиною заходів безпеки, які застосовуються для допомогизабезпечити розгортання IoT.Існує кілька сфер безпеки, які слід врахувати:

1. Управління ідентифікацією та доступом

2. Захист даних

3. Моніторинг, аналіз та реагування на безпеку

4. Управління життєвим циклом системи, додатків та рішень

Кожен із цих напрямків коротко обговорюється нижче.

Управління ідентифікацією та доступом

Як і в будь-якій обчислювальній системі, повинна виконуватися ідентифікація всіх суб’єктів - користувачів, систем, програм. Ідентифікація та управління пристроєм обов’язково передбачає кілька організацій, починаючи з виробників мікросхем та пристроїв, включаючи постачальників платформ IoT, а такожвключаючи корпоративних користувачів та операторів пристроїв. У рішеннях IoT часто буває, що множинні організації продовжуватимуть спілкуватися та звертатися до пристроїв IoT протягом усього свого функціонування.

Захист даних

Дані в пристрої, під час польоту по всій загальнодоступній мережі, хмарі постачальника та корпоративній мережі, повинні бути захищені від невідповідного доступу тавикористання. Можна використовувати кілька методів, і справді, у багатьох випадках застосовують декілька методіводночасно, забезпечувати різні рівні захисту даних від різних типів загроз або ізоляцій від різних сутностей, що підтримують систему. Захист лінії зв'язку може використовуватися в додатку до індивідуального шифрування на рівні поля даних та підписання, зробленого в пристрої для забезпечення як наскрізного, так і точкового захисту зв'язку. Дані в стані спокою в різних форматах можутьбути зашифрованими на полі, в базі даних і навіть на цілому диску або носії для захисту від витоків та неправильного використання. Збільшення збору даних також призводить до необхідності враховувати потенційну конфіденційність, що вимагають додаткової уваги до розподілу даних, редагування та спеціальної обробки. Важливо врахувати, чи включати дані, що беруть участь у системі IoT, особисті дані- що передбачає юридичні та нормативні зобов’язання, які іноді називають „конфіденційністю”. В деяких випадках, пристрої можуть бути безпосередньо пов'язані з фізичними особами, або фізичні особи можуть бути фізичними особамиякі є предметом даних датчиків. Якщо є можливість пов’язати

пристрій або дані з окремою особою,тоді дані, швидше за все, будуть ідентифікаційними. Важливо визнати, що при достатній кількості цього спостерігається інформація, сукупні дані можуть бути використані для ідентифікації особи, до якої вона відноситься. Як приклад, побутовий лічильник електроенергії генерує показання, які можуть бутипов'язані з особами, які проживають у відповідних приміщеннях, отже, показання лічильника повинні розглядатися як ІПІ. Інформація про персональну інформацію, як правило, є предметом законів та нормативних актів, і система IoT повинна бути розроблена відповідно, щоб забезпечити відповідний захист даних цих типів. Захист може передбачати, де і як можуть дані зберігатися та які обмеження використання даних повинні бути застосовані.Міркування щодо захисту даних можуть мати широкий спектр наслідків. Це може бути лише один випадок, коли дані, зібрані пристроєм, повинні зберігатися в тому самому районі, де він збирається,на пристрої або на шлюзі IoT, який знаходиться недалеко від пристрою - його неможливо передати нацентральне розташування, наприклад хмара провайдера.

Моніторинг, аналіз та реагування на безпеку

Кожна система повинна мати вбудований моніторинг для навколишнього середовища, щоб активні атаки, були виявленими при дії на неї. Через масштаб систем IoT, кількість пристроїв, а також обсяг інформації, що обробляється, є вимогою автоматизованої реакції на відомі атаки, а також автоматичне виявлення підозрілої поведінки. Відповідьдо нападів та підозрілої поведінки може належати тимчасовій ізоляції, карантин або вилучення частинсистеми IoT, а також формальних процесів реагування на інциденти для усунення вразливостей, яківиявляються після введення в експлуатацію систем. Як і IT-безпека, існує потреба в розкритті таких вразливих місць, щоб усі сторони, які постраждали, могли застосувати відповідні пом'якшення,зміни та своєчасне оновлення. Зверніть увагу, що атаки можуть бути найрізноманітніших форм. Як лише один із прикладів, напад може мати форму ін’єкції фальшивих, помилкових або хибних даних датчиків в систему IoT, намагаючись направити автоматизовані частини системи, що приймають рішеннядіяти бажаним способом (зловмисником). Такі

атаки також слід очікувати.

Управління життєвим циклом системи, програми та рішення

Управління життєвим циклом системи IoT є складним, багатогранним та пов'язаним із ідентичністю управління, управління пристроями, ланцюжок поставок, розробка програм та програмного забезпечення, аж до системноъ операції та управління змінами розгорнутих систем, що працюють. Увага до безпеки, всі ці області потрібні для запобігання різноманітним атакам, починаючи від шкідливого, до ефективного управління криптографічними ключами.

Код, ключовий матеріал і навіть фізичні компоненти повинні бути перевірені, оскільки вони надходять із закупівель тастворення до їх встановлення на пристроях, шлюзах IoT та системах, що складають IoT системи. Система IoT також повинна забезпечувати можливість оновлення окремих компонентів у безпеці, таким чином, як для усунення вразливостей, так і для вирішення функціональних удосконалень протягом усього життяс. Подібні міркування щодо життєвого циклу стосуються і конфіденційності та захисту даних.

На рисунку 2.4 наведено більш детальний огляд компонентів, підкомпонентів та взаємозв'язків для архітектури хмарних рішень IoT.

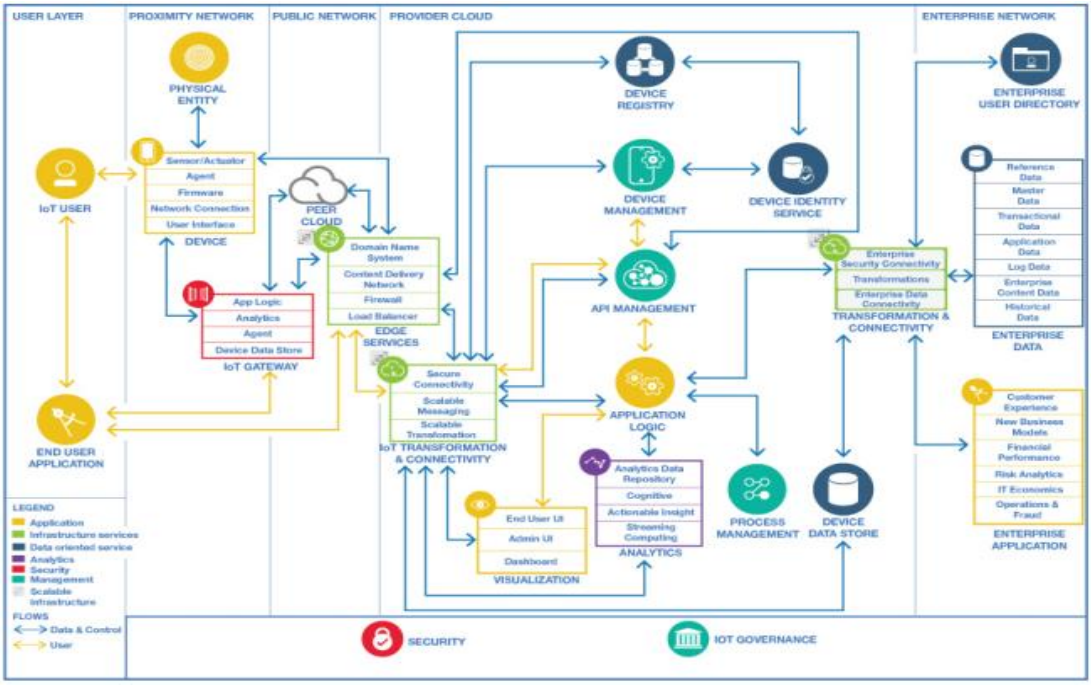

рис.2.4 - Детальна схема компонентів

Потік виконання

Рисунок 2.5 ілюструє потік випадків використання підключеної страхової послуги для IoT.

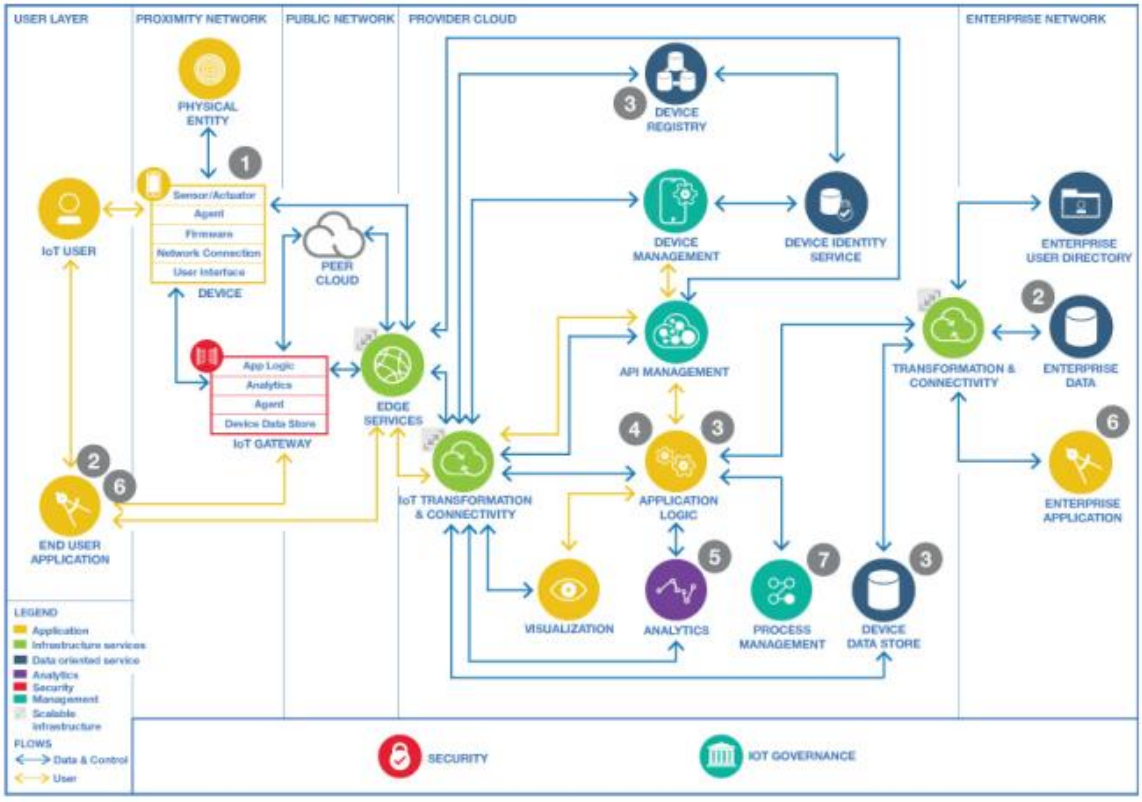

рис.2.5 - Потік випадків страхового сценарію для IoT

У цьому прикладі розумні будинки з підключеними пристроями / датчиками надають страховим компаніям можливість покращити послуги для своїх страхувальників, одночасно отримуючи уявлення про ризики вдома. Це дозволяє страхувальникам отримувати повідомлення про потенційну небезпеку для дому та взаємодіяти зі страховиком у більш ініціативний спосіб. Підключаючи домашніх екосистемних партнерів, страховиків та інші служби, такі як інформація про погоду підключена страхова послуга використовує ключові компоненти Довідкового матеріалу IoT. Як приклад можна використати датчики виявлення витоків і клапани, які забезпечуєстрахувальник з моніторингом витоків води та захистом від пошкоджень. Датчики придбані з кількох джерел та встановлені вдома, що включає підключення їх до пристрою виробників хмарних сервісів. Тоді

страхувальник уповноважує хмарну службу страхування підключатися до хмарної служби виробників пристроїв, що надають доступ до даних пристрою. Виробник пристрою відповідає за життєвий цикл пристроїв, а страхова компанія отримує вигоду від доступу до даних цих пристроїв та забезпечує покращений досвід для своїх страхувальників. Основний інформаційний потік включає:

1. Датчики та виконавчі механізми розміщені в будинку та прикріплені до хмари виробників пристроїв обслуговування. Як приклад датчики можуть включати виявлення витоків води, витрату води, температуру а виконавчі механізми можуть включати автоматичні запірні клапани.

2. Власник житла входить у мобільний додаток для страхування та уповноважує страхову послугу отримати доступ до хмари виробників пристроїв (однорангової мережі) та даних їх пристроїв. Мобільний додаток надсилає маркер авторизації та ідентифікатор страхової компанії для хмарної служби.

3. Ця інформація використовується для відображення користувача, пристроїв та страхового полісу в хмарній службі.

4. Страхова служба отримує авторизацію / деталі пристрою / страховий ідентифікатор від страховки через мобільний додаток і обробляє це в декількох вузлах (логіка програми, реєстр пристроїв тазберігання даних в пристрою). Пристрої реєструються в реєстрі пристроїв, а відображення даних - оновлюється в логічному компоненті програми.

5. Програма страхової послуги підключається до хмари виробника пристроїв (однорангової мережі) за допомогою авторизаціїмаркер і запитує дані. Програма налаштована на отримання даних через заданий інтервал. Окрім даних пристрою, програму можна налаштувати для доступу до інших джерел даних, таких як служба даних про погоду для використання в аналізі.

6. Дані з пристроїв та інших джерел, таких як метеорологічна служба, постійно оновлюються танаправляється в аналітику, щоб визначити, чи перевищено поріг потенційного ризику. Ці дані аналізуються, щоб визначити, чи існує можливість пошкодження будинку (включаючи пошкодження водою, потенціал заморожування тощо). Як тільки буде встановлено, що проблема існує,

використовуючи аналіз відкроку 5 сповіщення надсилаються власнику житла та страховій компанії. Власник житлапотім може вжити заходів, щоб відповісти на повідомлення та визначити, чи стався збитокі страхова компанія може ініціювати процес розгляду претензій.

7. Якщо шкода сталася, тоді розпочинається страховий бізнес-процес управління претензіями.Страхові бізнес-процеси можуть здійснюватися в хмарній службі, їх підприємствіпрограми або їх мобільні програми.

Хмарна архітектура полегшує впровадження та обслуговування такого типу рішень.

Оскільки IoT страждає від обмежених можливостей з точки зору обчислювальної потужності та зберігання, вона також повинна боротися з проблемами такі як: продуктивність, безпека, конфіденційність, надійність. Інтеграція IoT з хмарою, безумовно, найкращий спосіб подолати більшість із цих питань. Хмара може навіть виграти від IoT, розширивши його межі за допомогою об'єктів реального світу в більш динамічний і розподілений спосіб, і надання нових послуг для мільярдів пристроїв у різних сценаріях реального життя. Крім того, хмара забезпечує простоту використання та зменшує витрати на використання програм та послуг для користувачів. Хмара також спрощує потік даних IoT збір та обробка, а також забезпечує швидку, низьку вартість встановлення та інтеграція для складної обробки даних та розгортання.

Переваги інтеграції IoT з хмарою:

Спілкування

Застосування та обмін даними - дві важливі особливостіпарадигми IoT на основі хмари. Всюдисущі програми можуть передаватися через IoT, в той час як автоматизація може полегшити розподіл та збір даних.Хмара - це ефективне та економічне рішення, яке може використовуватися для підключення, управління та відстеження будь-чого за допомогою вбудованої програми. Наявність швидкоїсистеми полегшує динамічний моніторинг та управління віддаленими об'єктами, а також доступ до даних у режимі реального часу. Хоча хмара може значно розвинути та полегшитивзаємозв'язок IoT, він все ще має слабкі місця в

певних сферах.Таким чином, практичні обмеження можуть з'явитися, коли величезнукількість даних потрібно передати з Інтернету в Хмару.

Зберігання

Оскільки IoT можна використовувати на мільярдах пристроїв, IoT міститьвеличезну кількість джерел інформації, які генеруютьвелечезні обсяги напівструктурованих або неструктурованих даних. Нам це відоме як Великі дані яка має три характеристики: різноманітність (наприклад, типи даних), швидкість (наприклад, генерація даних, частота) та обсяг (наприклад, розмір даних). Хмара вважається одним з найбільш економічно вигідних та придатних рішенн, коли справа стосується величезної сумиданих, створених IoT. Більше того, це дає нові шансидля інтеграції, агрегування та обміну даними з третіми сторонами.

Можливості обробки

Пристрої IoT характеризуються обмеженою обробкою можливостей, які запобігають локальним та складним данимобробки. Натомість зібрані дані передаються у вузли, якімають високі можливості; справді, саме тут відбувається агрегація та обробка. Однак досягнення масштабованостізалишається проблемою без відповідної основи інфраструктури. Пропонуючи рішення, Cloud надає необмежені можливості віртуальної обробки та запит на замовлення моделі використання. Прогнозовані алгоритми та керування даними можуть бути інтегрованими в IoT для того, щоб збільшити дохід та зменшити ризики за менших витрат.

Сфера застосування

Світ швидко рухається до Інтернету всього, мільярди користувачівспілкуються між собоюразом і різноманітна інформація постійно збирається.Інтернет - всього - мережа мереж з мільярдами речей, які генерують нові шанси та ризики. IoT на основі хмари забезпечує нові програми та послуги, засновані нарозширення Хмари за допомогою об'єктів IoT, що в свою чергудозволяє Хмарі працювати з низкою нових реальних сценаріїв, і призводить до появи нових послуг.

3 ЗАСТОСУВАННЯ IOT НА ОСНОВІ ХМАРИ

3.1 Розробка технології IDM для моделі IoT

Почнемо з того, що ми просуваємо поняття задач про корисність Інтернету речей, приклад на рис.3.1, тому що комунікувати повинна будь-яка річ, комунікувати в любий час и в любому місці, тому любий користувач використовуючи будь-який ідентифікатор, власний пристрій або пристрій в мережі любого обраного або доступного на сьогоднішній день в цей момент "Тут і зараз", оператор повинен отримати потрібну послугу за умовами "Тут і зараз", котрі релевантні ситуації, що склалася.

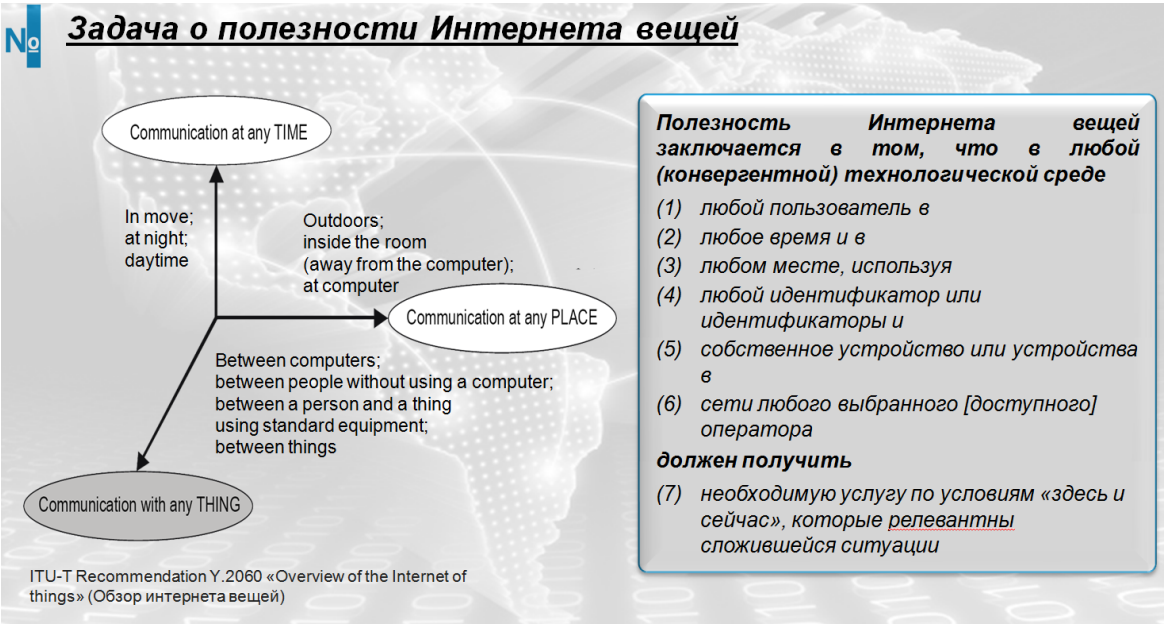

рис.3.1 - Корисність інтернету речей

Існує еталонна модель IoT, як показана на рис.3.2, яка визначає рівень пристроїв, рівень мережі, рівень підтримки послуг, рівень додатків. На всіх цих рівнях ми знаєм, які фунції вирішуються і як вони вирішуються, але є одна проблема це місце функції управління IndetityManagment, справа в тому що, без

вирішення цієї функції, розуміння місця цієї функції ми з вами будемо скочуватися в навал всіляких ідентифікаторів, цифрових об'єктів з не розумінням їх функціоналу, властивостей, ми то з можемо розібрати функціонал та їх властивості, але все це буде нести не системний характер.

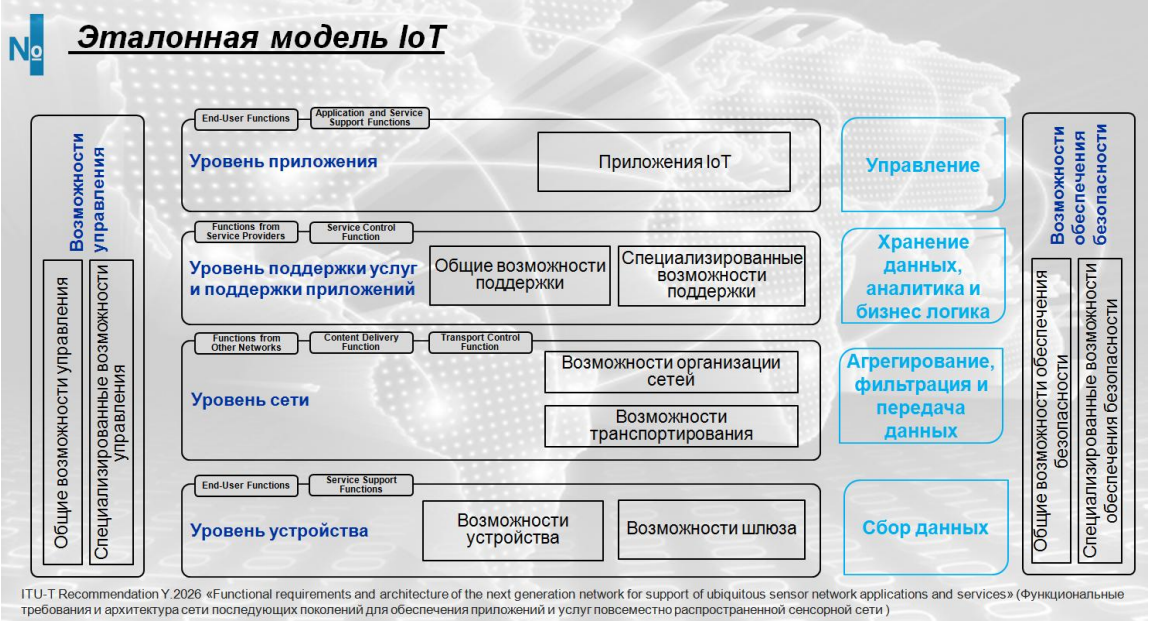

рис.3.2 - Еталонна модель IoT

Пропоную ввести 5 рівень в модель IoT(рівень керування ідентифікацією) на якому відбувається керування властивостями ідентифікаторів і управління процесами ідентифікації. Чому саме в цьому місці, тому, що здійснюється передача від рівнів мережі на рівень підтримки послуг, тобто фактично в рівень зберігання даних, аналітики та бізнес-логіки, ось тут потрібно забезпечити якийсь буфер котрий об'єднує і дозволяє керувати властивостями ідентифікації і фактично маршутизації тих потоків, яких потрібно дотримуватись в рамках системи яку ви будуєте. На рис.3.3 показана модель IoT з додаванням IDM.

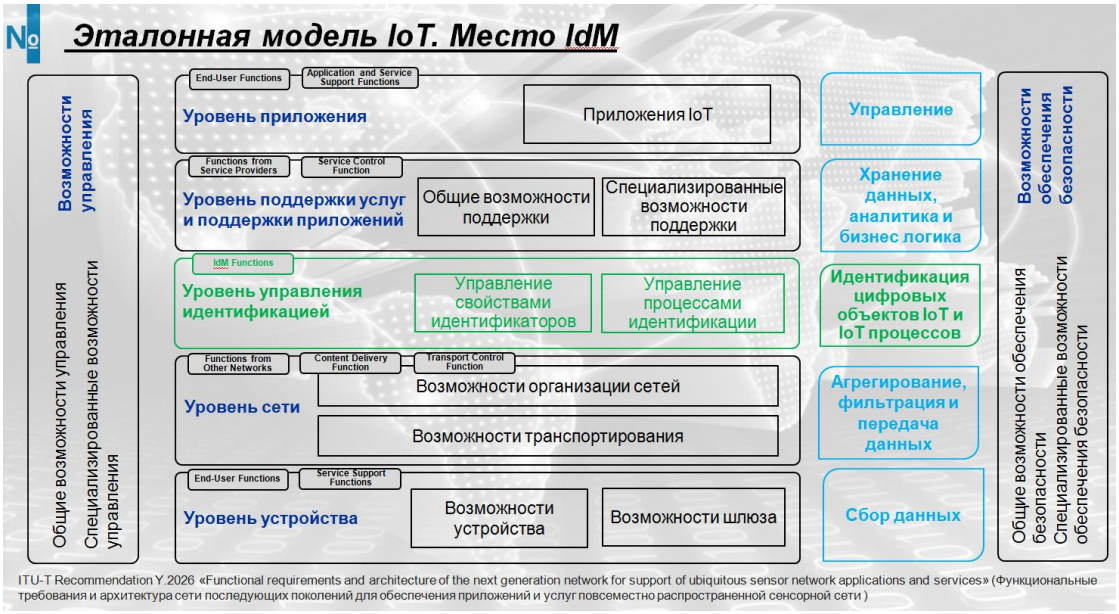

рис.3.3 - Модель IoT з IDM

І тут повертаємося до питання управління ідентичністю або управління ідентифікацією, рис.3.4. Справді поняття ідентичність це категорія більш гуманітарна, а нам потрібно вирішувати інженерні задачі, тому ідентифікація це категорія інженерна, яку можна розібрати на гвинтики і знову зібрати. Можемо цілком вирішити задачі в будь-якому середовищі , мережі забезпечити їх сумісність, розділити мето-данні та данні самого об'єкта.

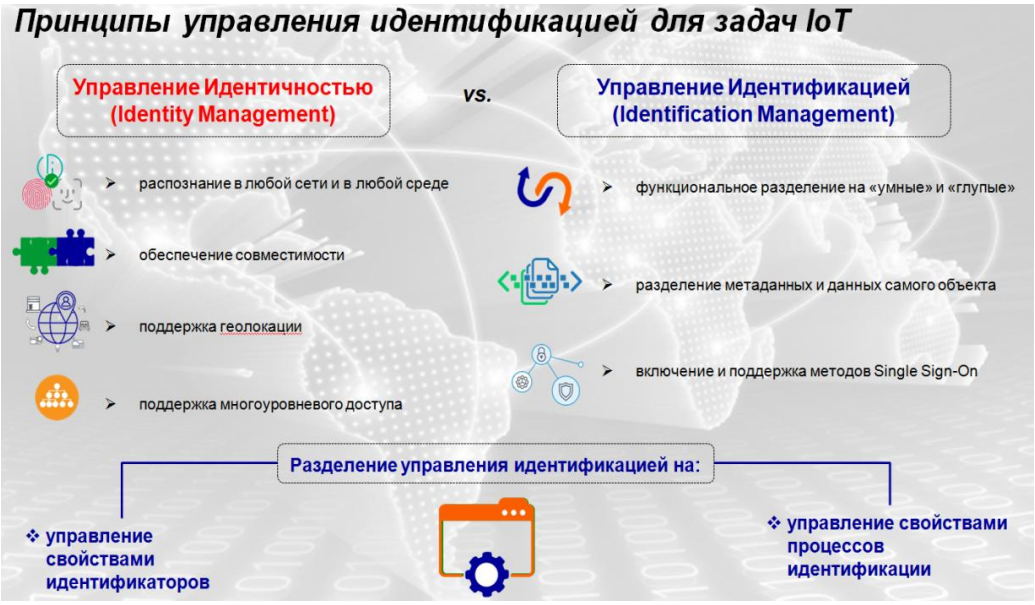

рис.3.4 - Принцип управління ідентифікацією для задач IoT

Сьогодні стає дуже важкою задачею підтримка методів SingleSign-On, як показано на рис.3.5. Але саме головне, що потрібно розділити управління ідентифікації на два процеси: управління властивостями ідентифікаторів та управління властивостями процесів ідентифікації. Оскільки якщо ми навчимося управляти властивостями ідентифікаторів, то ми фактично вирішимо наступну задачу, нам буде все рівно які протоколи, які ідентифікатори систем ідентифікації використовуються в системах IoT. Ми можемо створювати нормальні системи в яких дуже багато існує цифрових об'єктів, де кожний працює за своїм протоколом і це є нашою реальністю. І також дуже важливо розуміти як керувати властивостями процесів ідентифікації. Задача Single-On (технологія єдиного входу для IT) у нас існує дуже багато пристроїв і є якийсь технологічний процес і ми породжуємо локальні сесії, де кожна сесія повинна підтримуватися одноразовим або відновлюватися багаторазовим, це як би не дуже вдале рішення, тому існуючий вихід з положення, коли йде глобальна сесія і існує якийсь сервер SSO(Технологія єдиного входу). Цей сервер знаходиться у indetityпровайдераі сам технологічний процес це сервіс провайдер, який використовує інформацію, що надходить від пристроїв, пристроїв може бути дуже багато, це можуть бути десятки тисяч. Що ми при цьому маємо, два типа запросів: запрос технологічного процесу к простроям або запрос простоїв до технологічного процесу.

Для прикладу, на рис.3.5 показана синім кольором камера, а тепер увага скільки на сьогоднішній момент зламаних відеокамер, з простої причини тому що, локальні сесії це правдо кажучи "прохідний двір" тут же потрібно робити глобальну сесію, тобто потрібно тримати якийсь захист, потрібно ідентифікувати цифрові об'єкти та формувати аутентифікаційні запроси. Вирішується ця задача з допомогою деяких назвемо їх умовно "книгою захисних механізмів"за існуючою технологією єдиного входу. В новий технологіний ланцюг вписуєтьсяidentityпровайдер, який залишає в себе ці сліди. Питання наскільки захищена і безпечна система при кількості пристроїв в десятки тисяч і де залишаються сліди про ці самі захисні механізми в існуючій технології для

інтернету речей. Питання на сьогоднішній день підвисає в повітрі, я маю на увазі надійність. Тобто заист від витоку данних серверів ні ким не гарантований.

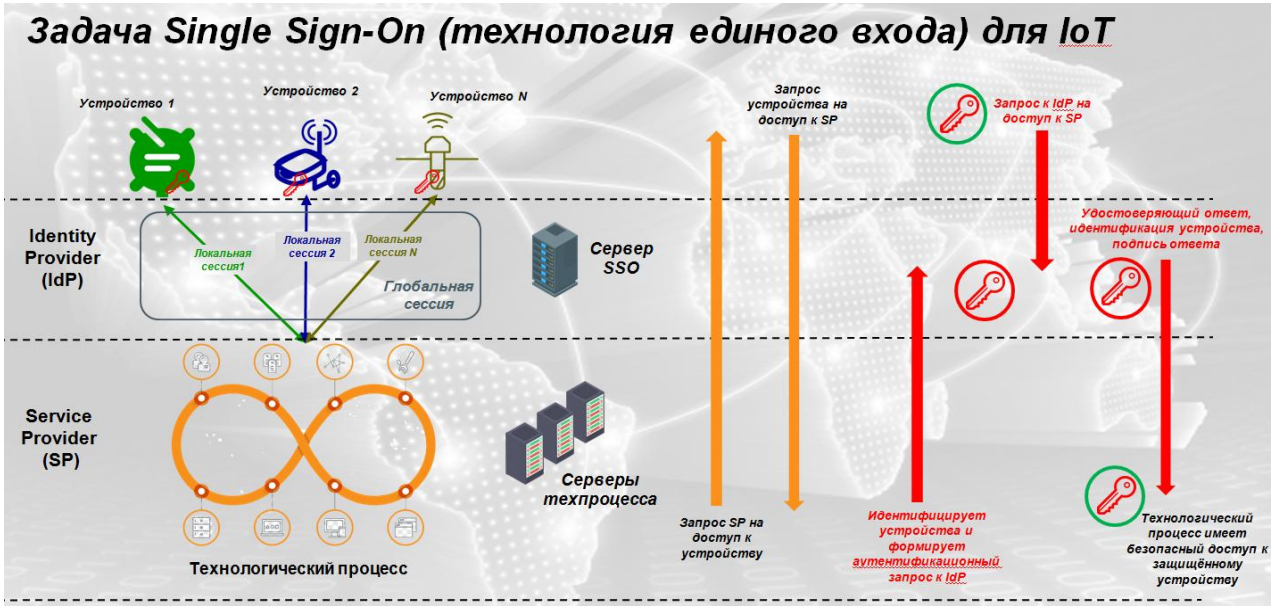

рис.3.5 - SingleSign-On

Но я пропоную технологію, зображена на рис.3.6, технологію яка дозволяє піти від розуміння Identity провайдер. Ця технологія одночасно передбачає вирішення тих самих питанн зв'язаних з управлінням властивостей ідентифікаторів і з управлінням процесу ідентифікації. Ми залишимося на тому, що є якийсь базовий ідентифікатор користувача сервіса або у користувача якогось процеса. ЦеMSISDN(користувач сервіса), далі ми включаємо механізм формування ENUM доменіві технологій ENUM, але тільки це не класична технологія ENUM яка описана в рекомендаціях ITU. Я прийшов до думки та висновку, що необхідно змінити архітектуру застосованої в ITU. Я ввів таке поняття як реєстр сервіс. Технологія ENUM на сьогоднішній день дозволяє оброблювати тільки телекомунікаційні сервіси, їх протоколи вживлені в тіло самих телекомунікацій, а що робити якщо ми працюємо з протоколами послуг медицини, або ми працюємо з технологіями які визначають функціювання технологічних процесів на підприємстві, тому другий елемент це технологія реєстрація IT сервісів для створення асоціацій. З низу на картинці, ми маємо

записи які дозволяють формувати асоціації, по перше вони дозволяють формувати самі ссилки на сервіси, сервіси записані в реєстрі сервісів інформації, тому вони дозволяють формувати ці ссилки і асоціації між сервісами і на виході створити нову конфігурацію взаємозв'язку між цими сервісами. Після цього як це було зроблено, у нас виникає третій елемент обеспечення учасників системи сертифікатами. Інформація про сертифікати з'являється в цих записах у вигляді відкритих ключів, частина відкритих ключів та частина закритих ключів. Далі наступає четвертий елемент запит на обслуговування та надання послуг, виходить ми звертаємося до операторів IT-сервісів. Наступним етапом виходить, що оператори тоже мають ці ключі, тут ми звертаємо увагу на те що ми захищаємо наші транзакції, захищаємо вхід і також ми визначаємо захищену аутентифікацію . І можемо за рахунок записів, ось цієї самої технології ENUM 2.0, здійснювати поділ прав доступу, тобто реальне функціонування авторизації. Далі відбувається сервісний виклик, в підтверджені чи може цей виклик бути обслуговуваним з тим ключем, який є у запитувача відносно того ключа, який є у запитуваного. Тобто получити до нього певний доступ рівнем доступності даного ключа. І у випадку, якщо все добре, з'являється відповідь.

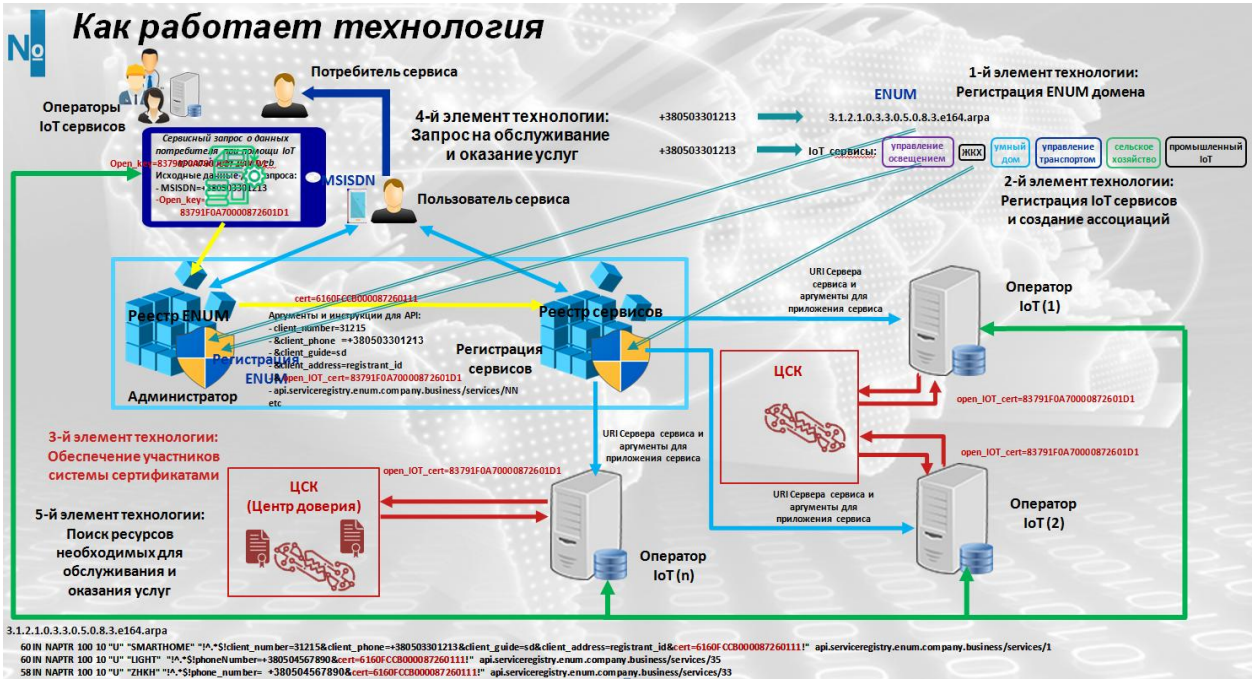

рис.3.6 - Як працює технологія

Далі наведені різносторонні галузі де може використовуватися технологія IoTна основі нашої хмари:

Хмарний підхід IoT запровадив ряд додатків та інтелектуальних послуг, які вплинули на щоденне життя. Тут я подав коротке обговорення деяких додатків з повним описом, які вдосконалені хмарною системою.

Охорона здоров'я - хмарний йот приніс багато переваг та можливостей у галузі охорони здоров'я. Він може чітко розвивати та вдосконалювати послуги охорони здоров'я та підтримувати сферу інноваційною (інтелектуальний контроль лікарських засобів / ліків, управління лікарнею).

Розумні міста - проміжне програмне забезпечення для майбутніх розумних міст можна забезпечити через IoT, отримуючи дані з інфраструктури зондування, технологій IoT та послідовно розміщуючи інформацію. Це призведе до створення служб, які можуть спілкуватися з навколишнім середовищем. На рис.. показана коротка інфраструктура розумного міста, з основними технологіями , такі як: захист, геолокація вашого місця перебуття, розумні лікарні,мережа, екологія, мобільність та також ресурси(енергія, вода).

рис.3.7 - Розумне місто

Розумні будинки - велика кількість хмарних додатків IoT дозволили автоматизувати домашню діяльність, де впровадження різних вбудованих пристроїв та хмарних обчислень дозволило автоматизувати внутрішні дії (контроль безпеки будинку, розумне вимірювання, енергозбереження).

Відеоспостереження- охоплюючи хмарний IoT, інтелектуальне відеоспостереження дасть можливість легко та ефективно керувати, зберігати та обробляти відеовміст із датчиків відео; це також дозволить автоматично витягувати інформацію зі сцен. Це стало одним з найвищих інструментів для багатьох програм, пов'язаних з безпекою (бездротові камери відеоспостереження, система виявлення руху).

Автомобільна та інтелектуальна мобільність - інтеграція хмарних обчислень у глобальну систему позиціонування (GPS) та інші транспортні технології представляє перспективну можливість вирішити багато існуючих проблем (прогнозування стану дорожнього руху, повідомлення, віддалені транспортні засоби).

Розумна енергія та розумна мережа - хмарні обчислення та IoT можуть ефективно працювати разом, щоб забезпечити споживачам розумне управління споживанням енергії (розумні лічильники, розумні прилади, поновлювані джерела енергії).

Розумна логістика - вона дозволяє і полегшує автоматизоване управління товарним потоком між виробниками та споживачами, одночасно дозволяючи відстежувати товари в дорозі (логістична галузь, відстеження відправлень).

Моніторинг навколишнього середовища - шляхом поєднання хмари з IoT може бути забезпечена високошвидкісна інформаційна система, яка зв’яже організацію, яка здійснює моніторинг навколишнього середовища в широкій зоні та датчики, які були належним чином розгорнуті в цій зоні (моніторинг джерел забруднення, моніторинг якості води, моніторинг якості повітря).

3.2 Проблеми інтеграції IoT на основі хмари та дослідження їх напрямків

В процесі дослідження інтеграцій IoTта хмари були виявлені певні проблеми, з якими необхідно боротися для захисту цінних даних:

Безпека та конфіденційність

IoT на основі хмари дозволяє транспортувати дані з реального світу до Хмари. Дійсно, одне особливе важливе питання, яке ще не вирішено, - це як забезпечити відповідні правила та політики авторизації, одночасно забезпечуючи доступ до конфіденційних даних, мають лише авторизовані користувачі; це є вирішальне значення, коли мова йде про збереження конфіденційності користувачів, і особливо коли цілісність даних повинна бути гарантована. Крім того, коли критичні програми IoT переходять у хмару,проблеми виникають через відсутність довіри до постачальника послуг,інформація щодо угод про рівень обслуговування (SLA) тафізичне розташування даних.Нові виклики також вимагають особливої уваги.Наприклад, розподілена система піддається кількості можливих атак.

Неоднорідність

Особливо важливою проблемою, з якою стикається хмарний підхід IoT, є велика неоднорідність, існуючих пристроїв, платформ, операційних системи та служб які можуть використовуватися для нових або розроблених додатків. Хмарна платформа страждає від проблем неоднорідності. Наприклад, Хмарні сервіси, як правило, мають власні інтерфейси що дозволяють інтегрувати ресурси на основі конкретних постачальників. Крім того, проблема гетерогенності може посилюватися, коли кінцеві користувачі застосовують мультихмарні підходи,і, отже, послуги залежатимуть від покращення кількох постачальників, продуктивність програми та стійкість.

Великі дані

IoT генерує величезну кількість даних: від датчиків, прикріплених до деталей машини або датчиків навколишнього середовища, або від слів, які ми кричимо на своїх розумних колонках. Це означає, що IoT є вагомим фактором

проектів аналізу великих даних, оскільки дозволяє компаніям створювати величезні масиви даних та аналізувати їх. Надання виробнику величезної кількості даних про те, як його компоненти поводяться в реальних ситуаціях, може допомогти їм зробити набагато швидше вдосконалення, тоді як дані, вибрані з датчиків по місту, можуть допомогти планувальникам зробити транспортні потоки більш ефективними.

Ці дані надходитимуть у різних формах - голосові запити, відео, показники температури або інші датчики, і все це можна видобути для ознайомлення. Як зазначає аналітик IDC, категорія метаданих IoT стає все більшим джерелом даних, якими слід керувати та використовувати їх. "Метадані є головним кандидатом для включення до баз даних NoSQL, таких як MongoDB, щоб привести структуру до неструктурованого вмісту або до когнітивних систем, щоб принести нові рівні розуміння, інтелекту та порядку в зовні випадкові середовища", - йдеться в повідомленні.

Зокрема, IoT буде доставляти великі обсяги даних у режимі реального часу. Cisco розраховує, що міжмережеві з'єднання, що підтримують додатки IoT, становитимуть більше половини із загальної кількості 27,1 мільярда пристроїв та з'єднань і становитимуть 5% глобального IP-трафіку до 2021 року.

Багатохтопрогнозує, щовеликіданісягнуть 50 мільярдів.ПристроямIoTдо 2021рокуважливозвертатибільшеувагинатранспортування, доступ, зберіганнятаобробкадебудевикористовуватисявеличезнийобсягданих. Справді, з огляду на останні технологічні розробки, очевидно, що IoT буде одним з основних джерел великих даних, і це Хмара може полегшити зберігання цих даних протягом тривалого періоду часу, крім того, що він піддається комплексному аналізу. Обробка величезного обсягу даних є значною проблемою, так як повна продуктивність програми в значній мірі залежить від властивості цієї служби управління даними.

Пошук ідеального рішення для управління даними, яке дозволить хмарі керувати великими обсягами даних - всеще велика проблема.Крім того, цілісність даних є життєво важливи мелементом не тільки тому, що потрібен вплив на якість

послуги, атакож через проблеми безпеки та конфіденційності, більшість з яких стосуються аутсорсингових даних.

Продуктивність

Передача величезного обсягу даних, створених з IoTпристроїв до хмари вимагає високої пропускної здатності. Як результат, ключовим питанням є отримання належної продуктивності мережі в порядкупередавати дані в хмарні середовища. Зростання широкосмугового зв'язку не йде в ногу зі зберіганням і еволюційними обчисленнями. У ряді сценаріїв послуги тобто надання даних повинно бути досягнуте з високою реакційною здатністю. Це тому, що на своєчасність можуть вплинутинепередбачувані справи та програми в реальному часі.

Великі масштаби

Хмарна парадигма IoT дозволяє проектувати нові програми, спрямовані на інтеграцію та аналіз надходжених даних з реального світу в об’єкти IoT. Це вимагає взаємодії з мільярдами пристроїв, які розповсюджуються серед багатьох різних місцевостей. Великий масштаб отриманих систем породжує багато нових проблем, які важко подолати. Наприклад, досягнення обчислювальних можливостей та ємності зберігання стає дужеважким. Більше того, моніторинг процес зробив розповсюдження пристроїв IoT більш важкими, оскільки пристроям IoT доводиться стикатися з проблемами підключення та динамікою латентності.

Що стосується майбутніх напрямків досліджень та відкритих питаннь IoT на основі хмарних технологій. Тут будуть розглянуті деякі відкриті питання та майбутні напрямки досліджень, пов’язані з IoT на основі хмарних технологій, і які досі вимагають більших зусиль щодо досліджень. Ці питання включають:

Стандартизація

Багато досліджень висвітлювали проблеми браку стандартів, що вважається критичним стосовно хмарної парадигми IoT. Хоча низка запропонованих стандартизацій була висунута науковим товариством для розгортання підходів IoT та Хмари це очевидно що архітектури, стандартні протоколи та API вимагають

взаємозв'язок між неоднорідними розумними речами та генерацією нових сервісів, які складають хмарну парадигму IoT.

Туманні обчислення

Туманні обчислення - це модель, яка розширює послуги хмарних обчислень до краю мережі. Подібно до Хмари, Туман постачає користувачеві служби додатків. Туман можна по суті вважати розширенням хмарних обчислень яка виконує роль проміжного проміжку між краєм мережі і хмарою,справді, це працює з чутливістю до затримок програм, яким потрібні інші вузли, щоб задовольнити вимоги затримки. Хоча зберігання, обчислення та мережа є основними ресурсами як туману, так і хмари, Туман має певні особливості, такі як обізнаність про місцезнаходження та крайнє розташування, що забезпечує географічний розподіл, і низьку латентність, до того ж є великі вузли; це на відміну із хмарою, яка підтримується для взаємодії в реальному часі та мобільністю.

Хмарні можливості

Як і в будь-якому мережевому середовищі, безпека вважається одним з основних питань парадигми IoT на основі хмарних технологій. Є більше шансів на атаки як на IoT, так і на Хмарну сторону. У контексті IoT цілісність даних, конфіденційність, а справжність можна гарантувати за допомогою шифрування. Однак інсайдерські атаки не можуть бути вирішені, і їх також важко використовувати IoT на пристроях з обмеженими можливостями.

Виконання SLA

Користувачам IoT на основі хмари потрібні створені дані для передачі і обробки на основі обмежень, залежних від програм, що може бути важким у деяких випадках. Забезпечення певної якості рівня обслуговування (QoS) щодо хмарних ресурсів залежно від провайдерів порушує багато питань. Однак динамічно вибираючи найбільш підходящу суміш хмари постачальники все ще представляють відкрите питання через час, витрати та неоднорідність підтримки управління якістю.

Великі дані

У попередньому розділі ми обговорювали великі дані як критичні виклики, які тісно поєднаний із хмарною IoT парадигмою. Хоча ряд внесків було запропоновано, Великі дані все ще вважаються критично відкритим питанням, і потребують додаткових досліджень. Хмарний підхід IoT передбачає управління та переробку величезних обсягів даних, що приходять з різних місцевостей та з різнорідних джерел.

Енергоефективність

Останні додатки IoT на базі хмарних технологій містять часті дані що передаються від об'єктів IoT до Хмари, яка швидко споживає енергію вузла. Таким чином, генерування ефективної енергії, коли мова йде про обробку та передачу даних залишається значним відкритим питанням. Кілька напрямків було запропоновано подолати цю проблему, таку як стиснення технології, ефективна передача даних, кешування даних та методи повторного використання зібраних даних з урахуванням часу.

Безпека та конфіденційність

Хоча безпека та конфіденційність є важливим дослідженимпитанням, яким приділено велику увагу, вони є досі відкритими, які вимагають більше зусиль. Дійсно, пристосовуватись до різних загроз з боку хакерів залишається проблемою. Більше того, ще однією проблемою є забезпечення відповідних правил та політики авторизації, забезпечуючи лише тих уповноважених користувачів які мають доступ до конфіденційних даних. Це має вирішальне значення для збереження конфіденційності користувачів, зокрема, коли цілісність даних повинна бути гарантованою.

Міркування щодо розгортання

Хмарне середовище пропонує надзвичайну гнучкість з меншим занепокоєнням щодо фізичного стану компонентів підключений. Потреба в розширеному плануванні зменшується, але все ще важлива. Тут я пропоную пропозиції щодо кращого забезпечення даних та обчислювальних ресурсів.

Масштабованість та еластичність

Пропускна здатність даних

Суверенітет даних

Стійкість

Процесор та обчислення

Обсяг даних

Безпека

Оптимізоване забезпечення

Жодне хмарне середовище не оптимізує всі ці критерії. Трохи вдосконалене планування робить довгий шлях до забезпечення задоволеності користувачів і це допомагає підтримувати витрати відповідно до очікувань.

Масштабованість та еластичність

В архітектурі IoT кількість датчиків може бути дуже великою, і пов'язана з цим кількість транзакцій може бути ще більшим. Це ще більше примножується у випадках, таких як підключення автомобілів до інших даних, таких як дорожній рух та погода. Трансформація IoT та підключення повинні забезпечувати масштабованість обміну повідомленнями та масштабоване перетворення даних у хмарі для цих потоків даних. Еластичність - це здатність до хмарного рішення забезпечити та скасувати обчислювальні ресурси на вимогу в міру зміни навантаження. Громадські хмари мають очевидні переваги, оскільки вони, як правило, мають більші ресурси.

Пропускна здатність даних

Державні та приватні хмари потрібно оптимізувати для великих даних. Великі набори хмарних даних, що вимагають швидкого доступу від обробки компонентів із швидким та ефективним доступом до даних. У багатьох випадках це означає переміщення обробки до даних, або навпаки. Хмарні системи можуть ефективно приховувати фізичне місцезнаходження обробки даних. Налаштування може здійснюватися безперервно з мінімальним впливом на розгорнуті програми.

Суверенітет даних

Фізичне місце, де зберігаються дані, може регулюватися, при цьому правила можуть відрізнятися(різні країни). Особливо це стосується інформації, що

дозволяє ідентифікувати особу (ІПІ) та конфіденційні дані, такі як дані про стан здоров'я та фінансові записи. Як результат, будь-яка хмарна система IoT повинна взяти на себеправила суверенітету даних облікового запису і зберігати та обробляти дані лише в тих місцях, які дозволеноправилами - для цього потрібно, щоб хмара постачальника надавала клієнту хмарних послуг, контрольнад місцями зберігання та обробки.

Стійкість

У системах IoT стійкість і відмовостійкість дуже важливі. Системи IoT не повинні залежати від одного компонента в будь-якій точці і повинен терпіти відмову одного компонента, наприклад, одного IoTпристрою. Компоненти в хмарі постачальника можна зробити еластичними завдяки використанню декількох екземплярів програм та хмарних служб, пов’язаними з реплікацією та надлишковістю даних на декількох системах зберігання.Мережі також повинні бути стійкими, наприклад, з декількома шляхами та кількома провайдерами в загальнодоступній мережі. Немає срібної кулі, яка б постійно робила всю мережу доступною, але вона повинна бути високодоступною і стійкою. Важливо переконатися, що можливості підключення можуть підтримувати стійкість.

Процесор та обчислення

Наявність недорогих товарних процесорів означає, що державні, приватні та гібридні хмарниі сервери , як правило, дуже масштабовані. Сучасні середовища розробки, що використовують Hadoop, Spark та Jupyter(iPython) користуються перевагами цих масово паралельних систем. Потоки та високошвидкісна аналітика - цеобласть, що розвивається, де хмарні додатки використовують потужніші пули процесорів, що дозволяють в реальному часі створювати швидкі рішення для передачі даних. Виділене обладнання дозволяє швидше розробляти та тестувати перед міграцієюдо гібридного та громадського середовища.

Обсяг даних

У системах IoT обсяг даних може перевищувати поріг, при якому традиційні аналітичні набори інструментів іпідходи можуть більше не масштабуватись у задоволенні вимог щодо ефективності. Тому ретельне планування зберігання

даниху публічній хмарі, приватній хмарі чи традиційному центрі обробки даних дуже важливо. Потокове передавання даних у випадках погоди або використання карти для GPS може призвести до величезного набору даних для аналізу. Зберігання даних вимагає невеликих експериментів, якщо це спеціально не регулюється нормативними актамиполітики.

Безпека

Оскільки більше даних про людей, фінансові операції та оперативні рішення збирається, уточнюється тазберігаються, проблеми, пов'язані з управлінням інформацією та безпекою, зростають. Конфіденційність даних тауправління ідентифікацією пристроїв та окремих людей дуже важливо з точки зору хмарних обчислень. Хмара, як правило, дозволяє швидше розгортати нові інструменти відповідності та контролю. Хмарні концентратори даних можуть бути хорошим варіантом, якщо виступити яккоординаційні центри для збору та розподілу даних. Інструменти, що контролюють активність та доступ до даних,можуть насправдізробити хмарні системи більш безпечними, ніж автономні системи. Гібридні системи пропонують унікальне застосуванняособливості управління: Програмне забезпечення можна централізовано підтримувати в розподіленому середовищі з даними які зберігаються у приміщенні для дотримання політики юрисдикції.

ВИСНОВКИ

На мою думку, IoT стає все більш повсюдною обчислювальною технікою, яка вимагає величезних обсягів зберігання даних і можливостей обробки.IoTмає обмежені можливості в умовах обробки потужності та зберігання, хоча також існують такі, як безпека, конфіденційність, продуктивність, та надійність.Загалом можна сказати, що ці дві галузі змінюють наш світ найкраще, тобто спрощують обробку та використання даними. Інтеграція Хмари та IoT надає змогу за лічені секунди обробити та предати різноманітні дані в будь-яку точку світу і це є значною перевагою для суспільства. Об'єднуючись ці технології стають одним цілим, бо разом вони доповнюють один одного в різних функціональних можливостях.Таким чином, інтеграція Хмари в IoTдуже корисна з точки зору подолання цих викликів. У цій роботі я представив необхідність створення Хмарного підходу до IoT.Обговорення також було зосереджено на архітектурі IoT на основі хмари, різнісценарії застосування, проблеми, що стоять перед успішною інтеграцією, та відкриті дослідження. Інтернет речей - це динамічна та захоплююча сфера IT. Буде створено багато систем IoT протягом наступних кількох років, охоплюючи багато різноманітніх випадків використання у різноманітних побутових, комерційних,промислових, медичних та державних контекстах.Системи IoT включають безліч різних компонентів, кожен зі своїми проблемами. Аспекти масштабу, швидкості, безпека, безпека та конфіденційність поширені в системах IoT і потребують пильної уваги. Архітектура, описана в цій роботі, забезпечує надійну основу для розуміння систем IoT та для вирішення різних завдань систематичним та логічним способом.