УДК 004.056.5
DOI: 10.31673/2409-7292.2020.033438

Колісник Д.Р., Місевич К.С., Коваленко С.В.

СИСТЕМНА АРХІТЕКТУРА IOT-FOG-CLOUD ДЛЯ СИСТЕМ АНАЛІЗУ ВЕЛИКИХ ДАНИХ І КІБЕРБЕЗПЕКИ: ОГЛЯД ТУМАННИХ ОБЧИСЛЕНЬ, ВПРОВАДЖЕННЯ АУДИТУ ІНТЕРНЕТУ РЕЧЕЙ

В статті розглянуто питання щодо системної архітектури IoT-Fog-Cloud, розглянуто взаємодію між трьома рівнями IoT, Fog і Cloud для ефективного впровадження програм для аналізу великих даних і кібербезпеки. В статті також розглядаються проблеми безпеки, рішення та направлення майбутніх досліджень в галузі Інтернету речей та туманних обчислень.

Ключові слова: туманні обчислення, хмарні обчислення, Інтернет речей, кібератаки, проблеми, рішення, аудит.

Вступ

В умовах швидкого зростання Інтернету речей (IoT - Internet of things) сучасні хмарні системи стикаються з різними проблемами, такими як відсутність підтримки мобільності, визначення місця розташування, географічний розподіл, висока затримка, а також кіберзагрози. Туманно-граничні обчислення були запропоновані для усунення деяких недоліків, оскільки вони дозволяють обчислювати ресурси на межах мережі і локально пропонують аналітику великих даних, а не передачу їх в хмару. Fog визначається як хмарна система, що має аналогічні функції, включаючи програмне забезпечення, платформу і інфраструктуру як послуги. Розгортання додатків Fog стикається з різними проблемами безпеки, пов'язаними з віртуалізацією, моніторингом мережі, захистом даних і виявленням атак. Інтернет речей з'явився для оцифрування повсякденних завдань в різних системах. Оскільки хмарні системи пропонують високу обчислювальну інфраструктуру, потужність, пропускну здатність, програмне забезпечення, платформи і сховище, додатки IoT інтегруються з хмарними системами в мережевих системах [2, 3]. Мережі IoT включають в себе сукупність датчиків, виконавчих механізмів і сервісів, які вимагають великих обчислювальних ресурсів для виконання програм для аналізу великих даних і кібербезпеки. Вони як і раніше страждають недоліками масштабованості і працездатності, коли різнорідні джерела даних збираються і аналізуються на трьох рівнях систем IoT, Fog і Cloud [1, 4, 5].

Виклад основного матеріалу

Інтернет речей поступово змінив спосіб виконання щоденних задач. Крім надання розумних рішень для житлових спільнот, IoT також застосовується як інструмент у бізнес середовищі різних сфер. Тим не менш, з великою кількістю даних, які генеруються IoT, велика частина навантаження припадає на інфраструктуру Інтернету. Це змусило підприємства та організації шукати рішення, яке би зменшило це навантаження. Важливо взяти до уваги одну з основних складових - Cloud Backend. Він несе відповідальність за отримання інформації з шлюзу IoT, зберігання і її обробку у діючих ресурсах і її надсилання до інтерфейсу користувача. У деяких вдосконалених рішеннях IoT хмарні додатки IoT також підтримують машинне навчання та штучний інтелект. Такі нововведення в розробці додатків хмари IoT гарантують, що рішення IoT здатні вирішувати складні бізнес-проблеми в галузях промислової автоматизації. Існує нерозривний зв'язок між IoT і Cloud. Дані, зібрані датчиками, досить великі у випадку промислового застосування IoT і шлюз не здатний обробляти і зберігати їх. Ці дані потрібно зберігати в захищеній базі даних і обробляти доступним і масштабованим способом.

Існує декілька протоколів, які з'єднують шлюзи з хмарними програмами IoT, і найбільш поширеним серед них є MQTT. Датчики збирають і подають дані, величезний масив даних після агрегації і деякої попередньої обробки передається в хмару для зберігання та обробки.

Взаємозв'язок IoT і Cloud Computing

Хмарні обчислення, а також IoT, працюють у напрямку підвищення ефективності повсякденних завдань, і обидва мають взаємодоповнюючий характер. З одного боку, IoT

© Д.Р. Колісник, К.С. Місевич, С.В. Коваленко, 2020

генерує багато даних, а з іншого боку, хмарні обчислення прокладають шлях для цих даних. Крім того, хмарний хостинг як послуга додає цінності стартапу IoT, забезпечуючи економію від масштабу, щоб зменшити загальні витрати. На додаток до цього, хмарні обчислення, допомагаючи розробникам зберігати дані та мати доступ до даних віддалено, хмара дозволяє розробникам реалізовувати проекти без затримки. Крім того, зберігаючи дані в хмарі, компанії IoT можуть отримати доступ до великих масивів даних.

Нині багато нововведень у сфері IoT розглядають хостинг-послуги plug-and-play. Саме тому хмара ідеально підходить для IoT. Хостинг провайдери не повинні залежати від масового обладнання або навіть від будь-яких апаратних засобів, які не підтримують вимоги до пристроїв IoT. Хмара діє як посередник або комунікатор, коли мова йде про IoT. Багато потужних API, такі як Cloudflare, CloudCache і Dropstr, що використовують хмарні комунікації, дозволяють користувачу легко зв’язуватись із смартфоном. Було б справедливо сказати, що хмара може прискорити зростання IoT. Однак розгортання хмарних технологій також має певні проблеми та недоліки. Не тому, що хмара є недосконалою як технологія, проте комбінація хмари та IoT може обтяжувати користувачів деякими перешкодами. Залежно від характеру реалізації IoT, хмара може мати різну ступінь складності. У простих додатках хмара може складатися з бази даних, в якій зберігаються дані, зібрані IoT, а також інформація користувачів, які мають право доступу/зміни даних. У великих і складніших реалізаціях хмарні додатки IoT можуть також мати можливість машинного навчання, виконання аналітики, генерації звітів і багато іншого. Деякі протоколи, такі як MQTT, Websocket, CoAP і AMQP, використовуються для розробки потужного та безпечного інтерфейсу, який полегшує безперешкодний зв'язок між датчиками та хмарою.

Деякі переваги хмари в екосистемі IoT

- Забезпечує зберігання та обробку даних IoT.
- Розширена аналітика та моніторинг.
- Сумісність зв'язку між пристроями. У IoT датчики взаємодіють не тільки з користувачами, вони також взаємодіють один з одним. Застосування IoT Cloud разом з шлюзом IoT гарантує, що різні датчики та виконавці можуть взаємодіяти один з одним без будь-якої несумісності.

Хмарні системи в формі програмного забезпечення, платформ та інфраструктури можуть вирішити проблеми масштабованості і працездатності, надаючи послуги користувачам і організаціям. Однак хмарні системи страждають від відсутності підтримки мобільності, затримок, визначення місця розташування і географічного розподілу [1, 6]. Парадигми Fog / Edge були запропоновані для усунення недоліків хмарних систем і забезпечення можливості аналізу великих даних на кордоні мережі [4]. Термін «туманні обчислення» був придуманий Консорціумом OpenFog [1, 5], який являє собою архітектуру, яка розширює основні функції хмари для надання послуг на кордоні мережі, і представляє собою віртуалізувану архітектуру пулу ресурсів. The Fog - це децентралізована інфраструктура, в якій дані реєструються і аналізуються між клієнтами і центрами обробки даних Cloud. Він призначений для застосування методів аналізу в реальному часі і великих даних, що значно підтримує розподілені системи управління даними [1, 3, 4, 6].

Поточні дослідження [4 – 9] припускають, що технологія Fog буде розроблена в майбутньому, щоб запропонувати поліпшену і ту, що заслуговує довіри архітектури для обробки постійно зростаючої кількості взаємопов'язаних пристроїв і послуг. Автори в [1, 3, 4, 6] запропонували різні методи для розгортання рішень безпеки, включаючи шифрування, контроль доступу, міжмережевий екран, аутентифікацію і системи виявлення та запобігання вторгнень, в шарі Fog. Оскільки Fog залежить від розподілених архітектур, які з'єднують IoT і хмарні системи, Advanced Persistent Threats (APT) [7] може використовувати пристрої та сервіси Fog, якщо системи безпеки погано спроектовані для ефективного моніторингу та захисту вузлів Fog [1, 5].

Азам і ін. [8] розробили методику підключення модуля інтелектуального зв'язку і попередньої обробки даних в мережах Cloud-IoT. Ця технологія об'єднала інтелектуальний

© Д.Р. Колісник, К.С. Місевич, С.В. Коваленко, 2020

шлюз з технікою туманних обчислень, щоб зменшити накладні витрати на обчислення на стороні хмари. Alrawais і інші запропонувала схему туманних обчислень для вирішення проблем аутентифікації в мережах IoT. Обчислювальний пристрій Fog діє як шлюз для пристроїв IoT для розподілу відкликання сертифікату. Альмадхор [8] використовував парадигму туманних обчислень для захисту платформ Cloud-IoT. Яссен і ін. [7] використовували деякі можливості туманних обчислень для розробки системи виявлення вторгнень для розпізнавання кібер атак в бездротових сенсорних мережах. Dsouza і інші [8] запропонували управління на основі політик для захисту співробітництва та взаємодії між різними вимогами клієнтів в вузлах Fog. В [9] автори запропонували структуру фізичної безпеки для інтеграції функцій систем IoT, Fog і Cloud. Sandhu і інші [8] запропонували структуру для виявлення зловмисних дій з кордонів мережі.

Парадигма Fog була спочатку запропонована Cisco, щоб стати розширенням архітектури хмарних систем, які забезпечують послуги обчислень, зберігання і зв'язку між хмарними серверами і клієнтськими системами [1, 5, 9]. Вона дозволяє виконувати обчислення і обробку даних на межі мережі. Це означає, що Fog є додатковим шаром хмарних систем, який пропонує дизайн розподіленої архітектури. Архітектура може обробляти різнорідні джерела даних мереж бездротового доступу IoT. Аналітика великих даних може бути реалізована на кордонах мережі швидше, ніж централізовані хмарні системи [1].

Консорціум OpenFog почав свою діяльність в 2016 році з метою розробки стандартизованих відкритих середовищ туманних обчислень. Наприклад, була запропонована структура Open-Machine-to-Machine (OpenM2M) для поєднання пристроїв і сервісів Fog і IoT. У цій структурі вузли Fog були розгорнуті в прикордонних інфраструктурах з декількома додатками M2M. Потім була запропонована інша архітектура Fog, в якій був розроблений набір інтерфейсів додатків, що дозволяють віртуальним машинам одержувати доступ для збору інформації на вузлах Fog. Sang та інші запропонували структуру Fog, яка є контекстно-залежною інфраструктурою. Платформа підтримує різні периферійні технології, включаючи можливості Wi-Fi, LTE і Bluetooth, які підтримують програмно-конфігуровані мережі (SDN) і інструменти віртуалізації. Також пропонується розгорнути системи Airborne Fog, де повітряні пристрої, такі як дрони, можуть виступати в якості вузлів Fog для полегшення різних додатків і послуг для кінцевих користувачів.

Туманні обчислення відносно схожі на мобільні граничні обчислення (MEC) і мобільні хмарні обчислення (MCC) [4]. MEC концентрується на серверах Fog, таких як хмарні сховища, які реалізуються на межі мобільних мереж, в той час як MCC є інфраструктурою, в якій обробка і зберігання даних виконуються поза мобільними пристроями.

У Fog є кілька властивостей, які дозволяють його інтегрувати з IoT і хмарними системами, як зазначено нижче:

• Він визначає місцезнаходження на кордоні мережі і обробляє інформацію про місцезнаходження і низьку затримку, оскільки вузли Fog пропонують локалізацію (тобто один перехід від пристрою до вузла Fog) і підтримують кінцеві точки з різноманітними послугами на межі мережі;

• Він забезпечує щільний і розріджений географічний розподіл, де служби і додатки Fog вимагають розподіленого розгортання;

• Він може використовувати великомасштабні сенсорні мережі для моніторингу хмарних систем і систем Інтернету речей;

• Має велику кількість вузлів для демонстрації можливості великомасштабного географічного розподілу;

• Він спрощує використання мобільності, що допомагає користувачам Fog отримувати доступ до інформації для підвищення якості послуг;

• Забезпечує взаємодію в реальному часі для обробки важливих додатків Fog;

© Д.Р. Колісник, К.С. Місевич, С.В. Коваленко, 2020

• Він підтримує бездротовий зв'язок M2M, яка споживає мало енергії для підтримки масштабованості і мобільності;

• Він обробляє різні динамічні і різнорідні джерела на різних рівнях мережевої ієрархії;

• Забезпечує гнучке, недороге і портативне розгортання апаратного і програмного забезпечення;

• Він може легко інтегрувати IoT і хмарні додатки для онлайн-аналітики великих даних.

Оскільки пристрої Fog підключені до систем Cloud і IoT, мережі IoT можуть використовуватися з використанням різних кіберзагроз. Це пов'язано з тим, що пристрої розгортаються в незахищених місцях, які не контролюються і не захищаються. Відкрита архітектура Fog призводить до появи вразливостей, які дозволяють зловмисникам скомпрометувати пристрої та служби Fog, на додаток до загрози конфіденційності великих масивів даних .

Аудит Інтернету речей

Багато компаній використовують аудит не тільки як можливість звірки достовірності даних перед обов'язковими перевірками податкових органів. Аудит - це також можливість зрозуміти, які технології і бізнес-процеси потребують поліпшення або зміни. Ухвалення рішення про підвищення ефективності бізнесу, запуск нових продуктів і послуг практично завжди вимагає аудиту всіх сторін діяльності компанії.

Підприємство, яке планує застосування в своїй діяльності технології Інтернету речей, проводить аудит бізнесу IoT для розуміння необхідності впровадження розумних технологій в ті чи інші процеси. Повний аналіз фінансово-господарської діяльності підприємства з точки зору аудиту бізнесу IoT - це визначення проблем і вузьких місць у виробництві, які можуть бути вирішені за допомогою технологій Інтернету речей, впливу нових технологій на зниження собівартості продукції і підвищення її конкурентних якостей. Таке дослідження дозволить оцінити можливість технічного переоснащення кожної ділянки, запланувати ресурси, необхідні для проведення технічної модернізації підприємства в цілому, оцінити необхідність у скороченні персоналу або набір співробітників необхідної кваліфікації.

Аудит бізнесу IoT допоможе визначити необхідність і вартість впровадження інновацій, спрямованих на зниження витрат на електроенергію і підвищення енергоефективності підприємства в цілому. Аналіз IoT, наприклад, транспортно-експедиторських компаній, може показати значне зниження витрат на ПММ в разі застосування технології Інтернету речей, а також скорочення парку автомашин і персоналу за рахунок оптимізації логістики і скорочення часових затримок на позапланові ремонти [10]. З іншого боку, аудит бізнесу підприємств, що вже застосовують технології Інтернету речей, може проводитися частіше за рахунок скорочення часу і задіяного персоналу, що в підсумку також позначиться на ефективності підприємства в цілому.

Висновок

У статті розглянуто системну архітектура IoT-Fog-Cloud для систем аналізу великих даних і кібербезпеки та взаємодію між трьома рівнями IoT, Fog і Cloud для ефективного впровадження програм для аналізу великих даних і кібербезпеки

Аналіз даної технології може бути використаний у роботі фахівцями з питань вивчення хмарних та туманних технологій для кращого розуміння наслідків впровадження даних технологій.

Подальшим напрямком досліджень є архітектура IoT-Fog-Cloud в інформаційних системах типу «розумне місто».

Перелік посилань

1. Collaborative Working Architecture for IoT-Based Applications / Higinio Mora, María Teresa Signes-Pont, David Gil, Magnus Johnsson, 2018. [Електронний ресурс]. – Режим доступу: https://www.ncbi.nlm.nih.gov/pmc/articles /PMC6022002/ (05.09.2020)

© Д.Р. Колісник, К.С. Місевич, С.В. Коваленко, 2020

2. How Fog Computing Powers AI, IoT, and 5G, Madhavan Sridharan, April 9, 2019. [Електронний ресурс]. – Режим доступу: https://www.datastax.com/2019 /04/how-fog-computing-powers-ai-iot-and-5g (05.06.2020)

3. How the introduction of IoT applications is transforming various industries and markets, 2019. [Електронний ресурс]. – Режим доступу: https://channels.theinnovationenterprise.com/articles/the-internet-of-things-iotapplications-that-are-changing-the-future (05. 06.2020)

4. Internet of Things: Architectures, Protocols, and Applications / Pallavi Sethi, Smruti R. Sarangi // Journal of Electrical and Computer Engineering – 2017. [Електронний ресурс]. – Режим доступу: https://www.hindawi.com/journals/jece/2017/9324035/ (05.06.2020)

5. Importance of Cloud Computing for Large Scale IoT Solutions, 2018. [Електронний ресурс]. – Режим доступу: https://www.einfochips.com/blog/importance-of-cloud-computing-for-large-scaleiot-solutions/ (05.06.2020)

6. OneM2M -A Common Service Layer for IoT Basic principles and architecture overview, 2018. – [Електронний ресурс]. – Режим доступу: https://portail-qualite.public.lu/damassets/publications/normalisation/2018/workshop-etsi/4-xavier-piednoir-onem2mworkshop-ilnas-etsi.pdf (05.06.2020)

7. Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities, 2018. – [Електронний ресурс]. – Режим доступу: http://www.yurradnik.com.ua/stride/ur/index.php?m=archive&y=2005&mag =4&art=89 (05.06.2020)

8. Role of Cloud Backend in IoT and Basics of IoT Cloud Applications, 2018. . [Електронний ресурс]. – Режим доступу: https://www.embitel.com/blog /embedded-blog/role-of-cloud-backend-in-iot-andbasics-of-iot-cloud-applications (05.06.2020)

9. Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities, 2018. – [Електронний ресурс]. – Режим доступу: http://www.yurradnik.com.ua/stride/ur/index.php?m=archive&y=2005&mag =4&art=89 (05.06.2020)

10. Аудит бізнесу для IoT [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://kauri-iot.com/blog-post/audit-biznesa-dlja-iot/ (07.06.2020)

Надійшла: 30.06.2020 Рецензент: д.т.н., професор Савченко В.А.

© Д.Р. Колісник, К.С. Місевич, С.В. Коваленко, 2020