ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)*

УДК 004.056.5 DOI: https://doi.org/10.30837/ITSSI.2024.27.054

О. Журило, О. Ляшенко

АРХІТЕКТУРА ТА СИСТЕМИ БЕЗПЕКИ *IoT* НА ОСНОВІ ТУМАННИХ ОБЧИСЛЕНЬ

Предметом дослідження в статті є архітектура безпеки Інтернету речей (*IoT*) на основі туманних обчислень, які надають ефективні та безпечні послуги для багатьох користувачів *IoT*. **Метою роботи** є дослідження архітектури безпеки для систем Інтернету речей на основі туманних обчислень. Для досягнення поставленої мети в статті було виконано такі **завдання**: описано концепцію туманних обчислень, розглянуто їх архітектуру та зроблено порівняльний аналіз архітектур туманних і хмарних обчислень; окреслено принципи проєктування та реалізації архітектури системи туманних обчислень; досліджено багаторівневі заходи безпеки на основі туманних обчислень та описано сфери використання мереж Інтернету речей на основі туманних обчислень. Для вирішення перелічених завдань упроваджено такі **методи дослідження**: теоретичний аналіз літературних джерел; порівняння архітектури хмарних обчислень з архітектурою туманних обчислень; абстрагування та узагальнення для визначення принципів проєктування та реалізації архітектури безпеки Інтернету речей. Здобуто такі **результати**: розглянуто архітектуру туманних обчислень і порівняно її з хмарною архітектурою; сформульовано принципи проєктування та реалізації архітектури систем туманних обчислень; запропоновано багаторівневі заходи безпеки *IoT* на основі туманних обчислень. **Висновки**. Дослідження системи безпеки *IoT* на основі туманних обчислень мають важливе теоретичне значення. Архітектура туманних обчислень, на відміну від хмарної, краще задовільняє попит на високий трафік і низьку затримку мобільних застосунків, надаючи більше переваг для систем, що потребують оброблення інформації в режимі реального часу. У проєктуванні та реалізації архітектури систем туманних обчислень необхідно зважати на фактори обсягу пам'яті, затримки та корисності для ефективної інтеграції туманних технологій з *IoT*. Для забезпечення високого рівня захищеності систем важливо впроваджувати багаторівневі заходи безпеки, використовуючи як програмні, так і апаратні рішення.

Ключові слова: хмара; туманні обчислення; архітектура; Інтернет речей; безпека *IoT*.

Вступ

Інтернет речей дедалі більше перетворюється на основний чинник проривних змін у сфері інформаційних технологій. З постійним розвитком *IoT* кількість його користувачів поступово збільшується, а обсяг передачі даних стрімко зростає, що призводить до перевантаження хмарного сервера. Класична парадигма централізованих хмарних обчислень стикається з низкою проблем, таких як висока затримка, низька пропускна спроможність і збої в роботі мережі.

Як нова модель обчислень, туманні обчислення пропонують новий спосіб зменшити навантаження на хмарні сервери. Туман забезпечує оброблення та збереження інформації *IoT* локально на пристроях *IoT* замість того, щоб відправляти їх у хмару. На відміну від хмари, туман надає послуги зі швидшим відгуком і вищою якістю. Тому туманні обчислення можна вважати найкращим вибором для того, щоб дозволити Інтернету речей надавати ефективні та безпечні послуги для багатьох користувачів *IoT*. Однак раціональне використання ресурсів туманного вузла все ще залишається складним і ключовим моментом.

Дослідження безпеки *IoT* на основі туманних обчислень було розглянуто в роботах [1, 2], де автори запропонували систему управління ресурсами на основі політики в туманних обчисленнях, розширюючи поточну платформу туманних обчислень для підтримки безпечної співпраці та сумісності між ресурсами, запитуваними різними користувачами в туманних обчисленнях. У роботі [3] запропоновано механізм, який використовує туманні обчислення для покращення розподілу інформації про відкликання сертифікатів у пристроях *IoT* з метою покращення безпеки. У статті [4] подано ефективну централізовану архітектуру безпеки для наскрізної інтеграції систем охорони здоров'я на основі *IoT*, розгорнутих у хмарних середовищах. У роботах [5, 6] проаналізовано архітектури туманних обчислень і вказано на пов'язані з цим потенційні проблеми безпеки та довіри, а також окреслено основні проблеми, виклики та напрямки майбутніх досліджень бізнес-процесів, що підтримують туманні обчислення у послугах *IoT*.

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27) ISSN 2524-2296 (online)

У попередніх студіях ми робили огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень в *IoT*. У роботі [7] наведено, що апаратні компоненти будь-якої системи, особливо системи Інтернету речей, пов'язані з туманними обчисленнями, не схильні до кібератак, зломів, вторгнень, маніпуляцій та вільні від них. Оскільки застосування розглянутих апаратних засобів безпеки може допомогти зберегти конфіденційність, цілісність і доступність інформації, що циркулює в мережі, та підвищити загальну стійкість системи до можливих атак, необхідно детальніше розглянути питання побудови архітектури безпеки Інтернету речей на основі туманних обчислень.

Отже, метою роботи є дослідження побудови архітектури безпеки для систем Інтернету речей на основі туманних обчислень.

Для досягнення поставленої мети необхідно виконати такі завдання: розглянути архітектуру туманних обчислень та порівняти її з архітектурою хмарних обчислень; окреслити принципи проєктування та реалізації архітектури системи туманних обчислень та дослідити багаторівневі заходи безпеки на основі туманних обчислень.

Архітектура системи туманних обчислень

Якщо порівнювати тришарову архітектуру системи хмарних обчислень (рівень кінцевого користувача хмарних обчислень, мережний рівень і хмарний рівень) з архітектурою туманних обчислень, то другу систему можна розподілити на п'ять шарів: рівень кінцевого користувача, рівень мережі доступу, туманний рівень, основний мережний рівень і хмарний рівень, відповідно, як показано на рис. 1.

Неважко помітити, що ближче до нижнього рівня, то більша зона поширення і менша затримка передачі даних кінцевого користувача на цей рівень [8]. У табл. 1 наведено основне обладнання та найважливіші функції зазначених п'яти рівнів.

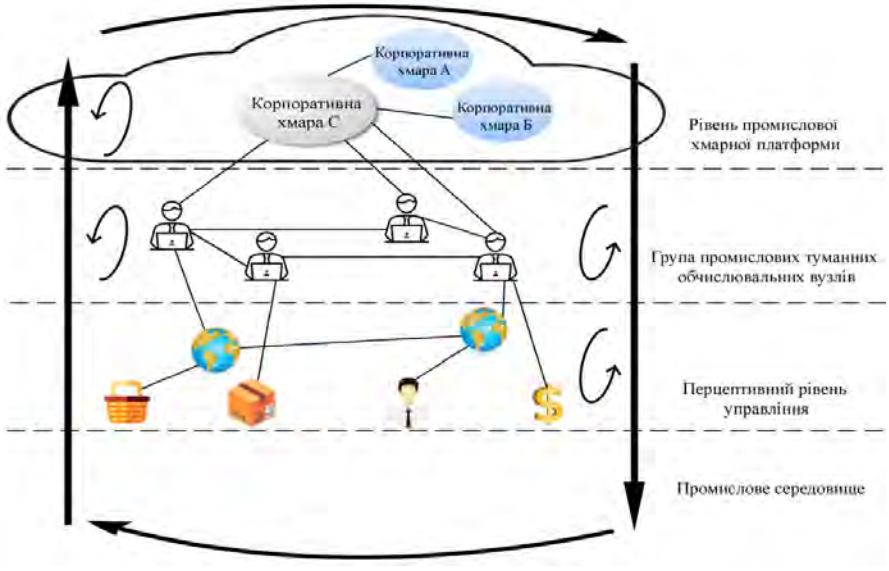

Рис. 1. Системна архітектура туманних обчислень

Таблиця 1. *Системна архітектура туманних обчислень*

Рівень	Основне обладнання	Основна функція
Рівень кінцевого користувача	Термінальні пристрої та сенсорні вузли мобільних телефонів користувачів, портативних комп'ютерів тощо	Термінальні пристрої та сенсорні вузли мобільних телефонів, портативних комп'ютерів тощо
Рівень мережного доступу	Бездротове мережне обладнання є основою, яку доповнює дротове мережне обладнання	Надсилати завдання кінцевого користувача на відповідний вузол туману за заздалегідь визначеним правилом
Туманний рівень	Туманний периферійний вузол, мікротуман, туманний сервер	Забезпечити певний рівень обчислень, зберігання та зв'язку
Основний мережний рівень	Основне мережне обладнання	Надсилайте завдання, що виходять за межі обчислення шару туману або ємності зберігання, до хмарного центру оброблення даних
Хмарний рівень	Сервер хмарного дата-центру	Резервне копіювання даних, оброблення великих обчислювальних завдань

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

У запропонованій концепції туманних обчислень завдяки розширенню туманного шару з можливостями обчислень і зберігання між хмарним сервером і термінальним пристроєм ключові дані та обчислювальні сервіси, необхідні для локалізації на хмарному сервері, переміщуються на туманний сервер, розташований ближче до термінального пристрою. Забезпечуючи кешування даних, локалізовані обчислення та інші функції, можна краще задовільнити попит на високий трафік і низьку затримку мобільних застосунків.

Основними елементами рівня кінцевого користувача зазвичай є мобільний телефон, портативний комп'ютер та інші термінальні пристрої. Із розвитком технології сенсорних мереж сенсорний вузол також відіграватиме важливу роль на цьому рівні. Ними можуть бути розміщені десь стаціонарні пристрої, наприклад датчики на світлофорах по обидва боки дороги або мобільні термінали, зокрема мобільні телефони й ноутбуки користувачів. На цьому рівні ці пристрої є генераторами і користувачами контенту. На зазначеному рівні генеруються завдання, а оброблені результати повертаються на цей самий рівень. Крім того, термінальний пристрій також має виявити та вказати туманний вузол, що відповідає переадресації завдання [9].

Проєктування та реалізація архітектури системи туманних обчислень

Розглянувши різні реалізації архітектури, зауважимо: щодо реалізації *CISCO* пропонує фреймворк *IOx*, де користувачі можуть розробляти застосунки для розгортання [10]. Для незначних туманних застосунків була реалізована невелика універсальна платформа туманних обчислень з використанням *Raspberry Pi* [11]. Реалізовано конфігурацію термінального пристрою, центру хмарних обчислень та мережного каналу, а алгоритм планування та управління ресурсами туманних обчислень може бути реалізований у різних сценаріях відповідно до реальних потреб. Крім того, продуктивність усього алгоритму проєктування може базуватися на затримці та енергоспоживанні, зайнятості мережних ресурсів та витратах на управління, а також на інших показниках для вимірювання. Хоча це відкриває нові можливості для дослідників алгоритмів планування, його функціональність не дуже висока; усе ще існують деякі відмінності між ефектами технології моделювання та фактичними результатами.

Під час туманних обчислень запускається віртуальна машина (ВМ) або завдання, завантажене в контейнер [12]. Для досягнення ефективного використання ресурсів фізичної машини, віртуальні машини або контейнери мігрують між фізичними машинами. Місцерозташування такої міграції ВМ або контейнера залежить від конструкції алгоритму планування. Розроблення алгоритму планування є більш складним, ніж у хмарних обчисленнях. З одного боку, туманні обчислення дуже чутливі до часу, отже, буде точно враховано час перебування користувача на туманному вузлі, час міграції завдання в різні туманні вузли й час, коли туманний вузол пересилає завдання до хмарного дата-центру. З іншого боку, туманний вузол установлює не тільки обчислювальні вузли, але також і вузли, пов'язані зі сховищем. Аналогічно, спосіб розміщення цих вузлів певною мірою впливає на якість відповідних послуг. Підсумовуючи, зауважимо, що в процесі розроблення алгоритму планування необхідно враховувати певні фактори.

1. *Обсяг пам'яті*. Однією з основних функцій шару туману є зберігання. Для розрахунку задачі необхідна вихідна інформація розкидається по кожному вузлу туману. Вимога до сховища полягає в тому, щоб мати змогу максимально наблизити дані до потреб користувача, але водночас вимагати, щоб простір для зберігання застосовувався якомога менше. У зв'язку з цим час збору інформації став найважливішим показником оцінки. Місцерозташування даних може бути використано безпосередньо для отримання часу їх відгуку. Але ці проблеми можна скоригувати, обмеживши кількість резервних копій даних. Тому для вимірювання ситуації зі зберіганням інформації також використовуватимуться ці два показники.

2. *Затримка*. На додаток до зберігання цієї функції, туманний вузол також приймає на себе функцію, обчислену в шарі туману, і однією з найважливіших метрик обчислювальної потужності є затримка. Порівняно з хмарними обчисленнями, обчислювальну задачу туманних обчислень можна виконувати безпосередньо на туманному вузлі, не завантажуючи її спочатку в хмарний центр оброблення даних, а потім на вузол, що дає змогу ефективно зменшити затримку. Час проходження в обидва кінці – це найточніший спосіб визначити загальний час, необхідний для повернення результату

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

від початку виконання задачі термінальним пристроєм до термінального пристрою вивантаження. Хоча одна й та сама задача інтуїтивно зрозуміла та зручна для горизонтального порівняння, метод повністю ігнорує різницю між обсягом інформації, яку задача має передати, і обсягом обчислень задачі. Хоча кількість виконаних інструкцій вимірюється в одиницях часу, причиною специфічної для користувача реалізації може бути неможливість впоратися з програмою за умови постійного використання процесора. Тому цей метод вимірювання має проблеми з вимірюванням затримки обчислень. На сьогодні метод розрахунку затримки є більш обґрунтованим, ніж порушення угоди про рівень обслуговування (*SLA – Service Level Agreement*), що робить вимірювання дефіциту ресурсів більш обґрунтованим [13]. У разі порушення *SLA*, ступінь дефіциту визначається як:

$$SLA\,violation = \frac{\sum_{i=1}^{m}\int\left(r_i(t)-a_i(t)\right)dt}{\sum_{i=1}^{m}\int r_i(t)\,dt}, \qquad (1)$$

де m – кількість задач, t – кількість ресурсів, яку запитує t-та задача в t-й момент часу, а $a_i(t)$ – кількість ресурсів, що фактично виділяються i-й задачі в t-й момент часу. Як видно з рівняння, що вищий ступінь зайнятості ресурсів, то більшим стає ступінь затримки. За певних умов між ними існує лінійна залежність. У зв'язку з цим маємо такий доказ. Припускаючи, що кожне завдання є незалежним одне від одного, запитувана кількість ресурсу становить μ_i середнє X_i, а виділена кількість ресурсу $X_i+\varepsilon_i$, тоді очікувана величина дефіциту ресурсу в межах *SLA* буде такою:

$$E[SLA]=\sum_{i=1}^{m}E\left[\int\left(1-\frac{a_i(t)}{r_i(t)}\right)dt\right]=\sum_{i=1}^{m}\int E\left[1-\frac{a_i(t)}{r_i(t)}\right]dt=\sum_{i=1}^{m}\int\left(1-\frac{E[X_i]+E[\varepsilon_i]}{E[X_i]}\right)dt=-\sum_{i=1}^{m}\frac{E[\varepsilon_i]}{\mu_i}dt\,. \qquad (2)$$

Очікуване значення кількості інструкцій, які згенерували затримку через недостатність ресурсів, становить:

$$\sum_{i=1}^{m}\int E\left[X_i-(X_i+\varepsilon_i)\right]dt=-\sum_{i=1}^{m}\mu_i\int\frac{E[\varepsilon_i]}{\mu_i}dt\,. \qquad (3)$$

Видно, що існує пропорційна залежність між очікуваним значенням ступеня дефіциту ресурсів та очікуваним значенням кількості команд затримки, а кількість команд затримки також пропорційна часу затримки. Отже, можна зробити висновок, що існує пропорційна залежність між очікуваним значенням рівня дефіциту ресурсів і часом затримки.

Неважко помітити, що цей метод вимірювання не тільки ігнорує вартість затримки диференційних послуг у мережі, але й не відображає нелінійну вартість затримки. Тому необхідні подальші дослідження та вдосконалення визначення вартості затримки.

Енергоспоживання також є важливим показником обчислювальної потужності. Коли виконання завдань, як правило, завантажується на віртуальну машину, кілька віртуальних машин на одному пристрої спільно використовують ресурси пристрою, що може значно підвищити ефективність використання ресурсів. На рис. 2 показано параметри енергоспоживання деяких серверів.

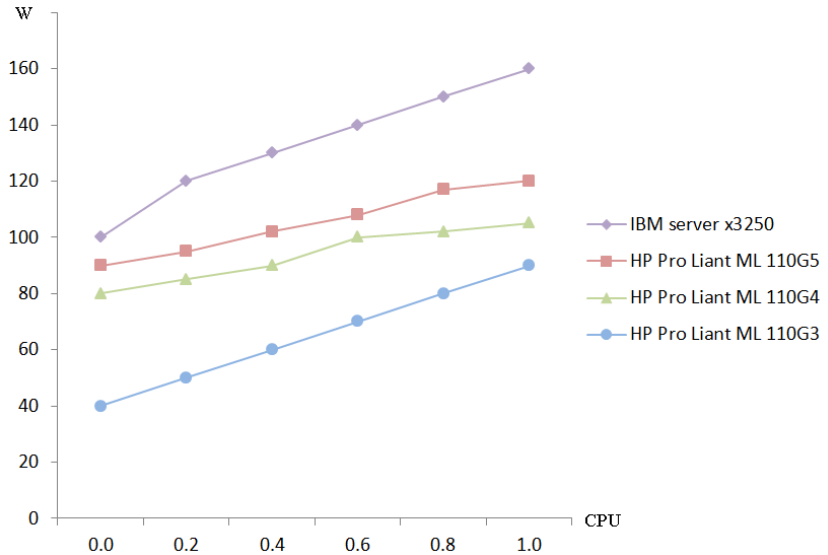

Рис. 2. Параметри енергоспоживання

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

Як видно з рис. 2, існує лінійна залежність між енергоспоживанням пристрою та використанням ресурсів процесора, до того ж найменше енергії споживає *IBM serverx3250*, а найбільше – *HP ProLiant ML110G3*. Отже, моделювання енергоспоживання можна визначити таким чином:

$$p = \int \sum_{i=1}^{m} \left[p_{idle_i} + \left(p_{max_i} - p_{idle_i} \right) \frac{a_i(t)}{c_i} \right] dt , \qquad (4)$$

де m – загальна кількість серверів; p_{idle_i} та p_{max_i} – енергоспоживання першого сервера в режимі очікування та енергоспоживання за умови повного завантаження відповідно; $a_i(t)$ та c_i – відповідно кількість ресурсів і ресурсів, зайнятих сервером. З рис. 2 також видно, що енергоспоживання, коли завантаженість процесора дорівнює 0, набагато більше, ніж енергоспоживання в режимі сну.

Тому люди планують встановлювати якомога менше віртуальних машин на якомога меншій кількості пристроїв, але що більший ступінь встановлення, то вищий ризик нестачі ресурсів, і ризик затримки зростає. Тому уніфікований розгляд обчислювальних потужностей, як правило, поєднує два показники: енергоспоживання та затримку. Крім того, існують подібні показники, такі як викиди CO_2, пропорційні споживанню ресурсів, що можуть мати такий самий ефект.

Корисність. Туманні обчислення мають таку саму комерційну цінність, як і хмарні обчислення. Більшість поточних розгортань туманних обчислень мають конкретні сценарії застосування, переважно приватний туман. Однак із зростанням популярності туманних обчислень завдання, завантажені на приватний туманний вузол, можуть бути не в змозі задовольнити їх власні потреби. Люди можуть орендувати туманні вузли, як орендують хмарні сервери. Наприклад, під час використання обчислювальних потужностей, що надаються навколишніми датчиками і розумними датчиками по обидва боки дороги в Інтернеті транспортних засобів, виникає проблема ціноутворення.

Проблема управління та планування ресурсів туманних обчислень є ключовою для впливу на продуктивність послуг туманних обчислень. Особливо в разі великомасштабних запитів на обслуговування, якщо проблема планування ресурсів не буде ефективно вирішена, це збільшить затримку обслуговування та зменшить використання ресурсів. Тому оптимальна мета може бути досягнута завдяки поглибленому вивченню питань управління ресурсами туманних обчислень та планування. Існує декілька реалізацій (фреймворків) хмарних обчислень на основі агентів з удосконаленням наявного фреймворку туманних обчислень. Крім того, існує також схема інтелектуального розподілу ресурсів на основі популярності сервісу (*SPSRP – service popularity-based smart resources partitioning*), яка дає змогу застосовувати *IoT* для туманних обчислень [14].

Багаторівневі заходи безпеки на основі туманних обчислень

Логічно розподілити *IoT* на три основні рівні: рівень сприйняття, транспортний рівень і рівень оброблення. Крім того, застосування інформації, сформованої на рівні оброблення, також можна розглядати як прикладний рівень. Кожен логічний рівень охоплюється базовою архітектурою безпеки *IoT*. Сторона сенсорного рівня та транспортного рівня, близькі до рівня зондування, здебільшого розподіляються за допомогою туманного обчислювального рівня, як показано на рис. 3.

Розглянуто та запропоновано різні заходи безпеки для апаратного рівня та рівня вбудованих пристроїв під шаром туманних обчислень для захисту від проблем безпеки, з якими система *IoT* має зіткнутися знизу [15]. Наприклад, щоб забезпечити відстеження та цілісність даних, необхідно використовувати функцію антиклонування датчика на фізичному рівні; щоб поліпшити управління надійністю, необхідна функція фізичного неклонування та лічильники продуктивності апаратного забезпечення; щоб поліпшити конфіденційність і захист приватності, необхідно застосовувати легковаговий алгоритм шифрування. На додаток до вищезазначених елементів захисту існують різні алгоритми, такі як алгоритми шифрування, хеш-функції та алгоритми обміну ключами, що можуть бути використані для парольних елементів захисту безпеки *IoT*. Використання різних криптографічних алгоритмів і вибір оброблення інформації в різних місцях оброблення може суттєво вплинути на споживання енергії. Тому, щоб не споживати занадто багато енергії, необхідно обрати певне місце оброблення і криптографічний алгоритм відповідно до обсягу інформації.

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Рис. 3. Відносне положення туманного обчислювального шару в системі Інтернету речей

Наприклад, у межах датчика він може обробляти дані розміром до 1 КБ; якщо обсяг інформації у межах 1 МБ, то як місце оброблення можна використовувати вузол туману; якщо дані в межах 1 ГБ або перевищують 1 ГБ, вони мають оброблятися на шлюзі або в об'єднаній інфраструктурі вищого рівня. Щоб скоротити час відгуку системи, необхідно повністю локалізувати інформацію, що значно підвищить ефективність системи *IoT*. Потужні мікроконтролери роблять систему інтелектуальних датчиків на чипі все більш досконалою. Наприклад, флеш-мікроконтролер виробництва *AD* має вбудовану програмну флеш-пам'ять обсягом 64 КБ і флеш-пам'ять даних 4 КБ, 2304 байти оперативної пам'яті даних і значну кількість периферійних пристроїв, таких як 12-розрядний АЦП/ЦАП (аналого-цифровий перетворювач / цифро-аналоговий перетворювач), лічильник часових інтервалів, сторожовий таймер тощо. Ядро 8052 використовується з тактовою частотою до 20 МГц. Такого рівня системи на кристалі достатньо для підтримки легких криптографічних операцій. Оскільки для управління сенсорною мережею в *IoT* зазвичай використовується 16/32-розрядний удосконалений *RISC*-процесор зі скороченим машинним набором інструкцій + вбудована архітектура *Linux* у поєднанні з повною підтримкою потужності та апаратного забезпечення, він повністю здатний забезпечити більш високий рівень захисту шифрування, робота якого здебільшого еквівалентна персональному комп'ютеру. Зарубіжні дослідники провели ґрунтовне вивчення, узагальнили наявні елементи шифрування різних рівнів *IoT* за результатами досліджень і склали відносно надійну рекомендацію (див. табл. 2).

Таблиця 2. *Елементи шифрування кожного рівня Інтернету речей*

	Датчик	**Вузол**	**Шлюз**	**Спільна архітектура**
Додавання та розшифровування	PRESENT	CLEFIA	ASE	RSA
Алгоритм	mCRYPTON	AES	ECC	
Хеш-функція	DM-PRESENT	PROP	HMAC	SHA-3
Алгоритм обміну ключами	DH-512	DH-512	ECDH	DH
Цифровий підпис	ECDSA-163	ECDSA-233	DSA	ECDSA-409

Щоб побудувати архітектуру безпеки *IoT* на основі рівня туманних обчислень, перше питання полягає у виборі правильної апаратної конфігурації туманних обчислень. Необхідно знайти відповідні заходи безпеки й розгорнути місце для створення та перевірки відповідного методу шифрування. Використовуючи новий рівень туманних обчислень для тестування наявного полегшеного методу шифрування на предмет затримки та енергоспоживання, можна покращити коефіцієнт безпеки, удосконаливши наявний простий метод шифрування або перейшовши на більш надійний алгоритм безпеки, щоб відповідати вищезазначеним вимогам. Після цього варто прагнути оптимізувати базову архітектуру системи *IoT*, а також консолідувати та зміцнити основу системи *IoT* способом зменшення обчислювальних затримок, викликаних використанням заходів безпеки,

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

без зниження показників безпеки та збільшення енергоспоживання. Для того, щоб побудувати систему безпеки *IoT* на основі туманних обчислень, необхідно повністю застосовувати всі види ресурсів, що вводяться на рівні туманних обчислень. На основі дотримання наявних заходів безпеки досягається максимальна інтенсивність безпеки.

Згідно з показниками коефіцієнт безпеки традиційних датчиків недостатньо високий, оскільки вони генерують лише відповідні цифрові результати вимірювань щодо об'єктивної кількості, зібраної ними самими, а потім безпосередньо шифрують і завантажують результати. Тепер є спосіб підвищити коефіцієнт безпеки датчика, який полягає в тому, щоб спробувати витягти унікальний ідентифікатор кожного датчика, а потім модифікувати відповідний алгоритм безпеки в датчику, щоб унікальний ідентифікатор датчика також використовувався для обчислення шифрування. Ці параметри значно покращать безпеку вихідної інформації.

Через обмеженість різних ресурсів на терміналах *IoT* легковагові алгоритми безпеки все ще залишаються найбільш широко використовуваними методами для терміналів *IoT*. Якщо *IoT*-термінал може надати більше обчислювальної потужності та простору завдяки туманним обчисленням, він має достатньо можливостей для підтримки алгоритмів безпеки з вищим ступенем захисту і складнішими обчисленнями. Отже, *IoT*-термінали можуть значно підвищити свою обчислювальну потужність і продуктивність безпеки. Однак для того, щоб реалізувати цю ідею, необхідно належним чином удосконалити та впровадити алгоритм безпеки на основі повного дослідження, зрозуміти наявні легковагові алгоритми безпеки, прискорити роботу, підвищити рівень безпеки та знизити енергоспоживання.

Вимірювання ресурсозабезпеченості туманних вузлів

Рівень туманних обчислень – це не просто сукупність туманних вузлів, оскільки кілька вузлів можуть утворювати кластер для досягнення ефективної інтеграції ресурсів. Для того щоб зрозуміти максимальний ресурсний потенціал, який може забезпечити шар туманних обчислень, необхідно сформувати відносно стабільний алгоритм оцінювання ресурсів вузла за допомогою відповідного стрес-тестування, що також має забезпечити реальний інструмент для майбутнього планування мережі *IoT*.

Ефект покращення алгоритму безпеки може бути виміряний багатьма різними показниками, такими як тривалість обчислювального часу пристрою, енергоспоживання та сила захисту від атак. У процесі постійної корекції та безперервного тестування алгоритмів безпеки дослідження вищезгаданих датчиків, вузлів, шлюзів і спільної архітектури для розшифрування матимуть значну користь в удосконаленні алгоритмів безпеки. Зі стрімким розвитком технологій Інтернету та Інтернету речей генерується значний обсяг даних і виникає питання, як використовувати великі дані швидко, безпечно та ефективно. Покращення можуть бути досягнуті завдяки оптимізації апаратних алгоритмів, таких як датчики, удосконалення алгоритмів безпеки, вимірювання ресурсозабезпеченості вузлів туману та вимірювання ступеня вдосконалення алгоритмів безпеки для досягнення рівня безпеки обчислення туману. Крім того, деякі вчені запропонували схему реагування на запити безпеки з підтримкою розрахунку туману для *IoE* (*Internet of Energy*), яка використовує консенсус і шифрування контролю доступу для запобігання атак змови [14].

Застосування туманних обчислень

Архітектура туманних обчислень може мати безліч функцій і компонентів. Вона містить шлюз туманних обчислень для отримання даних, зібраних із пристроїв *IoT*, а також може містити різноманітні дротові та бездротові кінцеві точки збору даних, зокрема надійні маршрутизатори та інші комутаційні пристрої. В інших аспектах вона може також містити клієнтський пристрій і шлюз для доступу до периферійного вузла. Крім того, архітектури туманних обчислень вищого рівня охоплюватимуть опорні мережі та маршрутизатори, а в кінцевому підсумку – глобальні хмарні сервіси й серверні системи. Група з розроблення еталонної архітектури *Open Fog Alliance* запропонувала три мети для розвитку фреймворку туманних обчислень. Туманне середовище є горизонтально масштабованим. Це означає, що воно підтримуватиме вертикальні застосунки в різних галузях; воно може забезпечити злагоджену роботу від хмари до об'єкта; це технологія системного рівня, яка поступово розвиватиметься від об'єктів і границь мережі.

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Туманні обчислення можуть використовуватись у різноманітних технологіях: Інтернеті речей, розумних будинках і містах, інтелектуальному водінні, програмно-визначених мережах, Тактильному Інтернеті (*Tactile Internet*) [16] та ін.

На прикладі інтелектуального водіння туманні обчислення можуть виконати обчислювальну задачу з високими вимогами до часу. Нижче наводимо приклад застосування туманних обчислень в інтелектуальному водінні.

Запроваджена модель інтелектуального водіння показана на рис. 4. У традиційному режимі водіння інформація про місцерозташування автомобіля надходить із супутника крізь датчик глобальної системи позиціонування (*GPS – global positioning system*), і інформація надсилається до хмарного дата-центру навігаційного програмного забезпечення. Після того, як центр оброблення даних збирає дані, вони ретельно розраховуються для отримання навігаційної інформації та її надсилання на транспортний засіб крізь мережу. Через обмеження затримки та безпеки мережі інформація, отримана таким методом, є відносно великою, може лише приблизно показувати шляхи руху дорогами, якими проїжджає транспортний засіб, і не може виконувати дії прискорення, уповільнення та уникнення транспортного засобу в режимі реального часу, так що безпілотне водіння не може бути досягнуте за таких умов. Порівняно з традиційним режимом водіння, інтелектуальне водіння може отримувати інформацію про ситуацію на дорозі в реальному часі за допомогою сенсорних пристроїв, таких як камера та ультразвук, тим самим забезпечуючи більш безпечне керування транспортним засобом без водія. Ключовою проблемою, яку необхідно вирішити в цих сценаріях, є необхідність швидко передавати, обробляти й перевіряти зібрану інформацію.

Рис. 4. Модель інтелектуального водіння

У конкретному застосуванні туманних обчислень вузьким місцем затримки, ймовірно, є мережна передача та оброблення завдань. У туманних обчисленнях мережна передача здебільшого містить мережі від користувачів до туманних вузлів, між туманними вузлами і від туманних вузлів до хмарних центрів оброблення даних. Оскільки туманний вузол має відповідати за оброблення завдань, чутливих до затримок, якість передачі бездротової мережі доступу кінцевого користувача до туманного вузла є особливо важливою. В інтелектуальному водінні навігаційна інформація транспортного засобу не вимагає затримки і тому може оброблятися віддаленим хмарним центром оброблення даних. Однак, щоб уникнути зіткнення з іншими транспортними засобами та пішоходами під час руху, існує висока потреба в уповільнені, і аварія може статися із незначною затримкою. Тому збір і оброблення даних мають виконуватися в приземному туманному вузлі. Однак швидкість передачі та якість сигналу сучасних бездротових мереж поки що не можуть задовольнити такі вимоги.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

Для розрахунків атомізації в таких застосунках, як інтелектуальне водіння, що надзвичайно чутливе до часової затримки, можна буде використовувати технологію 5G, оскільки швидкість передачі інформації в ній удесятеро вища, ніж 4G. Тому важливим напрямом досліджень надалі є поєднання туманних обчислень із технологією 5G. У процесі оброблення завдань узагальнюється наявний алгоритм розподілу ресурсів, щоб дозволити постачальнику послуг туманних обчислень виконати завдання більш ефективно. Через обмеженість обчислювальних потужностей самого транспортного засобу завдання може бути перенесено для виконання на туманний вузол за межами транспортного засобу. Як міграція віртуальної машини, так і міграція контейнера вимагають переміщення значної кількості інформації, що призводить до неприйнятних затримок. Сучасні дослідження технології віртуалізації для туманних обчислень усе ще перебувають на початковій стадії. Крім того, оскільки туманні обчислення повинні мати справу з реальним мережним середовищем, зміни в ній є більш серйозними та мають певний час і простір. Це потрібно вирішувати за допомогою адаптивного алгоритму, і передбачати розподіл не рекомендується. Поточний адаптивний алгоритм здебільшого реалізується алгоритмом навчання з підкріпленням, але для досягнення адаптивного ефекту метод має споживати велику кількість обчислювальних ресурсів. Тому його застосовність в туманних обчисленнях є сумнівною. Крім того, оскільки положення транспортного засобу сильно змінюється з часом за умови інтелектуального водіння, ця зміна також може призвести до додаткових затримок передачі інформації. Отже, питання, як використовувати ефективний і недорогий алгоритм адаптивного планування з метою вибору відповідного вузла атомізації для міграції та як дозволити користувачам інформації отримувати інформацію якомога швидше, є одне з нагальних, що необхідно вирішити.

Оскільки вузли туманних датчиків найчастіше розгортаються на відкритому просторі інтелектуального водіння, якщо злочинці викрадуть інформацію або вона буде підроблена, це призведе до катастрофічних наслідків [17]. Наприклад, якщо задній автомобіль прийняв рішення підготуватися до обгону, але передній автомобіль не отримав інформацію вчасно або повідомлення про помилку надійшло, але він не зміг вчасно її уникнути, це, швидше за все, призведе до дорожньо-транспортної пригоди. Тому ключовим моментом у цій технології є забезпечення цілісності та доступності повідомлення. Хоча в сучасній літературі проаналізовано можливу агресивну поведінку в туманних обчисленнях, затримка і стійкість запропонованого рішення в конкретних застосунках не були протестовані. Тому ефективні алгоритми шифрування та верифікації в туманних обчисленнях також будуть в центрі уваги подальших досліджень.

Сучасне промислове виробництво здебільшого основане на хмарних обчисленнях. Однак на практиці виявилося, що затримки хмарних серверів занадто великі, і багато дрібних операцій не можуть бути виконані вчасно (наприклад, різання мікрокомпонентів). Крім того, обсяг інформації, що збирають базові підприємства, збільшується, а основа підприємства також піддається тестуванню. Демонстраційний застосунок промислового Інтернету зображений на рис. 4. Для вирішення цих проблем із чутливими до затримок застосунками та вилученням функцій великих даних, організації можуть розгортати обчислювальні пристрої та пристрої зберігання між кінцевими пристроями і хмарними центрами оброблення даних на рівні туманного шару. Крім вимог до часової затримки та безпеки, це також ставить більш високі вимоги до єдності платформи та синергії між хмарами [18]. По-перше, оскільки базові компоненти, задіяні в промисловому виробничому середовищі, є більш складними, необхідно створити єдину платформу управління для ефективного охоплення та під'єднання хмарної архітектури, що дає змогу збирати інформацію та контролювати ці компоненти [19]. Водночас реалізована програмно-визначена група туманних вузлів, що ефективно охоплює та з'єднує хмарну платформу, гетерогенну мережу й великомасштабне термінальне обладнання, а також формує стандартний інтерфейс *API* та специфікацію з можливістю злиття хмарних технологій [20]. Однак поточні дослідження уніфікованих інтерфейсів усе ще перебувають на початковій стадії. Проте студій щодо кількості та місця розгортання контролерів усе ще недостатньо для управління такими ресурсами, як мережа, сховище та обчислювальні потужності. Це все питання, які необхідно вирішити в майбутньому. По-друге, крім застосунків, чутливих до затримок, туманні вузли в промислових виробничих середовищах вимагають попереднього вилучення функцій для оброблення інформації,

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

що передається в хмарний центр оброблення даних [21]. Щоб зменшити навантаження на магістраль підприємства, використовуються ключові технології хмарної конвергенції [22]. У цій технології необхідно вивчити, які завдання туманний шар подаватиме в хмарний дата-центр, статус подачі в хмарний дата-центр, який сервер подається в хмарний дата-центр, через який маршрут подачі та інші ключові питання.

Висновки

Інтернет речей стає невід'ємною частиною нашого життя. Він має здатність з'єднувати майже все з усім іншим у нашому оточенні. Пристрої Інтернету речей динамічні за своєю природою та мають обмежені можливості зберігання та оброблення інформації. Однак традиційна централізована хмара має чимало проблем, зокрема висока затримка та збої в роботі мережі. Для їх вирішення були розроблені туманні обчислення.

Мета туманних обчислень в *IoT* – підвищити ефективність, продуктивність і зменшити обсяг інформації, що передаються в хмару для оброблення, аналізу та зберігання. Отже, дані, зібрані датчиками, надсилатимуться на приграничні пристрої мережі для оброблення та тимчасового зберігання замість того, щоб відправляти їх у хмару, що дасть змогу зменшити мережний трафік і затримки. Туманні обчислення все ще перебувають на ранніх стадіях офіційного розгортання, але різні прикладні сценарії вважаються ідеальними для застосунків туманних обчислень. Інтеграція туманних обчислень з *IoT* надасть чимало переваг для різних застосунків *IoT*.

Нижче описано розвиток комбінації туманних обчислень та Інтернету речей у кількох сферах.

1. Підключені автомобілі. Поява напівавтоматичних і безпілотних транспортних засобів приведе до того, що все більше й більше інформації буде генеруватися транспортним засобом. Самостійне керування автомобілем потребує здатності аналізувати певні дані на місці, такі як довкілля, умови руху та його напрямок. Інша інформація може знадобитися для відправлення назад виробникові, щоб допомогти поліпшити обслуговування автомобіля або відстежити його використання. Туманне обчислювальне середовище підтримує зв'язок між усіма цими джерелами інформації на периферії (транспортний засіб) і зв'язок із терміналом (виробник).

2. Розумне місто та розумні мережі. Подібно до підключених автомобілів, енергосистеми все частіше використовують інформацію в режимі реального часу для більш ефективної роботи системи. Іноді ця інформація міститься у віддалених районах, і якщо ви хочете її обробити, потрібно перебувати близько до місця, де вона була згенерована. В інших випадках інформацію із значної кількості датчиків потрібно звести воєдино. Щоб вирішити обидві проблеми одночасно, можна розробити архітектуру туманних обчислень.

3. Аналіз у реальному часі. Від виробничих систем, що реагують на події, до фінансових установ, які використовують дані в реальному часі для прийняття рішень щодо транзакцій або моніторингу шахрайства, – значна кількість прикладних сценаріїв вимагає аналізу в реальному часі. Розгортання туманних обчислень допомагає передавати інформацію між місцем створення даних і місцем їх виконання.

У цій статті подано архітектуру систем туманних обчислень, описано принципи проєктування та реалізації архітектури цих систем, розглянуто й запропоновано багаторівневі заходи безпеки та визначено сфери, ефективність яких можна покращити за допомогою використання туманних технологій.

Дослідження системи безпеки *IoT* на основі туманних обчислень має важливе теоретичне значення. Водночас воно має дуже широкі перспективи застосування у сфері відстеження та цілісності даних системи *IoT*, автентифікації особистості, управління довірою, конфіденційності та захисту приватного життя, а також має дуже важливе інженерне значення. Удосконалення системи безпеки *IoT* може завоювати більше довіри користувачів до системи *IoT* і має велике значення для розвитку та просування самого *IoT*.

Отже, наші подальші дослідження будуть і надалі зосереджені на інтеграції туманних обчислень з *IoT* для підвищення рівня безпеки систем Інтернету речей.

Список літератури

1. Kartheek D., Bhushan Bharath Security Issues in Fog Computing for Internet of Things. *Security Issues in Fog Computing for Internet of Things*. 2020. 11 p. DOI: https://doi.org/10.4018/978-1-7998-0194-8.ch003

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)

2. Atlam H., Walters R., Wills G. Fog computing and the Internet of Things: a review. *Big Data Cogn Comput* Vol. 2(2):10.2018. DOI: https://www.mdpi.com/2504-2289/2/2/10
3. Alrawais A., Alhothaily A., Hu C. Fog computing for the Internet of Things: security and privacy issues. *IEEE Internet Comput* 2017. Vol.21(2). P. 34–42. https://ieeexplore.ieee.org/document/7867732
4. Thota C., Sundarasekar R., Manogaran G. Centralized fog computing security platform for IoT and cloud in healthcare system. *Fog computing: breakthroughs in research and practice*, 2018. P. 365–378. DOI: https://doi.org/10.4018/978-1-5225-5649-7.ch018
5. Zhang P.Y., Zhou M.C., Fortino G. Security and trust issues in fog computing: a survey. *Future Generation Computer Systems*. 2018. Vol. 88. P. 16–27. DOI: https://doi.org/10.1016/j.future.2018.05.008
6. Wen Z., Yang R., Garraghan P. Fog orchestration for Internet of Things services". *IEEE Internet Computing*, 2018. Vol.21(2). P. 16–24. DOI: https://ieeexplore.ieee.org/document/7867735
7. Журило О.Д., Ляшенко О.С., Аветісова К.А. Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень у Інтернеті речей. *Сучасний стан наукових досліджень та технологій в промисловості*. 2023. № 1 (23). С. 5–15. DOI: https://doi.org/10.30837/ITSSI.2023.23.005
8. Liu F., Liu Y., Jin D., Jia X., & Wang T. Research on workshop-based positioning technology based on internet of things in big data background", *Complexity Problems Handled by Big Data Technology.* 2018. P. 1–12. DOI: https://doi.org/10.1155/2018/7875460
9. S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan and Q. Cao. Multistage Signaling Game-Based Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloud-Based IoT Networks. *IEEE Internet of Things Journal, 2*, 2018. P. 1043–1054. DOI: https://ieeexplore.ieee.org/document/8264678
10. Mulfari D., Celesti A., & Villari M. A computer system architecture providing a user-friendly man machine interface for accessing assistive technology in cloud computing". *Journal of Systems and Software*. 2015. P. 129–138. DOI: https://doi.org/10.1016/j.jss.2014.10.035
11. Wang D., Fan J., Fu H., & Zhang B. Research on optimization of big data construction engineering quality management based on RNN-LSTM, *Complexity Problems Handled by Big Data Technology*. 2018. P. 1-17. DOI: https://doi.org/10.1155/2018/9691868
12. Sharma P. K., Chen M. Y., & Park J. H. A software defined fog node based distributed blockchain cloud architecture for IoT", *IEEE Access, 6.* 2017. P. 115–124. DOI: https://ieeexplore.ieee.org/document/8053750
13. Massonet P., Deru L., Achour A., Dupont S., Croisez L. M., Levin A., & Villari M. Security in lightweight network function virtualisation for federated cloud and IoT. *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. 2017. P. 148–154. DOI: https://ieeexplore.ieee.org/abstract/document/8114476
14. Li G., Wu J., Li J., Wang K., & Ye T. Service popularity-based smart resources partitioning for fog computing-enabled industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*. 2018. P. 4702–4711. DOI: https://ieeexplore.ieee.org/abstract/document/8377998
15. Aimin Y., Shanshan L., Honglei L., & Donghao J. Edge extraction of mineralogical phase based on fractal theory. *Chaos, Solitons & Fractals*, *117*. 2018. P. 215–221. DOI: https://doi.org/10.1016/j.chaos.2018.09.028
16. R. Yaroshevych, V. Tkachov, A. Kovalenko and D. Rosinskyi Modelling the Domain Architecture of the Tactile Internet Using a Foggy Infrastructure. *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, 2022. P. 512–516. DOI: 10.1109/PICST57299.2022.10238653
17. Dutta J., & Roy S. IoT-fog-cloud based architecture for smart city: Prototype of a smart building. *2017 7th international conference on cloud computing, data science & engineering-confluence.* 2017. P. 237–242. DOI: https://ieeexplore.ieee.org/abstract/document/7943156
18. Peralta G., Iglesias-Urkia M., Barcelo M., Gomez R., Moran A., & Bilbao J. Fog computing based efficient IoT scheme for the Industry 4.0", *2017 IEEE international workshop of electronics, control, measurement, signals and their application to mechatronics (ECMSM).* 2017. P. 1–6. DOI: https://ieeexplore.ieee.org/abstract/document/7945879
19. Fu H., Li Z., Liu Z., & Wang Z. Research on big data digging of hot topics about recycled water use on micro-blog based on particle swarm optimization", *Sustainability*, Vol. *10*. 2018. 2488 p. DOI: https://doi.org/10.3390/su10072488
20. Ong S.P., Cholia S., Jain A., Brafman M., Gunter D., Ceder G., & Persson K. A. The Materials Application Programming Interface (API): A simple, flexible and efficient API for materials data based on REpresentational State Transfer (REST) principles", *Computational Materials Science*, *97*. 2015. P. 209–215. DOI: https://doi.org/10.1016/j.commatsci.2014.10.037
21. Goldstein S. W. Information processing using a population of data acquisition devices *U.S. Patent No. 10,045,321*. 2018. URL: https://patents.google.com/patent/US20160309312A1/en
22. Son J., & Buyya R. A taxonomy of software-defined networking (SDN)-enabled cloud computing", *ACM computing surveys (CSUR)*, *51*. 2018. P. 1–36. DOI: https://doi.org/10.1145/3190617

Сучасний стан наукових досліджень та технологій в промисловості. 2024. №1 (27)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

References

1. Kartheek, D., Bhushan, Bharath. (2020), "Security Issues in Fog Computing for Internet of Things", *Security Issues in Fog Computing for Internet of Things*. 11 p. DOI: https://doi.org/10.4018/978-1-7998-0194-8.ch003
2. Atlam, H., Walters, R., Wills, G. (2018), "Fog computing and the Internet of Things: a review". *Big Data Cogn Comput*. Vol. 2(2): 10. DOI: https://www.mdpi.com/2504-2289/2/2/10
3. Alrawais, A., Alhothaily, A., Hu, C. (2017), "Fog computing for the Internet of Things: security and privacy issues". *IEEE Internet Comput* 21(2), P. 34–42. DOI: https://ieeexplore.ieee.org/document/7867732
4. Thota, C., Sundarasekar, R., Manogaran, G. (2018), "Centralized fog computing security platform for IoT and cloud in healthcare system". *Fog computing: breakthroughs in research and practice*, P. 365–378. DOI: https://doi.org/10.4018/978-1-5225-5649-7.ch018
5. Zhang, P.Y., Zhou, M.C., Fortino, G. (2018), "Security and trust issues in fog computing: a survey". *Future Generation Computer Systems*, 88, P. 16–27. DOI: https://doi.org/10.1016/j.future.2018.05.008
6. Wen, Z., Yang, R., Garraghan, P. (2018), "Fog orchestration for Internet of Things services". *IEEE Internet Computing*, 21(2), P. 16–24. DOI: https://ieeexplore.ieee.org/document/7867735
7. Oleh, Zhurylo, Oleksii, Liashenko, Karyna, Avetisova. (2023), "Hardware security overview of fog computing end devices in the internet of things", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (23), P. 5–15. DOI: https://doi.org/10.30837/ITSSI.2023.23.005
8. Liu, F., Liu, Y., Jin, D., Jia, X., & Wang, T. (2018), "Research on workshop-based positioning technology based on internet of things in big data background", *Complexity Problems Handled by Big Data Technology.* P. 1–12. DOI: https://doi.org/10.1155/2018/7875460
9. S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan and Q. Cao. (2018), "Multistage Signaling Game-Based Optimal Detection Strategies for Suppressing Malware Diffusion in Fog-Cloud-Based IoT Networks," *IEEE Internet of Things Journal, 2*, P. 1043–1054. DOI: https://ieeexplore.ieee.org/document/8264678
10. Mulfari, D., Celesti, A., & Villari, M. (2015), "A computer system architecture providing a user-friendly man machine interface for accessing assistive technology in cloud computing". *Journal of Systems and Software*, P. 129–138. DOI: https://doi.org/10.1016/j.jss.2014.10.035
11. Wang, D., Fan, J., Fu, H., & Zhang, B. (2018), "Research on optimization of big data construction engineering quality management based on RNN-LSTM", *Complexity Problems Handled by Big Data Technology*. P. 1–17. DOI: https://doi.org/10.1155/2018/9691868
12. Sharma, P. K., Chen, M. Y., & Park, J. H. (2017), "A software defined fog node based distributed blockchain cloud architecture for IoT", *IEEE Access, 6,* P. 115–124. DOI: https://ieeexplore.ieee.org/document/8053750
13. Massonet, P., Deru, L., Achour, A., Dupont, S., Croisez, L. M., Levin, A., & Villari, M. (2017), "Security in lightweight network function virtualisation for federated cloud and IoT", *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud)*. P. 148–154. DOI: https://ieeexplore.ieee.org/abstract/document/8114476
14. Li, G., Wu, J., Li, J., Wang, K., & Ye, T. (2018), "Service popularity-based smart resources partitioning for fog computing-enabled industrial Internet of Things", *IEEE Transactions on Industrial Informatics*, *14*, P. 4702–4711. DOI: https://ieeexplore.ieee.org/abstract/document/8377998
15. Aimin, Y., Shanshan, L., Honglei, L., & Donghao, J. (2018), "Edge extraction of mineralogical phase based on fractal theory", *Chaos, Solitons & Fractals*, *117*. P. 215–221. DOI: https://doi.org/10.1016/j.chaos.2018.09.028
16. R. Yaroshevych, V. Tkachov, A. Kovalenko and D. Rosinskyi (2022), "Modelling the Domain Architecture of the Tactile Internet Using a Foggy Infrastructure," *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. P. 512–516. DOI: 10.1109/PICST57299.2022.10238653
17. Dutta, J., & Roy, S. (2017), "IoT-fog-cloud based architecture for smart city: Prototype of a smart building". *2017 7th international conference on cloud computing, data science & engineering-confluenc.* P. 237–242. DOI: https://ieeexplore.ieee.org/abstract/document/7943156
18. Peralta, G., Iglesias-Urkia, M., Barcelo, M., Gomez, R., Moran, A., & Bilbao, J. (2017), "Fog computing based efficient IoT scheme for the Industry 4.0", *2017 IEEE international workshop of electronics, control, measurement, signals and their application to mechatronics (ECMSM).* P. 1–6. DOI: https://ieeexplore.ieee.org/abstract/document/7945879
19. Fu, H., Li, Z., Liu, Z., & Wang, Z. (2018), "Research on big data digging of hot topics about recycled water use on micro-blog based on particle swarm optimization", *Sustainability*, *10*. 2488 p. DOI: https://doi.org/10.3390/su10072488
20. Ong, S. P., Cholia, S., Jain, A., Brafman, M., Gunter, D., Ceder, G., & Persson, K. A. (2015), "The Materials Application Programming Interface (API): A simple, flexible and efficient API for materials data based on REpresentational State Transfer (REST) principles", *Computational Materials Science*, *97*, P. 209–215. DOI: https://doi.org/10.1016/j.commatsci.2014.10.037

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2024. No. 1 (27)*

23. Goldstein, S. W. (2018), Information processing using a population of data acquisition devices *U.S. Patent No. 10,045,321*. available at: https://patents.google.com/patent/US20160309312A1/en
21. Son, J., & Buyya, R. (2018), "A taxonomy of software-defined networking (SDN)-enabled cloud computing". *ACM computing surveys (CSUR)*, *51*. P. 1–36. DOI: https://doi.org/10.1145/3190617

Надійшла 14.02.2024

Відомості про авторів / About the Authors

Журило Олег Дмитрович – Харківський національний університет радіоелектроніки, аспірант кафедри безпеки інформаційних технологій, асистент кафедри електронних обчислювальних машин, Харків, Україна; e-mail: oleh.zhurylo@nure.ua; ORCID ID: https://orcid.org/0000-0001-7505-2022

Ляшенко Олексій Сергійович – кандидат технічних наук, доцент, Харківський національний університет радіоелектроніки, доцент кафедри електронних обчислювальних машин, Харків, Україна; e-mail: oleksii.liashenko@nure.ua; ORCID ID: https://orcid.org/0000-0002-0146-3934

Zhurylo Oleh – Kharkiv National University of Radio Electronics, Postgraduate Student at the Department of Information Technology Security, Assistant Lecturer at the Department of Electronic Computers, Kharkiv, Ukraine.

Liashenko Oleksii – PhD (Engineering Sciences), Associate Professor, Kharkiv National University of Radio Electronics, Associate Professor at the Department of Electronic Computers, Kharkiv, Ukraine.

ARCHITECTURE AND IOT SECURITY SYSTEMS BASED ON FOG COMPUTING

The subject of the study is is the security architecture of the Internet of Things (IoT) based on fog computing, which allows providing efficient and secure services for many IoT users. The **goal** is to investigate the security architecture for IoT systems based on fog computing. To achieve the goal, the following **tasks** were solved: the concept of fog computing is proposed, its architecture is considered and a comparative analysis of fog and cloud computing architectures is made; the principles of designing and implementing the architecture of a fog computing system are outlined; multi-level security measures based on fog computing are investigated; and the areas of use of fog computing-based Internet of Things networks are described. When performing the tasks, such research **methods** were used as: theoretical analysis of literature sources; analysis of the principles of designing and implementing the security architecture of the Internet of Things; analysis of security measures at different levels of the architecture. The following **results** were obtained: the architecture of fog computing is considered and compared with the cloud architecture; the principles of designing and implementing the architecture of fog computing systems are formulated; multi-level IoT security measures based on fog computing are proposed. **Conclusions:** research on IoT security systems based on fog computing has important theoretical implications. The fog computing architecture, in contrast to the cloud architecture, better meets the demand for high traffic and low latency of mobile applications, providing more advantages for systems that require real-time information processing. When designing and implementing the architecture of fog computing systems, the factors of memory capacity, latency, and utility should be taken into account to effectively integrate fog technologies with IoT. To ensure a high level of system security, multi-level security measures should be implemented using both software and hardware solutions.

Keywords: cloud; fog computing; architecture; Internet of Things; IoT security.

Бібліографічні описи / Bibliographic descriptions

Журило О. Д., Ляшенко О. С. Архітектура та системи безпеки *IoT* на основі туманних обчислень. *Сучасний стан наукових досліджень та технологій в промисловості*. 2024. № 1 (27). С. 54–66. DOI: https://doi.org/10.30837/ITSSI.2024.27.054

Zhurylo, O., Liashenko, O. (2024), "Architecture and iot security systems based on fog computing", *Innovative Technologies and Scientific Solutions for Industries*, No. 1 (27), P. 54–66. DOI: https://doi.org/10.30837/ITSSI.2024.27.054