Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УДК 004.056.5
DOI: https://doi.org/10.30837/ITSSI.2023.23.057

О. Журило, О. Ляшенко, К. Аветісова

ОГЛЯД РІШЕНЬ З АПАРАТНОЇ БЕЗПЕКИ КІНЦЕВИХ ПРИСТРОЇВ ТУМАННИХ ОБЧИСЛЕНЬ У ІНТЕРНЕТІ РЕЧЕЙ

Предметом дослідження є можливі засоби підвищення апаратної безпеки кінцевих пристроїв туманних обчислень в мережах Інтернету речей (IoT), популярність якого щороку стрімко зростає та потребує високого рівня захищеності від усіх типів атак. **Метою роботи** є огляд доступних готових комерційних продуктів та/або концептуальних апаратних рішень для захисту бюджетних пристроїв у мережах Інтернету речей на основі туманних технологій. Для досягнення поставленої мети виконано такі **завдання**: запропоновано концепцію туманних обчислень та визначено переваги, які вона надає мережам IoT; розглянуто кіберзагрози та апаратні атаки на мережі IoT; описано наслідки використання мереж Інтернету речей на основі туманних обчислень; розглянуто апаратні засоби безпеки, такі як TRM, PUF, HSM тощо. Для вирішення завдань використано такі **методи** дослідження, як: теоретичний аналіз літературних джерел; порівняльний аналіз хмарних, туманних і мобільних обчислень; аналіз наявних апаратних засобів безпеки. Здобуто такі **результати**: туманні обчислення можна розглядати як шлюз між хмарними обчисленнями та Інтернетом речей; вони мають більшість із переваг хмарних обчислень, крім того, додатково дають змогу обробляти дані на кінцевих пристроях, не навантажуючи центральний сервер. **Висновки**: безпека апаратного забезпечення в системах Інтернету речей не менш важлива, ніж програмна безпека. Особливо вагомо це питання постає для систем на основі туманних обчислень, де дані оброблятимуться на периферії, без передачі в хмару. Для підвищення рівня апаратної безпеки пристроїв туманних обчислень пропонується використовувати стандартні апаратні платформи безпеки, такі як: фізично неклоновані функції, апаратний модуль безпеки, система на кристалі тощо. Апаратні компоненти системи, що застосовують туманні обчислення, менш схильні до кібератак, зломів, вторгнень чи маніпуляцій.

Ключові слова: хмара; туманні обчислення; апаратна безпека; IoT; IIoT; конфіденційність; захист; апаратний модуль безпеки; фізичні неклоновані функції.

Вступ

Інтернет речей наразі зазнає активної популярності, як інтернет два десятиліття тому. У попередніх дослідженнях ми розглядали безпеку Інтернету речей у системах "Розумний будинок". Проте ринок IoT зростає, і все більше сервісів і систем застосовують у свої мережах технології IoT, а отже, і потребують відповідного рівня безпеки. Очікується, що ринок IoT збільшиться з понад 15 млрд пристроїв 2016 р. до понад 75 млрд до 2025 р. [1]. З огляду на цю тенденцію кількість розгорнутих пристроїв IoT уже перевищила загальну кількість населення Землі. Крім того, за останнє десятиліття поширення мобільних комп'ютерів зросло в геометричній прогресії. Щоб зберегти швидке зростання та величезний споживчий ринок, яким володіє IoT, необхідна жорстка технологічна основа, що підтримуватиметься науковою спільнотою. Туманні обчислення є дуже сильним кандидатом на забезпечення цієї основи (частково або повністю) для IoT, надаючи кілька переваг в обчислювальному, архітектурному й мережному аспектах [2].

Зважаючи на останні тенденції та потреби, хмарні обчислення та IoT у найближчому майбутньому стануть додатковими технологіями інтернету, сформувавши концепцію під назвою "Хмара речей" (CoT – *Cloud of Things*). CoT використовуватиметься як "Речі як послуга" (TaaS – *Things as a Service*) у хмарних застосунках IoT для перенесення завдань і операцій, що споживають багато енергії, у хмару. Тим часом туманні обчислення та всі пов'язані з ними віртуальні / реальні сервіси можна розглядати як проміжний рівень для швидкого оброблення даних на периферії мережі, обслуговуючи потреби швидкої реакції гнучких програм.

Рівень туманних обчислень також можна використовувати як рівень безпеки для реалізації необхідних функцій конфіденційності та для захисту даних перед тим, як вони будуть вивантажені в хмару через незахищений і вразливий канал [3].

Отже, метою роботи є огляд доступних готових комерційних продуктів та/або концептуальних апаратних рішень для захисту бюджетних пристроїв у мережах Інтернету речей на основі туманних технологій.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

Для досягнення поставленої мети необхідно виконати такі завдання: запропонувати концепцію туманних обчислень та визначити переваги, які вона може надати для мереж IoT; розглянути наявні кіберзагрози й апаратні атаки на мережі IoT; окреслити наслідки використання мереж Інтернету речей на основі туманних обчислень; дослідити апаратні засоби безпеки, такі як TRM, PUF, HSM тощо.

Важливість безпеки в IoT і туманних обчисленнях

Як централізований ресурс поза межами досяжності та контролю користувачів, середовище хмарних обчислень має всі можливості для порушення конфіденційності користувачів. З'являється все більше новин, пов'язаних із безпекою Інтернету речей. Наприклад, *Mirai* та схожі на нього атаки ботнетів показали, що ботнети Інтернету речей можуть бути дуже ефективними в умовах широкомасштабного розгортання для здійснення атак розподіленої відмови в обслуговуванні (DdoS – *Distributed Denial of Service*).

Як обговорювалося раніше, туманні обчислення також стають невід'ємною частиною мереж IoT. Це не вирішує проблеми конфіденційності, але, можливо, збільшує (з погляду складності) право власності на дані, які створюються, передаються та обробляються. Тому в цій статті досліджується засіб, необхідний для розв'язання питання конфіденційності та безпеки користувачів у мережах Інтернету речей, що підтримують туманні обчислення.

В останні роки завдяки використанню IoT та інших датчиків кількість даних, що генеруються кінцевими пристроями, значно зросла. Питання в тому, де, коли та як необхідно аналізувати ці дані.

У хмарно орієнтованому дизайні хмарний сервер працює як центральний. Пристрої IoT генерують дані та надсилають їх у хмару для зберігання та аналізу. Широкомасштабне розгортання IoT створює ситуації, з якими хмарні обчислення не можуть впоратися ефективно та результативно.

Однак у туманних обчисленнях дані аналізуються на кінцевих станціях, і тільки необхідні результати (зведення) надсилаються на хмарний сервер для подальшого аналізу та зберігання. Наприклад, ця технологія може бути корисна для застосунків, яким потрібна низька затримка під час оброблення даних на периферії мережі. Аналіз даних можна зробити на місці, запустивши програмне забезпечення на місцевих станціях. Хмара все ще використовуватиметься, щоб зберігати результати аналізу для початкових цілей та аудиту. Агрегація даних зменшить пропускну здатність, а також витрати, пов'язані з пропускною здатністю.

Концепція туманних обчислень, запропонована компанією CISCO, була баченням, що дало змогу пристроям IoT працювати на периферії мережі. Туманні обчислення не є альтернативою хмарним обчисленням; крім того, туманні обчислення розширюють та доповнюють хмарні обчислення концепцією розумних пристроїв, що можуть працювати на периферії мережі.

В Інтернеті речей, коли різні типи даних генеруються різними неоднорідними вузлами, питання нероздільності постає як важлива проблема. Туманні обчислення можуть її вирішити, виконуючи конкретні завдання, пов'язані з транскодуванням, на периферії мережі [3].

Як показано на рис. 1, туманні обчислення можна розглядати як шлюз між хмарними обчисленнями та Інтернетом речей для підвищення якості обслуговування (QoS – *Quality of Service*) у деяких конкретних застосунках, таких як промисловий Інтернет речей (IIoT – *Industrial Internet of Things*), де швидка й гнучка відповідь має першочергове значення. Передбачалось, що туманні обчислення забезпечать вирішення давно відомих проблем і завдань хмари, а саме: агрегацію та оброблення даних із неоднорідних пристроїв разом із проблемами сумісності цих пристроїв; захист даних і безпеку конфіденційних даних користувача; надання послуг з урахуванням контексту та розміщення, особливо для служб на основі місця розташування (LBS – *location-based services*).

Використання хмарної парадигми полягає в тому, що дані потрібно спочатку зібрати та передати в центральне розташування для зберігання та подальшого аналізу через апаратні обмеження на периферії. Більша перевага віддається парадигмі туманних обчислень і обчисленням мобільних пристроїв, коли дані збираються на периферії та потребують негайного оброблення, щоб усунути затримку або зберегти доступність.

Поширення пристроїв IoT, таких як датчики, призвело до високої потреби в пропускній здатності даних від мережі IoT до хмари через величезну кількість інформації, що створюється та передається. Для вирішення цієї складної та зростальної проблеми

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

запропоновані туманні обчислення: замість того, щоб передавати всі дані IoT у хмару, туманні обчислення оброблятимуть дані на периферії. Однак ця інтеграція поставить перед дослідниками багато нових завдань, особливо під час розроблення рішень, пов'язаних із кібербезпекою. Тому цю інтеграцію необхідно підтримувати щодо кібербезпеки. Один із способів зробити це – використовувати стандартні апаратні платформи безпеки, такі як апаратний модуль безпеки (HSM – *Hardware Security Module*) і фізичні неклоновані функції (PUF – *Physically Unclonable Functions*).

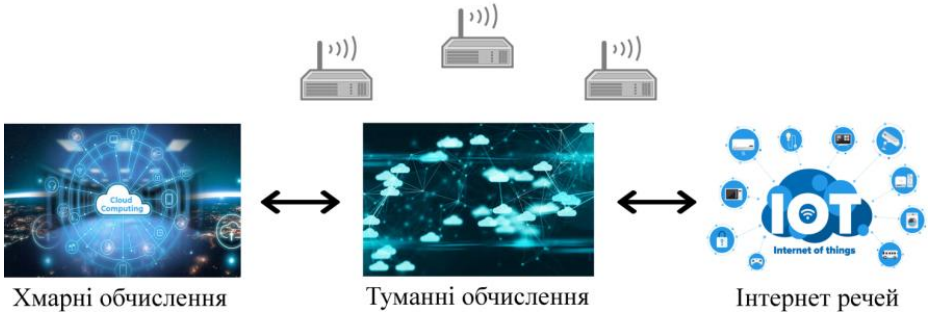

Рис. 1. Туманні обчислення як шлюз між хмарними обчисленнями та Інтернетом речей

Як показано на рис. 1, з концептуального погляду можна очікувати, що туманні обчислення слугуватимуть проміжним рівнем обслуговування для безпомилкового узгодження протоколів хмарних обчислень та IoT. Іноді в літературі цю послугу називають «Туман як послуга» (FaaS – *Fog as a Service*). FaaS надасть багато переваг для IoT та його користувачів:

– сервери хмарних обчислень надшвидкісні порівняно з кінцевими пристроями IoT. Шлюзи туманних обчислень (FCG – *Fog Computing Gateway*) забезпечать інтерфейс між двома віддаленими наборами цих пристроїв;

– проміжний рівень туманних обчислень дасть змогу легше та віддалено виконувати необхідні виправлення (зокрема керування виправленнями тощо). Замість того, щоб налаштовувати кінцеві пристрої IoT шляхом фізичного підключення, оновлення програмного забезпечення можна надсилати на туманні шлюзи, які потім доправляють виправлення на призначені кінцеві пристрої;

– туманні обчислення доповнять IoT всіма перевагами периферійних обчислень, наприклад: гнучкість, масштабованість, децентралізація тощо;

– туманні технології розширять хмарище, щоб надати додаткові ресурси базовим вузлам і мережам, використовуючи переваги концепції віртуалізації шляхом створення віртуальних датчиків і мереж, які застосовуватимуться різними службами;

– туманні технології створюють середовище для поширення розподілених програм IoT.

Туманні обчислення проти хмарних обчислень і обчислень мобільних пристроїв

Різниця між хмарними, туманними та мобільними обчисленнями описана в роботі [4]. Ми більш широко даємо цю інформацію в табл. 1.

Основні компроміси між туманними й хмарними обчисленнями подані таким чином:

– ефективність комунікації;

– загальне споживання електроенергії для послуги;

– час відповіді на запит або завдання в обидва боки.

Тут ми розширюємо цей список у такий спосіб:

– місце оброблення даних: туманні обчислення реалізують ідею перенесення функцій хмарних обчислень у джерело даних. Відтепер туманні обчислення розширюють послуги хмарних обчислень униз до периферії мережі;

– близькість до користувачів: шлюзи туманних обчислень розміщені дуже близько до користувачів і кінцевих пристроїв IoT, тоді як хмарні обчислення виконуються на серверах, розташованих далеко від користувачів IoT;

– затримка мережі: сервери хмарних обчислень зазвичай розташовані щонайменше в кількох переходах від користувачів і кінцевих пристроїв IoT. Тому в деяких випадках передача зв'язку в обидва боки (двобічна) може тривати близько кількох секунд.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

Завдяки ненавантаженій серверній архітектурі туманні обчислення можуть отримувати запити з мережі IoT і відповідати на них за мілісекунди. Тому вони є дуже перспективними для гнучких програм, таких як IIoT і CPS;

– послуги на основі місця розташування (LBS): однією з основних переваг туманних обчислень, порівняно з хмарними, є підтримка визначення місця розташування, що може бути дуже корисним для програм, що застосовують LBS;

– підтримка мобільності: в туманних обчисленнях це здійснюється завдяки використанню технологій віртуальної машини (VM – *virtual machine*). Однак для хмарних обчислень мобільність користувачів підтримується дуже обмежено.

Через помилкове уявлення туманні обчислення та обчислення мобільних пристроїв іноді застосовуються в літературі як взаємозамінні.

Однак вони відрізняються за такими ознаками:

– децентралізація: туманні обчислення забезпечують більш децентралізовану й розподілену архітектуру порівняно з мобільними обчисленнями, у яких базові станції стільникового зв'язку є основною точкою централізації;

– різноманітність постачальників: у мобільних обчисленнях апаратні / програмні компоненти залежать від постачальника, і на ринку немає чіткої стандартизації. Для туманних обчислень це неприйнятно. Вартість системи, якість, інновації, упровадження на ринок і поширення туманних обчислень – усе це залежить від стандартизації;

– різноманітний радіодоступ: більшість мобільних обчислювальних програм призначені для мобільних і/або стільникових мереж, тоді як туманні обчислення матимуть WiFi, LPWAN і WiMax, крім стільникової мережі.

Таблиця 1 – *Порівняння концепцій хмарних, туманних та мобільних обчислень*

Функція	Хмарні обчислення	Обчислення мобільних пристроїв	Туманні обчислення
Доступ до мережі	Проводовий (переважно оптоволоконний) або безпроводовий	Безпроводовий (переважно стільниковий)	Безпроводовий (стільниковий, WiMAX, IEEE802.15, LPWAN тощо)
Доступ до послуги	Через сервер	Через базову станцію	У шлюзах туманних обчислень
Оперативність	Повільна	Швидка	Найшвидша
Доступність	Здебільшого доступний	Здебільшого доступний	Здебільшого нестабільний
Використання пропускної здатності	Високе	Середнє	Низьке
Потужність – обчислення	Високе	Середнє	Низьке
Потужність – зберігання	Високе	Середнє	Низьке
Зв'язок	Інтернет	Багато протоколів (рис. 3)	Багато протоколів (рис. 3)
Контент поширюється на	Периферійний пристрій	Обмежено покриттям базової станції	Будь-де
Створення контенту	Створено людиною	Змішано	Створено датчиками
Контент генерується в	Центральному сервері	Базовій станції	Шлюзах туманних обчислень
Керування	Централізоване	Розподілене до базових станцій	Розподілене
Аналіз даних	Довгостроково	Миттєво / короткостроково	Миттєво / короткостроково
Затримка	Висока	Помірна	Низька
Оброблення / зберігання	Центр (сервер)	Мобільні периферії (базова станція)	Периферії (шлюзи туманних обчислень)
Масштабованість (по горизонталі$^{+}$)	Висока	Середня	Низька
Масштабованість (по вертикалі$^{\pm}$)	Висока	Середня	Низька
Безпека	Слабша	Сильніша	Сильніша
Мобільність	Не підтримується	Підтримується	Підтримується
Кількість користувачів	Мільярди	Мільйони / мільярди	Мільйони / мільярди
Віртуальна інфраструктура	Корпоративний сервер	Головний сервер	Пристрої користувача

У табл. 1 наведено порівняльні концепції туманних, мобільних і хмарних обчислень. Як видно, туманні обчислення забезпечують більшу гнучкість і швидкість реагування порівняно з мобільними й хмарними обчисленнями, і таким чином постають більш сильним кандидатом для технологічного

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

рішення з метою майбутніх реалізацій на основі IoT та IIoT.

Як згадувалося раніше, туманні обчислення можна розглядати як розширення хмарних обчислень до периферії мережі IoT із підвищеною гнучкістю. Отже, туманні обчислення пропонують такі переваги за умови використання для мереж IoT (і IIoT):

– економічна ефективність: дані оброблятимуться на периферії, а не в хмарі, що зрештою зменшить транспортування величезної кількості даних у хмару разом із відповідними витратами;

– підтримка сумісності: пристрої туманних обчислень можуть допомогти із завданнями, пов'язаними з транскодуванням, щоб усунути проблему сумісності неоднорідних кінцевих пристроїв IoT [3];

– зменшена затримка: хмарні обчислення не придатні для роботи з критично важливими за часом застосунками, наприклад для IIoT, оскільки загальна наскрізна затримка становить приблизно 100 мс (що є критично високим показником, особливо для автоматизації виробництва, яке потребує ізохронного відклику в лічені мілісекунди). Оскільки туманні обчислення розташовані на периферії мережі, вони є сильним кандидатом для забезпечення більш швидшого зв'язку й, отже, зменшення затримки для пакетів зв'язку;

– швидке реагування: програми реального часу, такі як IIoT, матимуть вигоду від концепції туманного обчислення завдяки підвищенню гнучкості на етапах аналізу та прийняття рішень у загальному циклі автоматизації процесів;

– підвищена безпека: за допомогою туманних обчислень постачальники послуг можуть легко фільтрувати конфіденційну персональну інформацію та обробляти її локально. Замість того, щоб надсилати всю інформацію, лише неконфіденційна інформація надсилається в хмару для подальшого оброблення.

Кібератаки та способи захисту мережі від них

На сьогодні було визначено багато атак у мережах IoT, таких як атаки ботнетів *Mirai* та *Torii*, а також різні атаки на промислові мережі, такі як *Stealthy*-атаки. Тож щоб мати надійні та працездатні системи й долати кібератаки, необхідно вживати заходів кібербезпеки. Кібербезпека будь-якої комп'ютерної системи має три рівні: запобігання, виявлення та пом'якшення наслідків.

Щодо виявлення вторгнень, то тут дуже часто використовується метод виявлення аномалій. Виявлення аномалій на основі журналів пристроїв або подій і моделі процесу (кіберзагрози та збої) є ще одним важливим аспектом запобігання можливим векторам атак, створених для цільових систем. В аналогічній роботі про промислові мережі запропоновано метод виявлення кібератак на промислові системи управління за допомогою аналізу процесів [5], однак в цьому дослідженні не враховуються атаки MITM, викрадення обладнання тощо.

Але не лише програмні системи, але й стандартні апаратні платформи вразливі до атак. Їх іноді також називають «зломи апаратного забезпечення», і вони нагадують розробникам систем про необхідність увімкнути перевірку автентичності на рівні апаратного забезпечення відразу після заводської виробничої лінії, потім ідуть процедури перевірки до та після встановлення.

Ця робота зосереджена на механізмах запобігання, щоб уникнути зловмисників, перш ніж будь-яка атака може статися. З боку кіберпрофілактики можна використовувати надійні апаратні компоненти: наприклад, системи інтелектуального моніторингу середовища (SEN – *Smart Environment Monitoring*), також розробляється чимало різноманітних програм для моніторингу даних середовища через IoT.

Туманні обчислення насправді є інструментом для хмарних служб (CBS – *Cloud-Based Services*), який можна уявити як інтерфейс між реальними кінцевими пристроями IoT та рештою хмарних служб. Як обговорювалося в роботі [6] CBS пропонує три основні компоненти послуг, а саме: інфраструктуру як послугу (IaaS – *Infrastructure as a Service*), платформу як послугу (PaaS – *Platform as a Service*) і програмне забезпечення як послугу (SaaS – *Software as a Service*). Прогнозуємо, що парадигма туманних обчислень розширить наявне уявлення, додавши FaaS як четвертий компонент моделі обслуговування (див. рис. 2).

Площина безпеки для хмарних служб, запропонована в роботі [6], розроблена для використання на зовнішніх пристроях IoT і для забезпечення інтерфейсу до хмари. Після запропонування туманних обчислень рішення площини безпеки є більш різноманітним і багатошаровим порівняно з попередньою версією (див. рис. 2). Тому розглядаємо туманні обчислення для надання додаткових послуг, такі як безпека на периферії хмари для CBS. Наприклад,

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

застосування туманних обчислень матиме користь для систем виявлення вторгнень (IDS – *Intrusion Detection Systems*), розроблених для IoT. Отже, раннє виявлення є важливим для запобігання згубних наслідків вторгнень, а туманні обчислення дадуть змогу раннього виявлення для алгоритмів IDS, що працюють в IoT.

Рис. 2. Модель "Туман як послуга"

Наслідки використання туманних обчислень в IoT

Відповідно до наукових прогнозів, очікується, що туманні обчислення стануть однією з основних опор IoT у найближчому майбутньому, трансформуючи IoT на основі хмарних обчислень у більш розподілену архітектуру [1]. Неминуче ця трансформація матиме такі наслідки:

– зв'язок з інтеграцією системи та/або підсистеми. Інтеграція систем та/або підсистем є важливим завданням для системних інженерів, оскільки їхній обов'язок – забезпечити безперебійну роботу всіх компонентів новоствореної системи;

– зв'язок з телекомунікаціями. У табл. 2 детально показано пов'язані з IoT телекомунікаційні технології. Вибір радіочастотних технологій може ґрунтуватися на передбачуваній функціональності та апаратних вимогах, а саме: пропускна здатність, вартість, енергоефективність, затримка, тип мережі тощо. Ці радіочастотні технології створюють основу для мережних технологій IoT;

– зв'язок із вартістю. Туманні обчислення допоможуть системам Інтернету речей, що підтримують хмарні обчислення, зменшити загальну вартість системи. Оскільки дані оброблятимуться на периферії, а не в хмарі, туманні технології зменшать накладні витрати на передачу інформації в хмару. Це матиме дві переваги: використання пропускної здатності передачі різко скоротиться та зменшиться розмір сховища даних у хмарі (разом із обробленням);

– зв'язок з якістю обслуговування. Це є важливим критерієм сервісу, що зрештою впливає на задоволеність користувачів. Для IoT тимчасова недоступність датчиків або виконувальних механізмів у застосунках IoT безпосередньо вплине на фізичний світ і, отже, різко знизить якість обслуговування для користувачів мережі. Чимало безпроводових програм мають різноманітні та обов'язкові вимоги до якості обслуговування, що ускладнює навантаження на інтеграцію IoT і хмари. Водночас нові рішення проміжного програмного забезпечення на основі туманних обчислень можуть бути корисними й зручними в тому сенсі, щоб запропонувати оброблення термінових завдань на периферії мережі та розвантажити дані з вузлів із дефіцитом енергії. Туманні обчислення можуть суттєво покращити якість обслуговування мереж IoT завдяки зменшенню "затримки пакетів" і "перенавантаженості мережі", одночасно збільшуючи "виявлення збоїв" і "відновлення втрат";

– зв'язок із безпекою. Реальне середовище відрізняється від ідеальних умов. Додаткові функції та компоненти іноді створюють єдину точку збою або ускладнюють роботу системи. У добре розроблених

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23) ISSN 2524-2296 (online)

і сплановані реалізаціях можна усунути одну точку збою та навантаження на систему, щоб покращити загальну продуктивність системи за бажанням. Це стосується як апаратного, так і програмного забезпечення та функцій безпеки, пов'язаних із включенням додаткового компонента.

Таблиця 2 – *Різні радіочастотні комунікаційні технології для IoT*

Технологія	Стандарт	Частота	Проникнення	Діапазон	Макс. швидкість передачі даних	Пропускна здатність каналу	Вартість мікросхем
NFC/RFID	ISO/IEC 18092	13.56 МГц	Високе	< 20 см	424 кбіт/с	106–424 Мбіт/с	$0.1+
Bluetooth	IEEE 802.15	2.4/2.5 ГГц	Низьке	50–100 м	2 Мбіт/с	2 МГц	$5+
Wi-Fi	IEEE 802.11	2.4/5.0 ГГц	Низьке	100 м	54 Мбіт/с	22 МГц	$1.5–30+
Zigbee	IEEE 802.15.4	868/915 МГц, 2.4 ГГц	Низьке / високе	< 1 км	250 кбіт/с	2 МГц	$2–20+
DASH7	ISO/ IEC 18000-7	433/868/915 МГц	Високе	0–5 км	167 кбіт/с	до 1.75 МГц	$3.00+
LoRa	Різні	868/915 МГц	Низьке	25 км	50 кбіт/с	125/250/500 кГц	~$2.00
SigFox	SigFox	915–928 МГц	Низьке / високе	40 км	100 біт/с	100 Гц	$0.25+
3G	UMTS/ W-CDMA	0.4–3 ГГц	Низьке / високе	5-35 км	0.38–21.6 Мбіт/с	3.6–21 Мбіт/с	варіюється
4G/LTE	3GPP-LTE	0.6–6 ГГц	Низьке / високе	5–100 км	100–300 Мбіт/с	100 Мбіт/с+	$6.5+
5G	5GTF/5G-SIG	0.6–4/100 ГГц	Низьке / високе	5–150 км	10 Гбіт/с	500 Мбіт/с+	$70+

У разі захоплення шлюзів туманних обчислень існує п'ять особливостей, що необхідно враховувати:

1. Контроль доступу: шлюзи туманних обчислень з'єднують мережі IoT / IIoT і хмару за допомогою двонаправленого каналу зв'язку. Дані збираються та передаються з пристроїв IoT у хмару, а повідомлення про рішення та команди надсилаються з хмари в мережі IoT. Пристрій FCG може ефективно керувати всіма підключеними пристроями IoT. Однак пристрої шлюзів туманних обчислень не мають змоги отримати прямий доступ до баз даних та інших обчислювальних ресурсів без призначеної хмарної служби.

2. Автентифікація: пристрій FCG може завдавати деяких наслідків залежно від обраного алгоритму автентифікації. Якщо автентифікація призначена для роботи лише з пристроями FCG, це збільшує ризик того, що вся мережа IoT буде зламана після того, як пристрій FCG буде зламано. Зазвичай двофакторна та багаторівнева автентифікація (одна у FCG, інша в хмарі тощо) зменшують ризик зламу FCG. У разі інциденту буде вражено лише підмножину підключених пристроїв IoT.

3. Доступність: хмарні ресурси більш стійкі до єдиної точки відмови. Дані відтворюються на кількох вузлах у хмарі, й аварійне переключення може буте досягнуте без проблем. Однак пристрої IoT більш схильні до збоїв. Наприклад, блокування зв'язку для ресурсів IoT може значно вплинути на доступність на основі критичного розташування шлюзу туманних обчислень.

4. Цілісність: залежно від обраної схеми зв'язку очікується незначний вплив захоплення шлюзу туманних обчислень на цілісність повідомлень, якщо не використовуватиметься наскрізне шифрування, і відсутність жодного ефекту у випадку застосування шифрування.

5. Конфіденційність. Будь-який витік даних і порушення конфіденційності користувачів у мережах IoT через пристрій FCG є серйозною проблемою, що не обмежується погіршенням репутації, фінансовими втратами чи іншими наслідками для організацій. Будь-який користувач, який застосовує пристрій IoT або зберігає на ньому дані, зазнає впливу через зламаний пристрій FCG. Однак це не позначиться на особистих даних у хмарі.

Усі комунікації між хмарою та IoT здійснюються через шлюз туманних обчислень. Отже, необхідно встановити достатню кількість комп'ютерів, щоб запобігти виникненню єдиної точки збоїв та безперебійно справлятись з подіями самовідновлення та аварійного перемикання. Оскільки весь потік даних буде заблоковано в разі будь-якого пошкодження або фізичної атаки, ми пропонуємо встановити декілька FCG у мережних архітектурах Інтернету речей із підтримкою туманних обчислень, із можливістю самовідновлення та безперебійного перемикання після збоїв.

Зламаний шлюз туманних обчислень впливає як на мережу IoT, так і на хмарний рівень. Безпека шлюзу туманних обчислень є важливою, і не потрібно залишати її незахищеною. Як обговорюватиметься

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

далі, необхідно використовувати апаратну безпеку, щоб надати FCG додатковий рівень захисту водночас із програмно орієнтованими рішеннями.

Апаратний захист пристроїв туманних обчислень

У роботі [7] автори дійшли висновку, що незахищена апаратна платформа призведе до незахищеного стеку програмного забезпечення, таким чином доведено важливість безпеки апаратного забезпечення. Безпека апаратного забезпечення недостатньо вивчена порівняно з проблемами та рішеннями кібербезпеки, пов'язаними з програмним забезпеченням. Останнім часом з'являються нові дослідження апаратної безпеки на пристроях, пов'язаних з Інтернетом речей, як-от: створення єдиної системи перевірки особистості на основі PUF, апаратна безпека FPGA для центрів оброблення даних, а також реконфігурований апаратний механізм ізоляції (IPM – *isolation and protection mechanism*) для пристроїв IoT, що використовують хмарне середовище. Усе це підтверджує наші зусилля щодо запровадження апаратних заходів безпеки для FCG. У цьому розділі стисло наведено всі можливі апаратні заходи безпеки, що можна розглянути для FCG під час прийняття рішення про забезпечення безпеки для загальної мережі IoT.

Як обговорювалося у праці [8], кібератаки на апаратні платформи можна досліджувати за трьома групами: агресивні, неагресивні та напівагресивні. Серед них найбільш складними є агресивні, оскільки вони безпосередньо втручаються в робочу структуру схем на апаратному забезпеченні. На рис. 3 показано додаткові деталі та класифікацію цих атак.

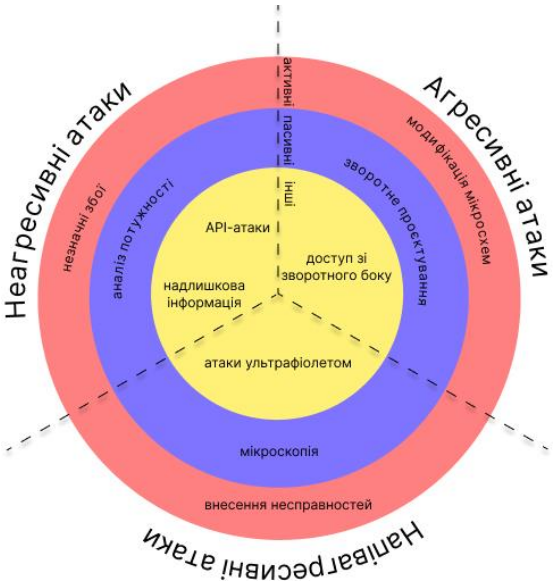

Рис. 3. Підмножина векторів атак, пов'язаних з апаратним забезпеченням, та їх співвідношення

Метод зворотного проєктування (RE – *Reverse Engineering*) застосовується для виявлення фізичних властивостей і функціональних можливостей апаратного забезпечення, щоб відтворювати технології або використовувати ймовірні вразливості. Метод аналізу потужності можна співвіднести зі зворотним проєктуванням, щоб дізнатися більше про властивості цільового обладнання. Ці атаки здебільшого застосовуються в промисловому шпигунстві для викрадення технологій конкурентів. Модифікації мікросхем також використовуються для моніторингу та керування апаратним блоком під час безпосереднього втручання в роботу інтегральної схеми. Упроваджувати несправності можна для порушення принципу КЦД (конфіденційності, цілісності, доступності), наприклад, для виведення пристрою з ладу з метою отримання доступу, припинення функціонування або виконання інших важливих завдань. Залишкове зберігання даних – це концепція розшифрування інформаційних бітів у фізичних пристроях, таких як пам'ять (SRAM, DRAM, EPROM тощо), і накопичувачах, щоб отримати ключі безпеки або іншу важливу інформацію.

У центрі уваги апаратної безпеки мають бути принаймні конфіденційність і цілісність. Прихована інформація про пристрій або дані не мають бути розкриті, і необхідно, щоб утручання до них було

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23) ISSN 2524-2296 (online)

попереджено. У промисловості секретна інформація зазвичай прив'язана до фізичного об'єкта, і апаратне забезпечення має її захищати. Наприклад, смарт-карти використовуються для кількох завдань, таких як доступ до об'єкта або зберігання грошової інформації тощо, і проста атака клонування може мати негайні наслідки. У разі успішного клонування банківських карток фінансові втрати будуть нищівними.

У табл. 3 наведено аналіз ризиків безпеки для апаратних кіберзагроз порівняно із загальними властивостями безпеки кінцевих пристроїв IoT на основі туманних обчислень, включаючи класифікацію векторів атак [9]. Наприклад, аналіз ризиків безпеки кінцевого пристрою, захопленого зловмисниками, щодо загальних властивостей безпеки виглядає таким чином: конфіденційність має помірний рівень, цілісність має помірний, доступність має помірний, а автентифікація і контроль доступу має значний вплив. Відповідний вектор атаки – In (агресивний) або S (напівагресивний).

Таблиця 3 – *Аналіз ризиків безпеки для апаратних кіберзагроз порівняно із загальними властивостями безпеки для кінцевих пристроїв IoT на основі туманних обчислень, включаючи класифікацію вектора атак*

Категорія загрози	**Серйозність ризику**				**Вектор**
	C	**I**	**A**	**Auth***	
Знищити, вилучити або викрасти кінцевий пристрій	Немає	Немає	Помірний	Немає	NI
Клонування пристрою	Помірний	Помірний	Мінімальний	Значний	In
Заміна прошивки	Помірний	Помірний	Мінімальний	Значний	In
Вилучення параметрів безпеки шляхом фізичного доступу	Помірний	Мінімальний	Мінімальний	Значний	In
Глушіння	Мінімальний	Мінімальний	Значний	Мінімальний	NI
Підроблений кінцевий пристрій	Помірний	Помірний	Помірний	Значний	In/ S
Підміна бітів	Мінімальний	Помірний	Мінімальний	Мінімальний	In

Умовні познаки: C – конфіденційність; I – цілісність; A – доступність; Auth – автентифікація та контроль доступу; In – агресивний; NI – неагресивний; S – напівагресивний.*

Існує кілька перешкод, які необхідно подолати, щоб забезпечити кібербезпеку для пристроїв IoT на основі туманних обчислень за допомогою апаратних рішень через проблеми, властиві IoT і самим кінцевим пристроям: фізичний доступ проти віддаленого доступу (апаратні рішення вимагатимуть фізичного доступу до реального пристрою, що іноді може стати серйозним тягарем); гнучкість (апаратні системи не настільки гнучкі, як програмні; хоча деякі апаратні платформи, наприклад програмовану логічну інтегральну схему (ПЛІС), можна переконфігурувати, але в такому вигляді вони дуже дорогі); масштабованість (через апаратні обмеження, вартість та інші виробничі обмеження апаратні рішення важко масштабувати); гнучкість (час, необхідний для встановлення апаратних виправлень, може виявитись значним).

"Стійкість до втручання" означає вжиття заходів з метою ускладнення зворотного проєктування для зловмисників або запобігання модифікації продукту проти волі виробника. Цього можна досягти трьома способами:

– використання програмного забезпечення. Програмне рішення для захисту від несанкційного доступу міститиме способи перетасування виконуваного коду в пам'яті, щоб він не розкривав зловмисникам конкретної інформації щодо будь-якого конфіденційного матеріалу. Одним із поширених методів для цього є обфускація коду. Історично склалося так, що методами захисту від втручання є такі: реалізація білого ящика, динамічний моніторинг програми, самохешування й контрольне підсумовування. Нарешті, технологія блокчейн також є життєздатним варіантом для забезпечення цілісності даних у мережі IoT за допомогою стратегії консенсусу між вузлами;

– використання апаратного забезпечення. Підмножиною відомих векторів атак на апаратне забезпечення є диференційний аналіз помилок, перезапис чипа, залишкова пам'ять та збої протоколу. Як превентивний метод можна застосовувати логічне блокування булевих схем [10]. Мікросхеми пам'яті із захистом від вторгнень (TRM – *Tamper Resistant Memory*) можуть бути призначені для вилучення їх конфіденційних даних, зокрема криптографічних ключів, якщо вони можуть виявити вторгнення в інкапсуляцію безпеки. Робочий механізм, що стоїть за цим, полягає в постійному оновленні комірок пам'яті, щоб запобігти залишкам слідів статичних даних на них. TRM здебільшого використовується для зберігання конфіденційної інформації, зокрема закритих ключів, інформації про електронні платежі

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

тощо. Іншим підходом може бути реалізація концепції апаратної системи на кристалі (SoC – *System on a Chip*). Наприклад, у роботі [11] запропоновано системи на кристалі для захисту вбудованих процесорів нижчого класу від атак потоку керування, особливо від атак повторного застосування коду (CRA – *Code Reuse Attacks*). Запропонована концепція забезпечує комплексний захист, поєднуючи методи виявлення, реагування, відновлення та виявлення вторгнень проти порушення потоку керування (спричиненого CRA), особливо за наявності переривань, операційних систем реального часу та виняткових функцій;

– безпечне проєктування. Структури IoT залежать від основного апаратного забезпечення та розумної електроніки як шлюзових пристроїв, зокрема датчиків і мікроконтролерів. Вони можуть бути під загрозою зловмисних апаратних троянів (HT – *Hardware Trojan*), вставлених ненадійними виробниками мікросхем. Апаратні трояни стратегічно вводяться в обладнання під нормальним виглядом за допомогою навичок RE та діють як бомба уповільненої дії: вони раптово активуються під час нормального режиму роботи апаратного забезпечення й можуть спричинити ненормальну та ненавмисну роботу. Захистом від такого виду атак може бути один із популярних методів, а саме функціональна та структурна обфускація, що виконується виробниками пристроїв перед етапом виготовлення чипів.

Фізично неклоновані функції (PUF)

Фізично неклоновані функції – це фізичний об’єкт, що забезпечує цифровий відбиток для апаратного забезпечення, наприклад мікропроцесорів, на основі різних вхідних даних і завдань. Отримані кремнієві схеми з унікальними характеристиками виробів неможливо фізично клонувати. Необхідно, щоб кожна схема PUF мала унікальну пару реакції на виклик (CRP), яку можна використовувати для ідентифікації та автентифікації. Виготовлення й архітектурні деталі слабких PUF (має незначну кількість CRP) і сильних PUF (має багато CRP) також важливі. Сильні PUF стійкі до атак грубою силою. Основними характеристиками фізично неклонованих функцій є надійність, непередбачуваність, неклонованість і фізична непорушність. Перевагами PUF є стійкість до агресивних атак і відсутність потреби в додатковому програмуванні, тестуванні та обчислювальній потужності [12].

Комірки SRAM стійкі до руйнування схеми й можуть використовуватися для створення надійних PUF на основі SRAM, що можна застосовувати для автентифікації та генерації секретних ключів. Автори роботи [13] показали, що PUF можна використовувати для перевірки особистості з метою захисту обладнання IoT за допомогою автентифікації пристрою. Це досягається шляхом удосконалення конфігурованих кільцевих осциляторів (CRO – *configurable ring oscillator*) PUF зі структурою засувки. Унікальний субцифровий підпис кожного чипа може бути згенерований шляхом виконання стратегії виклик-відповідь через PUF на основі CRO.

Аналіз PUF показав, що завдяки дослідницьким зусиллям незабаром відбудеться експоненціальне покращення в галузі мікросхем та енергоефективності.

У роботі [14] було показано, що PUF можуть використовуватися пристроями IoT для забезпечення захисту IP під час процедур оновлення програмного забезпечення. Відповідно, кінцевий пристрій IoT має підтвердити стирання своєї пам’яті протягом обмеженого часу, а PUF прив’язує нещодавно завантажену IP-адресу програмного забезпечення до цільової платформи. Використання PUF обіцяє підвищення рівня безпеки IoT з допомогою реалізації низькорівневої безпеки речей, а також завдяки розробленню криптографічних алгоритмів для виконання спеціальних завдань (зокрема перевірки тощо) [15]. Подібним чином туманні обчислення можуть застосовувати PUF, які вбудовані в туманні шлюзи та/або кінцеві пристрої IoT, щоб забезпечити захист IP під час оновлення виправлень.

Апаратний модуль безпеки (HSM)

Апаратний модуль безпеки – це фізичне обчислювальне обладнання, що захищає та координує цифрові ключі для надійної автентифікації та забезпечує основу для криптооброблення. Ці модулі подані або у вигляді з’ємної карти, або зовнішнього портативного пристрою, що можна підключити безпосередньо до комп’ютера або мережного сервера. Модулі HSM можуть бути реалізовані в шлюзі туманних обчислень мережі IoT на основі туманних обчислень для керування не лише розподілом ключів, але й пов’язаними з криптографією

Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

операціями, такими як автентифікація, шифрування / дешифрування тощо.

Існують різні конфігурації обладнання для кінцевих пристроїв IoT залежно від програми, для якої вони використовуються, а також від технології безпроводового зв'язку, яку вони застосовують. Наприклад, Bluetooth LE, Sigfox, LoRa, WiFi, WiMAX і NB-IoT є добре відомими технологіями безпроводового зв'язку для IoT з доступними на ринку наборами радіочипів. Отже, апаратні рішення безпеки не будуть загальними, оскільки вони мають враховувати всі компоненти, що використовуються в системі. Як показано на рис. 4, ми прогнозуємо, що згадані вище апаратні засоби безпеки, доступні на ринку, можуть бути засобом забезпечення кібербезпеки для мереж IoT із підтримкою туманних обчислень. TRM і PUF є порівняно дешевшими апаратними рішеннями безпеки й можуть застосовуватися для кінцевих пристроїв IoT-мереж із підтримкою туманних обчислень. Однак апаратні модулі безпеки є досить дорогими пристроями, і їх бажано встановлювати на шлюз туманних обчислень мережі IoT.

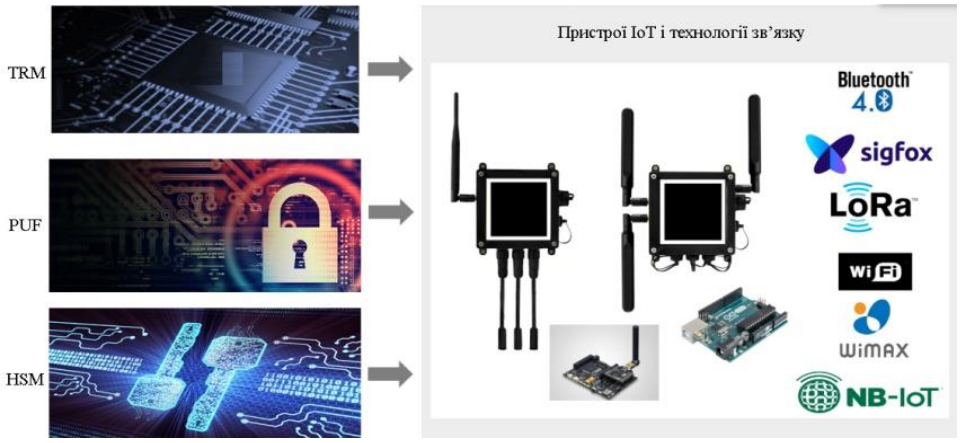

Рис. 4. Відображення "апаратної безпеки" для мереж IoT на основі туманних обчислень

Сценарії практичного застосування туманних обчислень в IoT

Завдяки впровадженню гнучкого реагування поблизу периферійних компонентів очікуємо швидкого впровадження та зростання бізнесу туманних обчислень для майбутніх застосунків IoT, таких як інтелектуальні транспортні системи (ITS), Розумні фабрики, Розумні міста тощо. На рис. 5 зображено різні можливості застосування туманних обчислень.

Концепція Розумного будинку запропонована 1975 р., коли в Шотландії була розроблена технологія X10 [16]. Зараз для застосунків домашньої автоматизації переважно використовуються *Zigbee* або *Z-wave*. Здебільшого це протоколи безпроводової мережі. Щоб захистити Розумні будинки, необхідно розглянути інфраструктуру безпеки, яка застосовує моніторинг мережі, виявлення аномалій тощо для протидії фізичним, мережним і програмним атакам.

Розумні міста можуть бути ітегровані в концепцію інтелектуальної транспортної системи способом підтримки IoT і туманних обчислень, щоб сприяти сталому економічному розвитку нашого світу (розподіл енергії / комунальних послуг тощо), безпеці, транспорту (планування руху, системи сигналізації тощо), сприяючи прийняттю рішень за допомогою концепції локалізації. Як обговорювалося в роботі [17], Розумні міста будуть вразливі до багатьох кібератак і потребуватимуть надійної архітектури безпеки, для якої можна використовувати апаратні засоби безпеки, що підтримують туманні обчислення.

Розумні виробництва та промисловий Інтернет речей: процеси автоматизації можна покращити шляхом збору даних за допомогою датчиків Інтернету речей та аналізу даних у середовищі туманних обчислень. За допомогою цієї методології можна легко виконати аудит робочого процесу та збір даних.

Розумна охорона здоров'я: IoT і туманні обчислення можуть допомогти в удосконаленні інструментів і платформ у галузі охорони здоров'я. Фінансове вдосконалення, спостереження за безпекою, збір інформації та координація важливих даних про медичні пристрої можуть мати користь. Апаратна безпека з підтримкою туманних обчислень здатна покращити безпеку розумних систем охорони здоров'я.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

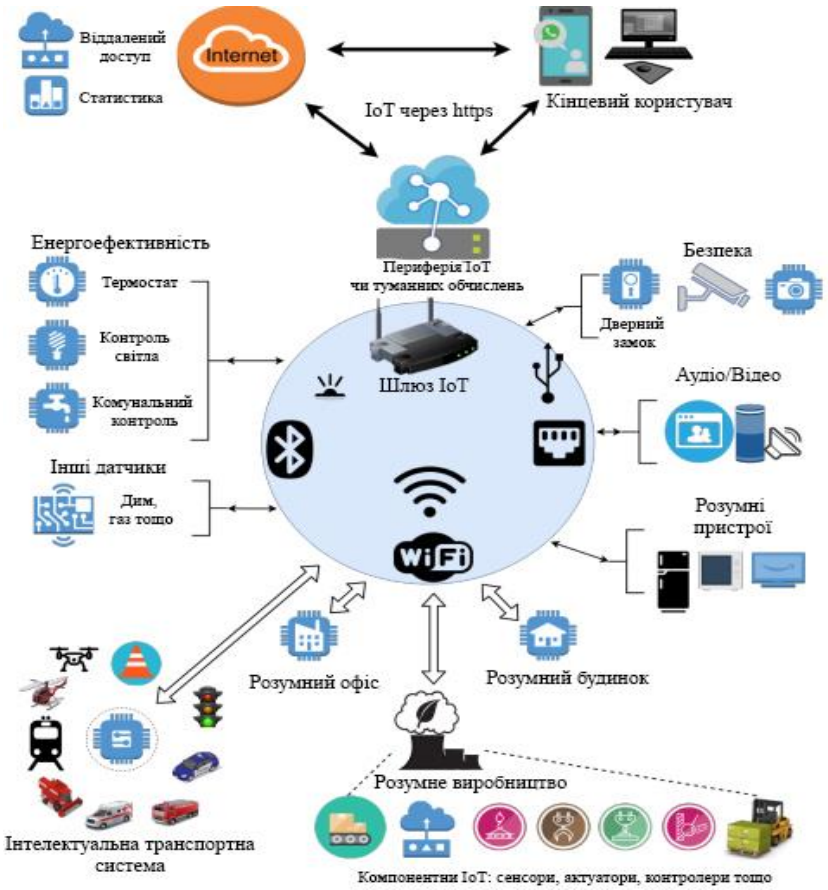

Рис. 5. Ілюстрація чотирьох різних можливих застосунків із використанням туманних обчислень із мережами IoT: Розумний офіс, Розумне виробництво, Розумний будинок та інтелектуальна транспортна система

Інтелектуальні транспортні системи (ITS – *Intelligent Transportation Systems*) можна вважати акронімом для автомобільних мереж і автомобільних мереж IoT. Очікується, що туманні обчислення розширять охоплення та зменшать час відгуку інтелектуальних транспортних систем. Загалом, ITS може мати вигоду від туманних обчислень для підвищення якості обслуговування в таких прикладах сценаріїв, як: швидка зміна маршруту руху, швидка служба буксування, екстрені служби в разі аварій і, нарешті, забезпечення необхідних шляхів евакуації в екстремальних погодних умовах, наприклад у разі ураганів.

Висновки

Поширення побутової техніки наблизило пристрої та датчикм Інтернету речей до кожного з нас. Це незамінна розробка, і туманні обчислення зроблять можливим і подальший розвиток цих технологій завдяки їх перевагам. У цій статті наголошувалося про наслідки використання туманних обчислень як базової архітектури для IoT, особливо щодо кібербезпеки.

Централізовані хмарні центри оброблення даних можуть виходити з ладу в процесі зберігання або оброблення запитів від мільйонів розподілених кінцевих пристроїв IoT через перевантажену мережу, високу затримку в службі, перевантаження в обмеженій пропускній здатності тощо. Тому з метою вирішення цієї проблеми прогнозується, що дуже корисною буде концепція туманних обчислень, особливо для чутливих до затримки програм, таких як промислова автоматизація в IIoT. Концепції підтримки мобільності, георозподілу, визначення місця розташування та низької затримки є важливими під час розгортання пристроїв Інтернету речей, і туманні обчислення є сильним кандидатом на допомогу в усіх цих питаннях.

Це дослідження також показало, що апаратні компоненти будь-якої системи, особливо системи IoT, пов’язані з туманними обчисленнями, не схильні до кібератак, зломів, вторгнень, маніпуляцій та вільні від них. У цій роботі класифікуються кілька кібератак на апаратні платформи разом із механізмами захисту

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23) ISSN 2524-2296 (online)

в узагальненому вигляді. Як також зазначено в роботі [18], тісніша взаємодія між розробниками мікросхем і розробниками протоколів буде необхідною для пристроїв IoT наступного покоління, щоб забезпечити бажаний рівень безпеки за мінімальних витрат на енергію / площу, одночасно гарантуючи гнучкість для майбутнього апаратного забезпечення.

Використання розглянутих у роботі апаратних засобів безпеки може допомогти зберегти конфіденційність, цілісність і доступність інформації, що циркулює в мережі, та підвищити загальну стійкість системи до можливих атак.

Передбачаємо, що найближчим часом кількість кібератак на апаратне забезпечення буде збільшуватись, особливо на вбудовані бюджетні пристрої. Отже, апаратні рішення кібербезпеки будуть дуже корисним інструментом для захисту від цих атак, що більш важливо для мереж Інтернету речей, основаних на туманних обчисленнях. Тож наші майбутні дослідження будуть і надалі присвячені пошуку можливих засобів захисту системи Інтернету речей.

Список літератури

1. Friedman, V. (2018) "On The Edge: Solving The Challenges Of Edge Computing In The Era Of IoT". URL: https://data-economy.com/on-the-edge-solving-the-challenges-of-edge-computing-in-the-eraof-iot/.
2. Kocakulak, M.; Butun, I. (2017, January) "An overview of Wireless Sensor Networks towards internet of things", *In Proceedings of the IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, P. 1–6. URL: https://researchr.org/publication/ccwc-2017
3. Aazam, M.; Zeadally, S.; Harras, K.A. (2018) "Fog computing architecture, evaluation, and future research directions", *IEEE Commun. Mag. 2018*, P. 46-52. URL: https://link.springer.com/chapter/10.1007/978-3-030-34957-8_8
4. Munir, A.; Kansakar, P.; Khan, S.U. (2017) "IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things", *IEEE Consum. Electron. Mag. 6*, P. 74–82. URL: https://www.sciencedirect.com/science/article/pii/S0167404822002164#!
5. Myers, D. (2019) "Detecting Cyber Attacks on Industrial Control Systems Using Process Mining". *Ph.D. Thesis, Queensland University of Technology, Brisbane City, Australia*. URL: https://www.mdpi.com/1424-8220/20/20/5729
6. Butun, I.; Kantarci, B.; Erol-Kantarci, M. (2015) "Anomaly detection and privacy preservation in cloud-centric Internet of Things", *In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK*, P. 2610–2615. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7601476/
7. Arias, O.; Wurm, J.; Hoang, K.; Jin, Y. (2015) "Privacy and Security in Internet of Things and Wearable Devices", *IEEE Trans. Multi-Scale Comput. Sys. 1*, P. 99–109. URL: https://ieeexplore.ieee.org/document/7321811
8. Skorobogatov, S.P. "Semi-Invasive Attacks – A New Approach to Hardware Security". URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf.
9. Butun, I.; Pereira, N.; Gidlund, M. (2019) "Security risk analysis of LoRaWAN and future directions", *Future Internet, 11, 3*. URL: https://www.mdpi.com/1999-5903/11/1/3
10. Yasin, M. (2019) "Logic Locking of Boolean Circuits: Provable Hardware-Based Obfuscation from a Tamper-Proof Memory". *In Proceedings of the 12th International Conference on Innovative Security Solutions for Information Technology and Communications (SecITC), Bucharest, Romania*, 172 p. URL: https://nyuscholars.nyu.edu/en/publications/logic-locking-of-boolean-circuits-provable-hardware-based-obfusca
11. DaSilva, P.R.; Fortier, P.J. (2019) "Hardware Based Detection, Recovery, and Tamper Evident Concept to Protect from Control Flow Violations in Embedded Processing", *In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA*, P. 1–6. URL: https://www.academia.edu/72492295/Hardware_Security_of_Fog_End_Devices_for_the_Internet_of_Things
12. Shanta, A.S.; Majumder, M.B.; Hasan, M.S.; Rose, G.S. (2020) "Physically Unclonable and Reconfigurable Computing System (PURCS) for Hardware Security Applications". *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* DOI: https://doi.org/10.3390/s20205729
13. Huang, Z.; Wang, Q. (2020) "A PUF-based unified identity verification framework for secure IoT hardware via device authentication", *World Wide Web, 23*, P. 1057-1088. URL: https://www.mdpi.com/1424-8220/22/4/1325?type=check_update&version=1
14. Huth, C.; Duplys, P.; Güneysu, T. (2016) "Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions", *In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, NSW, Australia*, P. 1–6. URL: https://www.researchgate.net/publication/301583647_Secure_software_update_and_IP_protection_for_untrusted_devices_in_the_Internet_of_Things_via_physically_unclonable_functions

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 1 (23)

15. Butun, I.; Österberg, P.; Song, H. (2019) "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures", *IEEE Commun. Surv. Tutor., 22,* P. 616-644. DOI: 10.1109/COMST.2019.2953364
16. Stojkoska, B.L.R.; Trivodaliev, K.V. (2017) "A review of Internet of Things for smart home: Challenges and solutions", *J. Clean. Prod., 140,* P. 1454–1464. URL: https://iotiran.com/wp-content/uploads/2021/02/A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions.pdf
17. Butun, I.; Österberg, P. (2019) "Detecting Intrusions in Cyber-Physical Systems of Smart Cities: Challenges and Directions. In Secure Cyber-Physical Systems for Smart Cities", *IGI Global: Hershey, PA, USA,* P. 74-102. DOI: https://doi.org/10.3390/s20205729
18. Alioto, M. (2019) "Trends in Hardware Security: From basics to ASICs", *IEEE Solid-State Circuits Mag., 11,* P. 56–74. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9955388

References

1. Friedman, V. (2018) "On The Edge: Solving The Challenges Of Edge Computing In The Era Of IoT". URL: https://data-economy.com/on-the-edge-solving-the-challenges-of-edge-computing-in-the-eraof-iot/.
2. Kocakulak, M.; Butun, I. (2017, January) "An overview of Wireless Sensor Networks towards internet of things", *In Proceedings of the IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC),* P. 1–6. URL: https://researchr.org/publication/ccwc-2017
3. Aazam, M.; Zeadally, S.; Harras, K.A. (2018) "Fog computing architecture, evaluation, and future research directions", *IEEE Commun. Mag. 2018,* P. 46–52. URL: https://link.springer.com/chapter/10.1007/978-3-030-34957-8_8
4. Munir, A.; Kansakar, P.; Khan, S.U. (2017) "IFCIoT: Integrated Fog Cloud IoT: A novel architectural paradigm for the future Internet of Things", *IEEE Consum. Electron. Mag. 6,* P. 74-82. URL: https://www.sciencedirect.com/science/article/pii/S0167404822002164#!
5. Myers, D. (2019) "Detecting Cyber Attacks on Industrial Control Systems Using Process Mining". *Ph.D. Thesis, Queensland University of Technology, Brisbane City, Australia.* URL: https://www.mdpi.com/1424-8220/20/20/5729
6. Butun, I.; Kantarci, B.; Erol-Kantarci, M. (2015) "Anomaly detection and privacy preservation in cloud-centric Internet of Things", *In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK,* P. 2610–2615. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7601476/
7. Arias, O.; Wurm, J.; Hoang, K.; Jin, Y. (2015) "Privacy and Security in Internet of Things and Wearable Devices", *IEEE Trans. Multi-Scale Comput. Sys. 1,* P. 99–109. URL: https://ieeexplore.ieee.org/document/7321811
8. Skorobogatov, S.P. "Semi-Invasive Attacks – A New Approach to Hardware Security". URL: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-630.pdf.
9. Butun, I.; Pereira, N.; Gidlund, M. (2019) "Security risk analysis of LoRaWAN and future directions", *Future Internet, 11, 3.* URL: https://www.mdpi.com/1999-5903/11/1/3
10. Yasin, M. (2019) "Logic Locking of Boolean Circuits: Provable Hardware-Based Obfuscation from a Tamper-Proof Memory". *In Proceedings of the 12th International Conference on Innovative Security Solutions for Information Technology and Communications (SecITC), Bucharest, Romania,* 172 p. URL: https://nyuscholars.nyu.edu/en/publications/logic-locking-of-boolean-circuits-provable-hardware-based-obfusca
11. DaSilva, P.R.; Fortier, P.J. (2019) "Hardware Based Detection, Recovery, and Tamper Evident Concept to Protect from Control Flow Violations in Embedded Processing", *In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA,* P. 1–6. URL: https://www.academia.edu/72492295/Hardware_Security_of_Fog_End_Devices_for_the_Internet_of_Things
12. Shanta, A.S.; Majumder, M.B.; Hasan, M.S.; Rose, G.S. (2020) "Physically Unclonable and Reconfigurable Computing System (PURCS) for Hardware Security Applications". *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* DOI: https://doi.org/10.3390/s20205729
13. Huang, Z.; Wang, Q. (2020) "A PUF-based unified identity verification framework for secure IoT hardware via device authentication", *World Wide Web, 23,* P. 1057-1088. URL: https://www.mdpi.com/1424-8220/22/4/1325?type=check_update&version=1
14. Huth, C.; Duplys, P.; Güneysu, T. (2016) "Secure software update and IP protection for untrusted devices in the Internet of Things via physically unclonable functions", *In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, NSW, Australia,* P. 1–6. URL: https://www.researchgate.net/publication/301583647_Secure_software_update_and_IP_protection_for_untrusted_devices_in_the_Internet_of_Things_via_physically_unclonable_functions
15. Butun, I.; Österberg, P.; Song, H. (2019) "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures", *IEEE Commun. Surv. Tutor., 22,* P. 616-644. DOI: 10.1109/COMST.2019.2953364
16. Stojkoska, B.L.R.; Trivodaliev, K.V. (2017) "A review of Internet of Things for smart home: Challenges and solutions", *J. Clean. Prod., 140,* P. 1454–1464. URL: https://iotiran.com/wp-content/uploads/2021/02/A_review_of_Internet_of_Things_for_smart_home_Challenges_and_solutions.pdf

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1 (23) *ISSN 2524-2296 (online)*

17. Butun, I.; Österberg, P. (2019) "Detecting Intrusions in Cyber-Physical Systems of Smart Cities: Challenges and Directions. In Secure Cyber-Physical Systems for Smart Cities", *IGI Global: Hershey, PA, USA*, P. 74–102. DOI https://doi.org/10.3390/s20205729
18. Alioto, M. (2019) "Trends in Hardware Security: From basics to ASICs", *IEEE Solid-State Circuits Mag., 11*, P. 56–74. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9955388

Received 16.03.2023

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

Аветісова Карина Арменівна – Харківський національний університет радіоелектроніки, студентка кафедри безпеки інформаційних технологій, Харків, Україна; e-mail: karyna.avetisova@nure.ua ORCID ID: https://orcid.org/0009-0001-4273-8148

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

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

Avetisova Karyna – Kharkiv National University of Radio Electronics, Student of the Department of Information Technology Security, Kharkiv, Ukraine.

HARDWARE SECURITY OVERVIEW OF FOG COMPUTING END DEVICES IN THE INTERNET OF THINGS

The subject of the study is possible means of increasing the hardware security of end devices of fog computing in Internet of Things (IoT) networks, the spread of which is growing rapidly every year and requires a high level of of protection against all types of attacks. The **goal** of the work is to review available COTS (commercial off-the-shelf) and/or conceptual hardware solutions for protecting low-end devices in Internet of Things networks based on fog technologies. To achieve the goal, the following **tasks** were solved: the concept of fog computing and the advantages it will bring to IoT networks are presented; cyber threats and hardware attacks on IoT networks are considered; the consequences of using IoT networks based on fog computing are presented; hardware security tools such as TRM, PUF, HSM, etc. are considered. When performing the tasks, such research **methods** were used as: theoretical analysis of literary sources; comparative analysis of cloud, fog and mobile computing; analysis of existing security hardware. The following **results** were obtained: fog computing provides most of the advantages of cloud computing by additionally allowing data to be processed on end devices without burdening the central server. **Conclusions:** hardware security in IoT systems is no less important than software security. This issue is especially important for systems based on fog computing, where data will be processed on the periphery, without being transferred to the cloud. To increase the level of hardware security of fog computing devices, it is suggested to use standard hardware security platforms, such as: Physically Unclonable Functions, Hardware Security Module, System On a Chip, etc. The hardware components of the system using fog computing are less prone to cyber-attacks/hacking/intrusions/manipulation.

Keywords: cloud; fog computing; hardware security; IoT; IIoT; privacy; security; hardware security module; physically unclonable functions.

Бібліографічні описи / Bibliographic descriptions

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. 57–71. DOI: https://doi.org/10.30837/ITSSI.2023.23.057

Zhurylo, O., Liashenko, O., Avetisova, K. (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. 57–71. DOI: https://doi.org/10.30837/ITSSI.2023.23.057