https://doi.org/10.31649/1997-9266-2024-175-4-129-138

УДК 004.72

Л. В. Чепель[1]
Ю. В. Бойко[1]

ПІДХІД ДО БЕЗПЕКИ ТА ОРГАНІЗАЦІЇ МЕРЕЖ IOT З ВИКОРИСТАННЯМ БЛОКЧЕЙН ТЕХНОЛОГІЇ

[1]Київський національний університет імені Тараса Шевченка

В стрімкому розвитку інтернету речей (IoT) немає універсального механізму безпеки пристроїв через їхню різноманітність і апаратну обмеженість, проте використання розподіленої мережі, додаткового шифрування, обмеження невикористовуваних каналів передачі даних, ввід колективної атестації пристроїв, використання цифрових підписів, фільтрування пакетів даних дозволяють убезпечити пристрої від атак в класичному варіанті реалізації.

Розглянуто виклики та можливі атаки на безпеку пристроїв інтернету речей: для найкращого контролю безпеки в класичних мережах є використання програмно керованих мереж. Використання туманних обчислень знищує ризики центрального вузла, проте залишаються інші безпекові ризики. Альтернативою та комплексним рішенням є поєднання блокчейну з пристроями інтернету речей. Розглянуто декілька наявних систем, які дозволяють комплексно організувати безпеку, проте навіть вони мають певні недоліки, які автори спробували виправити в запропонованому варіанті побудови мережі інтернету речей.

Запропонований варіант побудови мережі інтернету речей з використанням блокчейн складається з декількох шарів: шару сенсорів та малопотужних пристроїв та шару локальної блокчейн-мережі, які об'єднуються в кластер. Комунікація між шарами забезпечена симетричним та асиметричним шифруванням, а правила роботи мережі можуть регулюватись смарт-контрактами. До того ж, існує взаємодія між кластерами, через що система є масштабованою, децентралізованою та безпечною.

Ключові слова: мережі IoT, блокчейн, децентралізовані мережі, захист інформації, безпека, побудова мереж IoT.

Вступ

Інтернет речей (далі IoT) поєднує різні пристрої, починаючи від звичайної світлодіодної лампи з віддаленим керуванням і закінчуючи складними медичними системами, системами розумного міста тощо Ці пристрої можуть знаходитись в будь-якому місці та бути підключеними за допомогою будь-яких протоколів зв'язку [1]. Усі ці складові мережі IoT повинні взаємодіяти з вузлами передачі/ прийому даних, встановлюючи певні безпечні канали зв'язку, безпечно масштабуватись та мати резервні варіанти передачі даних. Ця сфера настільки широка, що кількість пристроїв IoT зростає оціночно до 30 мільярдів активних пристроїв у 2025 році (рис. 1).

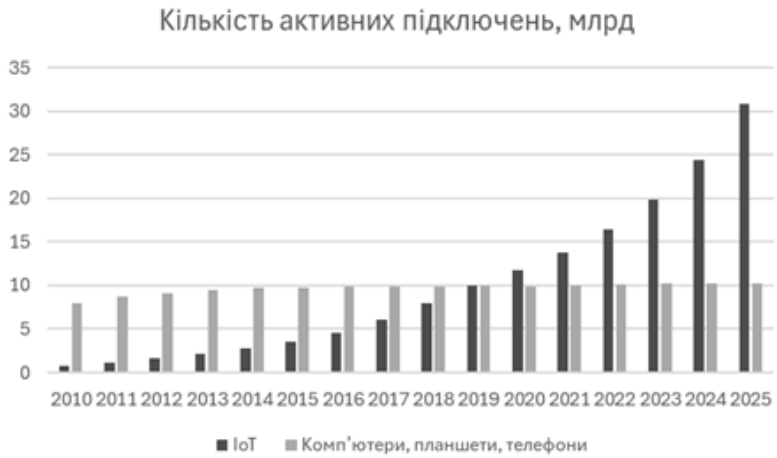

Рис. 1. Діаграма активних підключень пристроїв IoT та не IoT до мережі Інтернет [2]

У статті сфокусовано увагу на організації безпеки та ефективності IoT пристроїв, оскільки обмежені апаратні та програмні можливості можуть створювати ризики для кінцевого користувача, а стрімка масштабованість додає нових викликів в цій сфері.

Метою роботи є знаходження оптимального рішення з погляду безпеки та контролю в IoT-середовищі шляхом комбінації класичних та блокчейн підходів. Для аналізу та класифікації використаємо такі критерії:

1) безпека та керування кінцевими пристроями та середовища передачі даних;
2) опрацювання та зберігання даних;
3) аналіз безпекових ризиків та проактивний захист.

Огляд методів захисту інформації в мережах IoT

На сьогодні існує багато методів захисту інформації, забезпечених різноманітними алгоритмами та протоколами, однак застосувати щось уніфіковане для різного рівня потужності пристроїв досить проблематично через вимоги імплементації. Не всі підтримувані методи захисту є надійними, в деяких випадках необхідно застосовувати різноманітні комбінації. Наприклад, один з найвідоміших протоколів MQTT має 129 згадок щодо вразливостей згідно бази CVE [3]. Причому переважна частина цих вразливостей стосується програмної реалізації. Тобто потрібно розглядати проблему комплексно, оскільки, за безпечним пристроєм повинен стояти безпечний канал передачі даних з безпечним програмним забезпеченням на сервері. У разі зламу безпеки будь-якого з компонентів транзакція передачі даних не повинна відбутися.

Розглянемо класифікацію атак в IoT та наявні рішення для захисту від них [4]—[9].

Таблиця 1

Огляд основних атак в IoT

Назва атаки	Рішення
Атаки маршрутизації (wormhole, Sybil, Grayhole/selective forwarding, blackhole, sinkhole, replay, spoofing, hello flood)	Використання розподіленої мережі, опрацювання ризиків для критичних зон та використання шифрування за допомогою еліптичних кривих для обміну ключами [4]
RFID-атаки	Використання фізичних методів запобігання клонуванню [5]
MITM та DoS атаки	Фільтрування пакетів даних, використання ACL та шифрування [6]
Спам-атаки (підроблені QR коди тощо)	Впровадження цифрового підпису [7]
Ботнет-атаки	Закриття невикористовуваних портів, впровадження шифрування, використання спеціалізованих скриптів перевірки безпеки [8]
Шкідливе ПЗ / додавання шкідливого вузла	Ввід колективної атестації IoT-оточення [9]

Безпека та керування кінцевими пристроями та середовище передачі даних

В оглядовому критерії безпеки та керування кінцевими пристроями важливо вказати протоколи шифрування даних, автентифікації та авторизації пристрою, а також оновлення програмного забезпечення. В табл. 2 наведено основні технології, застосовані в мережах IoT.

Таблиця 2

Застосовані технології в IoT мережах згідно з [10]—[11]

Рівень	Застосовані технології
Мережевий рівень	IPv6, HIP, 6LoWPAN, BLE, ZigBee, Z-Wave
Транспортний рівень	DTLS, UDP
Прикладний рівень	JSON/CoAP/MQTT/ Z-Wave/ ZigBee/BLE з використанням симетричного шифрування, підтримкою авторизації та аунтифікації
Сервісні механізми	ACL, RBAC (як централізований, так і розподілений на прикладі Embedded PDP)

В залежності від наявних апаратних та програмних обмежень, не всі протоколи можна використати на малопотужних пристроях. Так, наприклад повноцінний TLS протокол працює на мікроконтролерах, які мають апаратне прискорення криптографічних функцій та використовують від 20 Кб оперативної пам’яті в найкращому випадку, тобто сам мікроконтролер вже має містити як мінімум вдвічі більше оперативної пам’яті для основної програми [12].

На менш потужних пристроях використовується оптимізований протокол DTLS для встановлення безпечного з’єднання в складі з протоколами CoAP або MQTT. DTLS — це TLS, побудова-

ний на базі UDP, який є набагато швидшим та менш ресурсоємним в порівнянні з TCP.

Як проаналізовано в [10], DTLS має низку проблем в залежності від методу використання:

– у разі використанні серверу делегування виникає проблема з масштабуванням та єдиною точкою відмови;

– у разі використанні DTLS на основі сертифікатів, проблеми з масштабуванням та єдиною точкою відмови вирішуються, натомість виникає надмірне використання пам'яті та ресурсів, пов'язане зі зберіганням, обміном та перевіркою сертифікатів.

Щодо авторизацій/автентифікації пристроїв — це можуть бути різні рішення: від вбудованих сертифікатів, токенів, простого визначення по MAC адресі до використання HIP протоколів з асиметричним шифруванням. Використання ACL списків та рольової моделі RBAC є одними з найпоширеніших сценаріїв. Проте, клои зловмисник заволодіє пристроєм, фізично підключившись до пам'яті пристрою, якщо вона не зашифрована, можна дістати певні дані, наприклад, сертифікат для встановлення з'єднання з сервером і підмінити поточний пристрій на пристрій зловмисника. Саме тому, крім забезпечення безпеки на кінцевому пристрої, система в цілому як мережа пристроїв повинна вміти виявляти аномалії та виконувати проактивні дії.

Мережі передачі даних в IoT умовно можемо поділити на дві категорії:

1. Обмеженої/внутрішньої мережі (ZigBee, 6LoWPAN, ZWave, BLE). Безпека налаштовується можливостями відповідного протоколу (табл. 3).

2. Глобальної мережі (Wi-Fi, Ethernet,3G/4G/5G) з використанням TLS/DTLS.

Таблиця 3

Огляд протоколів внутрішньої мережі

Протокол обмеженої/внутрішньої мережі	Ризики
ZigBee	ZigBee не гарантує комплексної безпеки (хоча має шифрування передачі даних), тому необхідно доповнювати рішення на основі ZigBee безпековими компонентами [13], [14]
6LoWPAN	Використання симетричного шифрування без механізму ротації ключів, ієрархічна топологія призводить до вразливості DoS атак [15]
ZWave	Закрита система, інформація обмежена
BLE	AES-128 [16], що може бути скомпрометована згідно з квантовою брут-форс атакою [17]

Аналізуючи криптографічні протоколи шифрування для різних пристроїв з [10], AES-128 може бути скомпроментованим з використанням квантової брут-форс атаки [17]. Тому що частіше відбувається зміна ключа, або використання безпечнішої системи шифрування, то безпечнішою буде передача даних між пристроями. Також в [17] автори оцінюють можливості квантових методів шифрування QKD та QKR, проте ці методи мають свої виклики, такі як декогеренція кубіту та генерація недостатньо безпечних ключів шифрування.

Одним з ризиків залишаються механізми оновлення ПЗ, оскільки не всі ОС для пристроїв з обмеженими апаратними можливостями мають вбудовані механізми оновлень, що спричиняє їхню вразливість. Можливим рішенням може бути обмеження їхньої взаємодії з певним шлюзом, який матиме всі необхідні оновлення, проте це не вирішує загальну проблему. До того ж кінцеві пристрої можуть не мати достатніх апаратних ресурсів, щоб встановити оновлення або навіть просто його завантажити та перевірити цілісність.

Виділимо такі виклики для кінцевих пристроїв:

1) енергоефективна асиметрична криптографія та обмін ключами;

2) використання надійнішого симетричного шифрування;

3) децентралізація мережі;

4) можливість оновлення програмного забезпечення;

5) комплексний підхід в забезпеченні безпеки.

Опрацювання та зберігання даних

Найчастіше дані передаються по вертикальній ієрархії, навіть якщо це mesh-системи, все одно є певні точки збору інформації. В основному дані передаються в хмарну інфраструктуру, а на кінцевих пристроях майже не зберігаються або зберігаються частково (оскільки є апаратні обмеження кінцевих пристроїв). Отже, класичний підхід ґрунтується на хмарних обчисленнях в питанні обро-

бки та збереження даних. Ризики з єдиною точкою підключення до хмари, MITM-атаками та DoS атаками залишаються.

Окрім традиційних IoT мереж, де дані в основному завантажуються в хмару, існує інший підхід — «туманні обчислення» або “fog computing”. Згідно з [18], «туманні обчислення» зберігають дані на найближчих вузлах, не передаючи все безпосередньо в хмару. Процесінг даних також може відбуватися на тих же вузлах. Ці мережі можуть використовуватись в розумних містах, роботизованих фабриках, інших сферах, де необхідна локальна організація поєднаних пристроїв. Оскільки дані розподілені на декількох вузлах, проблема однієї точки відмови (single point of failure) зникає, проте залишаються виклики безпеки самих пристроїв та безпосередньо мережі, які зазначені вище.

Хмарне опрацювання та зберігання даних вимагає певних можливостей масштабування у разі підключення більшої кількості пристроїв, внутрішніх налаштувань безпеки сервісів обробки та зберігання даних, тобто, це ще одна інфраструктура з власними безпековими викликами. Натомість туманні обчислення є новим підходом локального опрацювання даних. Кожне рішення щодо використання концепції побудови обробки даних повинно залежати та повністю розв’язувати поставлену задачу, проте з погляду авторів, поєднання децентралізованої мережі туманних обчислень з хмарною системою може забезпечити кращу стабільність роботи мережі IoT. Також часткове дублювання даних в мережі туманних обчислень та в хмарі, їхня децентралізація збільшує відмовостійкість та стабільність системи.

Аналіз безпекових ризиків та проактивний захист

Мережа IoT або її окремі сервіси повинні дозволяти виявляти проблеми несанкціонованого доступу, витоку даних, контролю пристроїв та інших зловмисних дій. Як зазначено в [10], використання системи судових розслідувань (Forensic framework) або методології для розслідування порушень безпеки/кібератак в системах інтернету речей дозволяє якісно та кількісно оцінювати проблеми в цих мережах. Проте це є виявленням проблеми після порушення безпеки — системи повинні мати проактивний захист, тобто максимальним чином не допустити порушення безпеки.

Одним з додаткових підходів у безпеці IoT є застосування SDN (Software Defined Network) [19]. Крім переваг в гнучкості, керованості, простоті мережевого дизайну, SDN дає потужний контроль безпеки мережі, включаючи контроль потоку даних, різноманітні оптимізації та шифрування, керування доступом. Таким чином SDN дозволяє налаштувати конфігурацію мережі в максимально строгому варіанті з певними правилами дій на випадок аномальної активності, яка може бути помічена окремими вузлами мережі.

Проте варто підкреслити, що SDN є централізованою ієрархічною структурою, тому варто враховувати всі ризики з DoS атаками та єдиною точкою відмови шляхом додавання резервних вузлів та балансування навантаження.

Поєднання SDN та системи розслідувань дозволяє вносити нові правила роботи мережі без фізичної взаємодії з її пристроями.

Альтернатива наявним концепціям: блокчейн-рішення в мережах IoT

Переваги блокчейну

Блокчейн збільшує стійкість мережі, зменшуючи ризик однієї точки відмови, дозволяє гнучко масштабувати систему завдяки децентралізації. Він побудований на ланцюжку блоків, у якому кожний наступний має інформацію у вигляді хешу про попередній блок. Таким чином формується цілісність даних, оскільки неможливо затерти історію. Транзакції підписані приватним ключем, а публічний ключ використовується для перевірки, часові мітки проставлені в кожній транзакції, тому можна аналізувати та фільтрувати дані за часом.

У блокчейн мережах розповсюджене також поняття смарт контрактів — програм на рівні мережі, які керують транзакціями в залежності від вказаних правил. Це аналог договорів в реальному житті.

Для додавання нових блоків використовуються консенсус алгоритми, саме вони прибирають колізії та вирішують який блок додати [20].

Доцільність впровадження блокчейну в IoT

Блокчейн дозволяє додати інший рівень безпеки, комунікації та оброблення даних в інтернеті речей. Маючи скомпрометований канал передачі даних, використання блокчейну унеможливить

витік даних, їхню модифікацію чи видалення.

Також блокчейн рішення завдяки консенсус-алгоритмам унеможливить додавання скомпрометованої або фальшивої інформації або вузла мережі до системи.

Організація смарт-контрактів на рівні мережі створює альтернативу SDN рішенням з перевагою в децентралізації та більшою простотою розгортання та налаштування.

Загалом, блокчейн-мережа пристроїв інтернету речей може розглядатися як комплексний підхід до безпеки, зберігання та передачі даних, а також керування роботою мережі. Це може спростити наявні комплексні підходи та поліпшити роботу IoT мережі в цілому.

Огляд рішень блокчейну в IoT

На сьогодні існує обмежений перелік рішень на блокчейні:

– Waltonchain. Побудова ланцюгів поставок на базі RFID міток з використанням блокчейну з власним консенсус-протоколом. Система поділяться на декілька рівнів та забезпечує один з найкращих підходів до безпеки. Обмеженнями є те, що в цій мережі працюють RFID мітки, розроблені компанією Waltonchain, тобто таке рішення досить вузькоспеціалізоване [21].

– IBM Watson. Блокчейн в хмарі: кінцевий IoT пристрій має підключитись за допомогою протоколу MQTT протоколу до хмари, де збираються дані, а потім оброблюються з використанням Hyperledger Fabric. Слабкою ланкою тут є централізоване підключення по MQTT, проте зменшуються інші безпекові ризики під час роботи з зібраними даними [22].

– IOTA реалізує архітектуру Tangle, що полягає в перевірці попередніх транзакцій з використанням напрямленого ациклічного графа. Це дозволяє спростити систему додавання нових блоків, проте якщо зловмисник заволодіє більше 30 % вузлів мережі, такий підхід буде вразливим, що виправляється впровадженням голосування в новій версії 2 [23].

– IoTeX проект характеризується використанням делегованого протоколу консенсусу Proof-of-Stake (DPoS), де до 50 делегатів голосують за додавання блока. Використовується система створення резервних точок (checkpoint), що дозволяє зберігати мінімум інформації на крихітному пристрої. Також присутня підтримка смарт-контрактів [24].

Серед розглянутих блокчейн-рішень IOTA дозволяє використати архітектуру Tangle на пристроях з обмеженими апаратними можливостями, починаючи з ESP32 [25]. IoTeX має клієнтську бібліотеку для малопотужних пристроїв, вона дозволяє підключатись до вузла IoTeX, що нагадує централізоване рішення. Розглянемо механізми запобігання атак в IoT за допомогою блокчейну (табл. 4).

Таблиця 4

Механізми запобігання атак в IoT за допомогою блокчейн

Назва атаки	Механізми блокчейну
Атаки маршрутизації (wormhole, Sybil, Grayhole / selective forwarding, blackhole, sinkhole, replay, spoofing, hello flood)	Децентралізація системи, де додавання нової інформації (створення нового блока або майнінг) контролюється консенсус-алгоритмами та структурою даних, коли нові дані неможливо додати без залежності від попередніх з надійним шифруванням [26]
RFID-атаки	Використання Waltonchain для захисту та динамічного оновлення інформації [21]
MITM та DoS-атаки	Використання приватного та публічного ключів. Лише у випадку компроментації приватного ключа можлива MITM атака. DoS-захист за рахунок децентралізації мережі
Спам-атаки (підроблені QR коди і тощо)	Вбудований цифровий підпис
Ботнет-атаки	Використання консенсус протоколів та прозора верифікація пакетів з цифровим підписом
Шкідливе ПЗ / додавання шкідливого вузла	Створення нових блоків вимагає певну комісію (gas), що не дасть зловмиснику створити нові блоки

Незважаючи на всі переваги блокчейну є й недоліки, такі як:

– зберігання даних — крихітні IoT-пристрої не мають можливості зберігати весь ланцюг даних. В такому випадку можна використати розподілену файлову систему IPFS [27].

– не всі IoT-пристрої мають достатню потужність для використання блокчейну або не всі при-

строї мають достатню потужність для складних алгоритмів цифрового підпису.

– масштабованість — що більша мережа, то складніше узгоджувати нові блоки. Ця проблема вирішується консенсус-алгоритмами, такими як DPoS або DAG.

Побудова гібридного варіанта організації безпеки мережі з використанням блокчейн

Враховуючи те, що є пристрої все ще недостатньо потужні для запуску на них повноцінного блокчейн-вузла, пропонується гібридний підхід. Щоб максимально відійти від централізованої точки комунікації крихітних IoT пристроїв та для максимального захисту всієї IoT інфраструктури пропонується створити багаторівневу схему блокчейн-мережі з поєднанням класичних методів на локальному рівні. Тож оптимальний варіант такої системи повинен бути менш вимогливим до апаратних ресурсів, зберігаючи при цьому достатній рівень шифрування, бути децентралізованим, масштабованим, а також гнучким до налаштувань та керування окремими вузлами.

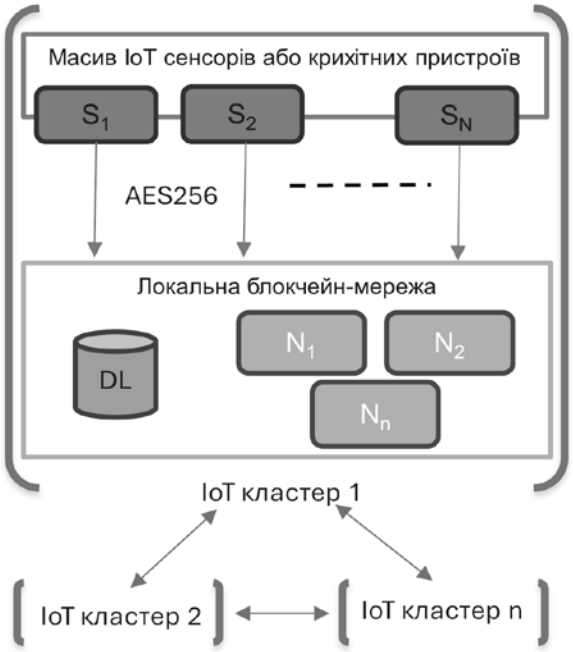

Рис. 2. Гібридна структура безпечної IoT мережі

На рис. 2 показано поділ на рівні елементи та їхню взаємодію в такій системі.

Розглянемо її роботу детальніше. Згідно з [28], пропонується побудувати безпековий механізм, що називається Blockchain Dynamic Table (далі BDT) з шифруванням AES, що запускається на енергоефективному мікроконтроллері з 16 МГц та 8 Кб оперативної пам'яті. Використавши оптимізований консенсус протокол з [29] та поєднавши його зі згортками даних (Zk-Rollup) з [30], створюється відтермінована система передачі даних з підтримкою смарт-контрактів для розв'язання конкретних задач на рівні мережі, що унеможливнює потенційні атаки на центральний вузол (оскільки його немає) та підміну пристроїв.

Перший рівень є сукупністю різноманітних сенсорів та виконавчих пристроїв з контролерами малої потужності, але які підключені за будь-яким протоколом з табл. 2. Як додаткове шифрування і додатковий захист для захисту самого протоколу (або за відсутності шифрованого каналу в якості захисту) комунікації додається BDT. Другий рівень пристроїв (блокчейн-вузли) обмінюються з сенсорами ключами AES, використовуючи асиметричне шифрування. Подальша комунікація зашифрована.

Другий рівень може виконувати смарт-контракти, куди можна прописати різноманітні безпекові механізми та загалом правила роботи системи. Перший та другий рівні є IoT кластерами — набором пристроїв, які входять в одну зону. До того ж, кожна зона може мати свої правила роботи, зони мають розподілене зберігання даних (distributed ledger, DL), що можна зв'язати за потреби з IPFS з [27].

Кожен IoT кластер може обмінюватись даними з іншими кластерами або хмарним блокчейном в ролі IoT кластера. Транзакції можуть бути узагальнені або комбіновані безпечним шляхом за допомогою підходу Zk-Rollups. Більше того, це ще й додатковий retry-механізм, що дозволяє накопичувати дані за необхідності, а згодом відправляти одним пакетом.

Хмарний блокчейн може вважатися третім рівнем і така система може також розглядатися як альтернатива туманним обчисленням (fog computing), оскільки кожний кластер є окремою системою пристроїв. Завдяки підтримці смарт-контрактів можна налаштовувати також міжкластерну взаємодію, щоб, наприклад, сенсор в кластері 1 зміг повпливати на виконавчий пристрій в кластері 2.

Переваги запропонованого рішення

З порівняння запропонованої системи з раніше розглянутими, випливає, що це рішення:

– не зав'язане на хмарну інфраструктуру (як IBM Watson), хоча вона може бути одним з рівнів;

– шифрування кінцевих пристроїв в доповнення до наявних стандартів унеможливлює підміну вузла або зчитування даних зловмисником (для порівняння IOTA не підтримується менш потуж-

ними пристроями, ніж рівень ESP32, а інші рішення покладаються на стандартні протоколи типу MQTT);

– дані між IoT кластерами можуть бути стиснутішими або трансформованими на місці з використанням смарт-контрактів та енергоефективного консенсус-алгоритму dPoS (ралізовано в IoTeX в повноцінних вузлах мережі);

– другий рівень може використовувати для реалізації підходи IOTA або IoTeX;

– цей підхід вирішує всі основні задачі безпеки та дозволяє безпечно масштабувати систему на більшій кількості пристроїв, ніж в наявних рішеннях, усунувши вразливості, проаналізовані раніше;

– цей підхід дозволяє перенести частину логіки роботи мережі IoT пристроїв на локальний рівень та раціонально використати ресурси, використавши перевірені безпекові рішення та взявши найкраще з погляду авторів у наявних підходах;

– практичне застосування є універсальним і може бути використаним, до прикладу, для організації роботи систем розумного міста, розумних будинків, систем сигналізації, різноманітних сенсорних систем тощо, де існують безпекові ризики та/або обчислювальна потужність обладнання, що не дозволяє використати інші рішення.

Аналіз інтеграції кінцевих IoT-пристроїв в блокчейн-мережу

Оскільки розгортання блокчейн мережі на звичайних комп'ютерних вузлах досить стандартизована задача, розглянемо лише практичну реалізацію запропонованої схеми на рис. 2 та бібліотек від наявних проектів на кінцевих пристроях. Основа блокчейну — криптографія, тому є сенс розглянути та проаналізувати наявні криптографічні бібліотеки та їхню роботу на крихітних пристроях.

Натепер великою популярністю користується проект MbedTLS [31] — бібліотека для реалізації різноманітного шифрування, розрахунку хеш-сум, цифрового підпису та протоколу DTLS. В сучасних мікроконтролерах ARM використовуються апаратні рішення для шифрування та хешування, тому навантаження на основний обчислювальний ресурс мінімальний.

Щодо інших мікроконтролерів, наприклад, таких як ATmega328P, наявність апаратного рішення для шифрування може бути відсутнє, а враховуючи невеликий запас апаратних ресурсів, необхідно максимально ефективно його використати. Тут використовується максимально оптимізована криптографія, з такими бібліотеками як tinyECC [32] та protectedAES [33]. Окрім окремих розробок, наявна бібліотека Crypto [34], яка поєднує в собі розробки для крихітних пристроїв, а також PSACrypto [35] від компанії IOTEX. Обидві бібліотеки пропонують асиметричне та симетричне шифрування, а також розрахунок хешів.

Скопмілювавши просту програму, яка шифрує за допомогою еліптичних кривих, а потім за допомогою AES256, розглянемо використання пам'яті в найпростішому мікроконтролері ATmega328P (табл. 5).

Таблиця 5

Порівняння використання ресурсів бібліотеками шифрування в мікроконтролері ATmega328P

Бібліотека	Використано ПЗУ, байт	Використано ОЗУ, байт
tinyECC + protectedAES	13984	419
PSACrypto	19296	1940
Crypto	15906	1449
MbedTLS	Не сумісна	

Для найменших контролерів найкращий варіант захисту — це використання оптимізованих бібліотек tinyECC та protectedAES, причому споживаний обсяг оперативної пам'яті мінімальний, що дозволяє інтегрувати підхід з періодичною зміною ключа шифрування практично в будь-який пристрій.

Бібліотека MbedTLS, PSACrypto, а також бібліотеки, що реалізують блокчейн-клієнти та перетворюють пристрій у частину більшої мережі (другий рівень на рис. 2) офіційно підтримують такі проекти як ESP32 [36], що по суті є енергоефективними Bluetooth + WiFi модулями з мікроконтролером до 240 МГц, 515 Кб оперативної пам'яті та до 8 Мбайт флеш-пам'яті. Це дозволяє безперешкодно робити високоефективний хаб для менш потужних пристроїв, комбінувати дані та відправляти їх в блокчейн-мережу.

Також з проектом web3-arduino [37] є підтримка Ethereum мереж на крихітних пристроях, що дозволяє не обмежуватись спеціалізованими проектами, такими як IOTA або IOTEX та розгортати власну локальну мережу для керування та організації безпеки підключених IoT пристроїв.

Висновки

Питання безпеки пристроїв IoT має вирішуватись комплексно. В результаті аналізу поточних викликів безпеки IoT-мереж та їхніх варіантів побудови універсального рішення не знайдено, оскільки конкретне рішення повинно виходити з можливостей пристроїв. Блокчейн дає додаткові переваги в організації та безпеці інформації IoT пристроїв та й мережі загалом.

Поєднання блокчейну та IoT дозволяє успішно вирішувати питання безпеки пристроїв, проте не завжди малопотужні пристрої можуть бути учасниками блокчейн-мережі через апаратні обмеження. Запропонована структура IoT мережі пропонує використання гібридного підходу до створення масштабованої IoT-мережі з акцентом на безпеку. Таке рішення поліпшує наявні підходи використання блокчейну в IoT шляхом введення додаткового шифрування та комбінації декількох блокчейн- мереж.

Розглянуті бібліотеки шифрування для крихітних пристроїв дозволяють розгорнути базовий функціонал для інтеграції у блокчейн-мережу. Отже, підхід з використанням блокчейну дозволяє комплексно вирішувати проблеми безпеки, масштабованості та обробки даних та є потужною альтернативою SDN.

Стаття буде корисною науковцям та розробникам, які працюють над впровадженням блокчейн-фреймворків та рішень в мережах IoT.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] *Towards a definition of the Internet of Things (IoT).* [Electronic resource]. Available: https://iot.ieee.org/definition.html. Accessed: 01.03.2024.

[2] *Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025[Electronic resource]. Available:* https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/ . Accessed: 01.03.2024.

[3] *Вразливості MQTT. База CVE*. [Електронний ресурс]. Режим доступу: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=MQTT . Дата звернення: 01.03.2024.

[4] Z. Alansari, N. B. Anuar, A. Kamsin, and M. R. Belgaum, “A systematic review of routing attacks detection in wireless sensor networks,” *PeerJ. Computer Science*, vol. 8, p. e1135, Oct. 2022, https://doi.org/10.7717/peerj-cs.1135 .

[5] M. A. Qureshi and A. Munir, “PUF-IPA: A PUF-based Identity Preserving Protocol for Internet of Things Authentication,” *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2020, pp. 1-7, https://doi.org/10.1109/CCNC46108.2020.9045264 .

[6] N. Hussein, and A. Nhlabatsi, “Living in the Dark: MQTT-Based exploitation of IoT security vulnerabilities in ZigBee networks for smart lighting control,” *IoT*, vol. 3, no. 4, pp. 450-472, Nov. 2022, https://doi.org/10.3390/iot3040024 .

[7] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, “A review on the security of the Internet of Things: Challenges and Solutions,” *Wireless Personal Communications*, vol. 119, no. 3, pp. 2603-2637, Mar. 2021, https://doi.org/10.1007/s11277-021-08348-9 .

[8] S. N. T. Vu, M. Stege, P. I. El-Habr, J. Bang, and N. Dragoni, “A survey on Botnets: Incentives, evolution, detection and current trends,” *Future Internet*, vol. 13, no. 8, p. 198, Jul. 2021, https://doi.org/10.3390/fi13080198 .

[9] L. Jong Hyup, “Collective attestation for manageable IoT environments,” *Applied Sciences*, vol. 8, no. 12, pp. 2652, Dec. 2018, https://doi.org/10.3390/app8122652 .

[10] M. Hossain, G. Kayas, R. Hasan, A. Skjellum, S. Noor, and S. M. R. Islam, “A Holistic analysis of Internet of Things (IoT) security: principles, practices, and new perspectives,” *Future Internet*, vol. 16, no. 2, p. 40, Jan. 2024, https://doi.org/10.3390/fi16020040 .

[11] M. M. Ogonji, G. Okeyo, and J. M. Wafula, “A survey on privacy and security of Internet of Things,” Computer Science Review, vol. 38, p. 100312, Nov. 2020, https://doi.org/10.1016/j.cosrev.2020.100312 .

[12] *Використання TLS на ESP32*. [Електронний ресурс]. Режим доступу: https://docs.espressif.com/projects/esp-idf/en/stable/esp32/api-reference/protocols/esp_tls.html#comparison-between-mbedtls-and-wolfssl . Дата звернення: 10.04.2024.

[13] *Zigbee Technology Security: Examination and Possible Solutions*. [Electronic resource]. Available: https://embeddedcomputing.com/technology/security/network-security/zigbee-technology-security-examination-and-possible-solutions . Accessed: 11.04.2024.

[14] *Maximizing security in ZigBee networks.* [Electronic resource]. Available: https://www.nxp.com/docs/en/supporting-information/MAXSECZBNETART.pdf . Accessed: 11.04.2024.

[15] F. F. Ashrif, E. A. Sundararajan, R. Ahmad, M. K. Hasan, and E. Yadegaridehkordi, “Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction,” *Journal of Network and Computer Applications*, vol. 221, pp. 103759, Jan. 2024, https://doi.org/10.1016/j.jnca.2023.103759 .

[16] *Bluetooth Core Specification Version 5.4*. [Electronic resource]. Available: https://www.bluetooth.com/wp-content/uploads/2023/02/2301_5.4_Tech_Overview_FINAL.pdf . Accessed: 11.04.2024.

[17] A. Alomari, and S. A. P. Kumar, “Securing IoT systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions,” *Internet of Things*, vol. 25, pp. 101132, Apr. 2024, https://doi.org/10.1016/j.iot.2024.101132 .

[18] M. A. Al-Shareeda, A. A. Alsadhan, H. H. Qasim, and S. Manickam, “The fog computing for internet of things: review, characteristics and challenges, and open issues,” *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 2, pp. 1080-1089, Apr. 2024, https://doi.org/10.11591/eei.v13i2.5555 .

[19] E. Shahri, P. Pedreiras, and L. Almeida, “A scalable Real-Time SDN-Based MQTT framework for industrial applications,” *IEEE Open Journal of the Industrial Electronics Society*, pp. 1-22, Jan. 2024, https://doi.org/10.1109/ojies.2024.3373232 .

[20] S. Latif, Z. Idrees, Z. E. Huma, and J. Ahmad, “Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, Jul. 2021, https://doi.org/10.1002/ett.4337 .

[21] Waltonchain white paper [Electronic resource]. Available: https://github.com/WaltonChain/WhitePaper/blob/master/Waltonchain%20White%20Paper%202.0_EN.pdf . Accessed: 01.04.2024.

[22] IBM IoT Blockchain [Електронний ресурс]. Режим доступу: https://www.ibm.com/topics/blockchain-iot . Дата звернення: 01.04.2024.

[23] S. Müller, A. Penzkofer, N. Polyanskii, J. Theis, W. Sanders, and H. Moog, “Tangle 2.0 Leaderless Nakamoto consensus on the heaviest DAG,” IEEE Access, vol. 10, pp. 105807–105842, Jan. 2022, https://doi.org/10.1109/access.2022.3211422.

[24] *IoTeX whitepaper*. [Electronic resource]. Available: https://whitepaper.io/document/131/iotex-whitepaper . Accessed: 06.04.2024.

[25] *Використання IOTA на ESP32.* [Електронний ресурс]. Режим доступу: https://github.com/iotaledger/esp32-client-sdk . Дата звернення: 05.04.2024.

[26] A. Pieroni, N. Scarpato, and L. Felli, “Blockchain and IoT Convergence — A systematic survey on technologies, protocols and security,” *Applied Sciences*, vol. 10, no. 19, p. 6749, Sep. 2020, Accessed: 10.3390/app10196749.

[27] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic, and M. Omar, “Trustworthy IoT data streaming using blockchain and IPFS,” *IEEE Access*, vol. 10, pp. 17707-17721, Jan. 2022, https://doi.org/10.1109/access.2022.3149312 .

[28] S. S. Hameedi, and O. Bayat, “Improving IoT data security and integrity using lightweight blockchain dynamic table,” Applied Sciences, vol. 12, no. 18, p. 9377, Sep. 2022, https://doi.org/10.3390/app12189377 .

[29] S. Wadhwa, S. Rani, Kavita, S. Verma, J. Shafi, and M. Wozniak, “Energy Efficient Consensus Approach of Blockchain for IoT Networks with Edge Computing,” Sensors, vol. 22, no. 10, p. 3733, May 2022, https://doi.org/10.3390/s22103733.

[30] T. Lavaur, J. Lacan, and C. P. C. Chanel, “Enabling Blockchain Services for IoE with Zk-Rollups,” *Sensors*, vol. 22, no. 17, p. 6493, Aug. 2022, https://doi.org/10.3390/s22176493 .

[31] *Проект MbedTLS.* [Електронний ресурс]. Режим доступу: https://github.com/Mbed-TLS/mbedtls . Дата звернення: 10.04.2024.

[32] *Проект TinyECC*. [Електронний ресурс]. Режим доступу: https://github.com/ShubhamAnnigeri/tinyECC-ArduinoIDE/tree/main . Дата звернення: 10.04.2024.

[33] *Проект ProtectedAES.* [Електронний ресурс]. Режим доступу: https://github.com/RaffaeleMorganti/protectedAES . Дата звернення: 10.04.2024.

[34] *Проект Arduino Crypto*. [Електронний ресурс]. Режим доступу: https://rweather.github.io/arduinolibs/crypto.html . Дата звернення: 10.04.2024.

[35] *Проект PSA Crypto*. [Електронний ресурс]. Режим доступу: https://github.com/machinefi/psa-crypto-arduino . Дата звернення: 10.04.2024.

[36] *Проект ESP32*. [Електронний ресурс]. Режим доступу: https://www.espressif.com/en/products/socs/esp32 . Дата звернення: 10.04.2024.

[37] *Проект WEB3-Arduino*. [Електронний ресурс]. Режим доступу: https://github.com/kopanitsa/web3-arduino . Дата звернення: 10.04.2024.

Рекомендована кафедрою комп’ютеризованих електромеханічних систем і комплексів ВНТУ

Стаття надійшла до редакції 17.07.2024

Чепель Леонід Валерійович — аспірант кафедри комп’ютерної інженерії, email: leonid.chepel@knu.ua ;

Бойко Юрій Володимирович — канд. фіз.-мат. наук, доцент, завідувач кафедри комп’ютерної інженерії, email: yuriyboyko@knu.ua .

Київський національний університет імені Тараса Шевченка, Київ

L. V. Chepel[1]
Yu. V. Boyko[1]

Approach to the Security and Organization of IoT Networks Using Blockchain Technology

[1]Taras Shevchenko National University of Kyiv

The rapid development of the Internet of Things (IoT) lacks a universal security mechanism for devices due to their diversity and hardware limitations. However, employing distributed networks, additional encryption, limiting unused data transmission channels, implementing collective device certification, using digital signatures, and filtering data packets can secure devices against classical attack scenarios.

The paper examines the challenges and potential attacks on the security of IoT devices. For optimal security control in traditional networks, the use of software-controlled networks is recommended. Usage of fog computing reduces the risks associated with a central node, but other security risks remain. More comprehensive solution involves integrating blockchain with IoT devices. The paper reviews several existing systems that offer more comprehensive security but still have certain shortcomings, which the authors attempt to address in the proposed model.

The proposed IoT network model using blockchain consists of multiple layers - a sensor and low-power device layer and a local blockchain network layer, which are combined into a cluster. Communication between layers is ensured by symmetric and asymmetric encryption, and the network operation rules can be regulated by smart contracts. Additionally, there is interaction between clusters, making the system scalable, decentralized, and secure.

Keywords: IoT networks, blockchain, decentralized networks, information protection, security, building IoT networks.

Chepel Leonid V. — Post-Graduate Student the Chair of Computer Engineering, e-mail: leonid.chepel@knu.ua ;
Boyko Yuriy V. — Cand. Sc. (Eng.), Associate Professor, Head of the Chair of Computer Engineering, e-mail: yuriyboyko@knu.ua