DOI: https://doi.org/10.36910/6775-2524-0560-2024-55-24
УДК 681.3.05:004.056
Розломій Інна Олександрівна[1], к.т.н., доцент
https://orcid.org/0000-0001-5065-9004
Симонюк Володимир Павлович[2], к.т.н., доцент
https://orcid.org/0000-0002-7624-4760
Науменко Сергій Васильовичм[1], аспірант
https://orcid.org/0000-0002-6337-1605
Михайловський Павло Васильович[1], аспірант
https://orcid.org/0009-0008-4324-1724
[1]Черкаський національний університет імені Богдана Хмельницького, м. Черкаси, Україна
[2]Луцький національний технічний університет, м. Луцьк, Україна

МОДЕЛЬ БЕЗПЕКИ ВЗАЄМОПОВ'ЯЗАНИХ ОБЧИСЛЮВАЛЬНИХ ПРИСТРОЇВ НА ОСНОВІ ПОЛЕГШЕНОЇ СХЕМИ ШИФРУВАННЯ ДЛЯ IoT

Розломій І.О., Симонюк В.П., Науменко С.В., Михайловський П.В. Модель безпеки взаємоповязаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT. У сучасному світі число пристроїв, підключених до інтернету речей (IoT), стрімко зростає, що породжує нові виклики у сфері забезпечення їхньої безпеки. Стаття присвячена розробці моделі безпеки для IoT пристроїв, яка враховує обмежені обчислювальні ресурси і мінімальне енергоспоживання, необхідні для ефективного функціонування криптографічних алгоритмів. Проблема полягає у відсутності універсальних полегшених криптографічних рішень, здатних забезпечити надійний захист в умовах IoT без значного збільшення витрат енергії чи обчислювальних ресурсів. У статті представлено аналіз сучасних досліджень та публікацій у цій сфері, зокрема, розглянуто новітні розробки в галузі полегшеної криптографії, що оптимізовані для IoT пристроїв. Особлива увага приділена легким криптографічним алгоритмам, які можуть забезпечити високу безпеку при мінімальному використанні ресурсів, таких як енергія та обчислювальна потужність. Запропонована модель включає як апаратні, так і програмні рішення для шифрування та управління ключами, з метою мінімізації ризиків компрометації даних. Досліджуються методи оцінки ефективності засобів захисту та моделі врахування обмежень ресурсів. У статті також розглядаються перспективи використання квантово-стійких криптографічних протоколів, які можуть стати основою для майбутніх стандартів безпеки IoT. Висновки підкреслюють важливість постійного вдосконалення захисних механізмів для підвищення рівня безпеки IoT технологій, що сприятиме зростанню довіри користувачів до цих систем і забезпечить надійний захист даних у глобальних мережах. Розробка та імплементація таких полегшених криптографічних рішень є критично важливими для захисту даних і забезпечення стабільної роботи IoT екосистем в умовах сучасних кіберзагроз.
Ключові слова: Інтернет речей, полегшена криптографія, шифрування, апаратні шифратори, криптографічні бібліотеки, керування ключами, обмеження ресурсів.

Rozlomii I., Symonyuk V., Naumenko S., Mykhailovskyi P. The security model of interconnected computing devices based on a lightweight encryption scheme for IoT. Today world, the number of devices connected to the Internet of Things (IoT) is growing rapidly, which creates new challenges in the field of ensuring their security. The article is devoted to the development of a security model for IoT devices, which takes into account the limited computing resources and minimal energy consumption necessary for the effective functioning of cryptographic algorithms. The problem is the lack of universal lightweight cryptographic solutions capable of providing reliable protection in the IoT environment without a significant increase in energy consumption or computing resources. The article presents an analysis of modern research and publications in this field, in particular, the latest developments in the field of lightweight cryptography optimized for IoT devices are considered. Special attention is paid to lightweight cryptographic algorithms that can provide high security with minimal use of resources such as energy and computing power. The proposed model includes both hardware and software solutions for encryption and key management in order to minimize the risks of data compromise. The methods of assessing the effectiveness of protective measures and the models for taking into account resource limitations are being studied. The article also discusses the prospects for using quantum-resistant cryptographic protocols that could become the basis for future IoT security standards. The conclusions emphasize the importance of continuous improvement of protective mechanisms to increase the level of security of IoT technologies, which will contribute to the growth of user trust in these systems and ensure reliable protection of data in global networks. The development and implementation of such lightweight cryptographic solutions are critical for protecting data and ensuring the stable operation of IoT ecosystems in the face of modern cyber threats.
Key words: Internet of Things, lightweight cryptography, encryption, hardware ciphers, cryptographic libraries, key management, resource limitations.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. З розвитком інтернету речей (IoT) постійно збільшується кількість пристроїв, які взаємодіють між собою через глобальні мережі. В кінці 2023 року кількість таких пристроїв перевищила 30 мільярдів, що в два рази більше, ніж п'ять років тому. Прогнози показують, що ця кількість може досягти 50 мільярдів до 2025 року, рисунок 1 [1]. Однак, стрімкий розвиток IoT

також призводить до збільшення кількості загроз безпеці цих пристроїв. До таких загроз належать витоки даних, несанкціоноване втручання та атаки на конфіденційність даних користувачів [2].

В умовах, коли кіберзлочинці вдосконалюють свої методи атак на системи IoT, наукові та практичні спільноти стикаються з нагальною потребою розробки ефективних, але при цьому ресурсно ощадних методів шифрування [3]. Багато існуючих рішень у сфері криптографії не враховують специфіку пристроїв IoT, які характеризуються обмеженими обчислювальними потужностями, малим розміром пам'яті та низьким енергоспоживанням.

Рис. 1. Графік зростання кількості IoT-пристроїв

Проблема полягає у відсутності універсальних легких криптографічних рішень, які здатні забезпечити надійний захист в обмежених умовах IoT без значного збільшення витрат енергії чи обчислювальних ресурсів. Це вимагає розробки нових алгоритмів шифрування та методів управління ключами, оптимізованих для масштабів IoT. Науковий та практичний інтерес до цієї проблеми обумовлений глобальною потребою в стандартизації та імплементації таких рішень на законодавчому рівні, що включає забезпечення відповідності міжнародним нормам та регуляціям у сфері захисту даних та конфіденційності. Вирішення цієї проблеми не лише посилить захист приватності та даних кінцевих користувачів, але й сприятиме подальшому розвитку та інтеграції IoT технологій у повсякденне життя. Отже, пошук рішень для цієї проблеми має важливе значення як з наукової, так і з практичної точки зору.

Актуальність дослідження зумовлена кількома ключовими факторами. Зростання кількості IoT-пристроїв, які є частиною критично важливих систем, таких як системи охорони здоров'я, інтелектуальні транспортні системи та промислове обладнання, вимагає високого рівня безпеки через їхній вплив на безпеку та добробут людей. Законодавчі та нормативні вимоги щодо захисту даних, встановлені регуляторними органами, такими як Європейський Союз із своїм Загальним регламентом про захист даних (GDPR), а також іншими міжнародними організаціями, посилюють необхідність розробки відповідних криптографічних технологій [4]. Збільшення різноманітності та складності кібератак змушує зловмисників шукати нові способи обходу традиційних захисних механізмів, що вимагає більш вдосконалених рішень для шифрування та аутентифікації.

Наукове співтовариство та індустрія також виявляють зростаючий інтерес до розвитку стійких до квантових обчислень криптографічних рішень, оскільки квантові технології можуть згодом зламати багато сучасних систем шифрування [5]. Адаптація легких криптографічних методів, що забезпечують захист від потенційних квантових загроз, стає критично важливою.

Всі ці фактори разом з нагальною потребою в ефективному, але ресурсно невимогливому шифруванні для забезпечення безпеки величезного масиву IoT-пристроїв роблять дане дослідження надзвичайно актуальним та важливим як з наукової, так і з практичної точки зору. Розробка та імплементація нових легких криптографічних рішень може суттєво зміцнити захист в IoT екосистемах, підвищити довіру користувачів і стимулювати подальший розвиток інтелектуальних технологій.

Аналіз останніх досліджень та публікацій. Сфера криптографічного захисту IoT набуває все

більшої актуальності, а зростаючий інтерес дослідників та розробників призводить до появи значної кількості наукових робіт, спрямованих на вдосконалення методів шифрування, які би задовольняли вимоги до пристроїв IoT [6]. Основна увага в сучасних дослідженнях приділяється розробці так званих «легких» криптографічних алгоритмів, що оптимізовані для обмеженого обчислювального потенціалу та мінімального енергоспоживання [7].

Одним з найважливіших напрямків у цьому контексті є робота [8], де представлено новий алгоритм шифрування, базований на структурі Feistel Network. Алгоритм показав високу стійкість до атак з відкритим текстом і при цьому демонструє значно нижчі вимоги до обчислювальних ресурсів порівняно з традиційними методами.

Варто також виділити дослідження Mahmood та співавторів, в якому представлено метод дворівневого шифрування, що інтегрує асиметричне шифрування для управління ключами і симетричне шифрування для передачі даних [9]. Цей підхід не тільки забезпечує високу безпеку, але й оптимізує процес використання енергії пристроєм.

Значну увагу привертає дослідження в області квантово-стійкого шифрування, яке є відповіддю на потенційні майбутні загрози квантових обчислень [10]. Робота демонструє новітній підхід до створення квантово-стійких криптографічних протоколів, які можуть бути ефективно імплементовані на IoT пристроях.

З огляду на зростаючі вимоги до безпеки даних в IoT, вчені також акцентують увагу на розробці універсальних рішень для управління ключами. Важливим напрямком є дослідження, які спрямовані на інтеграцію блокчейн технологій для децентралізованого управління криптографічними ключами в мережах IoT [11].

Ці дослідження є важливими кроками в розробці криптографічних рішень, які можуть ефективно функціонувати в умовах обмежених ресурсів, що є характерним для IoT пристроїв, і при цьому забезпечувати високий рівень безпеки і захисту даних.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Пристрої IoT широко використовуються в різних сферах, від побутових приладів до медичних пристроїв та інфраструктурних систем. Однак, через обмежені ресурси таких пристроїв, вони часто мають слабкі місця в системах захисту, що робить їх вразливими до різноманітних кібератак. Важливість забезпечення надійного захисту даних та безперебійної роботи цих пристроїв не можна переоцінити, оскільки порушення їх безпеки може мати серйозні наслідки для користувачів та організацій.

У взаємопов'язаних обчислювальних пристроях, зокрема в IoT, існують загрози безпеці, які можуть негативно вплинути на функціонування та цілісність системи, табл. 1.

Таблиця 1. Загрози безпеці пристроїв IoT

Загроза	**Опис**	**Наслідки**
Неавторизований доступ	Несанкціоноване проникнення у систему або пристрої	Крадіжка даних, маніпуляції пристроями
Атаки типу DoS	Спроба зробити систему або пристрій недоступними шляхом перенавантаження ресурсів	Недоступність системи, зупинка роботи
Атаки на конфіденційність	Перехоплення та використання чутливих даних	Витік конфіденційної інформації
Атаки на цілісність даних	Модифікація даних, що передаються між пристроями	Неправильні рішення або дії системи
Атаки на доступність	Спрямовані на порушення безперервної роботи пристроїв	Порушення функціонування системи
Зловмисне програмне забезпечення (Malware)	Впровадження шкідливих програм з метою крадіжки даних або порушення роботи пристроїв	Використання у ботнет-атаках, крадіжка інформації

У зв'язку з численними загрозами, які постають перед пристроями IoT, важливо забезпечити

надійний захист даних і безперебійне функціонування цих пристроїв. Основна увага приділяється розробці ефективних засобів захисту, які можуть протистояти кібератакам, зокрема неавторизованому доступу, атакам типу DoS, та іншим видам зловмисних дій [12]. Одним з таких засобів є полегшена криптографія, яка спеціально розроблена для пристроїв з обмеженими ресурсами. Обмеження обчислювальних можливостей пристроїв IoT вимагає пошуку ресурсоощадних засобів захисту інформації. Одним з таких є полегшена криптографія. Вона характеризується низьким споживанням енергії, невеликою пам'яттю та обчислювальними вимогами, що дозволяє застосовувати її в умовах обмежених апаратних можливостей.

Полегшена криптографія є важливим напрямом у галузі інформаційної безпеки, спрямованим на забезпечення захисту даних в умовах обмежених обчислювальних ресурсів, таких як енергія, пам'ять і обчислювальна потужність. Традиційні криптографічні алгоритми, такі як AES, потребують значних ресурсів, що робить їх непридатними для використання в багатьох пристроях IoT.

Полегшена криптографія базується на таких принципах:

1. Ефективність. Алгоритми повинні бути достатньо швидкими і не споживати багато енергії. Це дозволяє пристроям IoT працювати довше без заміни батарей або зарядки.
2. Мінімальне використання пам'яті. Алгоритми повинні вимагати мінімум оперативної пам'яті (RAM) для обробки даних, що особливо важливо для пристроїв з обмеженим об'ємом RAM.
3. Безпека. Незважаючи на свою «легкість», алгоритми повинні забезпечувати достатній рівень захисту даних від різних видів атак.

Захист пов'язаних пристроїв IoT на рівні мікроконтролерів можна забезпечити шляхом використання криптографічних бібліотек, які інтегровані у програмне забезпечення мікроконтролерів, або за допомогою апаратних шифраторів, якщо мікроконтролер має вбудований апаратний модуль для шифрування. Розглянемо детальніше захист інформації за допомогою використання бібліотек та апаратних шифраторів.

Криптографічні бібліотеки забезпечують програмну реалізацію полегшених криптографічних алгоритмів. Вони можуть бути інтегровані у програмне забезпечення мікроконтролерів для забезпечення шифрування та розшифрування даних. Це дозволяє пристроям IoT використовувати ефективні методи захисту інформації, не перевантажуючи обчислювальні ресурси. До популярних бібліотек належать [13]:

1. TinyCrypt – легка криптографічна бібліотека, розроблена для IoT пристроїв, що забезпечує базові криптографічні операції з мінімальним використанням ресурсів. Вона підтримує такі функції, як блокове шифрування, хешування та генерування ключів.
2. WolfSSL відома своєю високою продуктивністю та низькими вимогами до пам'яті. Ця бібліотека підтримує різні полегшені шифри та протоколи, що робить її ідеальною для IoT пристроїв. Вона включає такі функції, як SSL/TLS протоколи, а також підтримку алгоритмів, таких як RSA, ECC (еліптичні криві) та AES.
3. mbed TLS – легка криптографічна бібліотека з відкритим кодом, яка забезпечує широкий набір криптографічних примітивів і протоколів для IoT пристроїв. Вона підтримує різні алгоритми шифрування, аутентифікації та хешування.

Інтеграція криптографічної бібліотеки у програмне забезпечення мікроконтролера здійснюється на рівні прикладної програми та проміжного програмного шару (middleware). Спочатку бібліотека додається до проекту та ініціалізується у коді програми. Потім вона використовується для виконання криптографічних операцій, таких як шифрування, розшифрування та хешування даних. Це забезпечує захист інформації на рівні програмного забезпечення мікроконтролера. У контексті забезпечення безпеки IoT пристроїв важливо розглядати різні рівні, на яких можуть бути реалізовані захисні механізми. На рисунку 2 представлена схема основних шарів, починаючи від фізичного рівня IoT пристрою до апаратних і програмних рішень, які забезпечують криптографічний захист.

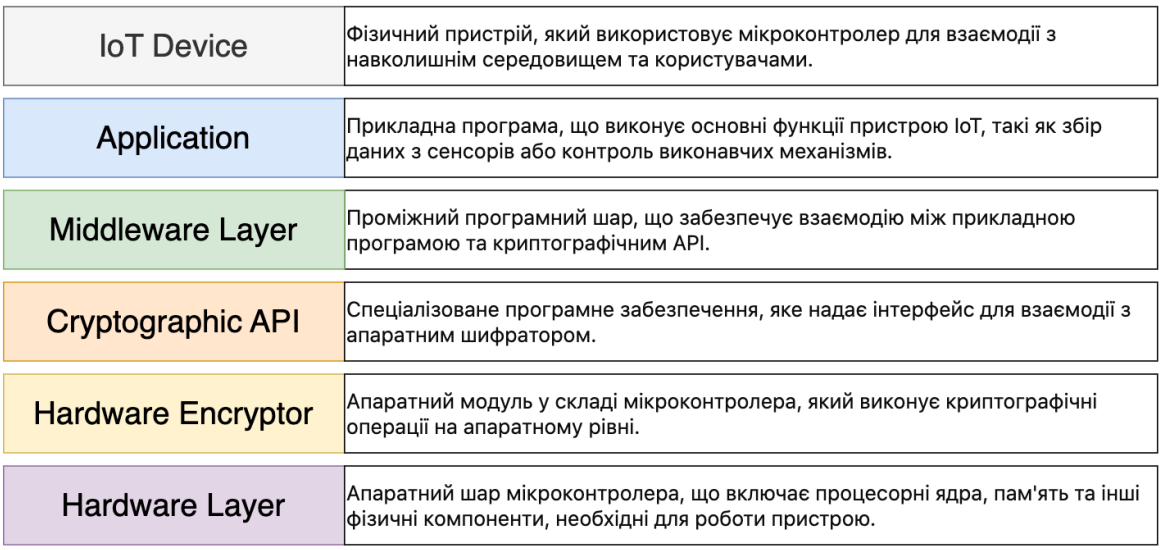

Рис. 2. Схема основних шарів IoT-системи

Більшість сучасних мікроконтролерів мають вбудовані апаратні шифратори, що забезпечують ефективне виконання криптографічних операцій. Ці апаратні модулі дозволяють швидко і з низьким енергоспоживанням виконувати шифрування, розшифрування та інші криптографічні завдання, не навантажуючи основний процесор мікроконтролера. Використання апаратних шифраторів значно підвищує продуктивність і безпеку IoT пристроїв. Апаратні шифратори інтегровані безпосередньо у мікроконтролер і можуть бути використані через спеціальні API, що надаються виробниками мікроконтролерів. Це забезпечує доступ до апаратних криптографічних модулів без необхідності реалізовувати складні криптографічні алгоритми на програмному рівні.

Мікроконтролери з вбудованими апаратними шифраторами, такі як STM32F429, ESP32, NXP LPC55S69, Nordic nRF52840 та Renesas RA6M3, підтримують різні алгоритми шифрування, включаючи AES, SHA-256, RSA та ECC. Ці мікроконтролери інтегрують спеціалізовані криптографічні блоки, які виконують шифрування та розшифрування даних на апаратному рівні, що значно знижує навантаження на основний процесор [14].

Криптографічні бібліотеки забезпечують програмну реалізацію криптографічних алгоритмів і можуть бути інтегровані у програмне забезпечення мікроконтролерів. Апаратні шифратори вбудовані безпосередньо у мікроконтролери і виконують криптографічні операції на апаратному рівні [15]. Це дозволяє значно підвищити продуктивність та знизити енергоспоживання.

Апаратне шифрування на мікроконтролерах має суттєві переваги перед програмним шифруванням за допомогою криптографічних бібліотек, особливо в контексті IoT пристроїв, де важливими є продуктивність, енергоефективність та безпека. Хоча обидва підходи мають свої переваги та недоліки, апаратні шифратори часто забезпечують кращу продуктивність і безпеку завдяки спеціалізованим модулям, які оптимізовані для виконання криптографічних операцій. В таблиці 2 представлено порівняння шифрування з використанням криптографічних бібліотек та апаратних шифраторів.

Вибір між криптографічними бібліотеками та апаратними шифраторами залежить від конкретних вимог до продуктивності, енергоефективності, гнучкості та безпеки IoT пристрою. Криптографічні бібліотеки пропонують велику гнучкість та низьку вартість впровадження, що робить їх привабливими для менш вимогливих застосувань. Водночас апаратні шифратори забезпечують високу продуктивність, енергоефективність та безпеку, що є критичним для багатьох застосувань IoT, особливо там, де потрібна висока швидкість обробки даних і низьке енергоспоживання.

Таблиця 2. Порівняння

Параметр	**Криптографічні бібліотеки**	**Апаратні шифратори**
Продуктивність	Помірна, залежить від потужності мікроконтролера	Висока, завдяки спеціалізованому обладнанню
Енергоефективність	Відносно високе споживання енергії	Низьке споживання енергії
Гнучкість	Висока, легко оновлюється та змінюється	Низька, важко змінювати алгоритми
Вартість	Низька, не потребує додаткового обладнання	Вища початкова вартість обладнання
Впровадження	Швидке, за рахунок програмного інтегрування	Складніше, потребує спеціалізованого апаратного забезпечення
Безпека	Залежить від реалізації та безпеки ПЗ	Висока, ключі та дані зберігаються у спеціалізованих модулях

Для побудови математичної моделі безпеки взаємопов'язаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT, розглянемо основні компоненти та операції, які включаються до такої моделі. Модель безпеки враховує дані, що передаються між пристроями, можливі загрози, а також засоби захисту даних як на апаратному рівні (апаратні шифратори), так і на програмному рівні (криптографічні бібліотеки). Представимо процес шифрування та дешифрування даних між пристроями IoT виразами (1) і (2) відповідно.

$$D_i' = E(D_i, K_i) \tag{1}$$

$$D_i = D(D_i', K_i) \tag{2}$$

де D_i – дані, які передаються між пристроями; K_i – криптографічні ключі, використовувані для шифрування даних; E – функція шифрування (апаратна або програмна); D – функція дешифрування (апаратна або програмна).

IoT-пристрої мають обмежені обчислювальні ресурси, тому важливо враховувати ці обмеження при реалізації заходів безпеки. Для врахування обмежень ресурсів IoT пристроїв при розробці криптографічних алгоритмів, необхідно детально проаналізувати їх вплив на ефективність і безпеку шифрування. Важливо, щоб обрані алгоритми були оптимізовані для мінімального використання енергії та обчислювальних потужностей, зберігаючи при цьому високий рівень безпеки. Розглянемо математичний вираз, який враховує ці обмеження (3).

$$\sum_{i=1}^{n} C_i \leq C_{total}$$

де C_i – обчислювальні ресурси, необхідні для виконання певної криптографічної операції на пристрої i; C_{total} – загальні доступні обчислювальні ресурси. Такий підхід дозволяє формалізувати та проаналізувати захист інформації в умовах обмежених ресурсів, характерних для IoT.

Для обчислення ризику компрометації даних залежно від ефективності засобів захисту та наявних загроз пропонується використання математичної моделі (4).

$$R = \sum_{j=1}^{m} \sum_{k=1}^{n} T_{jk} \cdot (1 - P_{jk})$$

де R – ризик компрометації даних; T_{jk} – ймовірність загрози j для засобу захисту k; P_{jk} – ймовірність протидії загрозі j засобом захисту k. Ця модель дозволяє кількісно оцінити рівень ризику, враховуючи різні фактори загроз і ефективність захисних заходів. Використання такого підходу допомагає ідентифікувати найуразливіші точки в системі та оптимізувати стратегії захисту для IoT

пристроїв.

Ефективність засобів захисту визначається як сукупна оцінка, що враховує вагу кожного засобу захисту і його здатність протидіяти загрозам (5).

$$E(P) = \sum_{k=1}^{n} \alpha_k \cdot P_k$$

де $E(P)$ – загальна ефективність засобів захисту; α_k – ваговий коефіцієнт для засобу захисту k. Ця модель дозволяє оцінити загальну ефективність захисних заходів, враховуючи відносну важливість кожного з них. Таким чином, можна визначити, які засоби захисту мають найбільший вплив на зменшення ризику компрометації даних в системі IoT.

Запропонована модель безпеки для пристроїв IoT забезпечує комплексний підхід до захисту даних, враховуючи як апаратні, так і програмні засоби. Вона дозволяє мінімізувати ризики, пов'язані із внутрішніми та зовнішніми загрозами, шляхом оптимального вибору засобів захисту при обмежених обчислювальних ресурсах.

Висновки та перспективи подальшого дослідження. У даній статті було розглянуто проблему забезпечення безпеки взаємопов'язаних обчислювальних пристроїв на основі полегшеної схеми шифрування для IoT. Було визначено, що сучасні методи шифрування часто не враховують обмежені обчислювальні ресурси та енергоспоживання IoT пристроїв, що створює необхідність у розробці спеціалізованих легких криптографічних рішень.

Запропонована модель безпеки, яка враховує як апаратні, так і програмні засоби шифрування та управління ключами, продемонструвала можливість забезпечення надійного захисту даних при мінімальних витратах ресурсів. Аналіз сучасних досліджень та публікацій виявив перспективні напрямки розвитку полегшеної криптографії, зокрема, використання квантово-стійких протоколів та інтеграції блокчейн технологій для децентралізованого управління криптографічними ключами.

Подальші дослідження можуть бути спрямовані на розробку нових легких криптографічних алгоритмів та методів управління ключами, які ще більше знизять енергоспоживання та покращать безпеку IoT пристроїв. Також перспективним є дослідження інтеграції штучного інтелекту для автоматизації процесів виявлення та протидії кібератакам на IoT системи.

Важливим напрямком є проведення експериментальних досліджень та тестування запропонованих рішень в реальних умовах, що дозволить оцінити їхню ефективність та надійність. Поглиблене вивчення можливостей апаратних шифраторів та оптимізація їх взаємодії з програмними засобами захисту може суттєво підвищити загальний рівень безпеки IoT екосистем.

Список бібліографічного опису

1. Marton, A., 2023. State of IoT – spring 2023, report by IoT analytics, safepay systems. Available from: https://iotac.eu/state-of-iot-spring-2023-by-iot-analytics/.
2. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.
3. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
4. Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12(1), 1-20.
5. Easttom, C. (2022). Quantum computing and cryptography. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 397-407). Cham: Springer International Publishing.
6. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In Proceedings of the 4th Edge Computing Workshop (doors 2024), Zhytomyr, Ukraine (pp. 85-96).
7. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2023). IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. In Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023) (pp. 145-146). Bratislava.
8. Abd Ali, S. M., & Hasan, H. F. (2019). Novel encryption algorithm for securing sensitive information based on feistel cipher. Test Engeenering Managenment, 19(80), 10-16.
9. Mahmood, Z., Ning, H., & Ghafoor, A. (2016, December). Lightweight two-level session key management for end user authentication in Internet of Things. In 2016 IEEE international conference on internet of things (iThings) and IEEE Green computing and communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 323-327). IEEE.
10. Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal, 7(7), 6457-6480.
11. Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and key management in distributed iot using blockchain technology. IEEE Internet of Things Journal, 8(16), 12947-12954.

12. Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. Journal of Network and Computer Applications, 169, 102763.
13. Restuccia, G., Tschofenig, H., & Baccelli, E. (2020, December). Low-power IoT communication security: On the performance of DTLS and TLS 1.3. In 2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN) (pp. 1-6). IEEE.
14. Pop, A. A. (2022). Incremental encoder speed acquisition using an STM32 microcontroller and NI ELVIS. Sensors, 22(14), 5127.
15. Розломій І.О., Косенюк Г.В., Науменко С.В., Михайловський П.В. (2023) Моделювання системи датчиків на базі мікроконтролера в ігровій симуляції «Смарт-будинок» з використанням шифрування. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. (53), 292-299. https://doi.org/10.36910/6775-2524-0560-2023-53-43

References

1. Marton, A., 2023. State of IoT – spring 2023, report by IoT analytics, safepay systems. Available from: https://iotac.eu/state-of-iot-spring-2023-by-iot-analytics/ .
2. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.
3. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access, 7, 82721-82743.
4. Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12(1), 1-20.
5. Easttom, C. (2022). Quantum computing and cryptography. In Modern Cryptography: Applied Mathematics for Encryption and Information Security (pp. 397-407). Cham: Springer International Publishing.
6. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In Proceedings of the 4th Edge Computing Workshop (doors 2024), Zhytomyr, Ukraine (pp. 85-96).
7. Rozlomii, I., Yarmilko, A., Naumenko, S., & Mykhailovskyi, P. (2023). IoT Smart Implants: Information Security and the Implementation of Lightweight Cryptography. In Proceedings of the 6th International Conference on Informatics & Data-Driven Medicine (IDDM'2023) (pp. 145-146). Bratislava.
8. Abd Ali, S. M., & Hasan, H. F. (2019). Novel encryption algorithm for securing sensitive information based on feistel cipher. Test Engeenering Managenment, 19(80), 10-16.
9. Mahmood, Z., Ning, H., & Ghafoor, A. (2016, December). Lightweight two-level session key management for end user authentication in Internet of Things. In 2016 IEEE international conference on internet of things (iThings) and IEEE Green computing and communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 323-327). IEEE.
10. Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal, 7(7), 6457-6480.
11. Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and key management in distributed iot using blockchain technology. IEEE Internet of Things Journal, 8(16), 12947-12954.
12. Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. Journal of Network and Computer Applications, 169, 102763.
13. Restuccia, G., Tschofenig, H., & Baccelli, E. (2020, December). Low-power IoT communication security: On the performance of DTLS and TLS 1.3. In 2020 9th IFIP International Conference on Performance Evaluation and Modeling in Wireless Networks (PEMWN) (pp. 1-6). IEEE.
14. Pop, A. A. (2022). Incremental encoder speed acquisition using an STM32 microcontroller and NI ELVIS. Sensors, 22(14), 5127.
15. Rozlomii I.O., Kosenyuk G.V., Naumenko S.V., Mykhaylovskyi P.V. (2023) Modeling a Microcontroller-Based Sensor System in a Smart Home Game Simulation Using Encryption. Computer-Integrated technologies: education, science, production. (53), 292-299. https://doi.org/10.36910/6775-2524-0560-2023-53-43