https://doi.org/10.31891/2219-9365-2026-86-6
УДК 004.056.55:004.738.5:004.65:004.75

ГРИГОР'ЄВ Костянтин
Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0009-0003-1316-4354
prizma2098@gmail.com

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В IOT-СИСТЕМАХ НА ОСНОВІ БЛОКЧЕЙН-ТЕХНОЛОГІЙ ЗА ДОПОМОГОЮ РОЗПОДІЛЕНОГО РЕЄСТРУ ДЛЯ ЗНИЖЕННЯ РИЗИКІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У статті досліджено проблему забезпечення цілісності інформації в IoT-системах, які функціонують у розподілених середовищах із обмеженими обчислювальними та енергетичними ресурсами. Проаналізовано сучасні підходи до захисту даних, зокрема централізовані моделі та криптографічні механізми, що використовуються для контролю цілісності, а також визначено їх обмеження у контексті IoT. Обґрунтовано доцільність використання блокчейн-технологій як інструменту децентралізованого забезпечення незмінності та перевірюваності даних. Запропоновано модель забезпечення цілісності інформації, яка поєднує полегшені криптографічні операції на рівні сенсорних вузлів із механізмами валідації та збереження даних у розподіленому реєстрі на рівні edge-вузлів. Модель передбачає ієрархічний розподіл функцій між вузлами системи та адаптацію криптографічних механізмів до ресурсних обмежень пристроїв. Виконано аналітичну оцінку ефективності запропонованого підходу за показниками енергоспоживання, затримок обробки даних та стійкості до атак. Отримані результати свідчать про зниження обчислювального навантаження на сенсорні вузли, підвищення рівня виявлення несанкціонованих змін інформації та покращення масштабованості системи. Практична значущість полягає у можливості застосування моделі в кіберфізичних системах, де критичною є достовірність даних, зокрема в медицині, промисловості та енергетиці.

Ключові слова: IoT-системи, цілісність інформації, блокчейн, розподілений реєстр, полегшена криптографія, edge-обчислення.

HRYHORIEV Kostiantyn
Open International University of Human Development «Ukraine»

MODEL FOR ENSURING INFORMATION INTEGRITY IN IOT SYSTEMS BASED ON BLOCKCHAIN TECHNOLOGY USING A DISTRIBUTED REGISTRY TO REDUCE THE RISKS OF UNAUTHORIZED ACCESS

The paper addresses the problem of ensuring data integrity in Internet of Things (IoT) systems operating in distributed environments with constrained computational and energy resources. The rapid growth of IoT infrastructures leads to increased complexity of data exchange processes and raises significant challenges related to unauthorized data modification and integrity violations. Existing approaches based on centralized control and traditional cryptographic mechanisms are analyzed, revealing their limitations in terms of scalability, resilience to attacks, and suitability for resource-constrained devices.

The study substantiates the feasibility of applying blockchain technology as a decentralized mechanism for ensuring data immutability, transparency, and verifiability without relying on a trusted central authority. A novel model for data integrity assurance in IoT systems is proposed, combining lightweight cryptographic operations at the sensor level with distributed validation and storage processes implemented at the edge layer using a blockchain-based distributed ledger. The model introduces a hierarchical distribution of computational tasks among system nodes, minimizing the load on low-power devices while maintaining robust integrity control.

The proposed approach includes a mathematical representation of data generation, hashing, transmission, validation, and recording processes, as well as a mechanism for adaptive allocation of cryptographic operations depending on node capabilities. Analytical evaluation of the model is conducted with respect to key performance indicators, including energy consumption, processing delay, and resistance to unauthorized data modification.

The obtained results demonstrate that the proposed model reduces energy consumption at the sensor level, improves detection of data tampering through multi-stage validation, and enhances overall system scalability. In comparison with centralized and conventional blockchain-based approaches, the model achieves a balanced trade-off between security, performance, and resource efficiency. The practical significance of the research lies in its applicability to cyber-physical systems where data integrity is critical, such as healthcare, industrial automation, and smart energy systems.

Keywords: IoT systems, data integrity, blockchain, distributed ledger, lightweight cryptography, edge computing.

Стаття надійшла до редакції / Received 14.03.2026
Прийнята до друку / Accepted 30.04.2026
Опубліковано / Published 31.05.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Стрімке зростання кількості пристроїв Інтернету речей призводить до формування складних розподілених середовищ, у яких відбувається безперервний обмін даними між сенсорами, виконавчими механізмами та хмарними сервісами [1]. Такі системи функціонують в умовах обмежених обчислювальних ресурсів, нестабільних каналів зв'язку та відсутності централізованого контролю, що ускладнює забезпечення

цілісності інформації [2]. Порушення цілісності даних у IoT-системах може призводити до критичних наслідків, зокрема у сферах медицини, промислової автоматизації, енергетики та транспорту, де достовірність даних безпосередньо впливає на прийняття рішень [3].

Сучасні підходи до захисту інформації в IoT здебільшого орієнтовані на використання централізованих моделей контролю доступу та перевірки даних, що створює єдині точки відмови та підвищує ризик несанкціонованого втручання. У таких умовах атаки типу підміни даних, несанкціонованої модифікації або повторного відтворення повідомлень можуть залишатися непоміченими або виявлятися із запізненням [4]. Крім того, традиційні криптографічні механізми, які забезпечують цілісність, не завжди адаптовані до ресурсних обмежень периферійних пристроїв, що знижує ефективність їх практичного застосування.

Перспективним напрямом вирішення зазначених проблем є використання технологій розподіленого реєстру, зокрема блокчейну, який дозволяє забезпечити незмінність записів, прозорість операцій та відсутність централізованого вузла керування. Інтеграція блокчейн-технологій в IoT-середовище відкриває можливості для створення децентралізованих механізмів контролю цілісності даних, де кожна транзакція фіксується у вигляді криптографічно захищеного запису [5]–[7]. Однак пряме застосування класичних блокчейн-рішень у IoT є ускладненим через їх високу обчислювальну складність, затримки підтвердження транзакцій та значні енергетичні витрати.

Виникає необхідність розроблення моделей, які поєднують переваги розподілених реєстрів із адаптацією до обмежених ресурсів IoT-пристроїв, забезпечуючи при цьому ефективний механізм виявлення та запобігання несанкціонованому доступу до даних. Особливо актуальним є формування підходів, що дозволяють знизити навантаження на кінцеві пристрої шляхом делегування частини обчислень на периферійні або граничні вузли, зберігаючи при цьому властивості незмінності та перевірюваності даних [8].

До ключових наукових і практичних завдань, з якими пов’язана дана проблема, належать:

- підвищення рівня достовірності даних у розподілених IoT-системах без збільшення енергоспоживання пристроїв;
- розроблення механізмів виявлення несанкціонованих змін інформації в реальному часі;
- інтеграція блокчейн-рішень у середовища з обмеженими обчислювальними ресурсами;
- мінімізація затримок при підтвердженні транзакцій у розподіленому реєстрі;
- забезпечення масштабованості системи при зростанні кількості підключених пристроїв.

Метою дослідження є розроблення моделі забезпечення цілісності інформації в IoT-системах на основі блокчейн-технологій із використанням розподіленого реєстру, яка дозволяє знизити ризики несанкціонованого доступу за рахунок децентралізованого контролю та адаптації криптографічних механізмів до обмежених ресурсів пристроїв.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Аналіз сучасних досліджень у сфері забезпечення цілісності інформації в IoT-системах свідчить про активний розвиток підходів, що поєднують криптографічні методи захисту з децентралізованими архітектурами обробки даних. Значна частина наукових праць присвячена використанню хеш-функцій, цифрових підписів та механізмів автентифікації для запобігання несанкціонованій модифікації інформації [9], [10]. Водночас у більшості випадків такі рішення базуються на централізованих серверах або довірених третіх сторонах, що обмежує їх стійкість до атак і створює додаткові ризики компрометації.

У контексті IoT особливу увагу приділено полегшеним криптографічним алгоритмам, які адаптовані до умов обмежених ресурсів. Дослідження демонструють ефективність використання lightweight-хешування та симетричних алгоритмів шифрування для перевірки цілісності даних на рівні сенсорних вузлів [11]. Проте такі підходи не вирішують проблему довіри між вузлами мережі, оскільки не передбачають надійного механізму фіксації та перевірки історії змін даних у розподіленому середовищі.

Значний інтерес у науковій спільноті викликає інтеграція блокчейн-технологій у IoT-системи [12]. У ряді робіт запропоновано використання розподілених реєстрів для збереження журналів подій, транзакцій сенсорних даних та результатів обробки інформації. Перевагами такого підходу є незмінність записів, прозорість операцій та можливість перевірки достовірності даних без необхідності довіряти окремому вузлу. Дослідження також демонструють можливість використання смарт-контрактів для автоматизації процесів контролю доступу та валідації даних.

Разом з тим, існуючі блокчейн-рішення, зокрема публічні мережі, характеризуються високими вимогами до обчислювальних ресурсів, значними затримками підтвердження транзакцій та підвищеним енергоспоживанням. У зв’язку з цим у наукових публікаціях активно розглядаються альтернативні підходи, такі як приватні або консорціумні блокчейни, а також використання полегшених механізмів консенсусу. Запропоновано архітектури, у яких функції обробки транзакцій і підтримки реєстру делегуються більш потужним вузлам периферійного або граничного рівня, тоді як IoT-пристрої виконують лише базові операції формування та передачі даних.

Окремі дослідження спрямовані на поєднання блокчейн-технологій із edge- та fog-обчисленнями для зниження затримок і оптимізації використання ресурсів. Такі підходи дозволяють розподілити навантаження

між різними рівнями архітектури, однак питання узгодженості даних, ефективного управління транзакціями та мінімізації обчислювальних витрат залишаються відкритими. Крім того, недостатньо досліджено механізми адаптивного вибору криптографічних операцій залежно від стану мережі та ресурсів пристроїв.

Аналіз наявних публікацій показує, що більшість існуючих рішень або орієнтовані на високопродуктивні середовища, або не враховують специфіку IoT-пристроїв із обмеженими ресурсами. Водночас відсутні комплексні моделі, які б поєднували механізми забезпечення цілісності даних, децентралізовану перевірку транзакцій та оптимізацію обчислювальних витрат у межах єдиної архітектури. Це обумовлює необхідність подальших досліджень у напрямі розроблення ефективних моделей забезпечення цілісності інформації в IoT-системах із використанням блокчейн-технологій, адаптованих до умов обмежених ресурсів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

У У сучасних IoT-системах забезпечення цілісності інформації ускладнюється через розподілений характер середовища, різнорідність пристроїв та обмеженість їх обчислювальних і енергетичних ресурсів. Модель середовища доцільно розглядати як сукупність взаємодіючих вузлів, серед яких виділяються сенсорні пристрої, що здійснюють первинний збір даних, шлюзи, які виконують агрегацію та попередню обробку, а також edge-вузли, відповідальні за більш складні обчислення та взаємодію з вищими рівнями інфраструктури. Передача даних між вузлами здійснюється через бездротові або змішані канали зв'язку, які характеризуються нестабільністю та підвищеною вразливістю до атак.

До основних загроз порушення цілісності належать підміна даних на рівні сенсорів, несанкціонована модифікація під час передачі, атаки повторного відтворення повідомлень, а також компрометація вузлів із подальшим внесенням фальсифікованої інформації. У таких умовах необхідно враховувати параметри системи, зокрема обсяг обчислювальних ресурсів кожного вузла, рівень енергоспоживання, затримки передачі даних та інтенсивність генерації повідомлень.

Загальна архітектура IoT-системи із виділенням основних рівнів та потоків даних наведена на рис. 1.

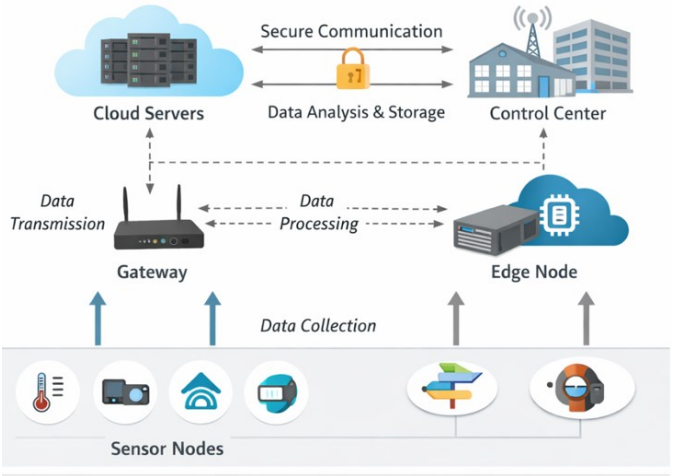

Рис. 1. Загальна архітектура IoT-системи з розподілом функцій між вузлами

На рис. 1 відображено взаємодію сенсорних пристроїв, шлюзів та edge-вузлів, а також напрямки передачі даних і місця потенційного виникнення загроз. Такий підхід дозволяє чітко ідентифікувати точки контролю цілісності інформації та визначити, на яких етапах доцільно застосовувати криптографічні механізми.

Характеристики основних типів вузлів IoT-системи наведено в табл. 1.

Аналіз наведених характеристик показує, що виконання складних криптографічних операцій доцільно переносити з сенсорного рівня на більш потужні вузли, що дозволяє зменшити навантаження на обмежені пристрої та підвищити загальну ефективність системи.

Таблиця 1

Характеристики вузлів IoT-системи

Тип вузла	Обчислювальні ресурси	Енергоспоживання	Основні функції
Сенсорний вузол	Низькі	Мінімальне	Збір даних, первинна обробка
Шлюз	Середні	Помірне	Агрегація, передача, фільтрація
Edge-вузол	Високі	Високе	Обробка, валідація, взаємодія з реєстром

У якості підходу до забезпечення цілісності даних розглядається використання розподіленого реєстру, який дозволяє фіксувати всі зміни інформації у вигляді послідовності взаємопов'язаних записів.

Вибір блокчейн-технології обумовлений її властивостями незмінності, децентралізації та криптографічного зв'язку між блоками. З огляду на обмеження IoT-середовища доцільним є використання приватного або консорціумного типу реєстру, що дозволяє зменшити затримки підтвердження транзакцій та знизити обчислювальні витрати.

Механізм формування транзакцій передбачає попереднє хешування даних на рівні сенсорного вузла з подальшою передачею агрегованих значень на edge-рівень, де відбувається формування блоку та його включення до ланцюга. Кожен новий блок містить хеш попереднього, що забезпечує неможливість непомітної модифікації інформації. Структура блокчейн-ланцюга з урахуванням транзакцій IoT-системи наведена на рис. 2.

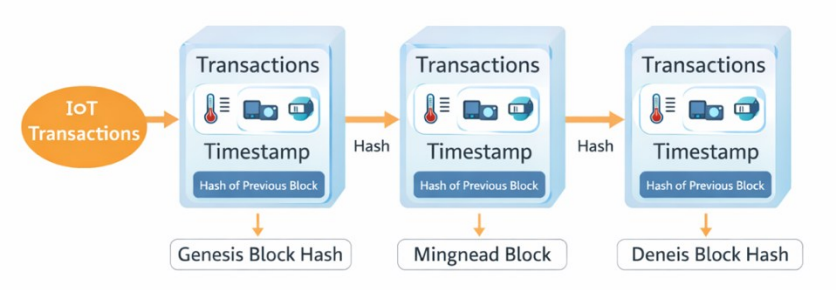

Рис. 2. Структура блокчейн-ланцюга з транзакціями IoT

На рис. 2 показано послідовність блоків, кожен з яких містить набір транзакцій, часову мітку та криптографічний зв'язок із попереднім блоком. Така структура забезпечує цілісність даних за рахунок неможливості зміни окремого запису без порушення всієї послідовності.

Порівняння централізованого та децентралізованого підходів до забезпечення цілісності інформації наведено в табл. 2.

Таблиця 2

Порівняння підходів до забезпечення цілісності даних

Критерій	Централізований підхід	Децентралізований підхід (блокчейн)
Точка контролю	Єдина	Розподілена
Стійкість до атак	Низька	Висока
Масштабованість	Обмежена	Висока
Затримки обробки	Низькі	Середні
Витрати ресурсів	Помірні	Вищі

Представлене порівняння демонструє, що використання розподіленого реєстру дозволяє підвищити стійкість до несанкціонованих змін та усунути єдину точку відмови, однак потребує оптимізації з точки зору ресурсних витрат. Це обумовлює необхідність подальшої розробки моделі, яка поєднує переваги блокчейн-технологій із адаптацією до умов IoT-середовища.

Запропонована модель забезпечення цілісності інформації в IoT-системах базується на поєднанні полегшених криптографічних операцій на рівні сенсорних вузлів із децентралізованим механізмом валідації та збереження даних у розподіленому реєстрі. Основна ідея полягає у розподілі функцій між вузлами системи таким чином, щоб мінімізувати навантаження на ресурсообмежені пристрої та забезпечити надійний контроль цілісності на більш потужних рівнях інфраструктури. Нехай IoT-система описується множиною вузлів $N = \{n_1, n_2, \dots, n_k\}$, де кожен вузол n_i генерує повідомлення $m_i \in M_m$.

На сенсорному рівні для кожного повідомлення обчислюється хеш-значення $h_i = H(m_i)$, де $H(\cdot)$ – полегшена криптографічна хеш-функція.

Сформоване повідомлення передається у вигляді структури $T_i = (m_i, h_i, t_i)$, де t_i – часова мітка генерації даних. На рівні edge-вузла виконується перевірка цілісності шляхом повторного обчислення хешу $h_i^* = H(m_i)$. Дані вважаються цілісними, якщо виконується умова $h_i^* = h_i$. Для кількісної оцінки рівня цілісності інформації вводиться коефіцієнт цілісності $I = \frac{N_{valid}}{N_{total}}$, де N_{valid} – кількість повідомлень, що пройшли перевірку, N_{total} – загальна кількість отриманих повідомлень. Значення $I \to 1$ відповідає високому рівню цілісності даних.

Ймовірність успішної несанкціонованої модифікації даних визначається як $P_{attack} = \frac{N_{comp}}{N_{total}}$, де N_{comp} – кількість скомпрометованих повідомлень.

Сукупні обчислювальні витрати системи можна представити у вигляді (1).

$$C_{total} = \sum_{i=1}^{k}(C_{hash}^{(i)} + C_{trans}^{(i)} + C_{val}^{(i)}) \quad (1)$$

де $C_{hash}^{(i)}$ – витрати на обчислення хешу на вузлі n_i, $C_{trans}^{(i)}$ – витрати на передачу даних, $C_{val}^{(i)}$ – витрати на перевірку та запис у реєстр.

Структурну схему моделі наведено на рис. 3.

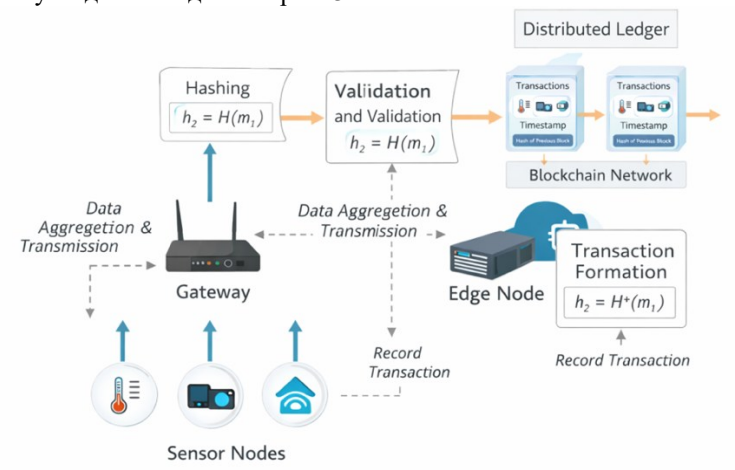

Рис. 3. Структурна схема моделі забезпечення цілісності інформації в IoT-системі

На рис. 3 відображено розподіл функцій між сенсорними вузлами, шлюзами та edge-рівнем, а також інтеграцію з блокчейн-мережею. Сенсорні вузли виконують лише базові операції хешування, тоді як більш складні процеси перевірки, агрегації та запису в реєстр делегуються на вищі рівні.

Основні параметри моделі наведено в табл. 3.

Таблиця 3

Параметри моделі

Параметр	Позначення	Опис
Кількість вузлів	N	Загальна кількість IoT-пристроїв
Повідомлення	M	Множина переданих даних
Хеш-значення	h_i	Результат $H(m_i)$
Часова мітка	t_i	Час генерації повідомлення
Цілісність	I	Частка коректних повідомлень
Ймовірність атаки	P_{attack}	Частка скомпрометованих даних
Витрати	C_{total}	Загальні обчислювальні витрати

Алгоритм функціонування моделі передбачає послідовну обробку даних від моменту їх генерації до збереження у розподіленому реєстрі. На першому етапі сенсорний вузол формує повідомлення mim та обчислює h_i. Далі формується структура T_i, яка передається через шлюз до edge-вузла. На цьому рівні виконується перевірка: обчислюється h_i^* та порівнюється з h_i У разі співпадіння формується транзакція, яка передається до блокчейн-мережі та включається до блоку.

Блок-схему алгоритму наведено на рис. 4.

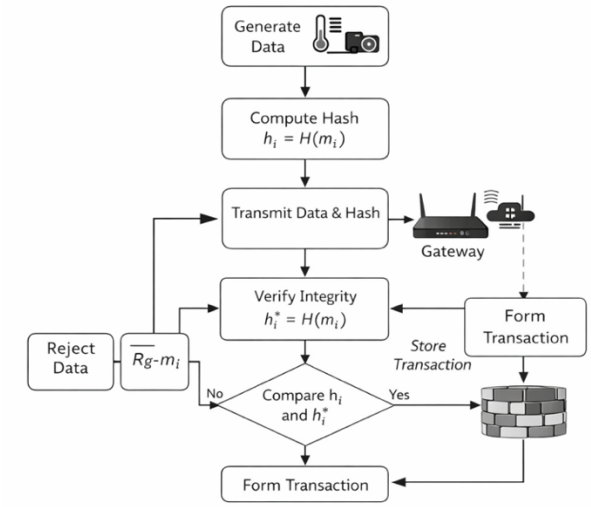

Рис. 4. Блок-схема алгоритму забезпечення цілісності інформації

На рис. 4 представлено послідовність обробки даних: генерація, хешування, передача, валідація та запис у розподілений реєстр. Така організація дозволяє здійснювати контроль цілісності на кожному етапі життєвого циклу інформації.

Взаємодія між вузлами реалізується за ієрархічним принципом із розподілом навантаження. Сенсорні пристрої виконують мінімальні обчислення, тоді як edge-вузли забезпечують перевірку та інтеграцію з блокчейн-мережею, що дозволяє адаптувати модель до умов обмежених ресурсів.

Етапи обробки даних та їх часові характеристики наведено в табл. 4.

Таблиця 4

Етапи обробки даних

Етап	Опис	Час виконання
Генерація	Формування повідомлення	Низький
Хешування	Обчислення $h_i = H(m_i)$	Низький
Передача	Передача через мережу	Середній
Валідація	Перевірка $h_i^* = H(m_i)$	Середній
Запис у блокчейн	Формування блоку та збереження	Високий

Запропонована модель дозволяє забезпечити контроль цілісності інформації з урахуванням ресурсних обмежень IoT-пристроїв, знижуючи ризики несанкціонованої модифікації даних та підвищуючи надійність функціонування системи.

Оцінювання ефективності запропонованої моделі здійснюється на основі аналітичного підходу з урахуванням ключових параметрів IoT-системи, зокрема кількості транзакцій, інтенсивності передачі даних, обчислювальних витрат та затримок у мережі. Для цього розглядається залежність енергоспоживання, часу обробки та рівня навантаження на вузли системи.

Енергоспоживання в системі визначається як сукупність витрат на обчислення, передачу та обробку даних і може бути представлене у вигляді (2).

$$E_{total} = \sum_{i=1}^{k}(E_{hash}^{(i)} + E_{trans}^{(i)} + E_{val}^{(i)}) \quad (2)$$

де $E_{hash}^{(i)}$ – енергоспоживання при обчисленні хешу, $E_{trans}^{(i)}$ – витрати енергії на передачу даних, $E_{val}^{(i)}$ – енергоспоживання під час валідації та запису в реєстр.

Залежність енергоспоживання від кількості транзакцій N_{tx} має майже лінійний характер для сенсорних вузлів і сублінійний для edge-рівня за рахунок агрегації даних. Графічну інтерпретацію цієї залежності наведено на рис. 5.

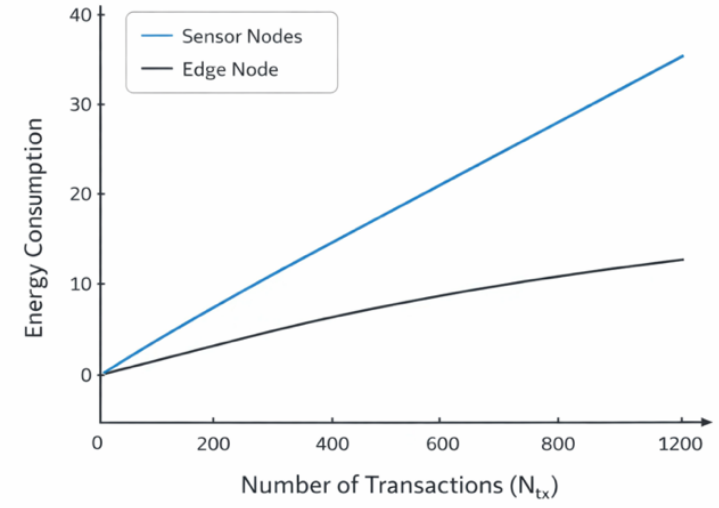

Рис. 5. Залежність енергоспоживання від кількості транзакцій

На рис. 5 видно, що використання розподіленого підходу дозволяє зменшити темпи зростання енергоспоживання за рахунок перенесення обчислювальних операцій на більш потужні вузли.

Затримка обробки даних у системі визначається як сумарний час проходження повідомлення через усі етапи (3).

$$T_{total} = T_{gen} + T_{hash} + T_{trans} + T_{val} + T_{block} \quad (3)$$

де T_{gen} – час генерації даних, T_{hash} – час обчислення хешу, T_{trans} – час передачі, T_{val} – час перевірки, T_{block} – час включення транзакції до блоку.

Залежність затримки від кількості транзакцій наведено на рис. 6.

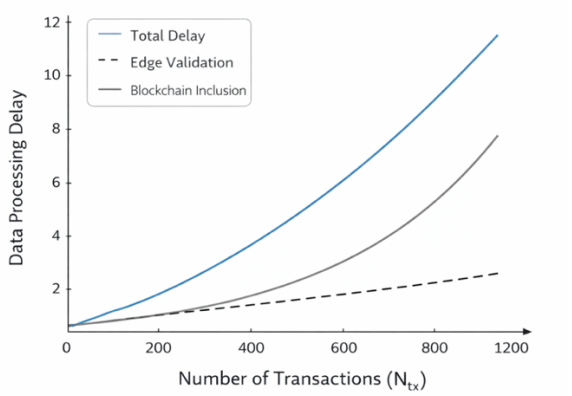

Рис. 6. Залежність затримки обробки даних від кількості транзакцій

Аналіз показує, що основний внесок у затримку формує етап запису в блокчейн, однак використання edge-вузлів дозволяє зменшити загальний час обробки за рахунок попередньої валідації та агрегації транзакцій.

Для оцінювання ефективності запропонованого підходу проведено порівняння з існуючими рішеннями, зокрема централізованими системами контролю цілісності та класичними блокчейн-підходами без адаптації до IoT. Результати порівняння наведено в табл. 5.

Таблиця 5

Порівняння підходів до забезпечення цілісності

Критерій	**Централізований підхід**	**Класичний блокчейн**	**Запропонована модель**
Енергоспоживання	Середнє	Високе	Низьке
Затримка	Низька	Висока	Середня
Масштабованість	Обмежена	Середня	Висока
Стійкість до атак	Низька	Висока	Висока
Адаптація до IoT	Низька	Низька	Висока

Отримані результати свідчать про те, що запропонована модель дозволяє досягти зниження енергоспоживання та забезпечити прийнятний рівень затримок при одночасному підвищенні стійкості до несанкціонованого доступу. Це підтверджує доцільність використання розподіленого реєстру з адаптивним розподілом криптографічного навантаження в IoT-середовищах.

ВИСНОВКИ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У У результаті проведеного дослідження розроблено модель забезпечення цілісності інформації в IoT-системах, яка поєднує полегшені криптографічні механізми з використанням розподіленого реєстру. Запропонований підхід базується на ієрархічному розподілі функцій між вузлами системи та передбачає перенесення ресурсоємних операцій на edge-рівень із мінімізацією навантаження на сенсорні пристрої.

Наукова новизна отриманих результатів полягає у формуванні моделі, що забезпечує адаптивний розподіл криптографічного навантаження між вузлами IoT-системи з урахуванням їх ресурсних обмежень, а також у вдосконаленні механізму фіксації даних у розподіленому реєстрі шляхом попередньої валідації транзакцій на периферійному рівні. Це дозволяє зменшити обсяг даних, що передаються до блокчейн-мережі, та скоротити затримки обробки без втрати властивостей незмінності та перевірюваності інформації.

Практична цінність запропонованої моделі полягає у зниженні енергоспоживання IoT-пристроїв за рахунок використання полегшених криптографічних операцій і делегування складних обчислень, підвищенні швидкості виявлення несанкціонованих змін даних завдяки багаторівневій перевірці цілісності, а також у зменшенні ризиків атак, пов’язаних із модифікацією інформації та компрометацією окремих вузлів. Отримані результати також свідчать про покращення масштабованості системи та її стійкості до зростання кількості транзакцій.

Перспективи подальших досліджень пов’язані з удосконаленням механізмів консенсусу для умов IoT-середовищ, розробкою адаптивних алгоритмів вибору криптографічних примітивів залежно від стану мережі та ресурсів вузлів, а також із впровадженням експериментальних реалізацій моделі на сучасних мікроконтролерних платформах із подальшим оцінюванням її ефективності в реальних умовах функціонування кіберфізичних систем.

Література

1. Kizza J. M. Internet of things (IoT): growth, challenges, and security. *Guide to computer network security*.

Cham: Springer International Publishing, 2024. P. 557–573. URL: https://doi.org/10.1007/978-3-031-47549-8_25

2. Rozlomii I., Yarmilko A., Naumenko S. Data security of IoT devices with limited resources: challenges and potential solutions. *Proceedings of the 4th Edge Computing Workshop (DOORS 2024)*. 2024. Vol. 3666. P. 85–96. URL: https://ceur-ws.org/Vol-3666/paper13.pdf

3. El-Hajj M. Preventing data integrity breaches in IoT applications using digital twins. *2025 23rd Mediterranean Communication and Computer Networking Conference (MedComNet)*. 2025. P. 1–6. URL: https://doi.org/10.1109/MedComNet65822.2025.11103570

4. Eghmazi A., Ataei M., Landry R. J., Chevrette G. Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. *IoT*. 2024. Vol. 5, no. 1. P. 20–34. URL: https://doi.org/10.3390/iot5010002

5. Gangwani P., Joshi S., Upadhyay H., Lagos L. IoT device identity management and blockchain for security and data integrity. *International Journal of Computer Applications*. 2023. Vol. 184, no. 42. P. 49–55.

6. Khan R., Teo J., Jan M. A., Verma S., Alturki R., Ghani A. A trustworthy, reliable, and lightweight privacy and data integrity approach for the Internet of Things. *IEEE Transactions on Industrial Informatics*. 2022. Vol. 19, no. 1. P. 511–518. URL: https://doi.org/10.1109/TII.2022.3179728

7. Kolevski D., Michael K. Edge computing and IoT data breaches: Security, privacy, trust, and regulation. *IEEE Technology and Society Magazine*. 2024. Vol. 43, no. 1. P. 22–32. URL: https://doi.org/10.1109/MTS.2024.3372605

8. Songshen H. A. N., Kaiyong X. U., Zhiqiang Z. H. U., Songhui G. U. O., Haidong L. I. U., Zuohui L. I. Hash-based signature for flexibility authentication of IoT devices. *Wuhan University Journal of Natural Sciences*. 2022. Vol. 27, no. 1. P. 1–10. URL: https://doi.org/10.1051/wujns/2022271001

9. Ali W., Ahmed A. A. An authenticated group shared key mechanism based on a combiner for hash functions over the industrial internet of things. *Processes*. 2023. Vol. 11, no. 5. P. 1558. URL: https://doi.org/10.3390/pr11051558

10. Vikram D., Jeyakkannan N., Santhoshkumar S. P., Karthika R., Punitha P., Ajina H. Securing IoT: Anomaly detection and behavioral analysis for data integrity. *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. 2024. P. 892–896.

11. Oudah M. S., Maolood A. T. Lightweight authentication model for IoT environments based on enhanced elliptic curve digital signature and Shamir secret share. *International Journal of Intelligent Engineering & Systems*. 2022. Vol. 15, no. 5. URL: https://doi.org/10.22266/ijies2022.1031.08

12. Григор'єв К., Павленко В. Система забезпечення конфіденційності транзакцій з даними з використанням протоколів нульового розголошення. *Measuring and computing devices in technological processes*. 2026. № 1(85). С. 208–214. URL: https://doi.org/10.31891/2219-9365-2026-85-26

References

1. Kizza J. M. Internet of things (IoT): growth, challenges, and security. *Guide to computer network security*. Cham: Springer International Publishing, 2024. P. 557–573. URL: https://doi.org/10.1007/978-3-031-47549-8_25

2. Rozlomii I., Yarmilko A., Naumenko S. Data security of IoT devices with limited resources: challenges and potential solutions. *Proceedings of the 4th Edge Computing Workshop (DOORS 2024)*. 2024. Vol. 3666. P. 85–96. URL: https://ceur-ws.org/Vol-3666/paper13.pdf

3. El-Hajj M. Preventing data integrity breaches in IoT applications using digital twins. *2025 23rd Mediterranean Communication and Computer Networking Conference (MedComNet)*. 2025. P. 1–6. URL: https://doi.org/10.1109/MedComNet65822.2025.11103570

4. Eghmazi A., Ataei M., Landry R. J., Chevrette G. Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. *IoT*. 2024. Vol. 5, no. 1. P. 20–34. URL: https://doi.org/10.3390/iot5010002

5. Gangwani P., Joshi S., Upadhyay H., Lagos L. IoT device identity management and blockchain for security and data integrity. *International Journal of Computer Applications*. 2023. Vol. 184, no. 42. P. 49–55.

6. Khan R., Teo J., Jan M. A., Verma S., Alturki R., Ghani A. A trustworthy, reliable, and lightweight privacy and data integrity approach for the Internet of Things. *IEEE Transactions on Industrial Informatics*. 2022. Vol. 19, no. 1. P. 511–518. URL: https://doi.org/10.1109/TII.2022.3179728

7. Kolevski D., Michael K. Edge computing and IoT data breaches: Security, privacy, trust, and regulation. *IEEE Technology and Society Magazine*. 2024. Vol. 43, no. 1. P. 22–32. URL: https://doi.org/10.1109/MTS.2024.3372605

8. Songshen H. A. N., Kaiyong X. U., Zhiqiang Z. H. U., Songhui G. U. O., Haidong L. I. U., Zuohui L. I. Hash-based signature for flexibility authentication of IoT devices. *Wuhan University Journal of Natural Sciences*. 2022. Vol. 27, no. 1. P. 1–10. URL: https://doi.org/10.1051/wujns/2022271001

9. Ali W., Ahmed A. A. An authenticated group shared key mechanism based on a combiner for hash functions over the industrial internet of things. *Processes*. 2023. Vol. 11, no. 5. P. 1558. URL: https://doi.org/10.3390/pr11051558

10. Vikram D., Jeyakkannan N., Santhoshkumar S. P., Karthika R., Punitha P., Ajina H. Securing IoT: Anomaly detection and behavioral analysis for data integrity. *2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*. 2024. P. 892–896.

11. Oudah M. S., Maolood A. T. Lightweight authentication model for IoT environments based on enhanced elliptic curve digital signature and Shamir secret share. *International Journal of Intelligent Engineering & Systems*. 2022. Vol. 15, no. 5. URL: https://doi.org/10.22266/ijies2022.1031.08

12. Hryhoriev K., Pavlenko V. System for ensuring confidentiality of data transactions using zero-disclosure protocols. *Measuring and computing devices in technological processes*. 2026. № 1(85). С. 208–214. URL: https://doi.org/10.31891/2219-9365-2026-85-26