УДК 004.75:004.056:004.77 DOI: 10.31673/2412-9070.2026.046913

І. О. РОЗЛОМІЙ[1], канд. техн. наук, доцент;
ORCID: 0000-0001-5065-9004
В. Г. БАБЕНКО[1,2], д-р техн. наук, професор;
ORCID: 0000-0003-2039-2841
С. В. НАУМЕНКО[3], викладач;
ORCID: 0000-0002-6337-1605
Н. О. ЛАЩЕВСЬКА[4], канд. техн. наук, доцент,
ORCID: 0000-0003-2148-115X
[1]Черкаський державний технологічний університет
[2]Державний університет інформаційно-комунікаційних технологій, Київ
[3]Черкаський національний університет імені Богдана Хмельницького
[4]Національний університет біоресурсів і природокористування України, Київ

МОДЕЛЬ ДЕЦЕНТРАЛІЗОВАНОГО УПРАВЛІННЯ ІДЕНТИЧНІСТЮ IoT ПРИСТРОЇВ У КРИТИЧНИХ ІНФРАСТРУКТУРАХ НА ОСНОВІ ХМАРНИХ СЕРВІСІВ І БЛОКЧЕЙН-РЕЄСТРІВ

У статті досліджено проблему децентралізованого управління ідентичністю IoT пристроїв у критичних інфраструктурах, що функціонують на основі хмарних сервісів, edge-обчислень і блокчейн-реєстрів. Актуальність роботи зумовлена зростанням кількості гетерогенних пристроїв у середовищах промислового інтернету речей (IIoT), необхідністю достовірної ідентифікації вузлів, забезпечення цілісності даних і зменшення залежності від централізованих сервісів автентифікації. Показано, що традиційні моделі управління ідентичністю мають обмеження, пов'язані з ризиком відмови єдиного центру довіри, складністю масштабування, затримками при обробці запитів і недостатньою адаптивністю до динамічних змін топології IoT мереж.

Запропоновано модель децентралізованого управління ідентичністю IoT пристроїв, у якій функції формування ідентичності, попередньої перевірки, зберігання записів і управління політиками розподілено між IoT пристроями, edge-вузлами, хмарними сервісами та блокчейн-реєстром. Розроблено структуру запису в реєстрі, модель транзакції для зміни стану ідентичності та алгоритм функціонування системи, що охоплює сценарії підключення нового пристрою, перевірки ідентичності, оновлення параметрів і відкликання у разі компрометації. Особливістю підходу є перенесення основних обчислювальних операцій на edge-рівень і спеціалізовані вузли блокчейн-мережі, що дозволяє зменшити навантаження на ресурсно-обмежені IoT пристрої.

Практична цінність моделі полягає у можливості її використання в енергетичних, транспортних, промислових та інших критичних інфраструктурах, де важливими є достовірність ідентифікації пристроїв, незмінність записів, масштабованість і стійкість до компрометації окремих вузлів.

Ключові слова: IoT пристрої, критична інфраструктура, децентралізована ідентичність, хмарні сервіси, блокчейн-реєстр, edge-обчислення.

Вступ

Стрімка цифровізація критичних інфраструктур, зокрема енергетичних систем, транспортних мереж, систем водопостачання та промислових об'єктів, супроводжується масовим впровадженням технологій Industrial Internet of Things (IIoT), що формують розподілене середовище з великою кількістю гетерогенних пристроїв. Такі пристрої здійснюють безперервний

збір, обробку та передачу телеметричних даних у хмарні середовища, забезпечуючи функціонування сервісів моніторингу, прогнозування та автоматизованого управління [1]. У цьому контексті ідентичність кожного пристрою стає ключовим елементом довіри до даних і рішень, що приймаються на їх основі.

Разом із тим централізовані підходи до управління ідентичністю, які базуються на класичних моделях аутентифікації через довірені центри сертифікації або хмарні служби, демонструють обмежену стійкість до сучасних загроз [2]–[4]. Вразливість до атак типу single point of failure, можливість компрометації реєстрів ідентифікаторів, затримки при масштабуванні та обмежена адаптивність до динамічних змін топології IoT-мереж знижують ефективність таких рішень у критичних інфраструктурах [5]. Особливо це проявляється в умовах високої щільності пристроїв, обмежених обчислювальних ресурсів мікроконтролерів та необхідності обробки даних у реальному часі [6].

Постановка проблеми

Сучасні наукові дослідження орієнтуються на пошук децентралізованих підходів до управління ідентичністю, серед яких особливу увагу привертають блокчейн-реєстри як засіб забезпечення незмінності записів, прозорості операцій та розподіленого зберігання довірених даних [7]–[9]. Інтеграція таких реєстрів із хмарними сервісами відкриває можливості для формування гібридних архітектур, у яких поєднуються масштабованість, доступність та відмовостійкість хмарних платформ із властивостями децентралізованого консенсусу. Водночас на практиці виникає низка невирішених питань, пов'язаних із адаптацією блокчейн-механізмів до обмежених ресурсів IoT-пристроїв, оптимізацією обміну даними між edge- та cloud-рівнями, а також забезпеченням ефективного управління життєвим циклом ідентичностей у динамічних середовищах.

Проблема ускладнюється необхідністю узгодження вимог до продуктивності, енергоефективності та затримок із вимогами до цілісності, автентичності та довіри до даних. У критичних інфраструктурах будь-яке порушення ідентичності пристрою або підміна даних може призвести до значних технічних і соціально-економічних наслідків, що визначає актуальність розробки нових моделей управління ідентичністю, здатних функціонувати в умовах обмежених ресурсів та високих вимог до надійності.

Аналіз останніх досліджень і публікацій

Актуальні дослідження у сфері управління ідентичністю IoT-пристроїв у критичних інфраструктурах формуються на перетині кількох напрямів, серед яких домінують хмарні обчислення, розподілені реєстри, edge-архітектури та підходи до децентралізованої ідентифікації [10], [11]. У класичних роботах, присвячених IIoT, управління ідентичністю розглядається як складова систем контролю доступу, що реалізуються через централізовані сервіси аутентифікації в хмарних середовищах. Такі підходи забезпечують уніфіковане адміністрування, однак обмежуються проблемами масштабованості, затримок і залежності від єдиного центру довіри [12].

Подальший розвиток досліджень пов'язаний із переходом до концепцій децентралізованої ідентичності, зокрема self-sovereign identity [13] та distributed identity management [14], які передбачають відмову від централізованих реєстрів і використання розподілених механізмів підтвердження ідентичності. У цьому контексті блокчейн-технології розглядаються як базова інфраструктура для зберігання ідентифікаторів, сертифікатів та історії взаємодій. У низці робіт запропоновано використання permissioned-блокчейнів для обмежених середовищ, що дозволяє зменшити накладні витрати консенсусу та адаптувати систему до вимог промислових застосувань [15], [16].

Окремий напрям досліджень зосереджений на інтеграції блокчейн-рішень із хмарними сервісами та edge-вузлами. У таких підходах хмарні платформи виконують функції обробки та агрегації даних, тоді як блокчейн-реєстри забезпечують зберігання довірених записів про ідентичність і події [17]. Запропоновані архітектури демонструють покращення відмовостій-

кості та прозорості, однак часто не враховують обмеження обчислювальних ресурсів IoT-пристроїв, що призводить до перевантаження мережі або підвищеного енергоспоживання.

У роботах, присвячених управлінню ідентичністю в критичних інфраструктурах, акцент робиться на необхідності забезпечення безперервності функціонування систем, стійкості до атак і здатності до швидкого відновлення після інцидентів [18], [19]. Розглядаються підходи на основі багаторівневих моделей довіри, проте більшість із них залишаються концептуальними та не містять детальних механізмів інтеграції з реальними IoT-платформами та мікроконтролерними реалізаціями.

Водночас сучасні публікації демонструють зростаючий інтерес до оптимізації криптографічних механізмів для ресурсно-обмежених пристроїв, включаючи використання полегшених алгоритмів і адаптивних протоколів обміну [20]. Проте питання узгодження цих механізмів із блокчейн-інфраструктурою, а також ефективного управління життєвим циклом ідентичностей у динамічних IoT-мережах залишається недостатньо дослідженим.

Аналіз існуючих досліджень свідчить про відсутність комплексного підходу, який би поєднував децентралізоване управління ідентичністю, інтеграцію з хмарними сервісами та врахування обмежених ресурсів IoT-пристроїв у контексті критичних інфраструктур. Це зумовлює необхідність розробки нової моделі, здатної забезпечити узгодження вимог до продуктивності, масштабованості та достовірності ідентифікаційних даних у розподілених середовищах.

Мета і задачі дослідження

Метою дослідження є розробка моделі децентралізованого управління ідентичністю IoT пристроїв у критичних інфраструктурах на основі інтеграції хмарних сервісів і блокчейн-реєстрів з урахуванням обмежених ресурсів пристроїв, динамічності мережевого середовища та вимог до цілісності і достовірності даних. Для досягнення поставленої мети необхідно вирішити такі задачі:

- проаналізувати сучасні підходи до управління ідентичністю IoT пристроїв у критичних інфраструктурах та визначити їхні обмеження;
- розробити архітектуру системи децентралізованого управління ідентичністю на основі інтеграції IoT пристроїв, edge-вузлів, хмарних сервісів і блокчейн-реєстру;
- описати модель ідентичності IoT пристрою, структуру запису в блокчейн-реєстрі та модель транзакцій для зміни стану ідентичності;
- розробити алгоритм функціонування системи, що охоплює сценарії реєстрації, перевірки, оновлення та відкликання ідентичностей;
- оцінити ефективність запропонованої моделі за показниками затримок, енергоспоживання, використання пам'яті та достовірності ідентифікації.

Результати дослідження

Функціонування сучасних критичних інфраструктур характеризується високим рівнем інтеграції сенсорних, обчислювальних і комунікаційних компонентів, що формують середовище IIoT з розподіленою топологією та динамічною поведінкою вузлів. У таких системах значна кількість пристроїв, побудованих на базі мікроконтролерів, здійснює збір телеметричних даних і передає їх до центрів обробки для подальшого аналізу та прийняття управлінських рішень. Особливістю цього середовища є обмеженість обчислювальних ресурсів пристроїв, наявність великої кількості точок входу до системи, а також необхідність забезпечення достовірності ідентифікації кожного вузла при взаємодії з іншими компонентами.

У запропонованій архітектурі система децентралізованого управління ідентичністю формується як багаторівнева структура, що включає IoT пристрої, edge-вузли, хмарні сервіси та блокчейн-реєстр. IoT пристрої виконують функції генерації даних і первинної ідентифікації, використовуючи вбудовані криптографічні механізми для формування унікальних ідентифікаторів. Edge-вузли виступають проміжним рівнем обробки, здійснюючи агрегацію, попередню верифікацію та оптимізацію потоків даних перед передачею до хмарного середовища. Хмарні сервіси забезпечують масштабовану обробку, управління політиками доступу та координацію

взаємодії між компонентами системи. Блокчейн-реєстр використовується як розподілена база довіри, у якій зберігаються записи про ідентичності пристроїв, їхній стан та історію змін.

Схема взаємодії компонентів системи наведена на рис. 1. На цьому рисунку відображено багаторівневу організацію середовища, де IoT пристрої взаємодіють з edge-вузлами, які, у свою чергу, забезпечують обмін із хмарними сервісами та блокчейн-реєстром. Така організація дозволяє розподілити обчислювальне навантаження, зменшити затримки передачі даних і забезпечити підвищену стійкість до відмов окремих елементів системи. Взаємодія з блокчейн-реєстром здійснюється через спеціалізовані вузли, що підтримують консенсус і виконують функції верифікації транзакцій, пов'язаних із ідентичностями.

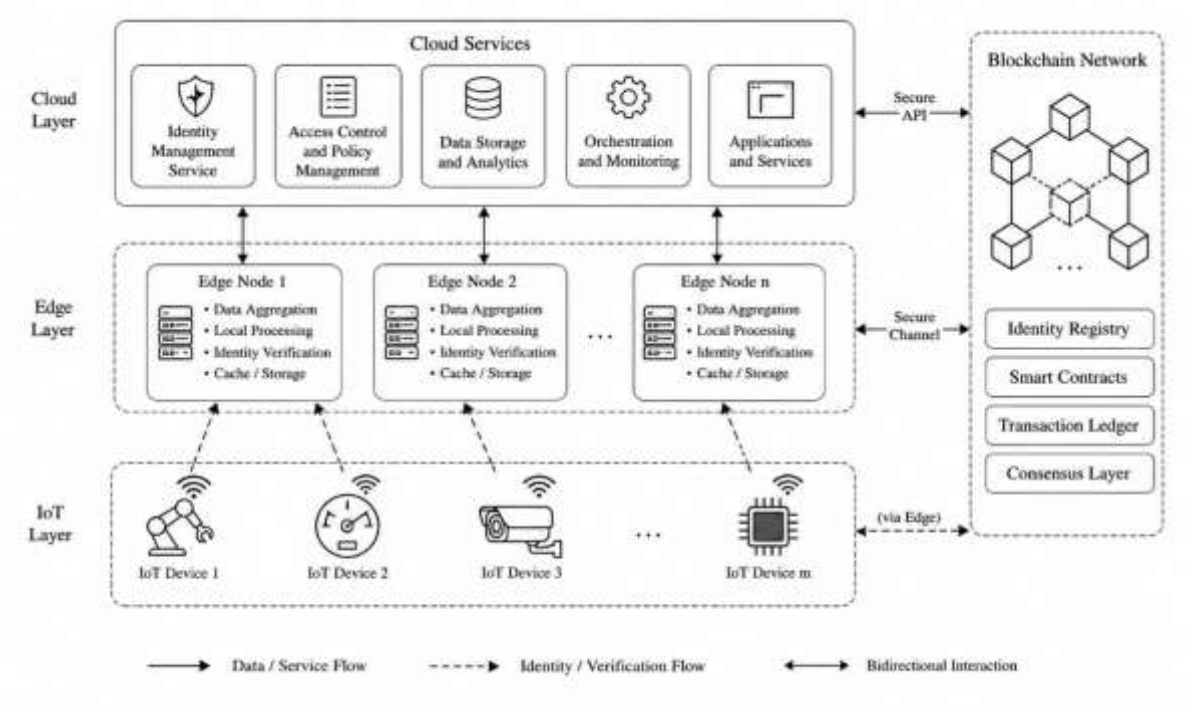

Рис. 1. Загальна архітектура системи децентралізованого управління ідентичністю IoT пристроїв

На схемі відображено багаторівневу організацію системи, що включає рівень пристроїв IoT, периферійний рівень, хмарні сервіси та блокчейн мережу. IoT пристрої генерують дані та формують первинну ідентичність, передаючи запити на edge nodes для попередньої обробки та локальної верифікації. Периферійний рівень виконує функції фільтрації, агрегації та зменшення навантаження на мережу.

Хмарні сервіси забезпечують централізовану координацію, управління політиками доступу та інтеграцію з прикладними сервісами. Блокчейн мережа виступає як розподілений реєстр, у якому зберігаються identity records, transaction logs та verification results. Взаємодія між компонентами реалізується через secure communication channels, що дозволяє забезпечити цілісність і узгодженість даних у всій системі.

Такий підхід дозволяє розмежувати функціональність між рівнями, мінімізувати затримки та забезпечити децентралізовану модель довіри без залежності від єдиного центру управління.

У межах формалізації моделі управління ідентичністю введено множину пристроїв $D = \{d_1, d_2, \dots, d_n\}$, кожен елемент якої відповідає окремому IoT вузлу. Кожному пристрою ставиться у відповідність множина ідентичностей $I = \{i_1, i_2, \dots, i_m\}$, що відображає можливість підтримки декількох контекстів взаємодії або ролей. Сукупність усіх змін станів ідентичностей описується множиною транзакцій $T = \{t_1, t_2, \dots, t_k\}$, які зберігаються у блокчейн-реєстрі та формують незмінну історію взаємодій.

Ідентифікатор пристрою розглядається як структурований об'єкт, що включає унікальний ID, криптографічну пару ключів та набір атрибутів, які характеризують функціональне призначення пристрою, його стан і рівень довіри. Формально ідентичність може бути представлена у вигляді кортежу (1):

$$i_j = \langle ID_j, K_j^{pub}, K_j^{priv}, A_j, S_j \rangle , \quad (1)$$

де ID_j – унікальний ідентифікатор, K_j^{pub} та K_j^{priv} – відкритий і закритий ключі відповідно, A_j – множина атрибутів, S_j – поточний стан ідентичності.

Життєвий цикл ідентичності описується як послідовність станів, що включає ініціалізацію, активне використання, модифікацію та відкликання. Перехід між станами моделюється через функцію (2):

$$S_j(t+1) = \Phi(S_j(t), t_k) , \quad (2)$$

де Φ визначає правило оновлення стану ідентичності під впливом транзакції t_k. Такий підхід дозволяє формалізувати динамічну поведінку ідентичностей у системі та забезпечити їх відстежуваність у часі.

Основні операції управління ідентичністю включають реєстрацію нового пристрою, автентифікацію під час взаємодії, оновлення атрибутів та відкликання у разі компрометації. Реєстрація реалізується як додавання нової транзакції до блокчейн-реєстру з початковими параметрами ідентичності. Автентифікація базується на перевірці криптографічного підпису та відповідності атрибутів у реєстрі. Оновлення передбачає зміну атрибутів або ключів із фіксацією змін у вигляді нової транзакції, тоді як відкликання відображається переходом ідентичності до неактивного стану.

Оцінка достовірності ідентичності здійснюється на основі узагальненої функції довіри, яка враховує історію транзакцій, актуальність атрибутів і цілісність записів у блокчейн-реєстрі. Формально рівень довіри до ідентичності може бути представлений як (3):

$$Trust(i_j) = \psi(H_j, V_j, C_j) , \quad (3)$$

де H_j – історія транзакцій ідентичності, V_j – валідність поточного стану, C_j – узгодженість записів у розподіленому реєстрі, а ψ – функція агрегації, що визначає інтегральний показник достовірності. Така модель дозволяє оцінювати ступінь довіри до кожного пристрою з урахуванням його поведінки в системі та забезпечує основу для прийняття рішень щодо доступу та взаємодії.

Блокчейн-механізм у запропонованій моделі використовується як розподілене середовище фіксації та верифікації станів ідентичностей IoT пристроїв, що забезпечує незмінність записів і узгодженість даних між усіма учасниками системи. На відміну від традиційних централізованих реєстрів, блокчейн дозволяє реалізувати децентралізовану модель довіри, у якій кожна зміна стану ідентичності підтверджується консенсусом мережі та зберігається у вигляді послідовності зв'язаних блоків.

Структура запису в реєстрі формується як агрегований об'єкт, що містить ідентифікатор пристрою, хеш його публічного ключа, множину атрибутів та службову інформацію щодо часу створення і стану. Кожен запис має вигляд (4):

$$R_k = \langle ID_j, H(K_j^{pub}), A_j, TS_k, S_j, H_{prev} \rangle , \quad (4)$$

де TS_k – часовий маркер транзакції, H_{prev} – хеш попереднього запису, що забезпечує ланцюгову структуру даних. Така організація дозволяє гарантувати цілісність і послідовність змін ідентичності, а також забезпечує можливість аудиту її життєвого циклу.

Модель транзакції для IoT ідентичності описується як формалізований запит на зміну стану або атрибутів ідентичності, який підписується приватним ключем пристрою або уповноваженого вузла. Транзакція визначається як (5):

$$t_k = \langle ID_j, Op_k, D_k, Sig_k, Ts_k \rangle , \quad (5)$$

де Op_k – тип операції, що може відповідати реєстрації, оновленню або відкликанню, D_k – набір змінюваних даних, Sig_k – цифровий підпис, що забезпечує автентичність джерела. Перед включенням до реєстру транзакція проходить процедуру верифікації, яка включає перевірку підпису, узгодженість із поточним станом ідентичності та відповідність політикам системи.

Алгоритм консенсусу адаптовано до умов обмежених ресурсів IoT-середовища шляхом перенесення основного обчислювального навантаження на edge- та спеціалізовані вузли ме-

режі. Використовується модифікований підхід, близький до Practical Byzantine Fault Tolerance, у якому обмежена кількість валідаторів забезпечує підтвердження транзакцій без необхідності виконання енергомістких операцій. У межах цієї моделі IoT пристрої не беруть участі у процесі консенсусу безпосередньо, а делегують функції перевірки edge-вузлам, що дозволяє суттєво знизити вимоги до їхніх ресурсів.

Процес взаємодії з блокчейн-реєстром передбачає послідовність дій, що починається з формування транзакції на рівні пристрою або edge-вузла, її передачею до мережі валідаторів, перевіркою та включенням до нового блоку. Верифікація ідентичності здійснюється шляхом запиту до реєстру з метою отримання актуального стану відповідного запису та перевірки його цілісності. Цей процес подано на рис. 2.

На схемі відображено послідовність взаємодії між IoT пристроєм, edge-вузлом, блокчейн-мережею та хмарним середовищем, що дозволяє забезпечити підтвердження ідентичності без прямої залежності від централізованого сервера.

Порівняльний аналіз різних типів блокчейн-рішень, що можуть бути використані в IoT-середовищах, наведено у табл. 1.

Інтеграція блокчейн-механізму з хмарними сервісами та edge-рівнем дозволяє сформувати гібридну архітектуру, у якій кожен рівень виконує специфічні функції. Edge-вузли забезпечують локальну обробку даних, кешування і попередню верифікацію ідентичностей, зменшуючи обсяг переданих даних і навантаження на мережу. Хмарні сервіси виконують функції централізованого управління політиками, аналітики та довгострокового зберігання даних.

Розподіл функцій між cloud та edge дозволяє мінімізувати затримки, пов'язані з передачею даних, і забезпечити оперативну реакцію системи на зміну станів пристроїв. При цьому критичні операції, пов'язані з перевіркою ідентичності, можуть виконуватися на edge-рівні без необхідності постійного звернення до хмари, що підвищує автономність системи.

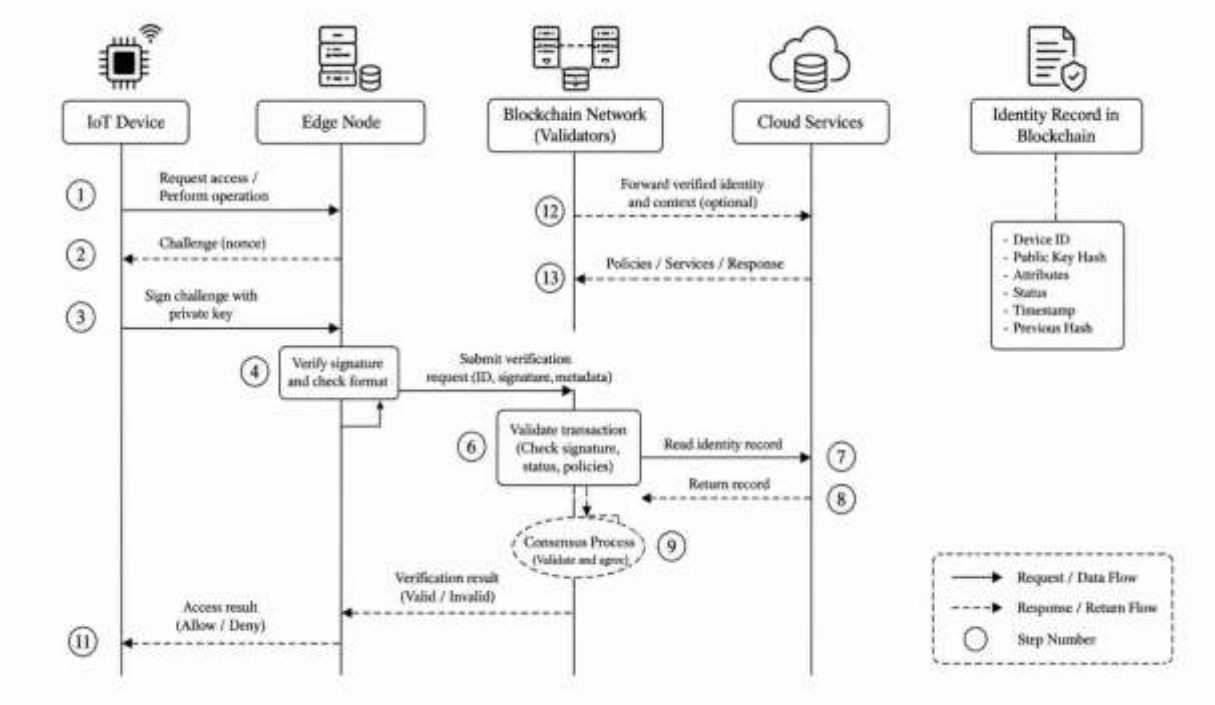

Рис. 2. Процес верифікації ідентичності

Таблиця 1

Порівняння блокчейн-рішень для IoT середовищ

Тип блокчейну	Рівень доступу	Продуктивність	Затримка	Придатність для IoT	Особливості застосування
Public	Відкритий	Низька	Висока	Обмежена	Висока децентралізація, значні витрати

Private	Закритий	Висока	Низька	Висока	Контроль доступу, централізоване управління
Consortium	Обмежено відкритий	Середня	Середня	Оптимальна	Баланс між довірою та ефективністю

Оптимізація обчислювального навантаження досягається шляхом адаптивного розподілу задач між рівнями системи з урахуванням доступних ресурсів. Зокрема, операції криптографічної обробки, що потребують значних ресурсів, виконуються на edge-вузлах або у хмарному середовищі, тоді як IoT пристрої здійснюють лише базові операції формування ідентичності та підпису транзакцій. Потоки даних між рівнями системи представлені на рис. 3.

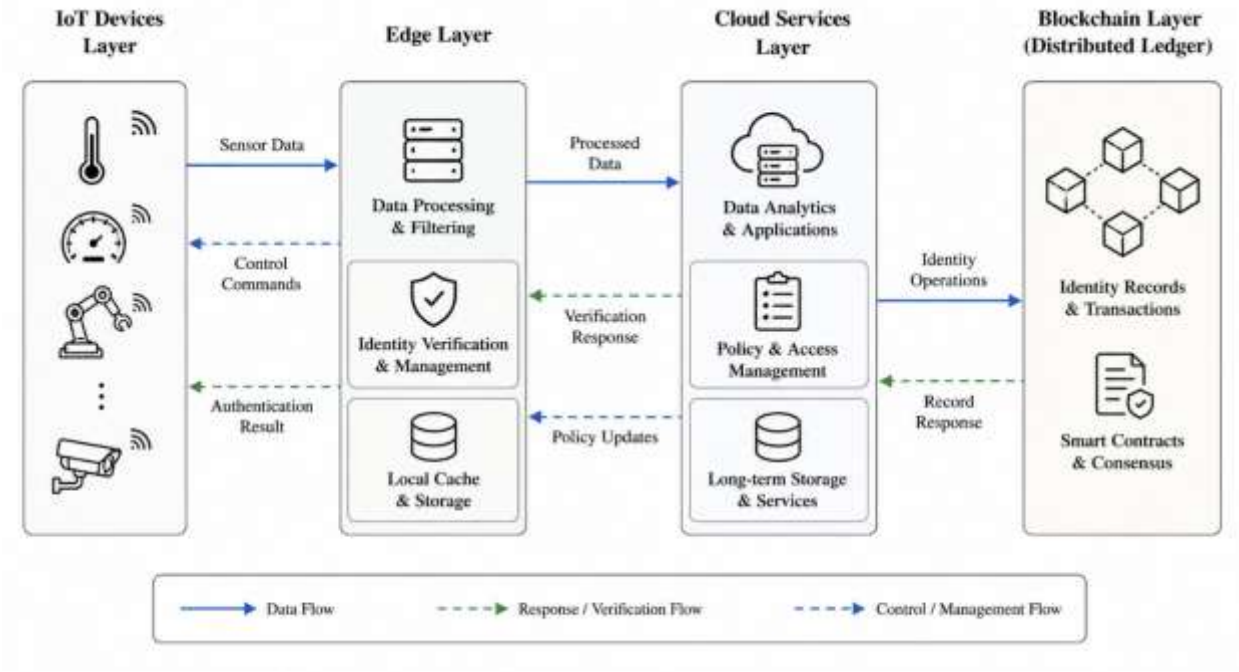

Рис. 3. Потоки даних між рівнями системи

На схемі відображено напрямки передачі телеметричних даних, ідентифікаційних запитів і відповідей верифікації, що забезпечують взаємодію між IoT, edge, cloud та блокчейн-рівнями.

Модель затримок і навантаження у системі описується як сукупність часових витрат на обробку, передачу та верифікацію даних на кожному рівні. Загальна затримка може бути представлена як $T_{total} = T_{IoT} + T_{edge} + T_{cloud} + T_{bc}$, де кожна складова відповідає затримці на відповідному рівні системи. Такий підхід дозволяє оцінити вплив архітектурних рішень на продуктивність системи та визначити оптимальні точки розподілу обчислювального навантаження.

Функціонування запропонованої моделі управління ідентичністю визначається послідовністю взаємопов'язаних операцій, що реалізують повний життєвий цикл ідентичності IoT пристрою у розподіленому середовищі. Алгоритм обробки ідентичності базується на узгодженій взаємодії між IoT пристроєм, edge-вузлом, хмарним середовищем та блокчейн-реєстром і передбачає поетапну перевірку, оновлення та фіксацію стану.

Початковим етапом є створення ідентичності пристрою, що включає генерацію криптографічної пари ключів та унікального ідентифікатора. Далі формується транзакція реєстрації, яка передається на edge-рівень для первинної перевірки. Edge-вузол виконує перевірку коректності даних і підпису, після чого транзакція надсилається до блокчейн-мережі. Після підтвердження транзакції запис додається до реєстру, що забезпечує його незмінність і доступність для подальших операцій.

У процесі експлуатації кожна взаємодія пристрою супроводжується перевіркою ідентичності, яка включає формування запиту, перевірку криптографічного підпису, звернення до реєстру та аналіз актуального стану. У разі зміни параметрів пристрою або політик доступу вико-

нується оновлення відповідного запису. Якщо виявляється відхилення у поведінці або загроза компрометації, ініціюється процедура відкликання ідентичності з подальшою фіксацією змін у системі.

Виділено три ключові сценарії функціонування. Підключення нового пристрою передбачає створення ідентичності та її реєстрацію в блокчейн-реєстрі. Перевірка ідентичності реалізується під час кожної взаємодії пристрою з іншими компонентами системи. У випадку компрометації виконується зміна статусу ідентичності або перевипуск ключів із фіксацією відповідних змін. Загальна логіка роботи системи представлена на рис. 4.

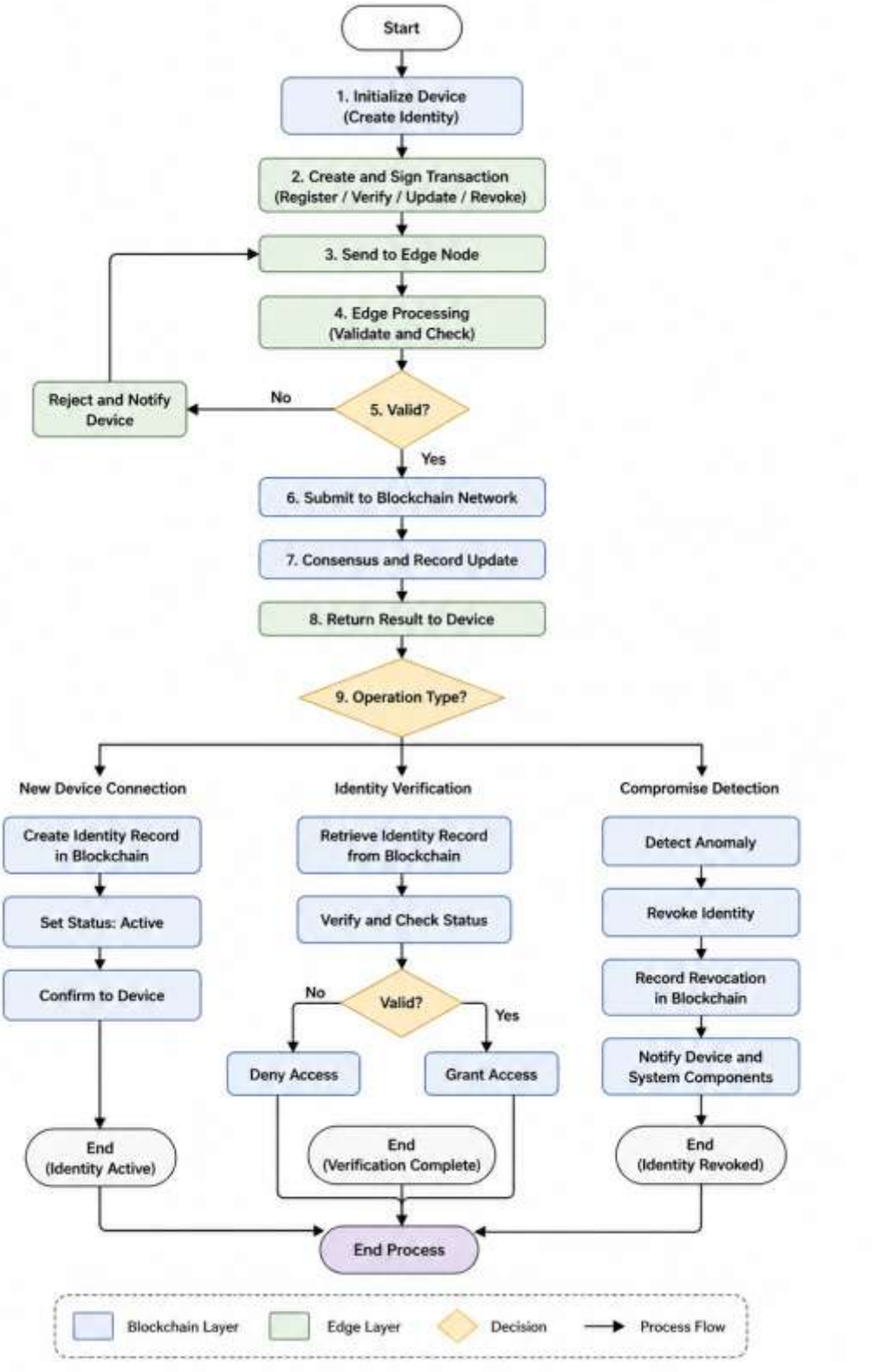

Рис. 4. Алгоритм роботи системи

На схемі відображено послідовність дій від моменту створення ідентичності до її перевірки та можливого відкликання, що дозволяє описати поведінку системи в умовах динамічного середовища.

Оцінювання ефективності запропонованої моделі базується на сукупності показників, що характеризують її придатність до використання у середовищах критичної інфраструктури з урахуванням обмежених ресурсів IoT пристроїв та вимог до достовірності ідентифікації. До основних показників віднесено затримку обробки запитів, енергоспоживання, обсяг пам'яті та рівень довіри до ідентичності.

Час обробки запиту визначається як сума часових витрат на кожному етапі обробки (6):

$$T = t_g + t_e + t_n + t_b + t_r \,, \tag{6}$$

де t_g – час генерації запиту на IoT пристрої (у середньому 5–8 мс), t_e – час обробки на edge-вузлі (10–15 мс), t_n – затримка передачі даних мережею (15–25 мс), t_b – час підтвердження транзакції у блокчейн-мережі (40–60 мс для permissioned середовища), t_r – час формування та повернення відповіді (5–10 мс). Таким чином, сумарна затримка становить у середньому $T \approx 75 - 118$ мс, що є прийнятним для більшості застосувань IIoT і демонструє зниження порівняно з класичними блокчейн-рішеннями, де затримки можуть перевищувати 200 мс.

Енергоспоживання IoT пристрою визначається сумарними витратами на обчислення та передачу даних (7):

$$E = \sum(e_c + e_t) \,, \tag{7}$$

де e_c – енергія, витрачена на криптографічні операції (наприклад, 12–18 мДж на одну операцію підпису), e_t – енергія передачі даних (8–12 мДж на пакет). За умови виконання частини обчислень на edge-рівні сумарне енергоспоживання одного циклу обробки зменшується до $E \approx 20 - 30$ мДж, що на 25–40% менше порівняно з підходами, де всі перевірки виконуються на пристрої.

Використання пам'яті визначається як сума ресурсів, необхідних для зберігання криптографічних ключів, атрибутів і локального кешу (8):

$$M = m_k + m_a + m_c \,, \tag{8}$$

де m_k – пам'ять для ключів (1–2 КБ), m_a – пам'ять для атрибутів (0.5–1 КБ), m_c – кеш перевірених записів (2–4 КБ). Загальний обсяг пам'яті становить $M \approx 7 - 4$ КБ, що дозволяє реалізувати модель навіть на мікроконтролерах класу STM32 або ESP32.

Рівень достовірності ідентичності визначається узгодженістю даних між локальним станом пристрою та записами у блокчейн-реєстрі і може бути представлений як (9):

$$D = \phi(i, h, s) \,, \tag{9}$$

де i – показник цілісності запису, h – історія змін, s – актуальність стану. Для permissioned блокчейн-середовища з обмеженою кількістю валідаторів рівень довіри наближається до $D \approx 0.97 - 0.99$, що суттєво перевищує централізовані системи, де цей показник знижується у разі компрометації центрального вузла.

Порівняльний аналіз показує, що централізовані системи характеризуються низькою затримкою (30–50 мс), але мають критичну залежність від одного центру та низьку стійкість до атак. Повністю децентралізовані блокчейн-рішення забезпечують високий рівень довіри, проте супроводжуються значними затримками (150–300 мс) і підвищеним енергоспоживанням. Запропонована модель дозволяє досягти компромісу між цими підходами, забезпечуючи помірні затримки, знижене енергоспоживання та високий рівень достовірності ідентифікації за рахунок інтеграції edge-рівня та оптимізованої взаємодії з блокчейн-реєстром.

Висновки та перспективи подальших досліджень

У статті розроблено модель децентралізованого управління ідентичністю IoT пристроїв у критичних інфраструктурах, що базується на поєднанні хмарних сервісів, edge-рівня та блокчейн-реєстрів. Запропонований підхід орієнтований на усунення основних недоліків централі-

зованих систем ідентифікації, зокрема залежності від єдиного центру довіри, обмеженої стійкості до відмов і складності масштабування в умовах динамічних IIoT середовищ.

У дослідженні представлено архітектуру системи, у якій IoT пристрої виконують базові операції створення ідентичності та підпису транзакцій, edge-вузли забезпечують попередню перевірку, агрегацію й кешування даних, хмарні сервіси відповідають за координацію, аналітику та управління політиками доступу, а блокчейн-реєстр використовується для незмінного зберігання записів про ідентичності, транзакції та зміну їхніх станів. Такий розподіл функцій дозволяє зменшити обчислювальне навантаження на ресурсно-обмежені пристрої та підвищити автономність системи.

Запропоновано структуру запису в блокчейн-реєстрі, модель транзакції для IoT ідентичності та алгоритм функціонування системи, що охоплює сценарії підключення нового пристрою, перевірки ідентичності, оновлення параметрів і відкликання у разі компрометації. Використання адаптованого механізму консенсусу з перенесенням основних обчислювальних операцій на edge- та спеціалізовані вузли дозволяє зберегти переваги децентралізованої довіри без надмірного навантаження на IoT пристрої.

Практична цінність запропонованої моделі полягає у можливості її застосування в енергетичних, транспортних, промислових та інших критичних інфраструктурах, де важливими є достовірність ідентифікації пристроїв, цілісність даних, безперервність функціонування та швидке реагування на компрометацію окремих вузлів. Наукова новизна полягає в інтеграції децентралізованого управління ідентичністю, блокчейн-реєстрів, хмарних сервісів і edge-обчислень у єдину модель, адаптовану до умов ресурсних обмежень і динамічної топології IIoT мереж.

Перспективи подальших досліджень доцільно спрямувати на експериментальну перевірку моделі на реальних або наближених до реальних IIoT стендах, оцінювання затримок, енергоспоживання та обсягу пам'яті для різних типів мікроконтролерів, а також на розробку прототипу з використанням permissioned-блокчейну та хмарно-периферійної інфраструктури.

Внесок авторів

Інна РОЗЛОМІЙ – концептуалізація дослідження, розробка методики децентралізованого управління ідентичністю IoT пристроїв, формалізація математичної моделі, підготовка висновків; Віра БАБЕНКО – аналіз наукових джерел, підготовка теоретичних основ дослідження, узагальнення підходів до інтеграції блокчейн-реєстрів і хмарних сервісів у критичних інфраструктурах; Сергій НАУМЕНКО – програмне забезпечення, моделювання алгоритму функціонування системи, підготовка структурних схем та аналіз потоків даних між рівнями системи; Наталія ЛАЩЕВСЬКА – збір і перевірка емпіричних даних, емпіричне дослідження показників затримок, енергоспоживання та використання пам'яті, порівняльний аналіз ефективності моделі.

Декларація про штучний інтелект

Під час підготовки статті використовувалися інструменти штучного інтелекту для побудови блок-схеми алгоритму функціонування системи (рис. 4) на основі авторського опису алгоритму та запропонованої моделі. Також інструменти штучного інтелекту застосовувалися для перевірки якості перекладу англомовної анотації. Усі наукові положення, результати дослідження, математичні моделі та висновки сформульовані авторами самостійно.

Конфлікт інтересів

Автори заявляють про відсутність конфлікту інтересів та підтверджують, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

Список використаної літератури

1. Dritsas, E., & Trigka, M. (2025). A survey on the applications of cloud computing in the industrial internet of things. Big Data and Cognitive Computing, 9(2), 44. https://doi.org/10.3390/bdcc9020044

2. Mostafa, A. M., Rushdy, E., Medhat, R., & Hanafy, A. (2023). An identity management scheme for cloud computing: Review, challenges, and future directions. Journal of Intelligent & Fuzzy Systems, 45(6), 11295–11317. https://doi.org/10.3233/JIFS-231911

3. Khayer, B., Mirzaei, S., Alavizadeh, H., & Salehi Shahraki, A. (2025). Blockchain for secure IoT: A review of identity management, access control, and trust mechanisms. IoT, 6(4), 65. https://doi.org/10.3390/iot6040065

4. Jimmy, M. J., John, N., Sreenath, V., Etemi, B. P., & Kanna, R. R. (2026). Identity and access management for IoT devices. In IoT Security (pp. 137–151). Elsevier. https://doi.org/10.1016/B978-0-443-34125-0.00020-9

5. George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51–75. https://doi.org/10.5281/zenodo.10639463

6. Yarmilko, A., Rozlomii, I., & Naumenko, S. (2024). Dependability of embedded systems in the industrial internet of things: Information security and reliability of the communication cluster. In Information Technology for Education, Science and Technics (pp. 235–249). Springer. https://doi.org/10.1007/978-3-031-71804-5_16

7. Hosseini, S. M., Ferreira, J., & Bartolomeu, P. C. (2023). Blockchain-based decentralized identification in IoT: An overview of existing frameworks and their limitations. Electronics, 12(6), 1283. https://doi.org/10.3390/electronics12061283

8. Buttar, A. M., Shahid, M. A., Arshad, M. N., & Akbar, M. A. (2024). Decentralized identity management using blockchain technology: Challenges and solutions. In Blockchain Transformations: Navigating the Decentralized Protocols Era (pp. 131–166). Springer. https://doi.org/10.1007/978-3-031-49593-9_8

9. Ramírez-Gordillo, T., Maciá-Lillo, A., Pujol, F. A., García-D'Urso, N., Azorín-López, J., & Mora, H. (2025). Decentralized identity management for internet of things devices using IOTA blockchain technology. Future Internet, 17(1), 49. https://doi.org/10.3390/fi17010049

10. Lizut, R. (2025). Security challenges of IoT integration in national and state critical infrastructures. Politics & Security, 13(3), 82–94. https://doi.org/10.54658/ps.28153324.2025.13.3.pp.82-94

11. Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. (2025). A literature review on security in the internet of things: Identifying and analysing critical categories. Computers, 14(2), 61. https://doi.org/10.3390/computers14020061

12. Almutairi, M., & Sheldon, F. T. (2025). IoT–cloud integration security: A survey of challenges, solutions, and directions. Electronics, 14(7), 1394. https://doi.org/10.3390/electronics14071394

13. Garzon, S. R., Yildiz, H., & Küpper, A. (2022). Decentralized identifiers and self-sovereign identity in 6G. IEEE Network, 36(4), 142–148. https://doi.org/10.1109/MNET.009.2100736

14. Ahmed, M. R., Islam, A. M., Shatabda, S., & Islam, S. (2022). Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access, 10, 113436–113481. https://doi.org/10.1109/ACCESS.2022.3216643

15. Nasir, N. M., Hassan, S., & Zaini, K. M. (2024). Securing permissioned blockchain-based systems: An analysis on the significance of consensus mechanisms. IEEE Access, 12, 138211–138238. https://doi.org/10.1109/ACCESS.2024.3465869

16. Al-Awamy, A. A., Al-Shaibany, N., Sikora, A., & Welte, D. (2025). Hybrid consensus mechanisms in blockchain: A comprehensive review. International Journal of Intelligent Systems, 2025(1), 5821997. https://doi.org/10.1155/int/5821997

17. Faure, E., Rozlomii, I., & Naumenko, S. (2025). Cryptographic load sharing method in critical infrastructure sensor networks. In Proceedings of the Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN'25) (pp. 5–15). https://ceur-ws.org/Vol-4024/paper01.pdf

18. Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. Information & Computer Security, 30(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

19. Qudus, L. (2025). Resilient systems: Building secure cyber-physical infrastructure for critical industries against emerging threats. International Journal of Research Publication and Reviews, 6(1), 3330–3346. https://doi.org/10.55248/gengpi.6.0125.0514

20. Rudnytskyi, V., Lada, N., Pochebut, M., Melnyk, O., & Tarasenko, Y. (2023). Increasing the cryptographic strength of CET encryption by ensuring the transformation quality of the information block. In 2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1–6). IEEE. https://doi.org/10.1109/DESSERT61349.2023.10416546

I. Rozlomii, V. Babenko, S. Naumenko, N. Lashchevska

A MODEL OF DECENTRALIZED IDENTITY MANAGEMENT OF IOT DEVICES IN CRITICAL INFRASTRUCTURES BASED ON CLOUD SERVICES AND BLOCKCHAIN REGISTRY

The paper addresses the problem of decentralized identity management for IoT devices operating within critical infrastructures based on cloud services, edge computing, and blockchain registries. The relevance of the study is driven by the rapid growth of heterogeneous devices in Industrial Internet of Things environments, the need for reliable device identification, data integrity assurance, and reduced dependence on centralized authentication services. It is shown that traditional identity management approaches are limited by the risk of a single point of failure, scalability constraints, increased latency, and insufficient adaptability to dynamic IoT network topologies.

A decentralized identity management model for IoT devices is proposed, in which the functions of identity generation, preliminary verification, record storage, and policy management are distributed across IoT devices, edge nodes, cloud services, and a blockchain registry. The paper presents the structure of identity records, a transaction model for updating identity states, and an operational algorithm covering key scenarios, including device onboarding, identity verification, parameter updates, and revocation in case of compromise. A key feature of the proposed approach is the offloading of computationally intensive operations to the edge layer and dedicated blockchain nodes, which significantly reduces the resource burden on constrained IoT devices.

The proposed model ensures improved scalability, enhanced fault tolerance, and higher trust in identity data compared to centralized solutions, while avoiding excessive overhead typical of fully decentralized blockchain systems. The practical value of the approach lies in its applicability to energy, transportation, and industrial infrastructures, where reliable identity management, data consistency, and system resilience are critical requirements.

Keywords: IoT devices, critical infrastructure, decentralized identity, cloud services, blockchain registry, edge computing.

Надійшла до редакції: 10.07.2026
Прийнята до друку: 24.07.2026
Опубліковано: 17.08.2026