DOI: https://doi.org/10.36910/6775-2524-0560-2026-62-23
УДК 004.056.55:004.774:004.9
Грищенко Вадим Юрійович, аспірант
https://orcid.org/0009-0004-4212-6661
Павленко Володимир Іванович, к.ф.-м.н., доцент
https://orcid.org/0000-0002-3958-0415
Відкритий міжнародний університет розвитку людини «Україна», м. Київ, Україна

АРХІТЕКТУРА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ ШЛЯХОМ ІНТЕГРАЦІЇ БЛОКЧЕЙНУ ТА OFF-CHAIN СХОВИЩ

Грищенко В.Ю., Павленко В.І. Архітектура обробки персональних даних шляхом інтеграції блокчейну та off-chain сховищ. У статті запропоновано гібридну архітектуру обробки персональних даних шляхом інтеграції технології блокчейн і off-chain-сховищ. Вона покликана вирішити суперечність між потребою в прозорості, незмінності та довірі з одного боку, і вимогами до конфіденційності, масштабованості та відповідності нормативним актам – з іншого. Централізовані рішення не гарантують довіри та є вразливими до внутрішніх загроз, тоді як повністю блокчейн-орієнтовані підходи не здатні забезпечити ефективну обробку об'ємних чутливих даних та реалізацію права на їх видалення. Архітектура, що пропонується, складається з п'яти основних компонентів: блокчейн-шару для фіксації транзакцій, off-chain-сховища для зберігання зашифрованих персональних даних, модуля контролю доступу з підтримкою RBAC/ABAC-моделей, API-шлюзів для зовнішньої інтеграції та смарт-контрактів для визначення політик доступу. Розглянуто модель обробки запитів на доступ до даних, що включає автентифікацію користувача, авторизацію, верифікацію хешу з блокчейну, зчитування інформації з офчейн-сховища та її дешифрування. Проведене моделювання підтверджує, що гібридна система має суттєві переваги у порівнянні з централізованими та блокчейн підходами. Зокрема, запропонована модель демонструє вдвічі меншу затримку в обробці запитів порівняно з повністю децентралізованими рішеннями, знижує навантаження на блокчейн-шар та зберігає можливість дотримання прав суб'єктів персональних даних.
Ключові слова: персональні дані, блокчейн, off-chain-сховище, гібридна архітектура, контроль доступу, інформаційна безпека.

Hryshchenko V.Y., Pavlenko V.I. Архітектура обробки персональних даних шляхом інтеграції блокчейну та off-chain сховищ. This paper presents a hybrid architecture for personal data processing that integrates blockchain technology with off-chain storage to address the growing challenges of transparency, trust, scalability, and regulatory compliance in data management systems. Traditional centralized solutions, while efficient in data storage and retrieval, often lack trustworthiness and are vulnerable to insider threats. Conversely, purely blockchain-based systems ensure data immutability and decentralized trust but struggle with processing latency, data deletion requirements, and scalability issues—especially in scenarios involving sensitive or high-volume personal data. The proposed architecture aims to balance these trade-offs by leveraging blockchain as a transparent and immutable layer for logging access events, storing metadata, and verifying data integrity via cryptographic hashes, while the actual encrypted personal data resides in flexible, scalable off-chain storage systems. This design enables compliance with data protection regulations such as the General Data Protection Regulation (GDPR), including support for the right to be forgotten and data minimization. The architecture consists of five interconnected components: a blockchain layer, an off-chain storage module, an access control subsystem, API gateways, and smart contracts. Access to data is regulated through attribute-based (ABAC) or role-based (RBAC) access models. A step-by-step model of query processing was developed, encompassing user authentication, authorization, hash verification via blockchain, retrieval from off-chain storage, and decryption. Simulation experiments were conducted to compare the performance of the hybrid model against purely centralized and blockchain-only architectures. Results showed that the hybrid solution offers a significant reduction in latency (140 ms versus 270 ms for blockchain-only) while maintaining cryptographic transparency and preserving compliance capabilities. The model also demonstrates reduced load on the blockchain layer and enables secure data deletion through controlled off-chain management. This solution is applicable in domains such as electronic health records, government registries, and financial services where a combination of confidentiality, auditability, and legal compliance is critical. The hybrid model bridges the gap between performance and trust, presenting a viable architecture for next-generation personal data processing systems.
Keywords: personal data, blockchain, off-chain storage, hybrid architecture, access control, information security.

Постановка проблеми та її зв'язок із важливими науковими чи практичними завданнями. Проблематика захисту персональних даних набуває особливої актуальності в умовах стрімкого зростання обсягів інформації, яка передається, обробляється та зберігається у цифрових системах [1]. Сучасні централізовані моделі управління даними мають низку критичних недоліків, зокрема вразливість до зовнішніх атак, зловживань з боку адміністраторів, а також проблеми із прозорістю доступу та відстеженням змін [2]. Порушення конфіденційності персональних даних стає регулярним явищем, що ставить під сумнів довіру користувачів до цифрових сервісів [3].

Водночас використання технології блокчейн дозволяє забезпечити незмінність записів, відстежуваність операцій і децентралізацію прийняття рішень [4]. Проте застосування блокчейну як основного сховища персональних даних є технічно та етично недоцільним через обмеження масштабованості, високу вартість зберігання, а також конфлікт із вимогами нормативних актів

© Грищенко В.Ю., Павленко В.І.

(наприклад, GDPR), які передбачають можливість видалення даних [5]. Це породжує потребу у створенні гібридних рішень, в яких блокчейн використовується для збереження контрольних точок, хешів або метаданих, а основний масив персональної інформації зберігається в off-chain сховищах з контрольованим доступом.

Вирішення цієї задачі потребує побудови архітектури, яка б поєднувала переваги обох підходів – незмінність, довіру і прозорість з боку блокчейну, а також гнучкість, масштабованість і відповідність регуляторним вимогам з боку традиційних сховищ. При цьому особливу увагу слід приділяти розмежуванню ролей учасників системи, моделі керування правами доступу, механізмам криптографічного захисту та інтеграції з наявною інфраструктурою.

Наукова значущість проблеми полягає у необхідності міждисциплінарного підходу до розробки архітектурних моделей, що включають елементи кібербезпеки, розподілених обчислень, баз даних та регуляторних обмежень. Практична важливість зумовлена потребою у реальних прикладних рішеннях для організацій, які обробляють великі обсяги персональних даних, таких як медичні установи, освітні заклади, фінансові структури, сервіси електронного урядування.

Метою дослідження є проєктування архітектури обробки персональних даних шляхом інтеграції блокчейну із off-chain сховищем, що дозволяє забезпечити контрольовану прозорість, незмінність критичних записів та відповідність вимогам конфіденційності.

Аналіз останніх досліджень та публікацій. У сфері захисту персональних даних активно досліджуються різні підходи до забезпечення прозорості, контролю доступу та довіри в інформаційних системах [6]. Окрему увагу привертає використання блокчейну як інструменту для забезпечення незмінності записів і формування механізмів довіри у децентралізованих середовищах [7]. У низці публікацій запропоновано моделі, в яких блокчейн використовується для реєстрації подій доступу до даних, збереження хешів файлів або транзакцій, пов'язаних з обробкою чутливої інформації. Наприклад, дослідження у сфері охорони здоров'я показують ефективність таких підходів для моніторингу доступу до електронних медичних карток, формування журналів активності та фіксації фактів зміни даних [8, 9].

Водночас у науковій літературі наголошується на обмеженнях блокчейну щодо обсягу даних, затримок обробки транзакцій і необхідності збереження конфіденційної інформації поза межами самого ланцюга. Це зумовлює інтерес до гібридних рішень, які передбачають інтеграцію блокчейну з off-chain-сховищами, такими як IPFS, традиційні бази даних або хмарні сервіси з контрольованим доступом [10, 11]. В роботах окреслюються різні схеми інтеграції: збереження лише хешів на блокчейні, використання смарт-контрактів для керування правами доступу до off-chain ресурсів, застосування атрибутивного шифрування для забезпечення конфіденційності.

Суттєву роль відіграють також дослідження, присвячені управлінню ідентифікацією користувачів та атестацією дій у розподілених системах. У публікаціях пропонуються механізми самоідентифікації (Self-Sovereign Identity), де користувачі самостійно керують своїми обліковими даними, використовуючи блокчейн як реєстр довірених перевірених тверджень [12, 13]. Це дозволяє зменшити залежність від централізованих органів та посилити контроль користувача над особистими даними.

Незважаючи на наявність численних концептуальних моделей, досі залишається відкритим питання побудови узгодженої архітектури, яка б забезпечувала не лише збереження і прозорість даних, а й відповідність правовим нормам щодо захисту персональної інформації, масштабованість для великої кількості користувачів і гнучкість доступу. Більшість рішень обмежується прототипами або прикладними кейсами в окремих доменах, з недостатньою увагою до архітектурних аспектів і моделювання інформаційних потоків між компонентами системи.

Виклад основного матеріалу й обґрунтування отриманих результатів дослідження. Одним із ключових викликів сучасного цифрового середовища є створення безпечної, надійної та масштабованої системи обробки персональних даних, яка водночас відповідатиме регуляторним вимогам та забезпечуватиме прозорість і контроль доступу. Використання виключно централізованих або, навпаки, повністю блокчейн-орієнтованих рішень не дозволяє досягти оптимального балансу між цими критеріями. З одного боку, централізовані сховища легко масштабуються, проте мають низький рівень довіри та є вразливими до внутрішніх загроз. З іншого боку, блокчейн гарантує незмінність і достовірність записів, але має обмеження щодо зберігання великих обсягів даних, обмежену швидкодію та суперечить вимогам, які передбачають можливість видалення персональної інформації.

У зв'язку з цим доцільним є впровадження гібридної архітектури, в якій поєднуються

© Грищенко В.Ю., Павленко В.І.

переваги обох підходів: блокчейн використовується для фіксації контрольних записів, хешів даних, подій доступу та верифікації, тоді як основні обсяги персональної інформації зберігаються в off-chain сховищах із гнучкими механізмами керування доступом. Така модель дає змогу досягти одночасно високого рівня довіри, контролю, масштабованості та відповідності нормативно-правовим вимогам, зокрема регламенту GDPR.

До основних функціональних вимог до запропонованої архітектури належать:

– незмінність і підтверджуваність записів дій щодо персональних даних;
– забезпечення конфіденційності та розмежування доступу;
– підтримка масштабування з можливістю обробки великої кількості запитів та зберігання значних обсягів даних;
– забезпечення права на забуття та видалення даних;
– аудит і прозорість усіх транзакцій, пов'язаних із доступом до інформації.

Розроблена архітектура може бути застосована в таких сферах, як медичні інформаційні системи (електронні медичні картки, реєстри пацієнтів), державні й освітні реєстри (зберігання даних про результати навчання, сертифікати), а також у фінансовому секторі (верифікація транзакцій, історії кредитування, реєстри клієнтів).

Запропонована архітектура включає п'ять основних компонентів: блокчейн-шар, off-chain-сховище, систему контролю доступу, API-шлюзи та смарт-контракти. Блокчейн відповідає за збереження хешів, подій доступу, записів підтвердження прав користувачів. Off-chain-сховище забезпечує зберігання зашифрованих персональних даних у базі даних або хмарному середовищі. Система контролю доступу керує авторизацією на основі атрибутів або ролей. API-шлюзи реалізують інтерфейси для взаємодії зовнішніх додатків із системою. Смарт-контракти фіксують правила перевірки доступу та забезпечують незмінність процедур.

Між компонентами існує чітка взаємодія. Запит від користувача надходить через API, далі система перевіряє права доступу, після чого відбувається зчитування гешу з блокчейну та порівняння його з обчисленим хешем із off-chain-сховища. У разі відповідності дані розшифровуються й надаються користувачеві. Усі дії логуються в блокчейні. Це гарантує незмінність та повну відстежуваність.

На рисунку 1 представлено загальну схему архітектури системи.

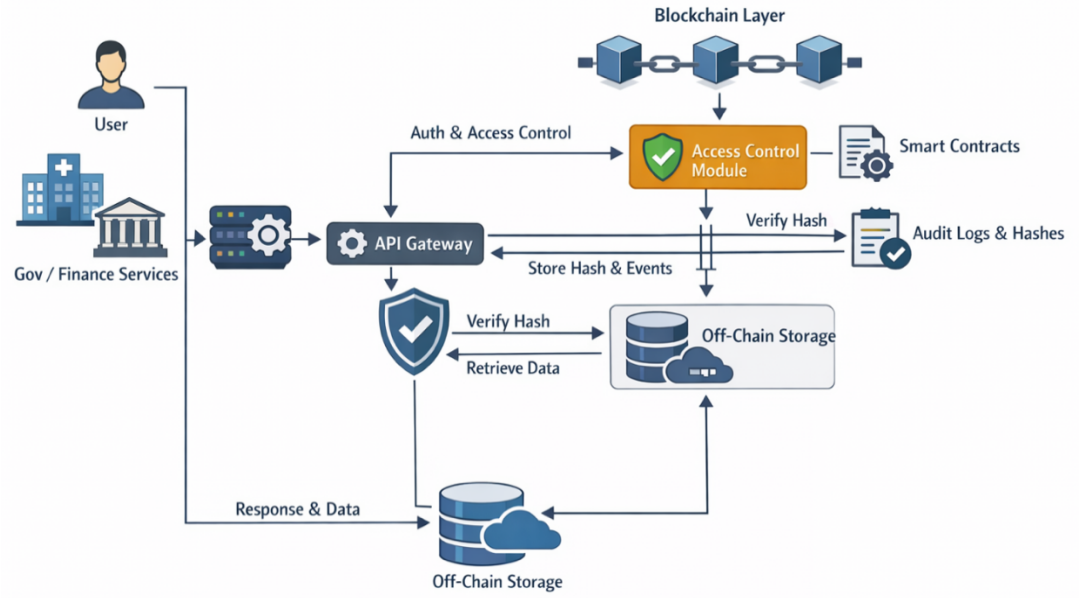

Рисунок 1 – Архітектура гібридної системи обробки персональних даних з інтеграцією блокчейн-шару та off-chain-сховища

Схема демонструє послідовність проходження запиту, взаємозв'язки між компонентами та точки фіксації критичних дій у блокчейні.

У таблиці 1 наведено узагальнені функції та ролі кожного з компонентів системи.

Таблиця 1 – Функції та ролі компонентів гібридної архітектури

Компонент	**Основна роль**
Блокчейн-	Реєстрація дій доступу, збереження хешів,

© Грищенко В.Ю., Павленко В.І.

шар	логування
Off-chain-сховище	Безпечне зберігання зашифрованих персональних даних
Система доступу	Авторизація, автентифікація, керування правами
API-шлюз	Інтерфейс для користувачів та зовнішніх сервісів
Смарт-контракти	Реалізація політик доступу, перевірка умов

Запропонована архітектура є основою для подальшого моделювання роботи системи, обґрунтування захисних механізмів та проведення оцінки ефективності.

Процес обробки запитів до персональних даних у запропонованій архітектурі реалізовано через чітку послідовність дій, що забезпечують автентифікацію, авторизацію, перевірку цілісності даних та їх безпечне отримання. Користувач або зовнішній сервіс ініціює запит через API-шлюз, після чого система автентифікує суб'єкта та виконує авторизацію на основі заздалегідь визначених політик доступу. У разі підтвердження прав, запит передається до модуля перевірки хешу, який звертається до блокчейн-шару для зчитування контрольного запису (гешу) щодо потрібного об'єкта даних. Отриманий хеш порівнюється з обчисленим хешем даних, отриманих з офчейн-сховища. У разі відповідності дані розшифровуються та передаються користувачеві.

Модель доступу реалізована із застосуванням механізмів RBAC (role-based access control) або ABAC (attribute-based access control), залежно від складності сценаріїв. У RBAC доступ надається відповідно до ролі суб'єкта (наприклад, лікар, адміністратор, пацієнт), тоді як ABAC враховує додаткові атрибути, такі як контекст запиту, тип даних, час або місце виконання дії. Це забезпечує гнучкість і дотримання принципу найменших привілеїв.

На рисунку 2 зображено блок-схему послідовності дій при обробці запиту.

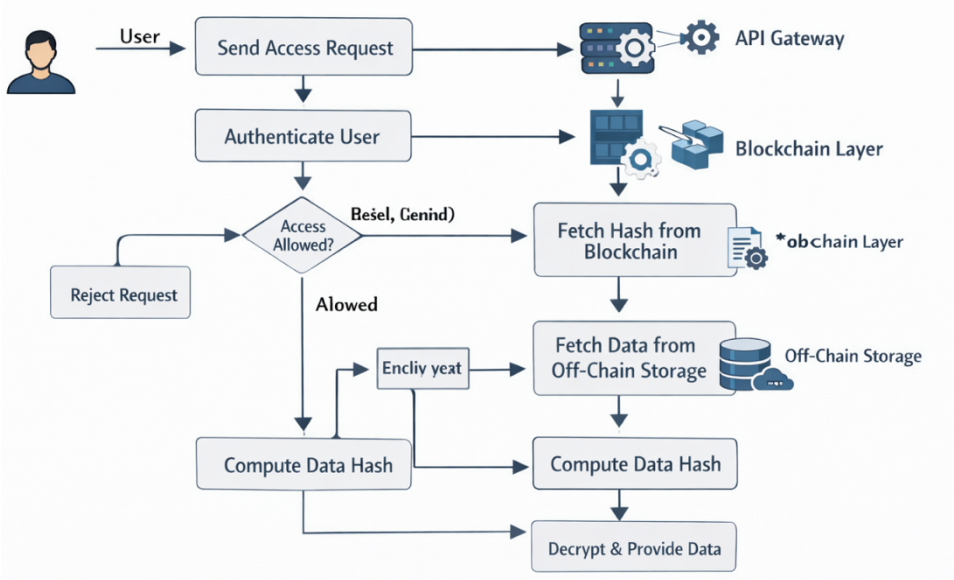

Рисунок 2 – Послідовність обробки запиту доступу до персональних даних у гібридній архітектурі

Схема демонструє типовий сценарій, який включає перевірку доступу, верифікацію цілісності, дії зі смарт-контрактом і передачу даних лише після дотримання всіх умов.

Забезпечення безпеки даних у гібридній архітектурі реалізовано на кількох рівнях. На рівні сховища персональні дані зберігаються в зашифрованому вигляді із застосуванням стійких алгоритмів симетричного шифрування, а доступ до ключів контролюється централізовано або із застосуванням систем керування секретами. Для передачі даних використовується шифрування TLS. На рівні блокчейн-шару всі операції журналюються у вигляді транзакцій із записом хешів дій, що гарантує їхню незмінність і можливість аудиту.

Асиметричне шифрування використовується при автентифікації учасників і верифікації підписаних транзакцій. Генерація та управління токенами доступу дозволяє контролювати сесії та запити користувачів, обмежуючи їхній термін дії та область застосування. Токени можуть

© Грищенко В.Ю., Павленко В.І.

додатково містити зашифровану інформацію про роль і рівень дозволу суб'єкта.

Архітектура враховує вимоги GDPR, зокрема право на забуття. Оскільки зберігання персональних даних відбувається поза блокчейном, видалення інформації з офчейн-сховища є можливим. У цьому разі в блокчейні зберігається запис про факт видалення без розкриття змісту. Мінімізація даних досягається шляхом збереження лише хешів і метаданих у ланцюзі блоків, а прозорість забезпечується відкритістю записів дій доступу без ідентифікації користувача, що запобігає витоку конфіденційної інформації.

Контроль транзакцій здійснюється через смарт-контракти, які автоматизують логіку перевірки умов доступу, обмеження за часом, типом даних або джерелом запиту. Журналювання в блокчейні забезпечує надійний слід дій, який не може бути змінено, що критично важливо для систем із високими вимогами до довіри.

Для оцінки ефективності запропонованої архітектури побудовано імітаційну модель, яка відтворює типову взаємодію між компонентами системи в умовах запитів на доступ до персональних даних. Модель реалізовано у середовищі Python із використанням бібліотек для моделювання мережевої взаємодії, черг повідомлень, обчислень хешів і криптографічних операцій. Структурно модель охоплює API-шлюз, блокчейн-шар, off-chain-сховище та модуль контролю доступу, з урахуванням затримок на кожному з етапів і ймовірності успішної авторизації.

Було проведено серію експериментів для різних сценаріїв: централізована модель без блокчейну, повністю децентралізована блокчейн-система, а також гібридна архітектура. У кожному сценарії вимірювалися: середній час обробки запиту, обсяг переданих даних, кількість записів у блокчейні, навантаження на off-chain-сховище та співвідношення вдалих/відхилених запитів. На рисунку 3 показано порівняння середнього часу обробки запиту для кожної з архітектур у рамках моделювання експериментів.

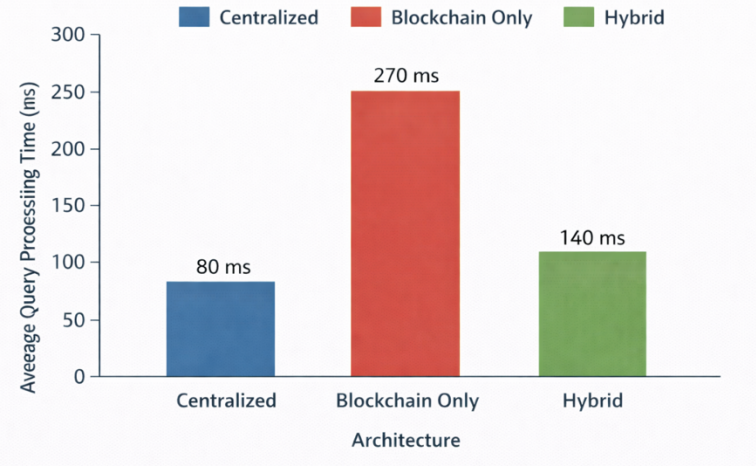

Рисунок 3 – Порівняння середнього часу обробки запиту в різних архітектурах

В таблиці 2 представлено узагальнені характеристики продуктивності кожного з досліджуваних підходів, що дозволяє наочно оцінити компроміси між продуктивністю, довірою та регуляторною відповідністю.

Таблиця 2. Характеристики продуктивності для трьох типів архітектур

Параметр	**Централізована**	**Блокчейн**	**Гібридна**
Середній час обробки запиту, мс	80	270	140
Обсяг переданих даних, КБ	250	80	160
Записи в блокчейні, шт	0	1	1
Навантаження на базу даних, %	100	0	60
Підтвердження хешу, % від запитів	0	100	100
Підтримка видалення даних	є	немає	є

Отримані результати демонструють, що гібридна архітектура забезпечує компроміс між продуктивністю, довірою та відповідністю нормативним вимогам. Зменшення затримок порівняно з блокчейн-only рішенням досягається за рахунок винесення зберігання даних за межі ланцюга блоків, тоді як контроль доступу та верифікація незмінності залишаються децентралізованими.

Запропонована архітектура має високу практичну цінність завдяки поєднанню прозорості

© Грищенко В.Ю., Павленко В.І.

дій у блокчейні з можливістю реалізації складної логіки доступу, гнучкого управління даними та відповідності регуляторним нормам, зокрема GDPR. Її впровадження можливе в системах, які обробляють персональні дані та потребують підвищеної довіри – зокрема в медичних, освітніх, адміністративних або фінансових реєстрах.

Наукова новизна полягає у створенні узгодженої моделі гібридної взаємодії, що формалізує розмежування функцій між шарами системи, дозволяє будувати математичні та імітаційні моделі, а також узагальнено підходить до впровадження політик доступу. У порівнянні з існуючими рішеннями, запропонована модель дає змогу адаптувати систему до конкретних законодавчих вимог, забезпечити масштабованість за рахунок off-chain-компонента та надати можливість аудитору повної прозорості всіх транзакцій без розкриття чутливої інформації.

Висновки та перспективи подальшого дослідження. У ході дослідження було розроблено архітектуру гібридної системи обробки персональних даних, що інтегрує переваги блокчейн-технологій і off-chain-сховищ. Такий підхід дозволяє досягти балансу між прозорістю, незмінністю та довірою з одного боку, і конфіденційністю, масштабованістю та відповідністю нормативним вимогам – з іншого. Запропонована модель передбачає чітке розмежування функцій між компонентами системи, що сприяє її гнучкості та адаптивності в різних прикладних галузях, зокрема в охороні здоров'я, фінансовому секторі, сфері державного управління. Проведене моделювання підтвердило ефективність запропонованої архітектури за показниками часу обробки запиту, навантаження на сховища та відповідності вимогам безпеки. У порівнянні з централізованими і повністю блокчейн-рішеннями гібридна система демонструє помірне навантаження, високу стійкість до маніпуляцій і здатність забезпечувати право на забуття.

Перспективи подальших досліджень передбачають удосконалення політик доступу на основі машинного навчання, впровадження адаптивного шифрування відповідно до чутливості даних, а також інтеграцію з сучасними цифровими ідентифікаційними системами. Окрему увагу слід приділити практичній реалізації запропонованої архітектури в умовах реальних інформаційних систем та проведенню оцінювання її продуктивності в динамічному середовищі з високою інтенсивністю запитів.

Список бібліографічного опису

1. Noninska, I., Romansky, R. Organization of technological structures for personal data protection. International Journal on Information Technologies and Security. 2022. Vol. 14. No. 1. P. 97–106.
2. Pestana, G., Sofou, S. Data governance to counter hybrid threats against critical infrastructures. Smart Cities. 2024. Vol. 7. No. 4. P. 1857–1877. https://doi.org/10.3390/smartcities7040072
3. Jamal, H., Algeelani, N. A., Al-Sammarraie, N. Safeguarding data privacy: strategies to counteract internal and external hacking threats. Computer Science and Information Technologies. 2024. Vol. 5. No. 1. P. 46–54. https://doi.org/10.11591/csit.v5i1.p46-54
4. Ahmed, S. Enhancing data security and transparency: The role of blockchain in decentralized systems. International Journal of Advanced Engineering, Management and Science. 2025. Vol. 11. No. 1. 593258. https://dx.doi.org/10.22161/ijaems.111.12
5. Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., Rana, F. A. Blockchain-based governance models in e-government: A comprehensive framework for legal, technical, ethical and security considerations. International Journal of Law and Management. 2025. Vol. 67. No. 1. https://doi.org/10.1108/IJLMA-08-2023-0172
6. Eyo-Udo, N. L., Apeh, C. E., Bristol-Alagbariya, B., Udeh, C. A., Ewim, C. P. M. The evolution of blockchain technology in accounting: A review of its implications for transparency and accountability. Account and Financial Management Journal. 2025. Vol. 10. No. 1. P. 2456–3374. https://doi.org/10.47191/afmj/v10i1.04
7. Voievodin, Y. V., Rozlomii, I. O. Advanced software framework for comparing balancing strategies in container orchestration systems. Proceedings of DOORS. 2024. April. P. 60–69. https://ceur-ws.org/Vol-3666/paper09.pdf
8. Alam, S., Bhatia, S., Shuaib, M., Khubrani, M. M., Alfayez, F., Malibari, A. A., Ahmad, S. An overview of blockchain and IoT integration for secure and reliable health records monitoring. Sustainability. 2023. Vol. 15. No. 7. Article 5660. https://doi.org/10.3390/su15075660
9. Kemalasari, N. P. Y., Putra, I. P. H. S. Protection of medical record data as a form of legal protection of health data through the personal data protection act. Journal of Digital Law and Policy. 2023. Vol. 2. No. 3. P. 111–118. https://doi.org/10.58982/jdlp.v2i3.338
10. Jayabalan, J., Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing. 2022. Vol. 164. P. 152–167. https://doi.org/10.1016/j.jpdc.2022.03.009
11. Voievodin, Y., Rozlomii, I., Yarmilko, A. Approach to evaluate scheduling strategies in container orchestration systems. Modeling, Control and Information Technologies. Proceedings of the International Scientific and Practical Conference. 2023. No. 6. P. 292–295. https://doi.org/10.31713/MCIT.2023.089
12. Lohar, S. N., Babar, S. D., Mahalle, P. N. A self-sovereign identity framework for context-aware decentralized identifier creation and credential verification. Engineered Science. 2025. Vol. 36. Article 1629. DOI:

© Грищенко В.Ю., Павленко В.І.

10.30919/es1629
13. Chan, W., Gai, K., Yu, J., Zhu, L. Blockchain-assisted self-sovereign identities in education: A survey. Blockchains. 2025. Vol. 3. No. 1. Article 3. DOI: https://doi.org/10.3390/blockchains3010003

References

1. Noninska, I., Romansky, R. Organization of technological structures for personal data protection. International Journal on Information Technologies and Security. 2022. Vol. 14. No. 1. P. 97–106.
2. Pestana, G., Sofou, S. Data governance to counter hybrid threats against critical infrastructures. Smart Cities. 2024. Vol. 7. No. 4. P. 1857–1877. https://doi.org/10.3390/smartcities7040072
3. Jamal, H., Algeelani, N. A., Al-Sammarraie, N. Safeguarding data privacy: strategies to counteract internal and external hacking threats. Computer Science and Information Technologies. 2024. Vol. 5. No. 1. P. 46–54. https://doi.org/10.11591/csit.v5i1.p46-54
4. Ahmed, S. Enhancing data security and transparency: The role of blockchain in decentralized systems. International Journal of Advanced Engineering, Management and Science. 2025. Vol. 11. No. 1. 593258. https://dx.doi.org/10.22161/ijaems.111.12
5. Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., Rana, F. A. Blockchain-based governance models in e-government: A comprehensive framework for legal, technical, ethical and security considerations. International Journal of Law and Management. 2025. Vol. 67. No. 1. https://doi.org/10.1108/IJLMA-08-2023-0172
6. Eyo-Udo, N. L., Apeh, C. E., Bristol-Alagbariya, B., Udeh, C. A., Ewim, C. P. M. The evolution of blockchain technology in accounting: A review of its implications for transparency and accountability. Account and Financial Management Journal. 2025. Vol. 10. No. 1. P. 2456–3374. https://doi.org/10.47191/afmj/v10i1.04
7. Voievodin, Y. V., Rozlomii, I. O. Advanced software framework for comparing balancing strategies in container orchestration systems. Proceedings of DOORS. 2024. April. P. 60–69. https://ceur-ws.org/Vol-3666/paper09.pdf
8. Alam, S., Bhatia, S., Shuaib, M., Khubrani, M. M., Alfayez, F., Malibari, A. A., Ahmad, S. An overview of blockchain and IoT integration for secure and reliable health records monitoring. Sustainability. 2023. Vol. 15. No. 7. Article 5660. https://doi.org/10.3390/su15075660
9. Kemalasari, N. P. Y., Putra, I. P. H. S. Protection of medical record data as a form of legal protection of health data through the personal data protection act. Journal of Digital Law and Policy. 2023. Vol. 2. No. 3. P. 111–118. https://doi.org/10.58982/jdlp.v2i3.338
10. Jayabalan, J., Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. Journal of Parallel and Distributed Computing. 2022. Vol. 164. P. 152–167. https://doi.org/10.1016/j.jpdc.2022.03.009
11. Voievodin, Y., Rozlomii, I., Yarmilko, A. Approach to evaluate scheduling strategies in container orchestration systems. Modeling, Control and Information Technologies. Proceedings of the International Scientific and Practical Conference. 2023. No. 6. P. 292–295. https://doi.org/10.31713/MCIT.2023.089
12. Lohar, S. N., Babar, S. D., Mahalle, P. N. A self-sovereign identity framework for context-aware decentralized identifier creation and credential verification. Engineered Science. 2025. Vol. 36. Article 1629. DOI: 10.30919/es1629
13. Chan, W., Gai, K., Yu, J., Zhu, L. Blockchain-assisted self-sovereign identities in education: A survey. Blockchains. 2025. Vol. 3. No. 1. Article 3. DOI: https://doi.org/10.3390/blockchains3010003

Історія статті:
Отримано: 10.02.2026 Доопрацьовано: 19.02.2026 Прийнято до друку: 23.03.2026 Опубліковано: 29.03.2026

© Грищенко В.Ю., Павленко В.І.