УДК 004.056.55:004.75:004.4 **doi: 10.26906/SUNZ.2025.2.210-217**

О. В. Шматко, О. Є. Рагулін, П. О. Кравченко, П. В. Буслов

Харківський національний університет радіоелектроніки, Харків, Україна

ДОСЛІДЖЕННЯ АРХІТЕКТУРНИХ РІШЕНЬ ДЛЯ ПОБУДОВИ БЕЗПЕЧНОЇ СИСТЕМИ ЗБЕРІГАННЯ ТА ПЕРЕДАЧІ КОНФІДЕНЦІЙНИХ ДАНИХ

Анотація. Актуальність. У сучасних умовах стрімкого розвитку цифрових технологій та зростання кіберзагроз захист конфіденційної інформації під час її зберігання та передачі є одним із ключових пріоритетів у проєктуванні інформаційних систем. Надійна архітектура таких систем забезпечує стійкість до атак, цілісність даних і контроль доступу. **Об'єкт дослідження:** архітектурні рішення для побудови програмного забезпечення захищеної системи зберігання та передачі конфіденційних даних. **Мета статті:** дослідження, проєктування та розробка архітектурних компонентів безпечної інформаційної системи, здатної забезпечити збереження конфіденційності даних у процесі передачі та зберігання. **Результати дослідження.** У статті представлено аналіз сучасних підходів до побудови захищених інформаційних систем, обґрунтовано вибір архітектурної моделі та програмних засобів. Розроблено прототип системи. Проведено тестування на відповідність вимогам захисту та продуктивності. **Висновки.** Запропоноване архітектурне рішення продемонструвало ефективність у забезпеченні цілісності, конфіденційності та доступності даних. Результати можуть бути використані для подальшого вдосконалення інформаційних систем у галузях, де обробляється критично важлива інформація.

Ключові слова: інформаційна безпека; конфіденційність; передача даних; зберігання даних; програмна архітектура; шифрування.

Вступ

Постановка проблеми. Останніми роками постійне зростання рівня економіки та якості життя спричинило суттєве зростання суспільного попиту на доступну та якісну медичну допомогу. Медична галузь перетворилася на одну з найбільших і найдинамічніших у світі, особливо після спалаху пандемії COVID-19, яка серйозно загрожувала здоров'ю населення, порушила функціонування глобальної економіки та призвела до суттєвого збільшення національних інвестицій у сферу охорони здоров'я [1]. Паралельно з цим, розвиток і впровадження сучасних технологій – зокрема штучного інтелекту, інтелектуальних діагностичних засобів і медичних інформаційних систем – сприяє трансформації охорони здоров'я у напрямі підвищення інтелектуальності, точності та цифровізації [2, 3].

У центрі цієї цифрової трансформації знаходяться медичні дані, які є основою для розбудови системи «розумної» та персоналізованої медицини. Вони відіграють ключову роль у біомедичних дослідженнях, розробці лікарських засобів, клінічних рішеннях і управлінні громадським здоров'ям. Водночас медичні дані мають складну структуру, обумовлену розмаїттям джерел, різноманітністю форматів і відмінностями у стандартах охорони здоров'я між регіонами. Через це вони розпорошені, мають несумісні формати та велику структурну гетерогенність, що ускладнює їх об'єднане управління та ефективне використання [4].

З метою подолання цих викликів було створено низку платформ для обробки медичних даних, які забезпечують стандартизований доступ до медичної інформації для лікарень, науково-дослідних інститутів, фармацевтичних компаній і регуляторних органів [5, 6]. Такі платформи агрегують дані з багатьох медичних установ, залучають фахівців для їх анотування та обробки за допомогою спеціалізованого програмного забезпечення й алгоритмів. Оброблені таким чином дані використовуються для створення моделей захворювань, які слугують основою для медичних досліджень [7], управління охороною здоров'я [8], державного планування [9] та розробки інноваційних препаратів [10].

Попри свою корисність, ці платформи мають істотні обмеження щодо можливості перевірки достовірності та цілісності медичних даних на всіх етапах – від збору до обробки та надання третім сторонам. Для таких користувачів, як наукові установи, фармацевтичні компанії чи органи державного управління, необхідне впровадження надійних механізмів, що дозволяють верифікувати як початкові дані, так і операції, що виконувалися під час їх обробки, а також кінцеві результати. Відповідно, усі етапи життєвого циклу медичних даних – включно з вхідними, проміжними та кінцевими даними, діями операторів і записами доступу – повинні бути прозорими, верифікованими та такими, що підлягають простежуваності [11].

Аналіз останніх досліджень і публікацій. У контексті зростання обсягів цифрових даних та активного поширення хмарних технологій, питання захищеного зберігання та передачі конфіденційної інформації є однією з головних проблем сучасної інформаційної безпеки. У працях [12, 13] підкреслюється важливість використання криптографічних алгоритмів у архітектурі інформаційних систем як основного інструмента забезпечення конфіденційності та цілісності даних. Одним із найпоширеніших підходів до побудови захищених систем є застосування симетричного та асиметричного шифрування, що було детально розглянуто в дослідженнях [14–16]. Алгоритми AES, RSA та ECC демонструють високу ефективність при обробці конфіденційної інформації у розподілених системах, однак вимагають оптимізації для роботи в обмежених обчислювальних середовищах [17].

У дослідженнях [18, 19] акцент зроблено на важливості побудови багаторівневої архітектури

інформаційної системи, що включає окремі модулі для зберігання, обробки, шифрування даних і моніторингу активності. Така модульність не тільки полегшує оновлення компонентів, але й сприяє масштабованості системи.

Питання безпечної передачі даних у відкритих мережах, включаючи інтернет та бездротові канали, розглядаються у роботах [20–21]. Пропонуються методи тунелювання, віртуальні приватні мережі (VPN), а також використання протоколів безпечного з'єднання, таких як TLS/SSL.

Окрему увагу приділено використанню хмарних сервісів і контейнеризації (Docker, Kubernetes) в архітектурі захищених систем [22, 23]. У таких умовах надзвичайно важливою є реалізація політик шифрування на рівні віртуальних машин і контейнерів.

Аналіз наукових джерел свідчить про необхідність комплексного підходу до проєктування систем захищеного зберігання і передачі даних — з урахуванням не лише криптографічних засобів, але й архітектурних, мережевих та політик доступу. Це створює підґрунтя для формування архітектурного рішення, представленого у цій статті.

Метою роботи є дослідження, проєктування та розробка архітектурних компонентів безпечної інформаційної системи, здатної забезпечити збереження конфіденційності даних у процесі передачі та зберігання.

Основний матеріал

Початкове застосування блокчейн-технології відбулося у 2008 році з появою криптовалюти Bitcoin. Три ключові характеристики — децентралізація, прозорість та конфіденційність — відрізняють блокчейн від інших технологічних рішень [1]. Саме ці властивості привернули увагу до можливого застосування блокчейну в інших галузях, орієнтованих на дані, зокрема в медицині [3]. Компанія IBM прогнозує значний вплив блокчейн-технологій у трьох основних напрямах охорони здоров'я: децентралізований обмін електронними медичними записами (EHR), адміністрування клінічних досліджень і дотримання нормативних вимог [4, 5].

У сучасному контексті блокчейн все частіше розглядається як ключова технологія для безпечного, прозорого та контрольованого управління даними в IoT-платформах. Застосування блокчейн у медицині дозволяє прискорити наукові дослідження, забезпечити захист конфіденційної інформації та створити нові канали співпраці між науковцями. Під час пандемії COVID-19 блокчейн продемонстрував ефективність у зборі та візуалізації даних, а також у боротьбі з маніпуляцією статистикою.

В роботі пропонується архітектура системи, реалізованої на основі Hyperledger Fabric, спрямована на забезпечення безпечного, надійного та контрольованого управління медичними даними в умовах багатосторонньої взаємодії між суб'єктами медичної сфери. Вона реалізує концепцію багаторівневої розподіленої системи, яка охоплює клієнтський рівень, рівень сервісної логіки, мережевий рівень розподіленого реєстру та інфраструктурний рівень зберігання даних. У такій архітектурі кожен структурний компонент виконує чітко визначену функцію, зберігаючи при цьому цілісність інформаційних потоків і відповідність стандартам інформаційної безпеки у сфері охорони здоров'я.

Клієнтський рівень представлено програмними інтерфейсами для трьох основних типів користувачів: пацієнтів, медичних працівників та адміністраторів. Застосунок для пацієнтів дозволяє керувати згодою на обробку персональних медичних даних та переглядати історію доступу до них. Медичний застосунок забезпечує введення нових медичних записів та запити на доступ до наявної інформації, а адміністративний інтерфейс використовується для конфігурації мережі, керування доступом та підтримки смарт-контрактів. Усі клієнтські застосунки взаємодіють з мережею за допомогою відповідних SDK, що реалізують механізми підпису, шифрування і надсилання транзакцій до блокчейн-мережі.

Сервісна логіка, що реалізується у вигляді незалежних прикладних сервісів, виконує основну бізнес-функціональність системи. Компонент автентифікації перевіряє сертифікати користувачів за допомогою Membership Service Provider (MSP), що функціонує в межах Fabric. Сервіс управління доступом обробляє запити на доступ, перевіряє дозволи та фіксує факти взаємодії з медичними даними у розподіленому реєстрі. Обробник медичних записів виконує синхронізацію між блокчейн-реєстром та зовнішнім сховищем, зберігаючи об'ємні або чутливі дані поза межами ланцюга блоків.

На рівні блокчейн-мережі функціонує інфраструктура Hyperledger Fabric, яка включає peer-вузли, ordering service, chaincode та інші допоміжні сервіси. Peer-вузли, що належать до організацій-учасників, приймають транзакції, виконують chaincode, зберігають журнали та забезпечують доступ до розподіленого реєстру. Ordering service формує блоки транзакцій і поширює їх серед peer-вузлів. Смарт-контракти, реалізовані як chaincode, виконують бізнес-логіку перевірки згод, реєстрації доступу та фіксації операцій. Верифікація всіх учасників, зокрема користувачів, застосунків і вузлів, здійснюється через MSP, який базується на сертифікатній інфраструктурі з використанням X.509-сертифікатів.

Для забезпечення ефективного зберігання медичних даних система використовує комбінований підхід, що поєднує збереження у розподіленому реєстрі (on-chain) і в зовнішніх базах даних (off-chain). У розподіленому реєстрі зберігається інформація про згоду, операції доступу та посилання на медичні записи, тоді як самі записи, через обсяг або конфіденційність, зберігаються у зовнішньому сховищі, наприклад, у PostgreSQL. Зв'язок між on-chain і off-chain елементами підтримується за допомогою хешів та ідентифікаторів, що гарантує контроль цілісності та узгодженості даних.

У контексті побудови децентралізованої системи для управління медичною інформацією модель даних має ключове значення для забезпечення структурованості, достовірності та відповідності право-

вим нормам. Оновлена модель охоплює чотири взаємопов'язані сутності: MedicalData, OperationalBehavior, User та Consent.

Сутність MedicalData описує кожен блок даних, що записується у блокчейн, із вказанням його типу, джерела, формату, стадії обробки та криптографічного підпису. Кожен медичний запис пов'язаний з операцією (OperationalBehavior), яка його згенерувала або модифікувала. Ця друга сутність відображає транзакційні дії в системі, їх авторство та входи/виходи у вигляді зв'язків з іншими медичними даними. Важливу роль відіграє атрибут OpSign, який виступає унікальним ідентифікатором кожної операції та пов'язує дії з результатами. Модель доповнюється сутністю User, яка репрезентує всіх учасників системи: пацієнтів, лікарів, адміністраторів або аудиторів. Кожен користувач має унікальний ідентифікатор, роль, криптографічний сертифікат та інформацію про організаційну приналежність. Це дозволяє контролювати права доступу та здійснювати персоніфіковану верифікацію транзакцій.

Сутність Consent формалізує процес надання або відкликання згоди користувачем на обробку його персональних медичних даних. Кожна згода пов'язується з конкретним користувачем, фіксується у вигляді транзакції в блокчейні, містить часові позначки, статус, а також може посилатися на відповідний DataSign. Завдяки цьому створюється юридично обґрунтована та технологічно верифікована модель управління доступом до чутливої інформації.

Загалом, запропонована структура забезпечує високий рівень простежуваності, контрольованості та відповідності принципам етичного поводження з персональними даними. Усі зв'язки моделі мають чітке семантичне обґрунтування та логічну відповідність вимогам до розподілених систем обміну медичними даними.

Концепція Data Lineage, або історії змін даних, у системах управління медичною інформацією, реалізованих на основі технологій розподіленого реєстру, виконує критично важливу функцію забезпечення простежуваності, достовірності та цілісності медичних записів протягом усього їх життєвого циклу. У запропонованій моделі, реалізованій у контексті Hyperledger Fabric, Data Lineage реалізується як послідовність зв'язаних транзакційних дій, які формують граф взаємозв'язку між первинними даними, операціями та результатами обробки (рис. 1).

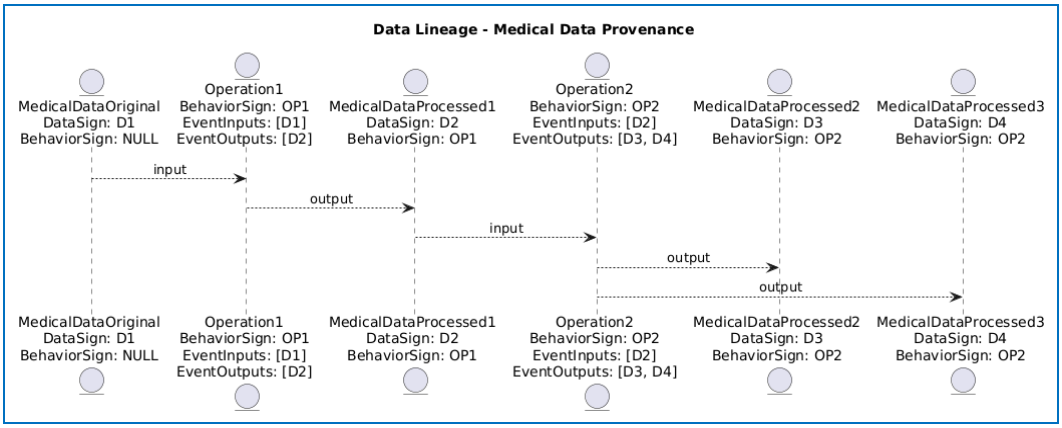

Рис. 1. Граф взаємозв'язку між первинними даними, операціями та результатами обробки

На логічному рівні, кожна одиниця медичних даних (MedicalData) має унікальний підпис (DataSign), який виступає криптографічним ідентифікатором конкретного об'єкта. Якщо запис є первинним, тобто ще не був оброблений у межах жодної транзакції, атрибут BehaviorSign, що вказує на породжуючу операцію, залишається порожнім (NULL). У цьому випадку об'єкт вважається джерелом походження (data origin).

Будь-яка транзакція, яка обробляє або модифікує медичні дані, представлена у системі як об'єкт типу OperationalBehavior. Така транзакція має унікальний ідентифікатор (BehaviorSign), та містить два основних компоненти: вхідні дані (EventInputs) і вихідні дані (EventOutputs), представлені у вигляді масивів DataSign. Таким чином, транзакція формує відображення даних до і даних після виконання певної операції, створюючи причинно-наслідкові зв'язки.

Наприклад, якщо первинний запис D1 є вхідним для транзакції OP1, яка породжує новий запис D2, то між D1 і D2 утворюється односпрямований зв'язок через OP1. Якщо ж D2 пізніше стає вхідним у транзакцію OP2, яка породжує D3 та D4, ланцюг змін продовжується. Така структура природно утворює орієнтований ациклічний граф (DAG), що дозволяє точно простежити шлях перетворення даних від початкового стану до будь-якого похідного.

У запропонованій медичній блокчейн-системі кожен об'єкт MedicalData є вершиною DAG, а кожна транзакція або операція OperationalBehavior, яка змінює ці дані, є окремим вузлом логіки перетворення. Зв'язки між вузлами реалізуються через пари:

- EventInputs — набір DataSign, що були використані як вхідні дані для операції;
- EventOutputs — набір DataSign, що були сформовані як результат цієї операції.

Таким чином, якщо Data D1 є початковим записом (із BehaviorSign = NULL), він може бути використаний в операції OP1, яка створює новий запис D2. Далі D2 може бути перетворений за допомогою іншої транзакції OP2 у записи D3 і D4. В результаті

цього виникає ланцюг перетворення даних, у якому кожен новий запис пов’язаний з попередніми на підставі визначених транзакцій, а весь ланцюг не містить циклів, що забезпечує однозначну історію змін.

У розширеній моделі також враховується інформація про ініціаторів змін (авторів транзакцій) та час виконання операцій, що дозволяє впроваджувати хронологічну простежуваність. Кожен вузол OperationalBehavior містить поля Author і Timestamp, що робить можливим формування темпоральних запитів і аналіз змін у динаміці.

Крім того, до DAG інтегруються об’єкти типу Consent, що встановлюють або обмежують доступ до певних DataSign. Це дозволяє поєднати технічну трасування з правовими аспектами обробки персональних даних.

Для перевірки ефективності створеної платформи управління медичними даними було проведено серію експериментів, що включали завантаження, запитування та простеження джерел медичних даних у блокчейн-мережі. Проведення експериментів охоплювало аналіз експериментального середовища, структури вхідних даних, а також оцінювання отриманих результатів.

Експериментальне середовище було реалізовано на базі трьох віртуальних серверів, розгорнутих у хмарному середовищі AWS EC2.

У рамках експерименту було розгорнуто сім організацій, що брали участь у симуляції взаємодії у сфері охорони здоров’я:

- 1 регуляторна організація (контроль доступу, аудит),
- 1 організація медичної хмари (централізоване сховище),
- 5 лікарень (розподілені учасники обміну даними).

Кожна організація мала три вузли типу peer, які брали участь у збереженні блоків, перевірці транзакцій та забезпеченні децентралізованої структури мережі. Кластер Orderer, відповідальний за узгодження транзакцій, було розгорнуто на сервері з найбільшою обчислювальною потужністю. Розподіл організацій між серверами відображено на рис. 2.

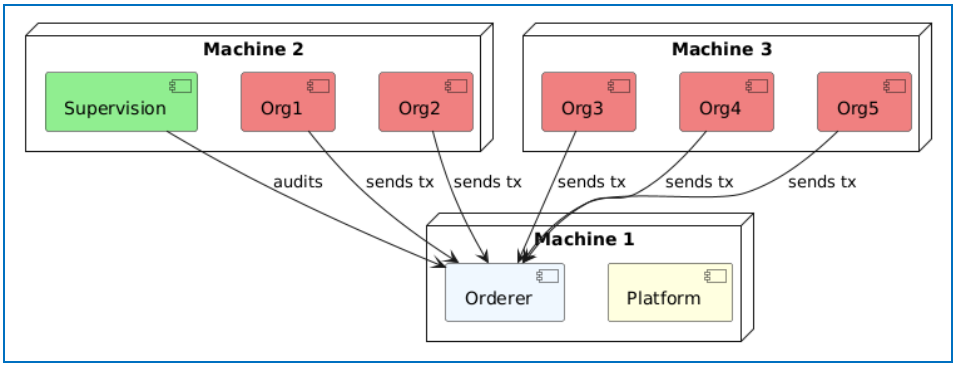

Рис. 2. Діаграма розгортання експериментальної платформи

Діаграма розгортання (рис. 2) моделює фізичне розміщення ключових компонентів Hyperledger Fabric у межах системи. Вузли мережі логічно поділені на три машини:

- Machine 1 виконує функції інфраструктури, зокрема обробку консенсусу через компонент Orderer та роботу з API або SDK через модуль Platform. Саме тут агрегуються транзакції, які надходять з організацій.
- Machine 2 слугує вузлом організаційної участі й нагляду, містить дві повноцінні організації (Org1, Org2) та компонент Supervision, який може виконувати функції аудитора, сертифікаційного органу (CA) або адміністрування консенсусу.
- Machine 3 об'єднує три організації (Org3, Org4, Org5), які ймовірно, беруть участь у мережі як endorsers, або забезпечують спеціалізовану обробку/читання транзакцій.

Логічні зв’язки вказують на взаємодію кожної організації з ордеринг-сервісом (Orderer), що відображає типову схему взаємодії Fabric peer-вузлів із ordering-сервісом для обробки транзакцій.

У рамках верифікації ефективності запропонованої платформи для управління конфіденційною медичною інформацією було сформовано експериментальний набір даних, який за структурою та обсягом відповідає типовим сценаріям використання в інформаційних системах охорони здоров’я. Дані було згенеровано штучно з метою забезпечення конфіденційності, однак вони відповідають загальноприйнятим стандартам представлення медичної інформації, зокрема HL7 та FHIR.

Експериментальні дані включали персоналізовані відомості про пацієнтів, історії хвороб, діагностичні результати, лікарські призначення, а також запити на доступ до медичних записів з боку різних організацій. Враховано також часову динаміку подій та взаємозв’язки між об’єктами, що дозволяє відтворити умови функціонування децентралізованої медичної системи в реальному часі.

Загальний обсяг експериментального набору склав понад 500 000 записів, які охоплюють понад 5 000 умовно унікальних пацієнтів, кілька сотень лікарів та десятки установ різного профілю. Дані подані у форматах JSON, XML та, частково, DICOM, що дозволяє адаптувати їх до потреб як внутрішнього зберігання в блокчейн-мережі, так і зовнішніх децентралізованих сховищ типу IPFS.

З метою оцінки продуктивності побудованої блокчейн-платформи управління медичною інфор-

мацією було проведено серію експериментів із завантаженням і запитом даних. Основною метою дослідження було вивчення впливу кількості організацій у мережі на ключові показники продуктивності, зокрема: швидкість надсилання запитів (Send Rate), максимальну затримку (Max Latency), мінімальну та середню затримки (Min / Avg Latency), а також пропускну здатність (Throughput).

Для тестування використовувався інструмент Hyperledger Caliper, у якому було налаштовано 10 віртуальних працівників (workers), які здійснили 100 000 випадкових операцій із завантаження та запитів медичних і поведінкових даних. Тестування проводилося на блокчейн-мережах із різною кількістю організацій (від 3 до 7). Після п'яти ітерацій кожного тесту було отримано усереднені результати. Результати експериментів свідчать, що із збільшенням кількості організацій спостерігається стабільна тенденція до зменшення показників пропускної здатності (TPS). Зокрема, для завантаження медичних даних при 3 організаціях throughput становив 1349,3 TPS, а при 7 організаціях – 782,8 TPS. Аналогічно зменшився send rate з 1361,7 до 794,7 TPS. При цьому максимальна затримка зросла з 2,05 с до 2,28 с, а середня – з 0,11 с до 0,37 с. Схожі результати були зафіксовані і для поведінкових даних. Так, при збільшенні кількості організацій з 3 до 7 throughput зменшився з 1247,1 до 778,6 TPS, а середня затримка зросла з 0,10 с до 0,37 с.

У разі виконання запитів до медичних даних, спостерігалася аналогічна тенденція: throughput зменшився з 1603,2 TPS до 1179,9 TPS, а середня затримка зросла з 0,09 с до 0,26 с. Поведінкові дані демонстрували схожі показники зниження, зокрема throughput зменшився з 1599,8 до 1173,8 TPS, а середня затримка зросла з 0,09 до 0,27 с.

Встановлено, що основною причиною зниження продуктивності при збільшенні кількості організацій є зростання витрат на досягнення консенсусу та міжорганізаційну комунікацію. Також відзначено, що throughput запитів стабільно перевищував throughput завантажень. Це пояснюється меншою обчислювальною складністю обробки запитів, які не потребують тривалих операцій запису до ланцюга блоків. Крім того, throughput завантаження медичних даних був дещо вищим за аналогічний показник поведінкових даних. Це пояснюється тим, що окремі об'єкти поведінкових даних мають більший обсяг, що спричиняє збільшення часу на їхнє оброблення.

У межах другого етапу експериментального дослідження було протестовано два підходи до реалізації простежуваності медичних даних: традиційний (naive) та графовий (на основі DAG — Directed Acyclic Graph). Тестування охоплювало перевірку прямого та зворотного простеження даних на основі п'яти варіантів обсягів експериментальних даних, що наведені в табл. 1.

У першому експерименті порівнювались середні показники продуктивності двох підходів. Для цього було використано 76 853 поведінкових даних і 200 000 медичних записів. Тестування здійснювалося за допомогою інструмента JMeter із використанням метрик: час виконання, кількість транзакцій за секунду (TPS), середній час відповіді на запит, пропускна здатність.

Таблиця 1 – **Порівняння TPS для різних методів простежуваності (на першому наборі даних)**

Метод	Тип трасування	TPS
Naive-forward	Пряме	0.54
Naive-backward	Зворотне	388.6
DAG-forward	Пряме	10 214
DAG-backward	Зворотне	10 086

Результати показали, що TPS для DAG-методу значно перевищує TPS для naive-підходу. Зокрема, TPS при прямому простеженні у naive-методі становив лише 0,54, що є недостатнім для практичного застосування. У той час як зворотне простеження в naive-підході демонструвало TPS, вищий приблизно у 718 разів, що свідчить про значну відмінність у часових витратах при різних типах трасування.

DAG-методи (як прямий, так і зворотний) показали TPS, що у 20–26 разів перевищує naive-зворотне простеження. Це пояснюється тим, що DAG реалізує попередньо побудовану структуру, яка дозволяє виконувати трасування без запитів до основного блокчейн-реєстру, обмежуючись операціями пошуку в графі.

У наступному експерименті було протестовано вплив довжини шляху трасування та обсягу даних на продуктивність системи. Встановлено, що TPS всіх методів знижується зі збільшенням довжини шляху, при цьому вплив обсягу даних є незначним. Зокрема, TPS DAG-підходів на довжині шляху 1 був у 20 разів вищим, ніж при довжині ≥7. Така залежність свідчить про тісний зв'язок продуктивності з кількістю кроків трасування в логічному ланцюзі подій (табл. 2).

Таблиця 2 – **Залежність TPS від довжини шляху для різних методів**

Довжина шляху	Naive-backward (TPS)	DAG-forward (TPS)	DAG-backward (TPS)
1	388.6	10 214	10 086
2	252.9	7 943	7 826
3	168.1	6 210	6 123
4	102.4	4 581	4 508
5	56.3	3 211	3 183
6	39.5	2 105	2 080
≥7	35.6	528	519

Для оцінки навантаження на платформу у частині хеш-верифікації було проведено заміри часу, необхідного на виконання базових операцій з блоками даних різного розміру. Результати наведені на рис. 3.

Аналіз даних показує, що час верифікації зростає майже лінійно зі збільшенням розміру пакету. Найменше навантаження спричиняє операція читання, тоді як оновлення є найбільш ресурсомісткою операцією, що потребує додаткових обчислень для перевірки цілісності попередніх та змінених станів. Згідно з отриманими результатами, при максималь-

ному розмірі пакету у 1000 байт час оновлення складає 490 мс, що є критичним показником при масштабних транзакційних навантаженнях.

Ще одним важливим експериментом було дослідження часу, необхідного для надання та відкликання згоди користувача на обробку медичних даних. Результати експерименту представлені на графіку на рис. 4. Аналіз сучасних підходів до зберігання, обміну та захисту медичних даних свідчить про активний розвиток блокчейн-орієнтованих медичних інформаційних систем, таких як MedRec [9], FHIRChain [14], MeDShare [15] та Ancile [8].

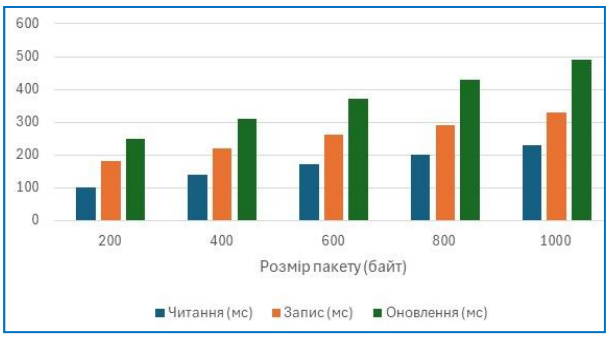

Рис. 3. Аналіз часу верифікації (мс)

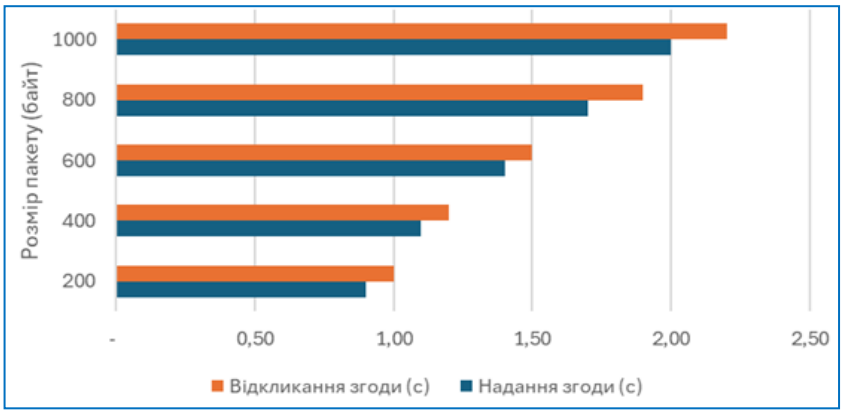

Рис. 4. Час обробки згоди (с)

Водночас, жодна з існуючих платформ не забезпечує повноцінної інтеграції усіх необхідних функцій для універсального управління електронними медичними записами, а також дотримання сучасних міжнародних стандартів, таких як HL7 FHIR.

На основі проведеного аналізу (табл.3) встановлено, що запропонована система, реалізована на базі Hyperledger Fabric, демонструє найбільш збалансовану архітектуру з точки зору функціональності, безпеки, масштабованості та сумісності. Вона забезпечує гібридну модель зберігання, де хеші та метадані зберігаються у блокчейні, а великі об'єми інформації — у зовнішньому репозиторії IPFS. Це дозволяє знизити навантаження на блокчейн без втрати можливості перевірки цілісності даних.

У контексті контролю доступу, запропонована система реалізує рольовий механізм на основі смарт-контрактів. Це забезпечує прозоре надання, обмеження або відкликання доступу до медичних записів пацієнта з юридичною чинністю. Аналогічний механізм підтримує Ancile [8], однак інші системи (зокрема MedRec) реалізують його частково або в обмеженому вигляді. Серед важливих переваг пропонованої платформи — повна підтримка HL7 FHIR, включаючи REST API, JSON-ресурси, авторизацію через OAuth2 та TLS-захист, що відображено в табл. 4. Це забезпечує інтеграцію з HIS, PACS та EHR-системами без потреби у дублюванні даних або зміні структур обміну. MedRec не реалізує FHIR, тоді як FHIRChain і MeDShare — лише частково.

Висновки

У ході виконання роботи було проаналізовано сучасний стан розробки блокчейн-рішень у сфері охорони здоров'я. Встановлено, що більшість існуючих систем (MedRec, FHIRChain, Ancile, MeDShare) реалізують обмежену функціональність: або зберігають лише метадані, або не забезпечують повної сумісності зі стандартами HL7/FHIR, або не підтримують масштабовану обробку транзакцій у реальному часі. Було виявлено, що лише окремі рішення частково реалізують контроль доступу через смарт-контракти, а повна простежуваність походження даних, як правило, відсутня.

Таблиця 3 – **Підтримка HL7 FHIR у різних системах**

Компонент FHIR / Технологія	Пропонована система	MedRec [24]	FHIRChain [25]	MeDShare [26]	Ancile [27]
REST API	Так	Ні	Так	Так	Так
JSON ресурси	Так	Так	Так	Так	Так
OAuth2 авторизація	Так	Ні	Так	Ні	Так
FHIR v4.0.1	Так	Ні	Так	Ні	Так
XML-підтримка	Ні	Ні	Ні	Ні	Ні
TLS-захист	Так	Ні	Так	Так	Так
AuditEvent (FHIR журнали)	Ні	Ні	Ні	Ні	Ні

Таблиця 4 – **Порівняльна характеристика пропонованої системи з іншими рішеннями**

Критерій	Пропонована система	MedRec	FHIRChain	MeDShare	Ancile
Блокчейн-платформа	Hyperledger Fabric	Ethereum	Ethereum	Fabric	Ethereum
Тип блокчейну	Приватний (permissioned)	Публічний	Публічний	Приватний	Публічний
Зберігання медичних даних	Гібридне (IPFS + hash)	Метадані	Метадані + FHIR	IPFS	Off-chain
Контроль доступу (смарт-контракти)	Так	Частково	Так	Так	Так
Надання/відкликання згоди	Так	Частково	Ні	Так	Так
Підтримка HL7 FHIR	Повна	Ні	Часткова	Часткова	Так
Аудит та журнал дій	Так	Частково	Частково	Так	Так
Простежуваність походження даних	Так	Ні	Ні	Частково	Так
Масштабованість (TPS)	Висока (≥100 TPS)	Низька	Середня	Висока	Середня
Інтероперабельність з HIS/EHR	Так	Ні	Так	Частково	Так

Запропонована система реалізує контрольовану децентралізацію з високим рівнем надійності, відмовостійкості та доступності. Смарт-контракти відіграють ключову роль у забезпеченні гнучкого та безпечного механізму доступу до інформації, дозволяючи пацієнтам надавати або відкликати згоду на обробку даних в інтерактивному режимі. Важливо, що вся історія змін, включаючи дії користувачів та логіку обробки, фіксується у блокчейні, що забезпечує повну прозорість та можливість аудиту. Порівняльний аналіз із наявними рішеннями показав, що розроблена система забезпечує найвищий рівень відповідності критеріям безпеки, функціональності, масштабованості та нормативної відповідності. Результати роботи мають практичну цінність для впровадження в реальні медичні установи, зокрема в контексті національної цифрової трансформації охорони здоров'я, а також можуть бути використані як основа для подальших наукових досліджень у галузі медичної інформатики, блокчейн-інфраструктур та захисту персональних даних.

СПИСОК ЛІТЕРАТУРИ

1. Борщ, В. В. (2019). Система охорони здоров'я як структурний елемент національної безпеки України. Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство, (23, Ч. 1), 19–23.
2. Борщ, В. І. (2018). Інтелектуалізація системи управління охороною здоров'я. Актуальні проблеми клінічної та профілактичної медицини, (2,№ 2-3), 11-20.
3. Гуменюк, Н. Є. (2024). Інтелектуалізація системи управління закладом охорони здоров'я (Doctoral dissertation, Тернопіль, ЗУНУ).
4. Косенко, В. В., & Невлюдов, І. Ш. (2019). Моделі структурного синтезу для управління параметрами інфокомунікаційних мереж систем критичної інфраструктури: монографія. Харків: ХНУРЕ.
5. Ляшук, А. (2023). Загрози і виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я. Публічне управління: концепції, парадигма, розвиток, удосконалення, (6), 113-121.
6. Сорока, І. М. (2023). Удосконалення медичних інформаційних систем як компонент розвитку системи охорони здоров'я. Вісник соціальної гігієни та організації охорони здоров'я України,(3), 62-69.
7. Mukherjee, P., Roy, S., Ghosh, D., & Nandi, S. K. (2022). Role of animal models in biomedical research: a review. Laboratory Animal Research, 38(1), 18. DOI:) https://doi.org/10.1186/s42826-022-00128-1
8. Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., ... & Mahamad, S. (2022, October). Recent advancements in emerging technologies for healthcare management systems: a survey. In Healthcare (Vol. 10, No. 10, p. 1940). DOI: https://doi.org/10.3390/healthcare10101940
9. Althunibat, A., Binsawad, M., Almaiah, M. A., Almomani, O., Alsaaidah, A., Al-Rahmi, W., & Seliaman, M. E. (2021). Sustainable applications of smart-government services: A model to understand smart-government adoption. Sustainability, 13(6), 3028. DOI: https://doi.org/10.3390/su13063028
10. Chen, Q., Yang, Z., Liu, H., Man, J., Oladejo, A. O., Ibrahim, S., ... & Hao, B. (2024). Novel Drug Delivery Systems: An Important Direction for Drug Innovation Research and Development. Pharmaceutics, 16(5), 674. DOI: https://doi.org/10.3390/pharmaceutics16050674
11. Zeydan, E., Arslan, S. S., & Liyanage, M. (2024). Managing Distributed Machine Learning Lifecycle for Healthcare Data in the Cloud. IEEE Access. DOI: 10.1109/ACCESS.2024.3443520
12. Can, O., Thabit, F., Aljahdali, A. O., Al-Homdy, S., & Alkhzaimi, H. A. (2023). A comprehensive literature of genetics cryptographic algorithms for data security in cloud computing. Cybernetics and Systems, 1-35. DOI: https://doi.org/10.1080/01969722.2023.2175117
13. Taherdoost, H., Le, T. V., & Slimani, K. (2025). Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review. Cryptography, 9(1), 17. DOI: https://doi.org/10.3390/cryptography9010017
14. Kshetri, N., Rahman, M. M., Rana, M. M., Osama, O. F., & Hutson, J. (2024). algoTRIC: Symmetric and asymmetric encryption algorithms for Cryptography--A comparative analysis in AI era. arXiv preprint arXiv:2412.15237. DOI: https://doi.org/10.48550/arXiv.2412.15237
15. Lalem, F., Laouid, A., Kara, M., Al-Khalidi, M., & Eleyan, A. (2023). A novel digital signature scheme for advanced asymmetric encryption techniques. Applied Sciences, 13(8), 5172. DOI: https://doi.org/10.3390/app13085172
16. Mihaljević, M. J., Knežević, M., Urošević, D., Wang, L., & Xu, S. (2023). An approach for blockchain and symmetric keys broadcast encryption based access control in IoT. Symmetry, 15(2), 299. DOI: https://doi.org/10.3390/sym15020299
17. Rehman, S., Talat Bajwa, N., Shah, M. A., Aseeri, A. O., & Anjum, A. (2021). Hybrid AES-ECC model for the security of data over cloud storage. Electronics, 10(21), 2673. DOI: https://doi.org/10.3390/electronics10212673

18. Gallo, G. D., & Micucci, D. (2025). Internet of Medical Things Systems Review: Insights into Non-Functional Factors. Sensors, 25(9), 2795. DOI: https://doi.org/10.3390/s25092795
19. Haritha, T., & Anitha, A. (2023). Multi-level security in healthcare by integrating lattice-based access control and blockchain-based smart contracts system. IEEE Access, 11, 114322-114340. DOI: 10.1109/ACCESS.2023.3324740
20. Rathod, T., Jadav, N. K., Alshehri, M. D., Tanwar, S., Sharma, R., Felseghi, R. A., & Raboaca, M. S. (2022). Blockchain for future wireless networks: A decade survey. Sensors, 22(11), 4182. DOI: https://doi.org/10.3390/s22114182
21. Yilmaz, S., & Dener, M. (2024). Security with Wireless Sensor Networks in Smart Grids: A Review. Symmetry, 16(10), 1295. DOI: https://doi.org/10.3390/sym16101295
22. Donca, I. C., Stan, O. P., Misaros, M., Stan, A., & Miclea, L. (2024). Comprehensive security for iot devices with kubernetes and raspberry pi cluster. Electronics, 13(9), 1613. DOI: https://doi.org/10.3390/electronics13091613
23. Nascimento, B., Santos, R., Henriques, J., Bernardo, M. V., & Caldeira, F. (2024). Availability, scalability, and security in the migration from container-based to cloud-native applications. Computers, 13(8), 192. DOI: https://doi.org/10.3390/computers13080192
24. Kashyap, N., Jeffery, S., & Agresta, T. (2024). From MedWreck to MedRec: A Call to Action to Improve Medication Reconciliation. Applied Clinical Informatics, 15(02), 230-233.
25. Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., ... & Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. Sustainability, 15(8), 6337. DOI: https://doi.org/10.3390/su15086337
26. Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain technology for electronic health records. International journal of environmental research and public health, 19(23), 15577. DOI: https://doi.org/10.3390/ijerph192315577
27. Lopez, L. J. R., Millan Mayorga, D., Martinez Poveda, L. H., Amaya, A. F. C., & Rojas Reales, W. (2024). Hybrid architectures used in the protection of large healthcare records based on cloud and blockchain integration: A review. Computers, 13(6), 152. DOI: https://doi.org/10.3390/computers13060152

Received (Надійшла) 14.03.2025
Accepted for publication (Прийнята до друку) 28.05.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Шматко Олександр Віталійович – кандидат технічних наук, доцент, доцент кафедри ЕОМ Харківського національного університету радіоелектроніки, Харків, Україна;
Oleksandr Shmatko – PhD, Ass.prof, Ass.prof of the Department of electronic computers, Kharkiv National University of radio electronics, Kharkiv, Ukraine;
e-mail: oleksandr.shmatko2@nure.ua; ORCID Author ID: https://orcid.org/0000-0002-2426-900X
Scopus Author ID: http://www.scopus.com/inward/authorDetails.url?authorID=6602623478&partnerID=MN8TOARS

Рагулін Олександр Євгенович – магістр кафедри ЕОМ, Харківського національного університету радіоелектроніки, Харків, Україна;
Oleksandr Rahulin – Master degree student, of the Department of electronic computers, Kharkiv National University of radio electronics, Kharkiv, Ukraine;
e-mail: oleksandr.rahulin@nure.ua; ORCID Author ID: https://orcid.org/0009-0008-2018-8262.

Кравченко Павло Олександрович – кандидат технічних наук, асистент кафедри ЕОМ, Харківського національного університету радіоелектроніки, Харків, Україна;
Pavlo Kravchenko – PhD, Assistant Lecturer of the Department of electronic computers, Kharkiv National University of radio electronics, Kharkiv, Ukraine;
e-mail: pavlo.kravchenko@nure.ua; ORCID Author ID: https://orcid.org/0000-0002-0456-3295;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57216151371.

Буслов Павло Володимирович – кандидат технічних наук, асистент кафедри БІТ Харківського національного університету радіоелектроніки, Харків, Україна;
Pavlo Buslov – PhD, Assistant Lecturer of the Department of cyber information technologies, Kharkiv National University of radio electronics, Kharkiv, Ukraine;
e-mail: p.buslov@ukr.net; ORCID Author ID: https://orcid.org/0000-0002-2558-4984;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57207767753&origin=resultslist.

Investigation of architectural solutions for building a secure system for confidential data storage and transmission

Oleksandr Shmatko, Oleksandr Rahulin, Pavlo Kravchenko, Pavlo Buslov

Abstract. Relevance. In the current landscape of rapid digitalization and increasing cyber threats, protecting confidential information during storage and transmission has become a critical priority in the design of information systems. A robust system architecture ensures resistance to attacks, data integrity, and access control. **Object of the study:** architectural solutions for developing secure software systems for storing and transmitting confidential data. **Purpose of the article:** to investigate, design, and develop architectural components of a secure information system capable of maintaining data confidentiality during transmission and storage. **Research results.** The article presents an analysis of current approaches to building secure information systems and justifies the selected architectural model and tools. A system prototype was developed. The system was tested for compliance with security and performance requirements. **Conclusions.** The proposed architectural solution demonstrated effectiveness in ensuring data integrity, confidentiality, and availability. The results can be applied to further improve information systems in fields dealing with sensitive or mission-critical information.

Keywords: information security; confidentiality; data transmission; data storage; software architecture; encryption.