DOI: https://doi.org/10.23939/csn2024.02.173

УДК 004.9; 007.5

АНОНІМІЗАЦІЯ ДАНИХ З ВИКОРИСТАННЯМ БЛОКЧЕЙН ТЕХНОЛОГІЇ: МОДЕЛЬ КЕРУВАННЯ ЖИТТЄВИМ ЦИКЛОМ ДАНИХ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРОЗОРОСТІ ТА ВІДПОВІДНОСТІ GDPR

А. С. Павлів

Національний університет "Львівська політехніка",
кафедра електронних обчислювальних машин
E-mail: andrii.s.pavliv@lpnu.ua

Швидке зростання обсягу персональних даних, що збираються та обробляються різними організаціями, створює значні виклики для забезпечення конфіденційності та безпеки інформації. Загальний регламент захисту даних (GDPR) Європейського Союзу визначає суворі вимоги до обробки, зберігання та видалення персональних даних, зокрема право на стирання, яке передбачає повне і безповоротне видалення інформації на запит користувача. Це створює проблеми для традиційних систем управління даними, які не можуть забезпечити автоматизоване видалення та надійний контроль за дотриманням термінів зберігання.

У даній статті запропоновано нову модель анонімізації даних на основі блокчейн-технологій, яка об'єднує смарт-контракти для автоматизації операцій з даними, використовуючи криптографічні методи для створення стійкої до деанонімізації системи. Модель забезпечує контроль та відповідність вимогам регуляторів, зберігаючи прозорість та безпеку всіх транзакцій.

Ключові слова: анонімізація даних, блокчейн, офчейн, право на стирання, смарт-контракти, управління даними.

1. Вступ

У сучасному цифровому середовищі, де кількість персональних даних, які обробляються організаціями, постійно зростає, зростають і ризики для конфіденційності та безпеки даних [1]. Впровадження Загального регламенту захисту даних (GDPR) [2] у Європейському Союзі запровадило суворі вимоги до зберігання та обробки даних, надаючи особливу увагу забезпеченню прав користувачів, таких як право на стирання [3]. Основною проблемою є забезпечення повної прозорості та можливості автоматизованого видалення даних при дотриманні вимог GDPR, оскільки традиційні системи часто не мають належних механізмів для дотримання цих вимог.

Існуючі методи анонімізації даних, такі як маскування, псевдонімізація та агрегація [4-6], мають суттєві недоліки щодо стійкості до деанонімізації, що дозволяє відновлювати початкові дані або ідентифікувати [7] особу. Анонімізація - це процес обробки даних, який робить ідентифікацію окремих осіб неможливою навіть за наявності додаткових зовнішніх даних [8]. Натомість, деанонімізація [9] є процесом відновлення або ідентифікації оригінальних даних з анонімізованих записів, що може призвести до розкриття особистої інформації. Тому, у контексті захисту конфіденційності, актуальним є питання пошуку нових підходів, які б забезпечували надійний захист даних та відповідність регуляторним вимогам.

Блокчейн-технології [10] пропонують можливість розв'язання цих проблем завдяки своїм децентралізованим [11] і прозорим властивостям. Проте, незмінність записів у блокчейні суперечить вимогам GDPR, що потребує інноваційних рішень для коректного видалення або зміни даних. Тому створення моделі, що поєднує анонімізацію з можливістю автоматизованого управління термінами зберігання даних, є актуальним завданням для наукової та практичної спільноти.

Запропоноване дослідження розглядає інтеграцію блокчейн-технологій із системою анонімізації даних, що забезпечує контроль, прозорість і відповідність регуляторним вимогам, вирішуючи ключові проблеми збереження конфіденційності та управління життєвим циклом даних.

2. Огляд літературних джерел

У сучасному контексті блокчейн-технології розглядаються як перспективний інструмент для забезпечення прозорості, безпеки та анонімності даних, особливо у сфері зберігання та обробки конфіденційної інформації. Проте блокчейн має власні обмеження, зокрема відсутність механізмів видалення даних, що ускладнює дотримання вимог GDPR, особливо права на стирання. Сучасні дослідження демонструють різноманітні підходи до подолання цих проблем, зокрема криптографічні методи, офчейн-рішення [12] та нульові докази з знанням (ZKP).

Одним із ключових напрямів є криптографічні методи для анонімізації даних. У роботі Wei Zhou et al. (2023) [13] досліджено використання кільцевих підписів (Ring Signatures) для забезпечення анонімності у блокчейн-системах, що робить транзакції невідстежуваними та захищає конфіденційність даних. Група дослідників на чолі з Quang et al. (2021) [14] пропонує гомоморфне шифрування для виконання обчислень над зашифрованими даними без їх розшифрування, що забезпечує конфіденційність інформації навіть у процесі аналізу. Інший підхід запропонували Haijun B et al. (2024) [15], які інтегрують мультипартійні обчислення для забезпечення стійкості до атак та підвищення конфіденційності у децентралізованих системах.

Локальна диференційована конфіденційність (LDP) є ще одним перспективним методом захисту даних, який передбачає додавання шуму до початкових даних, що мінімізує ризик їхньої деанонімізації навіть у разі компрометації. У дослідженні Wei Zhou et al. (2023) [16] представлено адаптивний алгоритм LDP для захисту транзакцій, який дозволяє зберігати корисність даних для аналітики, одночасно захищаючи їх від атак. Це є перспективним рішенням для систем з великою кількістю транзакцій, які вимагають високого рівня анонімності.

Офчейн-зберігання даних дозволяє зберігати великі обсяги даних поза межами блокчейну. У роботі Bandar Alamri (2021) [17] запропоновано інтеграцію блокчейн-технологій із зовнішніми сховищами, що дозволяє зберігати в блокчейні лише хеші або посилання на дані. Це значно полегшує видалення або модифікацію великих обсягів даних, зберігаючи цілісність блокчейн-записів. Такий підхід також робить можливим дотримання вимог GDPR, оскільки реальні дані можуть бути видалені з офчейн-сховищ, що відповідає вимогам "права на стирання".

Ще одним важливим методом є нульові докази з знанням (ZKP), які дозволяють підтвердити факт виконання певної операції (наприклад, видалення даних) без розкриття самої інформації. Дослідження Shashidhara R (2024) [18] показує, що ZKP можуть забезпечити високий рівень прозорості та анонімності у процесах підтвердження транзакцій і видалення даних. Схожі результати отримано у роботі Seval C et al. (2021) [19], де ZKP використовується для автоматизації контролю за видаленням даних, що забезпечує дотримання вимог GDPR.

Попри значний прогрес у розвитку технологій анонімізації даних, блокчейн-системи все ще стикаються з низкою серйозних проблем. Одним з найбільших викликів є реалізація принципів GDPR, зокрема "права на стирання". Оскільки блокчейн створює незмінні записи, це ускладнює видалення даних, яке необхідне для відповідності регуляторним вимогам. Для розв’язання цієї проблеми потрібно впроваджувати нові алгоритми, що можуть забезпечити ефективне видалення або, принаймні, унеможливити деанонімізацію користувачів без порушення цілісності системи.

Крім того, масштабованість залишається проблемною через високу обчислювальну складність криптографічних методів, що обмежує їхнє застосування в системах з великим обсягом даних. Актуальним залишається питання оптимізації алгоритмів для роботи в реальному часі, оскільки навіть незначні затримки під час обробки можуть призвести до зниження ефективності всієї системи. Особливо гостро стоїть проблема управління ключами шифрування. Відсутність гнучких і надійних механізмів управління ключами ускладнює реалізацію права на стирання, що потребує розробки підходів для знищення або динамічного оновлення ключів шифрування без ризику втрати доступу до інших частин даних.

Подальші дослідження повинні фокусуватися на розробці підходів, що інтегрують сучасні криптографічні алгоритми в блокчейн-системи, забезпечуючи баланс між незмінністю записів та можливістю видалення даних у випадках, коли це необхідно. Вдосконалення алгоритмів з акцентом на зниження їхньої складності, а також створення ефективних систем управління ключами дозволить блокчейну стати більш гнучким та адаптивним до вимог GDPR. Важливо також розробляти механізми, що забезпечують захист конфіденційності без необхідності розкриття інформації, використовуючи інноваційні підходи, як-от нульові докази знання (ZKP) та гомоморфне шифрування.

Таким чином, впровадження цих методів дозволить створити комплексні рішення для анонімізації, що відповідають вимогам GDPR, а також забезпечують прозорість та ефективність управління даними в умовах сучасних викликів, зокрема зростання обсягу транзакцій та різноманіття систем.

3. Мета та постановка задачі

У роботі розглядається проблема забезпечення конфіденційності даних та відповідності вимогам GDPR у системах, що використовують блокчейн-технології. Основним завданням є розробка моделі анонімізації даних з інтеграцією блокчейну та криптографічних методів, яка забезпечить стійкість до деанонімізації, прозорість дій над даними та можливість реалізації "права на стирання".

Мета дослідження полягає в створенні моделі, що дозволяє автоматизувати управління життєвим циклом даних, дотримуючись стандартів GDPR, з використанням смарт-контракту для керування термінами зберігання даних (SCDE).

4. Опис Моделі

Запропонована модель анонімізації даних з використанням блокчейн-технологій Рис. 1 створена для забезпечення прозорого та безпечного управління персональними даними відповідно до вимог GDPR. Модель передбачає використання смарт-контрактів для автоматизації ключових операцій, як-от керування термінами зберігання та реалізація "права на стирання". Завдяки комплексному підходу з інтеграцією криптографічних методів та офчейн-зберігання, модель мінімізує ризики деанонімізації та витоків даних.

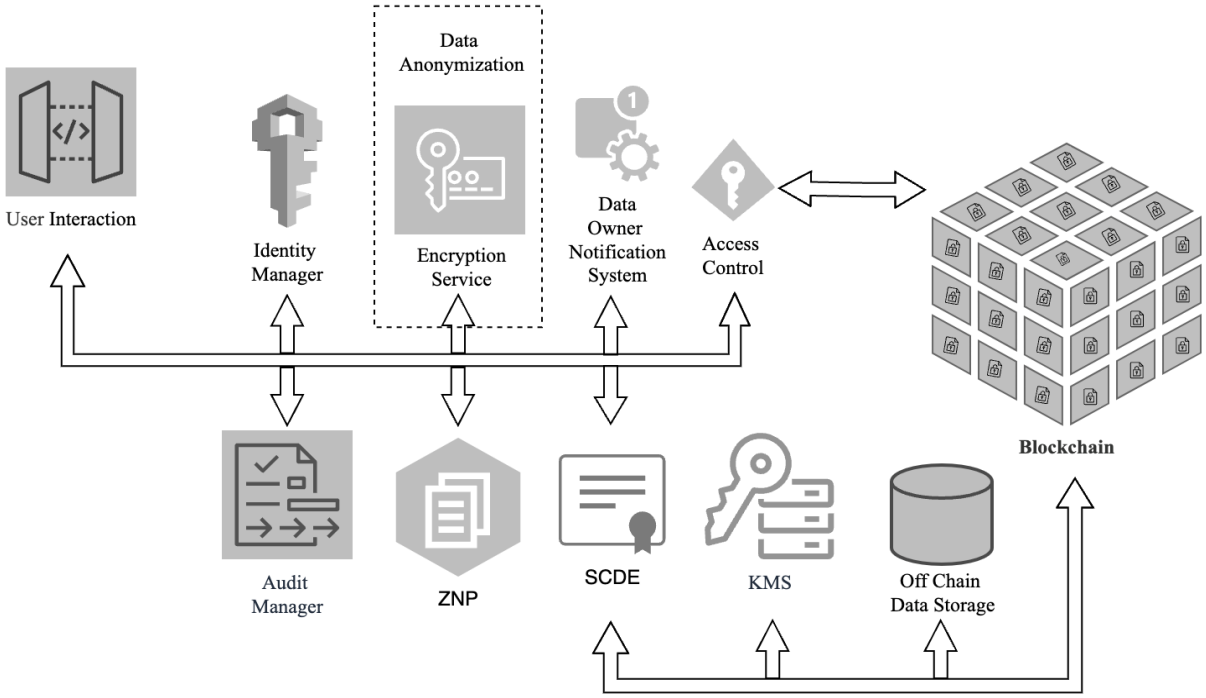

Рис. 1. Модель анонімізації даних.

Запропонована модель анонімізації даних з використанням блокчейн-технологій включає декілька ключових компонентів, кожен з яких виконує важливу роль у забезпеченні безпеки,

конфіденційності та відповідності нормативним вимогам, таким як GDPR. Центральним елементом є смарт-контракт для керування термінами зберігання даних (SCDE), який контролює всі операції з даними та автоматизує процеси їх видалення після закінчення терміну або за запитом користувача. Цей компонент не тільки фіксує всі дії в блокчейні, але й забезпечує дотримання політик зберігання, що мінімізує ризик людської помилки та підвищує прозорість процесів.

Для фізичного зберігання даних використовується офчейн-сховище (Off Chain Data Storage), яке дозволяє мінімізувати навантаження на блокчейн, зберігаючи у ньому лише хеші та метадані. Це рішення дає можливість ефективно видаляти або модифікувати дані у сховищі, не змінюючи основних записів у блокчейні, що важливо для відповідності вимогам GDPR. Всі дані перед передачею до сховища проходять процес шифрування за допомогою служби шифрування (Encryption Service), яка захищає їх від несанкціонованого доступу, навіть якщо офчейн-ресурси будуть скомпрометовані. Шифрування використовується для забезпечення цілісності та конфіденційності інформації, що зберігається.

Для управління шифрувальними ключами застосовується система управління ключами (Key Management System, KMS), яка генерує, зберігає та знищує ключі шифрування відповідно до встановлених політик. Якщо користувач подає запит на видалення даних або якщо термін їх зберігання завершується, KMS знищує відповідні ключі, що робить дані повністю недоступними, навіть у разі їхнього фізичного збереження у сховищі. Це реалізує принцип "права на стирання" без зміни блокчейн-записів, забезпечуючи незмінність та відповідність вимогам конфіденційності.

Основним елементом для забезпечення прозорості є блокчейн (Blockchain), який зберігає всі хеші та метадані транзакцій, створюючи незмінний журнал усіх операцій. Це дозволяє аудиторам перевіряти відповідність операцій регуляторним стандартам, забезпечуючи можливість детального контролю. Менеджер ідентифікації (Identity Manager, IDM) відповідає за аутентифікацію користувачів перед доступом до системи, перевіряючи права на виконання запитуваних операцій. Контроль доступу (Access Control) визначає політики доступу до даних на основі ролей користувачів, забезпечуючи гнучке управління доступом на основі атрибутів і контексту.

Менеджер аудиту (Audit Manager) зберігає детальний журнал усіх дій у системі, дозволяючи перевірити відповідність операцій нормативним вимогам і виконувати аналіз на відповідність політикам безпеки. Додатково у моделі використовується система повідомлень власника даних (Data Owner Notification System), яка інформує користувачів про запити на модифікацію чи видалення їхніх даних, забезпечуючи можливість підтвердження або скасування цих запитів, що гарантує додатковий рівень контролю.

Модуль нульових доказів знання (Zero-Knowledge Proof, ZNP) забезпечує перевірку операцій без розкриття самої інформації. Це особливо важливо для операцій видалення чи модифікації даних, де необхідно підтвердити факт дії без доступу до самих даних. Таким чином, завдяки чіткій взаємодії всіх компонентів, модель забезпечує комплексний захист та управління даними у блокчейні, зберігаючи високу прозорість та відповідність стандартам GDPR.

Операції з даними в моделі включають запис, читання, модифікацію, видалення та реалізацію права на стирання даних. Запропонована модель інтегрує різні криптографічні механізми та використовує блокчейн як основу для забезпечення незмінності, прозорості та високого рівня захисту операцій, що є критичним для відповідності вимогам GDPR.

Запис даних розпочинається з шифрування інформації перед її збереженням у зовнішньому офчейн-сховищі та створення хешу, що передається до блокчейну. Складність цієї операції визначається загальним часом, який залежить від шифрування, хешування та реєстрації транзакції у блокчейні. Загальна формула часу виконання виглядає наступним чином:

$$□_{□□□□□} = □_{□□□} + □_{h□□h} + □_{□□\_□□} ,$$

(1)

де: $□_{□□□}$ - час шифрування даних, $□_{h□□h}$ - час обчислення хешу, $□_{□□\_□□}$ - час реєстрації транзакції у блокчейні.

Читання даних здійснюється через перевірку прав доступу за допомогою модуля SCDE та компонента контролю доступу (Access Control). Після успішної авторизації система надає ключ

шифрування для розшифровки. Складність цієї операції можна оцінити за наступною формулою:

$$T_{read} = T_{dec} + T_{key\_access} + T_{access\_check},$$

(2)

де: T_{dec} - час розшифрування даних, T_{key_access} - час доступу до ключа шифрування, T_{access_check} - час перевірки прав доступу.

При модифікації даних створюється нова транзакція, яка містить новий хеш даних, замість видалення старих записів у блокчейні. Це дозволяє зберігати всю історію змін без порушення незмінності ланцюга. Формула для оцінки складності операції виглядає наступним чином:

$$T_{mod} = T_{write\_new} + T_{hash} + T_{blockchain\_update},$$

(3)

де: T_{write_new} - час запису нових даних, T_{hash} - час обчислення нового хешу, $T_{blockchain\_update}$ - час реєстрації оновленої транзакції у блокчейні.

Видалення даних ініціюється після завершення терміну зберігання або за запитом користувача. Після підтвердження видалення, SCDE ініціює процес стирання даних з офчейн-сховища та знищення відповідного ключа. Оцінка часу виконання:

$$T_{del} = T_{key\_destroy} + T_{offchain\_delete},$$

(4)

де: $T_{key\_destroy}$ - час знищення ключа, $T_{offchain\_delete}$ - час видалення даних з офчейн-сховища.

Реалізація права на стирання передбачає знищення всіх ключів шифрування для відповідних даних, що робить навіть зашифровану інформацію недоступною. Час виконання операції:

$$T_{erase} = T_{destroy} + T_{key\_destroy\_all},$$

(5)

де: $T_{key\_destroy\_all}$ - час знищення всіх пов'язаних ключів у системі KMS.

Ефективність різних операцій, таких як запис, читання, модифікація, видалення та стирання даних, була оцінена з точки зору їх складності та впливу на ресурси системи, що проілюстровано у Таблиці 1. Цей аналіз допомагає краще зрозуміти взаємодію компонентів моделі та можливі шляхи оптимізації для підвищення продуктивності та відповідності вимогам GDPR.

Таблиця 1

Оцінка ефективності операцій моделі

Операція	**Залучені компоненти**	**Оцінка ефективності**	**Опис операції**
Запис даних	SCDE, KMS, Off-chain Storage	Середня	Шифрування даних, збереження у сховище, запис хешу в блокчейн
Читання даних	SCDE, KMS, Off-chain Storage, Access Control	Висока	Перевірка прав доступу, розшифровка даних, передача запиту
Модифікація	SCDE, KMS, Off-chain Storage	Середня	Створення нової транзакції, оновлення хешу та метаданих
Видалення	SCDE, KMS, Off-chain Storage	Висока	Знищення ключа, видалення даних зі сховища
Стирання	SCDE, KMS	Дуже висока	Повне знищення всіх ключів, що робить дані недоступними навіть у зашифрованому вигляді

Завдяки чітко розподіленим ролям та ефективній взаємодії компонентів модель забезпечує комплексний підхід до анонімізації даних у блокчейні. Смарт-контракт SCDE, інтеграція з KMS та блокчейн-мережа дозволяють не лише автоматизувати процеси керування даними, але й забезпечують прозорість, незмінність та високий рівень захисту, що є критичними аспектами для реалізації регуляторних вимог та захисту конфіденційності користувачів.

5. Результати дослідження

Анонімізація даних стала важливим аспектом у контексті забезпечення конфіденційності та захисту інформації. З розвитком технологій, зокрема блокчейн, з'явилася можливість створити ефективну модель анонімізації, що відповідає сучасним вимогам безпеки. Ця апробація базується на архітектурі та концептуальній моделі анонімізації даних, зосереджуючись на можливих результатах, які можуть бути досягнуті в рамках реалізації цієї моделі.

Апробація запропонованої моделі була проведена для оцінки ефективності її архітектури у контексті вимог GDPR. Основною метою було визначення стійкості до різних типів атак та забезпечення надійності процесів анонімізації і реалізації права на стирання. У ході дослідження проводилось моделювання можливих загроз, аналіз продуктивності та відповідності системи регуляторним вимогам.

Модель протестована на стійкість проти атак на розкриття членства, розкриття атрибутів та атак схожості [20-23]. Під час таких атак зловмисники намагаються ідентифікувати певних користувачів або виявити атрибути, що належать конкретним особам. Для протидії цим загрозам у моделі використовуються динамічні алгоритми управління ключами та методи шифрування, що дозволяють обмежити доступ до даних навіть у разі компрометації частини системи. За рахунок використання нульових доказів знання (ZKP) вдалося підтвердити видалення або модифікацію даних без розкриття самого вмісту, що значно підвищує конфіденційність та прозорість операцій.

Таблиця 2 включає опис політик безпеки та перевірок, які активуються у відповідь на конкретні атаки:

Таблиця 2

Відповідності політик та перевірок

Тип Атаки	**Ціль Атаки**	**Компоненти для Захисту**	**Результат Перевірки**
Атака на розкриття членства	Виявлення участі певного користувача в системі	Система Управління Ключами (KMS), Блокчейн	Атака Відбита: Доступ до ключів заблоковано
Атака на розкриття атрибутів	Отримання атрибутів користувача	Модуль Нульових Доказів Знання (ZKP), Шифрування	Атака Відбита: Дані захищено методом ZKP
Атака схожості	Порівняння даних для виявлення схожих записів	Модуль Нульових Доказів Знання (ZKP), Блокчейн	Атака Відбита: Схожість не підтверджено
Атака на відновлення даних	Спроба відновити видалені дані після виконання права на стирання	Система Управління Ключами (KMS), Офчейн-Сховище (OCS)	Атака Відбита: Ключі знищені, дані недоступні

Кожен тип атаки націлений на компрометацію певного аспекту безпеки, зокрема ідентифікацію користувачів або розкриття конфіденційної інформації. У відповідь на кожну атаку задіюються відповідні компоненти системи, такі як система управління ключами (KMS), модуль нульових доказів знання (ZKP), блокчейн або шифрування даних. Перевірки, реалізовані в моделі, демонструють ефективність обраних методів захисту, забезпечуючи недоступність даних навіть у разі компрометації частини системи та блокуючи несанкціоновані запити.

Запропонована модель продемонструвала ефективність у виконанні критичних операцій з обробки даних. Запис нових даних відбувався з високою продуктивністю, що було підтверджено складністю операції на рівні:

$$□_{□□□□□} = □(□ * □), \quad (6)$$

де n — обсяг даних, а E — складність алгоритму шифрування. Це забезпечує стійкість до зростання обсягів даних. Процес модифікації передбачав додавання нових хешів. Видалення даних, реалізоване через знищення ключів у KMS, відбувалося з мінімальними затримками, а реалізація права на стирання забезпечила знищення всіх копій ключів, роблячи дані недоступними навіть у зашифрованому вигляді.

Апробація також показала, що продуктивність системи залишається стабільною навіть при великій кількості транзакцій. Це підтверджує, що запропоноване рішення може масштабуватися без суттєвих втрат ефективності. Кількісні оцінки продуктивності та складності операцій у моделі продемонстровані в Таблиці 3: запис, читання, модифікація, видалення та стирання даних.

Таблиця 3

Оцінка продуктивності та складність операцій

Операція	**Опис**	**Часова Складність**	**Продуктивність**	**Ресурсоємність**
Запис даних	Шифрування даних та реєстрація хешу у блокчейні	$□_{□□□□□} = □(□ * □)$	Середня	Висока
Читання даних	Перевірка прав доступу та розшифрування даних	$□_{□□□□□} = O(1)$	Висока	Низька
Модифікація даних	Додавання нової транзакції з новим хешем	$□_{□□□□□□} = O(m)$	Середня	Середня
Видалення даних	Знищення ключів у KMS та оновлення метаданих	$□_{□□□□□□} = O(1)$	Висока	Низька
Стирання даних	Видалення всіх ключів та створення нової версії запису в блокчейні	$□_{□□□□□□} = O(1)$	Висока	Низька

Примітки: n - обсяг даних, що додаються, E - складність шифрування, m – кількість модифікацій, T - часова складність операції.

Таблиця оцінок ефективності операцій показала, що запис даних має середню складність через необхідність шифрування, читання даних є менш ресурсоємним завдяки оптимізованій процедурі перевірки доступу, тоді як модифікація вимагає додаткових ресурсів для підтримки цілісності блокчейну. Видалення та стирання даних є найменш ресурсоємними операціями, оскільки вони реалізуються через просте знищення ключів у KMS та видаленні даних без використання криптографічних методів анонімізації.

Таким чином, результати апробації підтвердили, що запропонована модель ефективно протидіє критичним загрозам і забезпечує стійкість до атак на розкриття членства та атрибутів, а також відповідає основним вимогам GDPR щодо конфіденційності та безпеки персональних даних. Завдяки інтеграції блокчейн-технологій, динамічному управлінню ключами та криптографічним методам вдалося створити систему, яка забезпечує високу прозорість, незмінність та захист даних на кожному етапі життєвого циклу.

Висновки

Запропонована модель анонімізації даних на основі блокчейн-технологій ефективно вирішує питання прозорого та безпечного управління персональними даними відповідно до вимог GDPR. Основні компоненти моделі, такі як смарт-контракт для керування термінами зберігання (SCDE), система управління ключами (KMS), та блокчейн-мережа, забезпечують автоматизацію основних операцій з даними, що дозволяє підтримувати високий рівень конфіденційності, цілісності та контролю доступу.

Результати апробації підтвердили стійкість моделі до атак на розкриття членства та атрибутів завдяки використанню динамічних шифрувальних ключів та модулів нульових доказів знання (ZKP). Додатково оцінка ефективності операцій показала, що час виконання ключових операцій є оптимальним для систем з великим обсягом даних.

Поставлена мета щодо відповідності моделі вимогам регламенту GDPR досягнута, що підтверджується забезпеченням реалізації "права на стирання", надійної анонімізації та автоматизації процесів видалення даних. Практична значущість запропонованого рішення полягає у можливості його інтеграції в реальні системи для підвищення захисту персональних даних та забезпечення прозорого управління інформацією.

Подальші дослідження можуть бути спрямовані на оптимізацію продуктивності компонентів, зокрема SCDE та KMS, для підвищення масштабованості системи та зниження затримок у випадку інтеграції з іншими блокчейн-мережами. Також перспективним напрямком є вдосконалення механізмів управління ключами для забезпечення динамічного контролю доступу в умовах зміни політик безпеки.

Список літератури

1. *Dove, E. S. (2023). Confidentiality, public interest, and the human right to science: When can confidential information be used for the benefit of the wider community? Journal of Law and the Biosciences, 10(1), Article lsad013. https://doi.org/10.1093/jlb/lsad013*
2. *GDPR.eu. (n.d.). General Data Protection Regulation (GDPR) – Official Legal Text. Retrieved from https://gdpr-info.eu/.*
3. *GDPR.eu. (n.d.). Art. 17 GDPR – Right to erasure (‘right to be forgotten’). Retrieved from https://gdpr-info.eu/art-17-gdpr/.*
4. *Tachepun, C., & Thammaboosadee, S. (2020). A Data Masking Guideline for Optimizing Insights and Privacy Under GDPR Compliance. In Proceedings of the 11th International Conference on Advances in Information Technology (IAIT '20) (Article No. 22, pp. 1–9). Association for Computing Machinery. https://doi.org/10.1145/3406601.3406627*
5. *Kohlmayer, F., Lautenschläger, R., & Prasser, F. (2019). Pseudonymization for research data collection: Is the juice worth the squeeze? BMC Medical Informatics and Decision Making, 19, 178. https://doi.org/10.1186/s12911-019-0905-x*

6. *Cai, S., Gallina, B., Nyström, D., & Wąsowski, A. (2019). Data aggregation processes: A survey, a taxonomy, and design guidelines. Computing, 101(10), 1397-1429. https://doi.org/10.1007/s00607-018-0679-5*
7. *Riplinger, L., Piera-Jiménez, J., & Pursley Dooling, J. (2020). Patient Identification Techniques – Approaches, Implications, and Findings. Yearbook of Medical Informatics, 29(1), 81–86. https://doi.org/10.1055/s-0040-1701984*
8. *Monteiro, S., Oliveira, D., António, J., Martins, P., & Abbasi, M. (2024).* Data Anonymization: Techniques and Models*. In: Reis, J.L., Del Rio Araujo, M., Reis, L.P., dos Santos, J.P.M. (eds) Marketing and Smart Technologies. ICMarkTech 2022.* Smart Innovation, Systems and Technologies*, vol 344. Springer, Singapore. https://doi.org/10.1007/978-981-99-0333-7_6.*
9. *Shao, Y., Liu, J., Shi, S., & Zhang, Y. (2019). Fast de-anonymization of social networks with structural information. Data Science and Engineering, 4(1), 76-92. https://doi.org/10.1007/s41019-019-0086-8*
10. *Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Digital Applications and Technology, 3, Article 100344. https://doi.org/10.1016/j.dajour.2023.100344*
11. *Bodó, B., Brekke, J. K., & Hoepman, J. H. (2021). Decentralisation: A multidisciplinary perspective. Internet Policy Review, 10(2). https://doi.org/10.14763/2021.2.1563*
12. *Boumaouche, O., Ghenai, A., & Zeghib, N. (2020). Data Oriented Blockchain: Off-Chain Storage with Data Dedicated and Prunable Transactions. B* Advanced Communication Systems and Information Security *(ACOSIS 2019).* Communications in Computer and Information Science, vol 1264*. Springer, Cham. DOI: 10.1007/978-3-030-61143-9_16.*
13. *Wei Zhou et al., "A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT", Applied Sciences, 2023. DOI: 10.3390/app132212389.*
14. *Tran, Q. N., Turnbull, B. P., Wu, H., Hu, J., & Others. (2021). A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture. IEEE Open Journal of the Computer Society, 99, 1-1. https://doi.org/10.1109/OJCS.2021.3053032*
15. *Bao, H., Yuan, M., Deng, H., Xu, J., & Zhao, Y. (2024). Secure multiparty computation protocol based on homomorphic encryption and its application in blockchain. Heliyon, 10(1), e34458. https://doi.org/10.1016/j.heliyon.2024.e34458*
16. *Zhou, W., Zhang, D., Han, G., Wang, X., & other authors. (2023). A Blockchain-Based Privacy-Preserving and Fair Data Transaction Model in IoT. Applied Sciences, 13(22), 12389. https://doi.org/10.3390/app132212389*
17. *Alamri, B., Javed, I. T., & Margaria, T. (2021, April 19–21). A GDPR-Compliant Framework for IoT-Based Personal Health Records Using Blockchain. Proceedings of the 2021 International Conference on New Technologies, Mobility and Security (NTMS). IEEE. https://doi.org/10.1109/NTMS49979.2021.9432661*
18. *Shashidhara, R., Chirakarotu Nair, R., & Panakalapati, P. (2024). Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions. Security and Privacy, 2024. https://doi.org/10.1002/spy2.461*
19. *Capraz, S., & Ozsoy, A. (2021). Personal Data Protection in Blockchain with Zero-Knowledge Proof. In Proceedings of the 2021 International Conference on Information and Communication Technologies (ICT). Springer. https://doi.org/10.1007/978-981-33-6470-7_7*
20. *El Emam, K., Mosquera, L., & Fang, X. (2022). Validating a membership disclosure metric for synthetic health data. JAMIA Open, 5(4), ooac083. https://doi.org/10.1093/jamiaopen/ooac083*
21. *Torra, V., & Navarro-Arribas, G. (2023). Attribute disclosure risk for k-anonymity: The case of numerical data. International Journal of Information Security, 22, 2015–2024. https://doi.org/10.1007/s10207-023-00730-x*

22. *Su, B., Huang, J., Miao, K., Wang, Z., Zhang, X., & Chen, Y. (2023). K-Anonymity privacy protection algorithm for multi-dimensional data against skewness and similarity attacks. Sensors, 23(3), 1554. https://doi.org/10.3390/s23031554*
23. *Liu, J., Zhang, S., Luo, Y., & Cao, L. (2022). Machine Learning-Based Similarity Attacks for Chaos-Based Cryptosystems. IEEE Transactions on Emerging Topics in Computing, 10(2), 824–837. https://doi.org/10.1109/TETC.2020.3048498*

ANONYMIZATION OF DATA USING BLOCKCHAIN TECHNOLOGY: A MODEL FOR DATA LIFECYCLE MANAGEMENT TO ENSURE TRANSPARENCY AND COMPLIANCE WITH GDPR

A. S. Pavliv

National University "Lviv Polytechnic",
Department of Electronic Computing Machines
E-mail: andrii.s.pavliv@lpnu.ua

The rapid growth in the volume of personal data collected and processed by various organizations poses significant challenges for ensuring information privacy and security. The General Data Protection Regulation (GDPR) of the European Union sets strict requirements for the processing, storage, and deletion of personal data, including the right to be forgotten, which entails the complete and irreversible deletion of information upon user request. This creates problems for traditional data management systems that cannot provide automated deletion and reliable compliance monitoring.This article proposes a new model for data anonymization based on blockchain technologies that combines smart contracts to automate data operations while using cryptographic methods to create a system resilient to de-anonymization. The model ensures control and compliance with regulatory requirements while maintaining transparency and security for all transactions.

Keywords: blockchain, data anonymization, data management, offchain, right to be forgotten, smart contracts.