The Approach of IPFS Utilizing for the Medical Data Protection

Yurii Baryshev
Department of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
yuriy.baryshev@vntu.edu.ua

Vladyslava Lanova
Department of Information Protection
Vinnytsia National Technical University
Vinnytsia, Ukraine
lanovaia02y@gmail.com

Підхід до Застосування IPFS для Захисту Медичних Даних

Юрій Баришев
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
yuriy.baryshev@vntu.edu.ua

Владислава Ланова
Кафедра захисту інформації
Вінницький національний технічний університет
Вінниця, Україна
lanovaia02y@gmail.com

***Abstract* — The approach of IPFS utilizing for the medical data protection was investigated. IPFS emerged as the most suitable distributed storage option for data saving. Subsequently, a software module was developed to interact with IPFS for storing medical data. The development process began with constructing the algorithm scheme for the module's operation. Following this, a visual interface was created to allow healthcare providers to access and manage patient examination results. This developed module can be integrated into existing or under-development information systems.**

***Анотація* — Розглянуто підхід до застосування IPFS для захисту медичних даних. У ході дослідження було розглянуто відомі альтернативні рішення, де зроблено висновок, що найбільш доцільним розподіленим сховищем збереження даних є IPFS. Розроблено модуль взаємодії з IPFS для зберігання медичних даних, де спершу побудовано схему алгоритму роботи даного модуля, а згодом візуальний інтерфейс, який дозволяє лікарю взаємодіяти з результатами обстежень пацієнта. Таким чином, розроблений модуль може бути інтегрованим до відомих або таких, що розробляються, інформаційних систем.**

Keywords — cybersecurity, medical data, IPFS.

Ключові слова — кібербезпека, медичні дані, IPFS.

1. Вступ

Лікарні є об’єктами критичної інфраструктури, таким чином, постає актуальна задача забезпечити належний захист медичних даних. Для цього в багатьох країнах діє нормативно-правове регулювання цієї сфери: HIPAA [1], GDPR [2], Закон України «Основи законодавства України про охорону здоров'я» [3], Закон України «Про захист персональних даних» [4].

Таким чином, відповідно до чинного законодавства, медичним даним необхідно забезпечити захист цілісності, доступності та конфіденційності.

Для забезпечення такого рівня захищеності використовують як традиційні централізовані сховища, так і децентралізовані, такі як блокчейн. Децентралізація зберігання даних дозволяє усунути єдину точку відмови в таких інформаційних системах, а відтак — покращити захист доступності та цілісності інформації за рахунок послаблення або цілковитої відсутності захисту конфіденційності цих даних. При цьому блокчейн є не найкращим контейнером для зберігання даних великих за обсягів, які притаманні результатам медичних обстежень. Саме тому доцільно вивчити перспективи використання інших технологій розподіленого зберігання даних, таких як IPFS.

Метою роботи є покращення рівня захисту доступності та цілісності медичних даних.

Для досягнення мети необхідно розв’язати такі задачі:

проаналізувати відомі альтернативні рішення;

розробити модуль взаємодії з IPFS для зберігання медичних даних.

2. Аналіз відомих рішень

IPFS є досить унікальною технологією для розподіленого зберігання та обміну даними в Інтернеті, проте існують інші системи, які можуть конкурувати з нею у певних аспектах.

Swarm – децентралізована мережа зберігання, розроблена для блокчейну Ethereum. За допомогою

розподілених застосунків (dApps) Swarm зберігає дані, які в іншому випадку перевантажили б Ethereum, а транзакції посилаються на дані за допомогою гешованого ключа, створеного в Swarm. Недоліком є те, що Swarm призначений лише для блокчейну Ethereum, а тому його використання для задач цього дослідження накладає обмеження щодо масштабованості порівняно з IPFS [6].

BTFS є похідною від IPFS і підходить як для передачі, так і для зберігання файлів. Однак, на відміну від інших пропозицій децентралізованого зберігання даних, BTFS розроблено таким чином, що дозволяє користувачам видаляти будь-які незаконні або захищені авторським правом носії зі своїх вузлів. У випадку швидкості передачі даних, IPFS може мати перевагу, оскільки його технологія базується на механізмах, спрямованих на мінімізацію зайвого трафіку [7].

Ще одним розподіленим сховищем збереження даних є Storj, який зберігає дані в хмарі. Перевагою є те, що перед тим, як дані опиняться в хмарі, вони будуть зашифровані. Однак, є проблема з масштабованістю, оскільки Storj сприймає дані, які за обсягом менші, ніж це може забезпечити IPFS [7].

Таким чином, проаналізувавши відомі рішення, можна зробити висновок, що IPFS є найбільш доцільним сховищем збереження великих за обсягом даних, які стосуються медичної інформації. Однак, через те, що це сховище є відкритим, потрібно зберігати дані у знеособленому вигляді.

3. Результати розробки

Для застосування в системах зберігання медичних даних спершу було розроблено схему алгоритму роботи модуля взаємодії з IPFS (рис. 1)

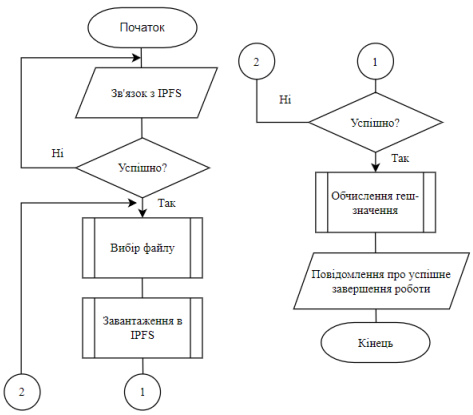

Рис. 1. – Вигляд схеми алгоритму модуля взаємодії з IPFS

Програма встановлює зв'язок з IPFS, якщо зв'язок встановлено успішно, програма запитує у користувача файл і завантажує його в IPFS. Після завантаження, обчислюється геш-значення файлу і з'являється повідомлення про успішне завершення роботи.

Розробка візуального інтерфейсу для роботи з IPFS буде виконуватись за допомогою HTML, CSS та JavaScript. Результат розробки форми для завантаження файлів в IPFS має такий вигляд (рис. 2).

Рис. 2. Вигляд успішного завантаження файлу

Для того, щоб сімейний лікар міг отримати результати обстеження передбачається застосування захищеної централізованої бази даних, яка дозволить за номером направлення знаходити геш-значення в IPFS, які водночас є адресами файлів, ввести у відповідне поле це геш-значення та власне завантажити файл.

4. Висновки

Таким чином, після проведеного дослідження було з'ясовано, що для взаємодії із чутливими даними, що стосуються результатів обстеження, доцільно застосувати додаткове децентралізоване сховище зберігання даних – IPFS. Наведений в роботі аналіз показав, що основною перевагою цього сховища є те, що воно може взаємодіяти з різними блокчейнами та базами даних, не обмежуючи масштабованість застосунків, які її використовують, що притаманно альтернативним рішенням. Останнє важливо у випадках обробки великих обсягів даних, де правила обробки регулюються на рівні законодавства, як-то медицина.

Для можливості інтеграції IPFS було розроблено програмний модуль, який дає можливість лікарю завантажувати результати обстеження пацієнтів, а також може бути інтегрованим до відомих або таких, що розробляються, інформаційних систем.

References

[1] E. Hing та G. A. Jensen, "Health Insurance Portability and Accountability Act of 1996", Med. Care, т. 37, № 7, с. 692–705, Jul. 1999. Available: https://doi.org/10.1097/00005650-199907000-00009. [Accessed: 06-May-2024].

[2] "Official Legal Text,"General Data Protection Regulation (GDPR), 27-Sep-2022. Available: https://gdpr-info.eu/.[Accessed: 06-May-2024].

[3] Закон України, "Основи законодавства України про охорону здоров'я". Available: https://zakon.rada.gov.ua/laws/show/2801-12 [Accessed: 06-May-2024].

[4] Закон України, "Про захист персональних даних," Available: https://zakon.rada.gov.ua/laws/show/2297-17. [Accessed: 06-May-2024].

[5] IPFS [Online]. Available: https://docs.ipfs.tech/. [Accessed: 06-May-2024].

[6] Swarm [Online]. Available: https://docs.ethswarm.org/. [Accessed: 06-May-2024].

[7] 7 decentralized data storage networks compared [Online]. Available: https://www.techtarget.com/searchstorage/tip/Comparing-4-decentralized-data-storage-offerings. [Accessed: 06-May-2024].