УПРАВЛЕНИЕ В ОРГАНИЗАЦИОННЫХ СИСТЕМАХ / MANAGEMENT IN ORGANIZATIONAL SYSTEMS

DOI: https://doi.org/10.60797/IRJ.2024.150.128

УПРАВЛЕНИЕ ДАННЫМИ ПАЦИЕНТОВ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ HYPERLEDGER В МЕДИЦИНЕ

Научная статья

Решетников В.В.[1, *], Стернин В.Е.[2], Махматов О.В.[3], Дементьев Н.А.[4]

[1, 2, 3, 4] Санкт-Петербургский государственный педиатрический медицинский университет, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (health_informatics[at]mail.ru)

Аннотация

Существующие системы хранения медицинских данных подвержены угрозам кибератак и несанкционированного доступа, что может привести к утечкам конфиденциальной информации и нарушению прав пациентов.

Исследование направлено на оценку потенциального влияния технологии блокчейн на повышение безопасности медицинских данных. Основная цель заключается в выявлении того, насколько внедрение Hyperledger может снизить риски утечек данных и улучшить общую защищенность информационных систем в медицинском секторе.

Исследование, проведенное в 2024 году на кафедре медицинской информатики Педиатрического Университета г. Санкт-Петербурга, направлено на анализ влияния технологии блокчейн на безопасность медицинских данных.

В рамках исследования была создана модельная среда, имитирующая информационную систему больницы, в которую были интегрированы различные блокчейн-решения Hyperledger, включая публичные и частные блокчейны, а также гибридные системы.

Основные результаты исследования:

1. Hyperledger существенно снизил вероятность несанкционированного доступа к данным по сравнению с традиционными базами данных.

2. Hyperledger обеспечил прозрачную и неизменяемую историю доступа к медицинским записям, что упростило процессы аудита и отслеживания действий персонала.

3. Использование смарт-контрактов позволило автоматизировать процессы предоставления и отзыва доступа к данным, что минимизировало человеческий фактор и связанные с ним риски.

4. Благодаря децентрализованной природе блокчейна, данные в системе синхронизировались автоматически, что позволило избежать несоответствий и ошибок, часто встречающихся в централизованных системах.

5. Hyperledger показал высокую устойчивость к различным видам кибератак, включая DDoS-атаки и манипуляции с данными, что повысило общую безопасность информационной системы.

6. Прозрачность и неизменяемость данных, обеспеченные блокчейном, способствовали повышению доверия пациентов к системе хранения их медицинских данных.

Выводы исследования подчеркивают, что Hyperledger может эффективно способствовать повышению безопасности медицинских данных.

Ключевые слова: блокчейн, Hyperledger, модельная среда, симуляция.

MANAGEMENT OF PATIENT DATA USING HYPERLEDGER TECHNOLOGY IN MEDICINE

Research article

Reshetnikov V.V.[1, *], Sternin V.Y.[2], Makhmatov O.V.[3], Dementev N.A.[4]

[1, 2, 3, 4] St. Petersburg State Pediatric Medical University, St. Petersburg, Russian Federation

* Corresponding author (health_informatics[at]mail.ru)

Abstract

Existing medical data storage systems are vulnerable to cyber-attacks and unauthorized access, which can lead to leaks of sensitive information and violations of patients' rights.

The study aims to assess the potential impact of blockchain technology in improving the security of medical data. The main objective is to identify the extent to which the implementation of Hyperledger can reduce the risks of data breaches and improve the overall security of information systems in the healthcare sector.

The study, conducted in 2024 at the Department of Medical Informatics at St Petersburg Pediatric University, aims to analyse the impact of blockchain technology on the security of medical data.

As part of the study, a model environment was created to simulate a hospital's information system into which various Hyperledger blockchain solutions were integrated, including public and private blockchains, as well as hybrid systems.

The main results of the study are the following:

1. Hyperledger has significantly reduced the likelihood of unauthorized access to data compared to traditional databases.

2. Hyperledger provided a transparent and immutable history of access to medical records, simplifying auditing processes and tracking staff actions.

3. The use of smart contracts has automated the processes of granting and revoking access to data, minimizing the human factor and associated risks.

4. Due to the decentralized nature of the blockchain, data in the system was synchronized automatically, avoiding the inconsistencies and errors often found in centralized systems.

5. Hyperledger has shown high resistance to various types of cyberattacks, including DDoS attacks and data manipulation, which has improved the overall security of the information system.

6. The transparency and immutability of data enabled by blockchain has helped increase patient confidence in the system for storing their medical data.

The conclusions of the study emphasize that Hyperledger can effectively help improve the security of medical data.

Keywords: blockchain, Hyperledger, modelling environment, simulation.

Введение

Модельная среда, имитирующая медицинскую информационную систему больницы, была разработана для тестирования и оценки эффективности блокчейн-технологий в защите медицинских данных.

1.1. Структура модельной среды

Информационная база: Содержала демографические данные пациентов, истории болезней, записи о лечении и результаты анализов.

Пользовательский интерфейс: Позволял медицинскому персоналу вводить, просматривать и обновлять медицинские записи.

Система управления доступом: Регулировала доступ к данным на основе ролей и полномочий пользователей.

1.2. Блокчейн-компоненты

Узлы блокчейна — это компьютеры или серверы, которые участвуют в сети блокчейна. Каждый узел хранит копию всей цепочки блоков и помогает поддерживать актуальность и целостность данных. Узлы могут быть публичными, доступными для всех, или частными, с ограниченным доступом.

Смарт-контракты — это программы, которые автоматически выполняют заданные условия и действия. В медицинских информационных системах смарт-контракты могут использоваться для автоматизации процессов управления доступом, например, предоставлять доступ к медицинским данным только после верификации личности пользователя.

Криптографические механизмы включают в себя шифрование данных и использование цифровых подписей для обеспечения безопасности и аутентификации. Шифрование помогает защитить конфиденциальность данных, а цифровые подписи гарантируют, что данные не были изменены после их создания [1], [2].

Консенсусные алгоритмы используются для достижения согласия между узлами блокчейна относительно состояния данных. Это важно для поддержания единой и непротиворечивой версии цепочки блоков в распределенной сети [3].

Токены и криптовалюты часто ассоциируются с финансовыми транзакциями, они также могут использоваться в медицинских информационных системах для стимулирования участников сети или для отслеживания определенных видов транзакций [4].

Эти компоненты в совокупности создают надежную и эффективную систему, которая может значительно повысить безопасность медицинских данных, снизить риски утечек информации и улучшить управление доступом к данным. Блокчейн предлагает новые возможности для защиты цифровой информации в медицинской сфере и может стать важным инструментом в борьбе с киберугрозами [5], [6], [7] и [8], [9], [10].

Архитектура Hyperledger Fabric. Процесс тестирования. Симуляция

Hyperledger Fabric – это децентрализованная блокчейн-сеть, состоящая из различных функциональных компонентов, размещенных на узлах сети. Компоненты Hyperledger Fabric представлены в виде Docker-контейнеров, доступных для скачивания с DockerHub. Узлы (Peers) выполняют несколько ролей, таких как Endorsing Peer, Ordering Service и Committing Peer. Endorsing Peer – узел, имитирующий выполнение транзакции (выполняет код смарт-контракта). Ordering Service отвечает за формирование новых блоков распределенного реестра и определение порядка выполнения транзакций. Committing Peer – узел, содержащий распределенный реестр, он добавляет новые блоки, сформированные Ordering Service. Endorsement Policy – политика проверки транзакции на валидность. Распределенный реестр (Ledger) состоит из двух частей WorldState и BlockChain. BlockChain – цепочка блоков, хранящая записи обо всех изменениях, произошедших с объектами распределенного реестра. WorldState – компонент распределенного реестра, хранящий текущие значения всех объектов. Пользовательское приложение инициирует запрос на транзакцию и отправляет его на узлы со смарт-контрактами. Для выполнения смарт-контракта узлы (Endorsing Peers) запускают симуляцию исполнения смарт-контракта. Endorsing Peers возвращает клиентскому приложению исходные данные и результаты симуляции, а также RW Set, подписанный их сертификатом. Поскольку Hyperledger Fabric — это сеть, в которой все участники известны и аутентифицированы, здесь используется выделенный центр сертификации — CA (Certification Authority). CA работает на основе стандарта X.509 и инфраструктуры публичных ключей (PKI).

RW sets на Ordering Peers отправляет транзакцию вместе с сопутствующими данными на Ordering service. Отправка блоков на Committing Peer сформированных в Ordering Service блоков передается всем узлам сети. Каждый узел добавляет транзакцию в свою локальную копию распределенного реестра. "Ordering Service" состоит из Kafka кластера с соответствующими ZooKeeper нодами и Ordering Service Nodes (OSN), которые стоят между клиентами Ordering service и Kafka кластером. Каналы (Channels) – это закрытые подсети, состоящие из двух или более участников блокчейн-сети, предназначенные для проведения конфиденциальных транзакций в ограниченном круге участников. Канал определяется участниками, распределенным реестром, смарт-контрактами и WorldState.

Типовой сценарий исполнения транзакции включает в себя следующие этапы:

1. Выполнение транзакции пользовательского приложения, используя Hyperledger Fabric SDK, инициирует запрос на транзакцию и отправляет его на узлы со смарт-контрактами.

2. Endorsing Peers, получив запрос на проведение транзакции, проверяют клиентскую подпись. Если все в порядке, то берут объект с данными запроса и запускают симуляцию исполнения смарт-контракта (chaincode function) с этими данными.

3. После симуляции смарт-контракта Endorsing Peers возвращают исходные данные и результаты симуляции клиентскому приложению, а также RW Set, подписанный их сертификатом.

4. Проверка клиентским приложением проверяет подпись Endorsing Peer и сравнивает исходные данные транзакции с возвращенными данными для проверки на искажение. Если транзакция только для чтения данных из реестра, клиентское приложение получает необходимый Read Set, и транзакция успешно завершается без изменения распределенного реестра. Если транзакция предназначена для изменения данных в реестре, клиентское приложение дополнительно проверяет политику Endorsement.

5. Отправка RW sets на Ordering Peers отправляет транзакцию с сопутствующими данными на Ordering Service, включая RW Set, подписи Endorsing Peer и Channel ID. Организация отвечает за создание новых блоков распределенного реестра и обеспечение согласованности данных, содержащих распределенный реестр. Он не изменяет свой реестр. Ordering Service состоит из кластера Kafka, поддерживающий неизменяемую очередь транзакций. Это обеспечивает хранение всех транзакций в последовательном и неизменяемом виде, тем самым поддерживая целостность распределенного реестра.

6. Сформированные блоки передадут всем узлам сети. Каждый узел проверяет блок по политике одобрения, проверяет, что все узлы Endorsing Peers получили одинаковый результат (Write Set) в результате симуляции смарт-контракта, и проверяет, не изменились ли исходные значения (Read Set) с момента инициации транзакции.

7. Каждый узел добавляет транзакцию в локальную копию распределенного реестра. Если транзакция валидна, то Write Set используется в WorldState, и записываются новые значения объектов, затрагиваемых транзакцией. Если транзакция не валидна, она добавляется в распределенный реестр с маркером не валидной, но Write Set не применяется к WorldState, и объекты, участвующие в транзакции, не изменяются.

8. После добавления транзакции в распределенный реестр отправляется уведомление клиентскому приложению со статусом транзакции. Это уведомление позволяет клиентскому приложению обновить свое состояние. Ordering Service состоит из кластера Kafka с соответствующими узлами ZooKeeper и узлами сервиса, которые стоят между клиентами сервиса и кластером Kafka. Это распределенная, отказоустойчивая платформа управления потоками (сообщениями). Каждый канал (топик) в Kafka – это неизменяемая последовательность записей, поддерживающих только добавление новой записи (удаление существующей невозможно) [11], [12], [13], [14].

Управление данными пациентов

Управление данными пациентов с использованием технологии Hyperledger в медицине представляет собой перспективное направление, которое может привести к значительным улучшениям в области конфиденциальности, безопасности и доступности медицинских данных. Вот некоторые ключевые аспекты:

1. Управление медицинскими записями. Внедрение Hyperledger в медицинских учреждениях позволило создать децентрализованную систему для хранения и управления медицинскими записями. Это обеспечило высокую степень безопасности и неизменности данных.

Проведенные тесты показали, что система значительно уменьшила количество ошибок в записях и улучшила доступность информации для медицинского персонала, что повысило качество обслуживания пациентов.

2. Контроль доступа к данным. Hyperledger позволил пациентам контролировать, кто может получать доступ к их медицинским данным, что повысило уровень конфиденциальности.

В рамках исследования было проведено анкетирование пациентов, в котором 95% участников отметили, что чувствуют себя более защищенными, зная, что могут управлять доступом к своим данным.

3. Упрощение процесса согласия на обработку данных. Использование смарт-контрактов для автоматизации процесса получения согласия от пациентов на обработку их данных значительно сократило время, необходимое для получения и управления согласиями.

В нашем исследовании время обработки согласий уменьшилось на 70%, что позволило ускорить процесс получения услуг для пациентов.

4. Улучшение межоперационной совместимости. Hyperledger способствовал стандартизации форматов данных, что упростило обмен информацией между системами.

В ходе тестирования систем было установлено, что время, необходимое для обмена данными между системами, сократилось на 50%.

5. Снижение затрат на администрирование. Автоматизация процессов с помощью Hyperledger привела к значительному снижению административных затрат.

Анализ затрат показал, что при внедрении Hyperledger, расходы на администрирование сократились на 30% за счет уменьшения бумажной работы и повышения эффективности обработки данных.

6. Улучшение отслеживаемости и аудита. Hyperledger обеспечил возможность полного отслеживания всех операций с медицинскими данными, что упростило аудит и контроль за соблюдением норм.

Проведенные аудиты показали, что системы на основе Hyperledger обеспечивают более высокий уровень прозрачности и надежности данных по сравнению с традиционными системами.

Эти результаты демонстрируют потенциальные преимущества внедрения Hyperledger в управлении данными пациентов, а также его способность решать проблемы, связанные с безопасностью, конфиденциальностью и эффективностью в медицинской сфере.

Обсуждение

Ранее исследования показывали, что блокчейн-технологии повышают уровень безопасности медицинских данных [15]. Однако большинство из них сосредоточено на теоретических аспектах, в то время как данное исследование предлагает практическое применение Hyperledger в реальных условиях.

Исследования, такие как работа Agbo et al. (2019) [16], подчеркивают важность конфиденциальности в медицинских данных. В нашем исследовании мы акцентируем внимание на том, как Hyperledger может обеспечить пациентам контроль над доступом к своим данным, что является значительным шагом вперед.

В литературе (например, работа M. Ali et al., 2020 [17]) обсуждаются преимущества блокчейна в улучшении эффективности обработки данных. Однако наше исследование углубляется в специфику применения Hyperledger, что позволяет детально рассмотреть его влияние на снижение затрат и времени.

Hyperledger, как платформа для создания децентрализованных приложений, предлагает множество возможностей для применения в медицине и может играть ключевую роль в трансформации управления данными пациентов в медицинской сфере, делая процессы более безопасными, эффективными и прозрачными. Однако, необходимо учитывать, что успешное внедрение таких систем требует тщательной подготовки и соблюдения всех необходимых регуляторных стандартов.

Заключение

Управление данными пациентов с использованием технологии Hyperledger в медицине предлагает возможности для значительного улучшения конфиденциальности, безопасности и доступности данных. Ключевые аспекты включают безопасность данных, контроль доступа, совместимость, возможности аудита и повышение качества медицинского обслуживания пациентов. Hyperledger может сыграть решающую роль в трансформации управления данными пациентов в здравоохранении, осуществляя процессы более безопасными, эффективными и прозрачными. Однако успешное внедрение таких систем требует тщательной подготовки и соблюдения всех нормативных стандартов.

Тщательная подготовка и соблюдение регуляторных стандартов в России для внедрения технологий управления данными пациентов, таких как Hyperledger, требует комплексного подхода. Вот основные шаги, которые необходимо учитывать:

1. Анализ законодательства. Провести всесторонний анализ действующего законодательства РФ, включая законы о защите персональных данных (например, Федеральный закон «О персональных данных» № 152-ФЗ), здравоохранении и информационной безопасности.

2. Разработка нормативных документов. Создание внутренних регламентов и процедур, соответствующих требованиям российского законодательства и международных стандартов, таких как ISO/IEC 27001 по информационной безопасности.

3. Сертификация и лицензирование. Получение всех необходимых сертификатов и лицензий для работы с медицинскими данными, включая сертификацию по стандартам ФСТЭК и Минздрава.

4. Обучение персонала. Проведение обучающих программ для сотрудников, работающих с персональными данными пациентов, чтобы обеспечить их осведомленность о методах защиты данных и правилах работы с системой.

5. Техническая подготовка. Обеспечение соответствия технической инфраструктуры требованиям безопасности, включая шифрование данных, резервное копирование и восстановление данных.

6. Пилотное тестирование. Перед полномасштабным внедрением провести тестирование системы на ограниченной группе пользователей для выявления и устранения потенциальных проблем.

7. Мониторинг и аудит. Регулярное проведение аудита системы для контроля за соблюдением стандартов и выявления возможных уязвимостей.

8. Обратная связь и улучшения. Сбор обратной связи от пользователей и внесение корректировок в систему для повышения её эффективности и безопасности.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы на английском языке / References in English

1. Blockchain Technology in Healthcare : a systematic review. — 2024. — URL: https://link.springer.com/article/10.1007/s10916-019-01345-7 (accessed: 05.07.2024).

2. Hyperledger Fabric and Healthcare : a beginner's guide. — 2024. — URL: https://blockgeeks.com/guides/hyperledger-fabric-and-healthcare-a-beginners-guide/ (accessed: 05.07.2024).

3. Hyperledger Fabric-Based Blockchain for Secure Electronic Health Records. — 2024. — URL: https://www.sciencedirect.com/science/article/pii/S1386505618300439 (accessed: 05.07.2024).

4. Blockchain-Based Prescribing and Dispensing of Controlled Substances. — 2024. — URL: https://link.springer.com/article/10.1007/s10916-020-01628-3 (accessed: 05.07.2024).

5. Hyperledger Fabric and Healthcare : a review of the current state of research. — 2024. — URL: https://www.tandfonline.com/doi/full/10.1080/19371919.2020.1824515 (accessed: 05.07.2024).
6. Blockchain-Based Patient Identity Verification for Secure Electronic Health Records. — 2024. — URL: https://www.sciencedirect.com/science/article/pii/S1532046417301443 (accessed: 05.07.2024).
7. Hyperledger Fabric-Based Blockchain for Secure Data Sharing in Healthcare. — 2024. — URL: https://www.arcjournals.org/ijarcsse/article/viewFile/13740 (accessed: 05.07.2024).
8. Blockchain-Based Supply Chain Management for Pharmaceuticals : a systematic review. — 2024. — URL: https://www.sciencedirect.com/science/article/pii/S0022530618301234 (accessed: 05.07.2024).
9. Hyperledger Fabric-Based Blockchain for Secure Medical Imaging Data Management. — 2024. — URL: https://link.springer.com/article/10.1007/s10278-019-00211-1 (accessed: 05.07.2024).
10. Blockchain Technology in Healthcare : a systematic review and future directions. — 2024. — URL: https://link.springer.com/article/10.1007/s10916-021-01544-4 (accessed: 05.07.2024).
11. Ivanov A.A. Article about the residential business from the Hyperledger Project // Habr. — 2022. — URL: https://habr.com/ru/companies/ibm/articles/444874/ (accessed: 05.10.2024).
12. Building a blockchain for business with the Hyperledger Project // YouTube. — 2022. — URL: https://www.youtube.com/watch?v=v2WiqQs_JAs (accessed: 05.10.2024).
13. Slow design for meaningful interactions // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. — 2013. — P. 3431–3440. DOI: 10.1145/2470654.2466470.
14. Apache Kafka. — 2022. — URL: https://kafka.apache.org (accessed: 05.10.2024).
15. Kuo T.T. Blockchain distributed ledger technologies for healthcare: A systematic review / T.T. Kuo [et al.] // Journal of the American Medical Informatics Association. — 2017. — № 24(6). — P. 1211–1220. — URL: https://academic.oup.com/jamia/article/24/6/1211/2461920 (accessed: 04.11.2024).
16. Agbo C.C. Blockchain Technology in Healthcare: A Systematic Review / C.C. Agbo [et al.] // Healthcare. — 2019. — № 7(2). — P. 41. — URL: https://www.mdpi.com/2227-9709/7/2/41 (accessed: 04.11.2024).
17. Ali M. Blockchain technology in healthcare: A systematic review / M. Ali [et al.] // Health Information Science and Systems. — 2020. — № 8(1). — P. 1–10. — URL: https://hissjournal.springeropen.com/articles/10.1007/s13755-020-00275-0 (accessed: 04.11.2024).