УДК 004.051;891.5;614.2

КОНФИДЕНЦИАЛЬНОСТЬ МЕДИЦИНСКИХ ДАННЫХ В СЕТИ IOT ДЛЯ IT ДИАГНОСТИКИ ПАЦИЕНТОВ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

В.А. Вишняков
Профессор кафедры ИКТ
БГУИР, д.т.н., профессор
vish@*bsuir.com*

С. Ивэй
Аспирант БГУИР
xiayiwei4@gmail.com

В.А. Вишняков

Окончил Минский радиотехнический институт. Область научных интересов связана с разработкой методов и алгоритмов инфокоммуникационных систем, организацией учебного и научно-исследовательского процессов в области сетей IoT и блокчейн.

С. Ивэй

Учится в аспирантуре в Белорусском государственном университете информатики и радиоэлектроники. Область научных интересов связана с ИТ-диагностикой и сетями интернета вещей (IoT).

Аннотация. Целью исследования является задача обеспечения конфиденциальности и безопасности при управлении медицинскими данными в сети Интернета вещей (*IoT*) ИТ-медицины. В докладе предлагается интеграция технологии Интернета вещей, блокчейн и файловой системы (*IPFS*) для защиты медицинских данных. Имеется неэффективность традиционных механизмов защиты данных при обработке конфиденциальной медицинской информации, генерируемой устройствами Интернета вещей. В исследовании предлагается подход для хранения персональных медицинских данных с использованием блокчейн, смарт-контрактов для обеспечения правил их обработки. Приведена структура такой системы, включающей сеть *IoT* и блокчейн. Файловая система *IPFS* используется для преодоления технических ограничений блокчейна при обработке крупномасштабных данных, обеспечивая хранение больших объемов медицинских данных.

Ключевые слова: блокчейн, конфиденциальность медицинских данных, сеть Интернет вещей (*IoT*), межпланетная файловая система (*IPFS*), смарт-контракты**.**

Введение. С развитием информационных технологий применение Интернета вещей (*IoT*) в ИТ-медицине становится все более распространенным, особенно в ИТ-диагностике заболеваний и мониторинге состояния пациентов. Эти технологические достижения продвинули развитие ИТ-здравоохранения, особенно в области мониторинга данных в режиме реального времени, удаленной диагностики и повышения эффективности и качества обслуживания пациентов. Однако экспоненциальный рост объема медицинских данных вызвал серьезные опасения по поводу их конфиденциальности и безопасности. Обеспечение сохранности этих конфиденциальных данных имеет решающее значение для поддержания доверия пациентов и соблюдения нормативных требований.

Проблема медицинских данных. С применением технологии Интернета вещей в

области ИТ-медицины соответственно увеличились исследования в области конфиденциальности медицинских данных. Анализ публикаций указывает на то, что, хотя устройства Интернета вещей играют решающую роль в повышении эффективности диагностики и лечения, они также создают новые проблемы в области безопасности данных и защиты частной жизни. *Newaz* и др. [1] продемонстрировали, что традиционные механизмы защиты данных неэффективны и уязвимы для атак при обработке больших объемов конфиденциальных медицинских данных, генерируемых устройствами Интернета вещей. *Yaqoob* и др. [2] подчеркнули, что существующим методам защиты данных часто не хватает достаточной прозрачности и прослеживаемости, которые особенно важны в области медицины.

Технологии блокчейн. Технология блокчейн, известная своей децентрализацией, неизменяемостью и прозрачностью, широко рассматривается как эффективное решение проблем конфиденциальности медицинских данных. Целью данного исследования является изучение того, как технология блокчейн может быть использована в среде Интернета вещей для защиты конфиденциальности и безопасности медицинских диагностических данных. В докладе рассмотрены текущие проблемы в области защиты конфиденциальности медицинских данных и потенциальные применения технологии блокчейн, предложена инновационная стратегия повышения конфиденциальности диагностических данных пациентов в контексте Интернета вещей. Исследование сосредоточено на том, как технология блокчейн может обеспечить безопасность данных, оптимизируя процессы медицинского обслуживания и повышая уверенность пациентов в защите их личной медицинской информации.

Технология блокчейн предлагает новое решение этих проблем. Ее основные функции включают децентрализацию, неизменяемость и прозрачность. В сети блокчейн данные организованы в ряд взаимосвязанных «блоков» и защищены сложными алгоритмами шифрования. Децентрализованный характер подразумевает, что ни одна организация не может контролировать всю сеть целиком, что снижает риск незаконного изменения или удаления данных. Неизменяемость гарантирует, что после записи данных в блокчейн они не могут быть изменены или стерты, что гарантирует подлинность и целостность данных. Более того, прозрачность блокчейна позволяет участникам сети видеть все записи транзакций, облегчая мониторинг и аудит. Однако, несмотря на теоретические преимущества технологии блокчейн, она сталкивается с проблемами и ограничениями в практическом применении, включая незрелую технологию, низкую скорость обработки и сложности интеграции с существующими медицинскими системами.

Защита конфиденциальности медицинских данных. В области медицины защита конфиденциальности данных пациентов имеет важное значение. Эти данные включают личную медицинскую информацию, медицинские записи и результаты диагностики, которые требуют высокого уровня конфиденциальности и безопасности. Однако традиционные методы защиты медицинских данных, такие как централизованные базы данных и стандартные технологии шифрования, сталкиваются с многочисленными проблемами при обработке и хранении больших объемов данных. Основные проблемы включают подверженность сетевым атакам, потенциальную утечку данных и отсутствие эффективных механизмов проверки целостности данных. Технология блокчейн обеспечивает решение этих проблем. Ее основные преимущества заключаются в повышении безопасности данных и защите конфиденциальности при одновременном повышении прозрачности. Ее использование в сети ИТ-диагностики достигает следующих результатов:

1 Безопасная передача и хранение данных: используя неизменяемость блокчейна, медицинские данные, попав в цепочку, не могут быть изменены, что обеспечивает

подлинность и целостность данных. Децентрализованный характер блокчейн означает, что данные больше не хранятся на одном сервере, что снижает риски возникновения отдельных точек сбоя и утечки данных.

2 Смарт-контракты на блокчейне – это протоколы автоматического исполнения, которые гарантируют, что обработка медицинских данных и обмен ими осуществляются в соответствии со строгими правилами, которые предварительно закодированы и согласованы. С помощью смарт-контрактов может быть реализован автоматический контроль разрешений на доступ к данным, защищая таким образом конфиденциальность пациентов.

3 Интеграция с файловой системой *InterPlanetary File System* (*IPFS*): чтобы устранить технические ограничения блокчейна при обработке крупномасштабных данных, в этом исследовании предлагается хранить файлы медицинских баз данных в распределенной файловой системе *IPFS*. Файловая система может эффективно и безопасно хранить огромные объемы данных при меньших затратах. Как только данные сохраняются в *IPFS*, система возвращает уникальное хэш-значение. Это хэш-значение затем сохраняется в смарт-контракте на блокчейне, обеспечивая целостность и неизменяемость данных и решая проблему ограниченной емкости хранилища блокчейна.

Интеграция сетей, блокчейн и файловой системы. В исследовании был реализован комплексный подход для обеспечения безопасного хранения и защиты конфиденциальности медицинских данных, используя возможности сетей IoT, блокчейн и файловой системы *IPFS*. Это обеспечило распределенное хранение медицинской информации в сочетании с технологией смарт-контрактов блокчейн *Ethereum*. На рисунке 1 представлена структурная схема всей системы, укрупненный алгоритм работы которой включает следующие шаги:

1 Медицинские данные, включая личную информацию пациентов, медицинские записи и результаты прогнозирования заболеваний, извлекаются из базы данных (*MongoDB*). Чтобы обеспечить безопасность этих данных во время их передачи и хранения, был использован метод шифрования *Advanced Encryption Standard* (*AES*). Метод шифрования, реализуемый на Python, гарантировал, что данные остаются защищенными и неповрежденными даже при передаче по сетям общего пользования.

2 Зашифрованные данные загружаются в *IPFS*. Являясь распределенной системой хранения файлов, *IPFS* повышает доступность данных и устойчивость к цензуре за счет фрагментации файлов на множество частей и распространения их по глобальной сети. Каждый файл, загруженный в *IPFS*, генерирует уникальное хэш-значение, что облегчает поиск данных и доступ к ним в будущем. использовали *IPFS API* или инструменты командной строки для загрузки файлов и тщательно записали соответствующее хэш-значение каждого файла.

3 Написание смарт-контракта на блокчейне *Ethereum* для обеспечения безопасного доступа и извлечения медицинских данных. Смарт-контракт включал в себя ключевые функции, такие как регистрация медицинских данных, генерация лицензии, утверждение заявки и валидация лицензии. Контракт был развернут в локальной тестовой сети *Ethereum* с использованием платформы разработки *Truffle Ethereum*. Развертывание и функциональность смарт-контракта были проверены с помощью программного обеспечения *GANACHE*, которое имитирует сетевую среду *Ethereum*.

4 Создание *JavaScript*-скрипта для взаимодействия с узлом *GANACHE* (действующим как представитель сети *Ethereum*) через *Web3.js*. Этот скрипт включал логику взаимодействия со смарт-контрактом, облегчая хранение и извлечение хэш-значений медицинских данных из *IPFS* в рамках смарт-контракта.

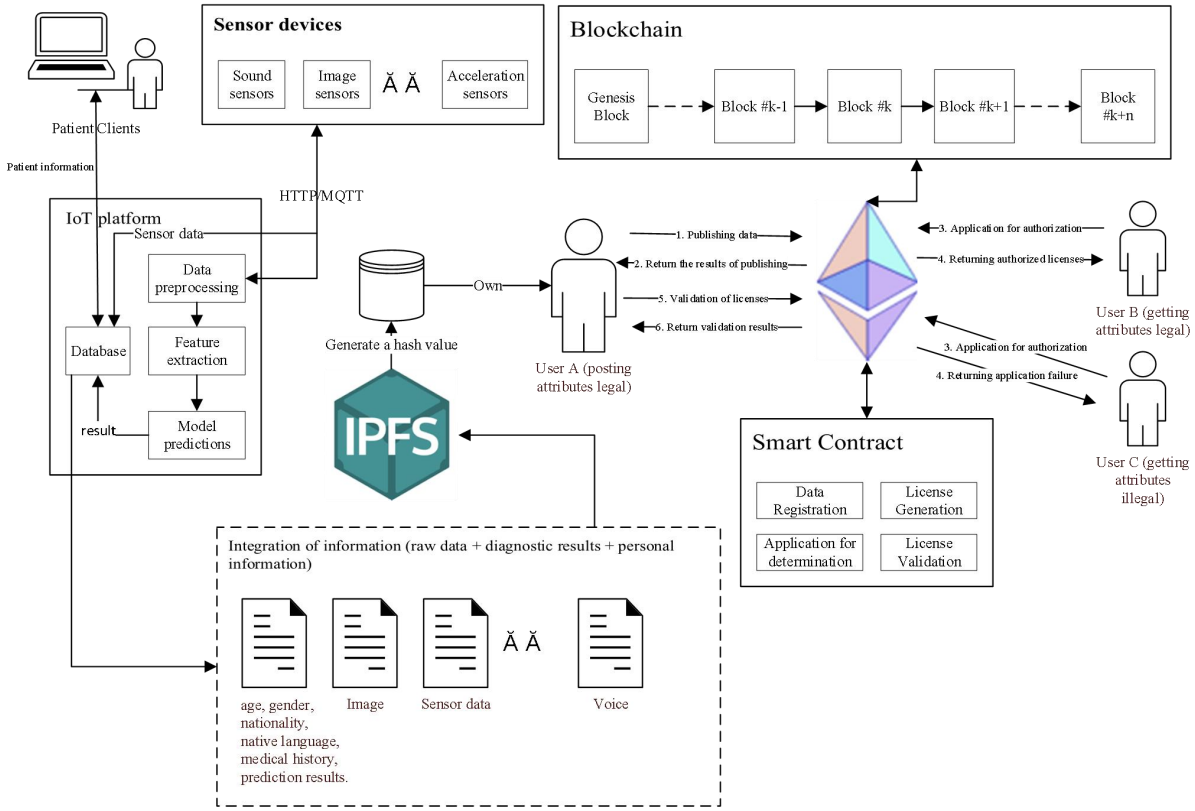

Рисунок 1. Структура хранения данных с *IoT* с использованием Ethereum

5 Запуск этого скрипта позволил извлечь хэш-значения медицинских данных, хранящихся в IPFS, из смарт-контракта. Эти хэш-значения затем используются для извлечения соответствующих зашифрованных файлов из сети *IPFS*.

Заключение. Благодаря интеграции сетей *IoT*, блокчейн и распределенной системы хранения файлов *IPFS* (смарт-контрактов *Ethereum*), разработана система, обеспечивающая конфиденциальность хранения медицинским данным. Описан укрупненный алгоритм работы системы, обеспечивающий конфиденциальность и целостность данных, демонстрируя потенциал технологии блокчейн в защите медицинских данных.

Список литературы

[1] Newaz, Akm Iqtidar, Amit Kumar Sikder, Mohammad Ashiqur Rahman, and A. Selcuk Uluagac. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2021. – 44 p.

[2] Yaqoob, Ibrar, Khaled Salah, Raja Jayaraman, Yousof Al-Hammadi. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 2021. – 16 p.

[3] Вишняков В.А., Ся Ивей. Распознавание признаков болезни Паркинсона на основе анализа голосовых маркеров и двигательной активности. Информатика. – 2023. − Т. 20, № 3. – С. 106–114.

Авторский вклад

Вишняков Владимир Анатольевич – руководство исследованием по использованию блокчейн в сетях ИВ ИТ-диагностики, концепция.

Ся Ивей – описание структуры системы, алгоритм ее работы

CONFIDENTIALITY OF MEDICAL DATA IN THE INTERNET OF THINGS IT DIAGNOSTICS OF PATIENTS BASED ON BLOCKCHAIN TECHNOLOGY

U.A. Vishniakou
Professor, Department of Infocommunication technology of BSUIR, Doctor of Technical sciences, Professor

X. Yiwei
PhD student, Department of Infocommunication technology of BSUIR

Abstract. The aim of the study is to ensure confidentiality and security in the management of medical data in the Internet of Things (IoT) network of IT medicine. The report proposes the integration of Internet of Things technology, blockchain and file system (IPFS) to protect medical data. There is an inefficiency of traditional data protection mechanisms when processing confidential medical information generated by IoT devices. The study proposes an approach for storing personal medical data using blockchain, smart contracts to ensure the rules of their processing. The structure of such a system, including the IoT network and the blockchain, is given. The IPFS file system is used to overcome the technical limitations of the blockchain when processing large-scale data, providing storage of large volumes of medical data.

Keywords: blockchain, confidentiality of medical data, Internet of Things (IoT), interplanetary file system (IPFS), smart contracts.