PQ-FundusChain: постквантовая блокчейн-структура для безопасного и конфиденциального обмена изображениями глазного дна в телеофтальмологии

Источник: Frontiers in Digital Health

Оригинал: https://www.frontiersin.org/articles/10.3389/fdgth.2026.1933562

безопасность | блокчейн | обмен изображениями | постквантовая криптография | телеофтальмология

Введение

Телеофтальмология зависит от безопасного обмена изображениями глазного дна между пунктами первичного скрининга и реферальными центрами. Существующие системы обмена изображениями остаются уязвимыми к квантовым атакам на криптографию с открытым ключом, а также к отказам централизованных хранилищ с ограниченными возможностями аудита.

Методы

В данной работе представлен PQ-FundusChain — консорциумная блокчейн-платформа для квантово-устойчивого обмена изображениями глазного дна. Каждое изображение шифруется с помощью сеансового ключа AES-256-GCM, инкапсулированного с использованием ML-KEM (FIPS 203). ML-DSA (FIPS 204) обеспечивает аутентификацию транзакций блокчейна. Зашифрованные изображения хранятся в децентрализованном офчейн-хранилище, тогда как хэши содержимого, метаданные и политики доступа записываются в ончейн. Запросы на доступ оцениваются через политику, учитывающую риски и

сочетающую показатели доверия, истории доступа и местоположения с показателем чувствительности изображений глазного дна, основанным на анатомии сетчатки и тяжести диабетической ретинопатии.

Результаты

Экспериментальная оценка на публичном наборе данных Messidor-2 показывает, что стоимость криптографических операций и хэширования на стороне отправителя составляет приблизительно 4,02 мс на изображение, стоимость на стороне получателя — приблизительно 3,48 мс, выполнение смарт-контрактов — приблизительно 0,25 мс как для AccessGrant, так и для PolicyUpdate, а размер ончейн-записи на одно изображение составляет приблизительно 4,83 КБ независимо от разрешения изображения. Дополнительная задержка, вносимая постквантовыми механизмами, остается ниже 1 мс для обмена изображениями.

Обсуждение

Результаты демонстрируют, что постквантовая защита может быть интегрирована в рабочие процессы телеофтальмологии с умеренными вычислительными накладными расходами; анализ безопасности подтверждает конфиденциальность, целостность, аутентификацию, неотказуемость, детализированный контроль доступа и устойчивость к атакам типа «собрать сейчас — расшифровать позже».
