TeleZK-FL: обеспечение доверенного и верифицируемого удалённого мониторинга пациентов через квантованное федеративное обучение с нулевым разглашением

Источник: Frontiers in Digital Health

Оригинал: https://www.frontiersin.org/articles/10.3389/fdgth.2026.1821129

zero-knowledge proofs | граничные вычисления | диагностика | кардиология | конфиденциальность | радиология | телемедицина | удалённый мониторинг пациентов | федеративное обучение

Введение

Быстрое расширение Интернета медицинских вещей (IoMT) и телемедицинских платформ породило огромные объёмы пациентских данных, пригодных для обучения диагностических моделей искусственного интеллекта (ИИ). Однако строгие правила конфиденциальности (HIPAA, GDPR) и риск утечек данных препятствуют централизации этой конфиденциальной информации. Хотя федеративное обучение (FL) позволяет проводить совместное обучение без передачи исходных пациентских данных, оно создаёт критический «дефицит доверия»: центральные агрегаторы не могут проверить целостность локальных обновлений модели без инспекции приватных данных, оставляя систему уязвимой для отравления модели и злонамеренных акторов.

Методы

Мы представляем TeleZK-FL — фреймворк сохранения конфиденциальности, разработанный специально для телемедицинских сред с ограниченными ресурсами. В отличие от существующих систем доказательства с нулевым разглашением (ZKP), которые требуют высокопроизводительных вычислений или перекладывают генерацию доказательств на доверенные периферийные серверы, TeleZK-FL интегрирует (1) квантование после обучения (PTQ) для сжатия градиентов модели от 32-битных чисел с плавающей запятой до 8-битных целых чисел и (2) оптимизированные аргументы таблицы поиска (LUT) для генерации криптографических доказательств целостности обучения на стороне клиента непосредственно на периферийных устройствах. Мы оценили фреймворк на двух клинических модальностях — CheXpert (рентгенограммы грудной клетки) и PTB-XL (12-отводные ЭКГ) — используя симулированные медицинские периферийные шлюзы (Raspberry Pi 4) как при гомогенном, так и при гетерогенном распределении данных.

Результаты

TeleZK-FL ускоряет генерацию криптографических доказательств примерно в 25 раз по сравнению со стандартными реализациями ZK-SNARK, генерируя доказательства полной модели примерно за 84 миллисекунды на клиента на периферийном оборудовании. Он сокращает объём коммуникационной нагрузки на 75% (уменьшение в 4,0 раза), сохраняя при этом диагностическую площадь под кривой (AUC) 0,877 на CheXpert и 0,891 на PTB-XL, что представляет деградацию всего на 0,1% и 0,3% соответственно по сравнению с неквантованными базовыми показателями 0,878 и 0,894.

Заключение

TeleZK-FL демонстрирует осуществимость верифицируемого, не требующего доверия федеративного обучения на стандартном телемедицинском оборудовании. Устраняя вычислительные узкие места генерации доказательств на стороне сервера и вызывая лишь деградацию AUC на 0,1%–0,3%, он обеспечивает эффективный, соответствующий регуляторным требованиям метод построения масштабируемых и безопасных децентрализованных медицинских сетей ИИ. Мы дополнительно обсуждаем присущий компромисс: эффективная для периферийных устройств конструкция на основе KZG является классически — а не постквантово — безопасной, что мы явно противопоставляем недавним альтернативам на основе решёток.