

Исследование с использованием моделирования: дифференциально приватное федеративное обучение с политикой нулевого доверия для медицинских IoT-устройств

Источник: Frontiers in Digital Health

Оригинал: <https://www.frontiersin.org/articles/10.3389/fdgth.2026.1807342>

Internet of Medical Things (IoMT)

ЭКГ

безопасность данных

диагностика

дифференциальная приватность

нулевое доверие

федеративное обучение

Искусственный интеллект всё чаще применяется в системах подключенных медицинских устройств для классификации физиологических сигналов и непрерывного мониторинга. В данной статье представлено исследование моделирования обучающего слоя и слоя политик нулевого доверия в рамках федеративного обучения для устройств Интернета медицинских вещей (IoMT). Реализованный прототип объединяет федеративное усреднение, гауссово возмущение обновлений клиентов, оценку доверия на уровне устройства и фильтрацию аномальных обновлений клиентов по величине градиента. Это исследование моделирования слоев федеративного обучения и политик нулевого доверия; криптографические компоненты, защищенный транспорт и аппаратная аттестация моделируются как соображения по развертыванию или накладные расходы и не реализуются в виде полноценных физических или протокольных модулей. Используя конвейер классификации ЭКГ, описанный в методологии, мы сравниваем централизованное обучение, традиционное федеративное обучение, дифференциально приватное федеративное обучение и предложенную конфигурацию федеративного обучения с нулевым доверием. Для предложенной конфигурации ZT-FL сообщается об точности 0,928, F1-мере 0,920 и площади под ROC-кривой (AUC) 0,968. Эти результаты подтверждают

целесообразность в рамках заявленного объема моделирования и не устанавливают клиническую валидность, формальный сквозной учет дифференциальной приватности, всестороннюю устойчивость к вредоносным воздействиям, соответствие нормативным требованиям или готовность к постквантовой криптографии.

Перевод выполнен: 29.09.2026 | ai4med.ru

Машинный перевод. Рекомендуем сверять с оригиналом при клиническом использовании.