УДК 004.056.5

МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ С ФЕДЕРАТИВНЫМ ОБУЧЕНИЕМ

Еритенко Н.А. (Университет ИТМО)
Научный руководитель – Менщиков А.А. (Университет ИТМО)

Аннотация. Данная работа посвящена анализу и систематизации современных аспектов технологии федеративного обучения: структурных и функциональных моделей, векторов и типовых алгоритмов атак, а также инструментов для уменьшения уязвимостей системы относительно данных злонамеренных действий для последующего формирования методики построения защищенных систем с федеративным обучением. Предложены предварительные варианты метрик, значения которых позволят оценить степень защищенности подобных систем.

Введение. Федеративное обучение - это развивающаяся схема машинного обучения, направленная на решение проблемы хранения данных при сохранении конфиденциальности. Оно объединяет локальные модели, обученные по локализованным данным, хранящимся у каждого клиента, для обновления обобщенной глобальной модели. Федеративное обучение в первую очередь устраняет проблемы конфиденциальности, но в нем отсутствует аудит локальных данных и контроль за поведением участников, что, вероятно, приведет к возникновению проблем с безопасностью. Чтобы построить безопасную систему, использующую технологию федеративного обучения, при ее проектировании необходимо исследовать возможные комбинации алгоритмов машинного обучения, датасетов, фреймворков, получить различные метрики эффективности и устойчивости разработанной системы.

Основная часть. Существуют разные топологии систем с федеративным обучением: централизованная – с единым центром-агрегатором обобщенной обучаемой модели, децентрализованная – агрегатором является каждый из клиентов и иерархическая – топология, имеющая структуру, подобную той, что используется DNS-серверами (системой доменных имен). Систему с федеративным обучением обычно можно поделить на условные две части: «удаленные пользователи» и «агрегатор». В централизованном и иерархическом вариантах федеративной системы каждый пользователь имеет доступ к своей собственной обучающей выборке и загружает на вышестоящий агрегирующий сервер результат обучения. В децентрализованном – каждый клиент является агрегатором. Разработка контрмер против атак безопасности является более сложной задачей, чем у классического, централизованного, не федеративного обучения, из-за отсутствия доступа к данным и ограниченного контроля над клиентами и имеет свои нюансы и особенности в зависимости от конфигурации.

Выводы. Для упрощения построения подобного рода систем необходим единый стандарт разработки и проектирования, которого не существует. Аналогом этого может послужить создание методики, которая позволит в систематизированном и упрощенном порядке спроектировать систему, отдавая отчет в возможных последствиях того или иного решения. Методика будет нести рекомендательный характер и будет охватывать текущие достижения и технологии, оставаясь, тем не менее, актуальной как системный подход. Данная работа является следующей ступенью для формирования алгоритма построения защищенных систем с федеративным обучением.

Список использованных источников:

1. K.Bonawith et al. Practical Secure Aggregation for Privacy-Preserving Machine Learning // CCS '17: Proceedings of the 2017 ACM SIGSAC // Conference on Computer and Communications Security - October 2017 // URL: https://doi.org/10.1145/3133956.3133982

2. Q Li, Z Wen, Z Wu, S Hu, N Wang, Y Li, X Liu, B He. A Survey on Federated Learning Systems: Vision, Hype and Reality for Data Privacy and Protection - 2021 // URL: https://doi.org/10.48550/arXiv.1907.09693

Еритенко Н.А. (автор) Подпись

Менщиков А.А. (научный руководитель) Подпись