УДК 004.056.5

МЕТОДЫ КОНФИДЕНЦИАЛЬНОЙ ОБРАБОТКИ ДАННЫХ В СЕТЯХ IOT

Иогансон И. Д. (Университет ИТМО)
Научный руководитель – доцент, д. т. н. Беззатеев С. В.
(Университет ИТМО)

Введение. В последние годы технологии Интернета Вещей (Internet of Things, IoT) набирают все большую популярность. Сеть IoT зачастую представляет из себя множество различных устройств IoT, объединённых в одной локальной сети, которые могут взаимодействовать (передавать данные или получать команды) с облачной инфраструктурой (удаленными серверами и хранилищами данных), которые отвечают за обработку и хранение полученной от устройств информации. Устройства IoT представляют собой, как правило, маломощные вычислительные устройства, которые собирают данные и обмениваются ими по сети. Это могут быть датчики, актуаторы, умные девайсы, промышленные контроллеры и другие устройства, способные взаимодействовать с окружающей средой, собирать и передавать данные.

Основной проблемой такого подхода является то, что с увеличением количества устройств в сети растет и нагрузка на облачную инфраструктуру и сеть. Также становится сложнее управлять безопасностью, так как все данные с устройств собираются в одном месте. Для решения этих проблем существуют различные методы, позволяющие обрабатывать данные непосредственно на устройствах и отправлять в «облако» только результат вычислений.

Основная часть. Одними из рассмотренных методов являются конфиденциальные вычисления. Конфиденциальные вычисления (Multi-Party Computation, MPC) – это криптографические протоколы, которые позволяют нескольким сторонам совместно выполнять вычисления над своими приватными данными, сохраняя при этом конфиденциальность этих данных. В MPC каждая сторона имеет свои собственные входные данные, и цель состоит в том, чтобы получить результат вычислений, не раскрывая свои конфиденциальные данные другим участникам.

Другими рассмотренными методами являются вычисления с помощью схем гомоморфного шифрования. Гомоморфное шифрование (Homomorphic Encryption) – это схема шифрования, которая позволяет выполнять операции над зашифрованными данными без необходимости их расшифровывать. Другими словами, гомоморфное шифрование позволяет производить вычисления над зашифрованными данными, не раскрывая исходные данные.

Выводы. В данной работе были рассмотрены различные методы конфиденциальной обработки данных, а также проведен анализ того насколько данные методы соответствуют требованиям, предъявляемым сетями IoT.

Список использованных источников:

1. Goyal, Himanshu & Saha, Sudipta. (2022). Multi-Party Computation in IoT for Privacy-Preservation. 10.48550/arXiv.2206.01956.
2. Loukil, Faiza & Ghedira, Chirine & Boukadi, Khouloud & Benharkat, Aïcha-Nabila. (2021). Privacy-Preserving IoT Data Aggregation Based on Blockchain and Homomorphic Encryption. Sensors. 21. 2452. 10.3390/s21072452.
3. Mohanta, B. K., Jena, D., & Sobhanayak, S. (2020). Multi-party computation review for secure data processing in IoT-fog computing environment. International Journal of Security and Networks, 15(3), 164. doi:10.1504/ijsn.2020.109697

Иогансон И. Д. (автор) Подпись

Беззатеев С. В. (научный руководитель) Подпись