

Исследование и разработка метода безопасной обработки данных в системах IoT

Сабирзянов И.Р.

Санкт-Петербург, Университет ИТМО

Научный руководитель – доцент, Донецкая Ю.В.

Санкт-Петербург, Университет ИТМО

Аннотация.

Анализ современных способов и методов безопасной обработки информации в IoT системах. Разработка защищенной архитектуры IoT системы и метода сжатия информации, основываясь на существующих решениях.

Введение.

Индустрия 4.0 предполагает новый подход к производству, основанный на массовом внедрении информационных технологий в промышленность, масштабной автоматизации бизнес-процессов и распространении искусственного интеллекта. Характерными чертами Индустрии 4.0 являются полностью автоматизированные производственные мощности, где все процессы управляются в режиме реального времени и с учетом меняющихся внешних условий. Киберфизические системы создают виртуальные копии объектов физического мира, управляют физическими процессами и принимают децентрализованные решения. Они способны объединяться в одну сеть, взаимодействовать в режиме реального времени, самонастраиваться и самообучаться. Одна из основных технологий, которая приведет к революции в современных производствах — это Интернет вещей (IoT). В этой технологии Интернет используется для обмена информацией между различными устройствами, датчиками и т.д. Такие устройства могут обмениваться данными и обрабатывать их без вмешательства человека. Одной из главных проблем таких систем является безопасная обработка и безопасное хранение генерируемых данных, их бесперебойная передача по сети.

Актуальность защиты обработки информации в системах Интернета вещей заключается в:

- 1) Снижение затрат на развертывание систем интернета вещей;
- 2) Снижение возможных потерь при получении конфиденциальной информации 3 лицами;
- 3) Снижение затрат на восстановление нормального функционирования системы интернета вещей.

Основная часть.

В данной работе представлен анализ существующих решений в области защищенной обработки информации IoT устройствами. Представлена сводная таблица всех проанализированных решений, описаны их достоинства и недостатки, а также определены свойства безопасности информации, подвергающиеся изменениям в результате применения таких решений. После анализа существующих защищенных способов обработки информации в IoT, наилучшие из них применяются в разработке собственной защищенной архитектуры системы IoT. В работе изображены блок-схемы процессов взаимодействия пользователя с такой системой, процессов регистрации и аутентификации, процесса генерации и обработки информации. Представлен

общий анализ существующих способов сжатия информации, в частности уменьшения объема визуальных данных при помощи алгоритмов машинного обучения.

Выводы.

Внедрение решений, основанных на новых технологиях, таких как fog/cloud IoT, требуют изучения аспектов кибербезопасности для оценки соответствующих мер по обеспечению безопасности инфраструктуры. Эта работа предоставляет анализ способов и методов обработки информации, генерируемой инфраструктурой интернета вещей на основе соответствующих решений в литературе. В работе проанализированы существующие методы сжатия данных и рассмотрены защищенные архитектуры систем Интернета вещей, описаны их преимущества и недостатки, а также названы свойства безопасности, подвергающиеся изменениям в результате применения таких решений. На основе проанализированных методов была предложена новая четырехуровневая архитектура на основе fog, которая должна обеспечить безопасное хранение и эффективную передачу данных Интернета вещей в реальном времени с наименьшей задержкой. Также были предложены схемы безопасной регистрации и схема действий пользователя в системе.

Сабирзянов И.Р. (автор)

Подпись

Донецкая Ю.В. (научный руководитель)

Подпись