АРХИТЕКТУРА БЕЗОПАСНОЙ IoT-СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ EDGE COMPUTING

Махмудов Шохжахон Дадажон угли, Хатамов Артур Пулатович
Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий
matm37543@gmail.com, a.xatamov@tuit.uz

Аннотация

В данной работе рассматриваются вопросы повышения информационной безопасности в системах Интернета вещей, функционирующих в условиях высокой распределённости и ограниченных вычислительных ресурсов. Предложена архитектура IoT-системы с использованием edge computing, позволяющая выполнять обработку данных на периферийном уровне и тем самым снижать задержки и нагрузку на сеть. Особое внимание уделено механизмам обнаружения аномалий в сетевом трафике и повышению устойчивости системы к кибератакам. Проведён сравнительный анализ традиционной облачной архитектуры и предложенного подхода, результаты которого демонстрируют существенные преимущества использования edge computing.

Ключевые слова: IoT, edge computing, информационная безопасность, аномалии, распределённые системы, киберугрозы.

Основная часть

Развитие Интернета вещей привело к широкому внедрению интеллектуальных систем в различные сферы, включая промышленность, сельское хозяйство, транспорт и городскую инфраструктуру. Увеличение количества подключённых устройств сопровождается ростом объёма передаваемых данных и повышением требований к их обработке. Вместе с

этим усиливаются угрозы информационной безопасности, поскольку IoT-системы часто обладают низким уровнем защиты и ограниченными вычислительными возможностями [1,2].

Традиционные архитектуры, основанные на централизованной обработке данных в облаке, сталкиваются с рядом проблем, таких как высокая задержка, перегрузка сети и уязвимость к централизованным атакам. В связи с этим особую актуальность приобретает концепция edge computing, предполагающая перенос вычислений на уровень, близкий к источнику данных [3].

Целью настоящей работы является разработка архитектуры безопасной IoT-системы с использованием edge computing и оценка её эффективности с точки зрения производительности и защиты данных. В ней рассматривается распределённая IoT-система, включающая множество устройств, генерирующих поток данных в режиме реального времени.

Основной задачей является обеспечение своевременной обработки информации, минимизация задержек передачи данных и выявление потенциальных угроз безопасности.

Необходимо разработать архитектурное решение, позволяющее:

- выполнять анализ данных на периферийном уровне
- обнаруживать аномалии в сетевом трафике
- снижать нагрузку на центральные серверы
- повышать устойчивость системы к внешним атакам

Разработанная архитектура включает три уровня:

- Первый уровень представлен IoT-устройствами, осуществляющими сбор данных с окружающей среды. Эти устройства характеризуются ограниченными вычислительными ресурсами и выполняют базовые функции передачи информации.

- Второй уровень - периферийный (edge layer). На данном уровне располагаются вычислительные узлы, обеспечивающие предварительную обработку данных. Здесь выполняется фильтрация, агрегация и анализ

информации, включая обнаружение аномалий. Основное преимущество данного уровня заключается в снижении объёма передаваемых данных и уменьшении времени отклика системы.

- Третий уровень - облачный. Он используется для хранения данных, проведения глубокого анализа и обучения моделей. Облачный уровень также обеспечивает централизованное управление системой.

Такое разделение позволяет эффективно распределить нагрузку и повысить общую устойчивость системы.

Для обеспечения безопасности предложенной архитектуры используются следующие подходы.

В первую очередь, реализуется механизм обнаружения аномалий на основе анализа сетевого трафика. Система отслеживает изменения в поведении устройств и выявляет отклонения от нормального состояния. Затем, применяется распределённая обработка данных, при которой критически важные вычисления выполняются на периферийных узлах. Это снижает вероятность успешной атаки на центральную систему. И в конце, минимизируется объём передаваемой информации за счёт предварительной обработки данных. Это уменьшает риск их перехвата и снижает нагрузку на сеть.

Для оценки эффективности предложенной архитектуры было проведено моделирование с использованием набора тестовых данных, имитирующих работу IoT-сети [4].

Сравнивались два подхода:

1. традиционная облачная обработка;
2. архитектура с использованием edge computing.

По результатам моделирования было получено следующее:

- средняя задержка обработки данных в облачной системе составила около 250 мс, тогда как при использовании edge computing она снизилась до 80 мс;
- точность обнаружения аномалий увеличилась с 85% до 94%;

- нагрузка на сеть уменьшилась за счёт сокращения объёма передаваемых данных.

Графическое отображение результатов работы в виде гистограммы представлено на рисунке 1.

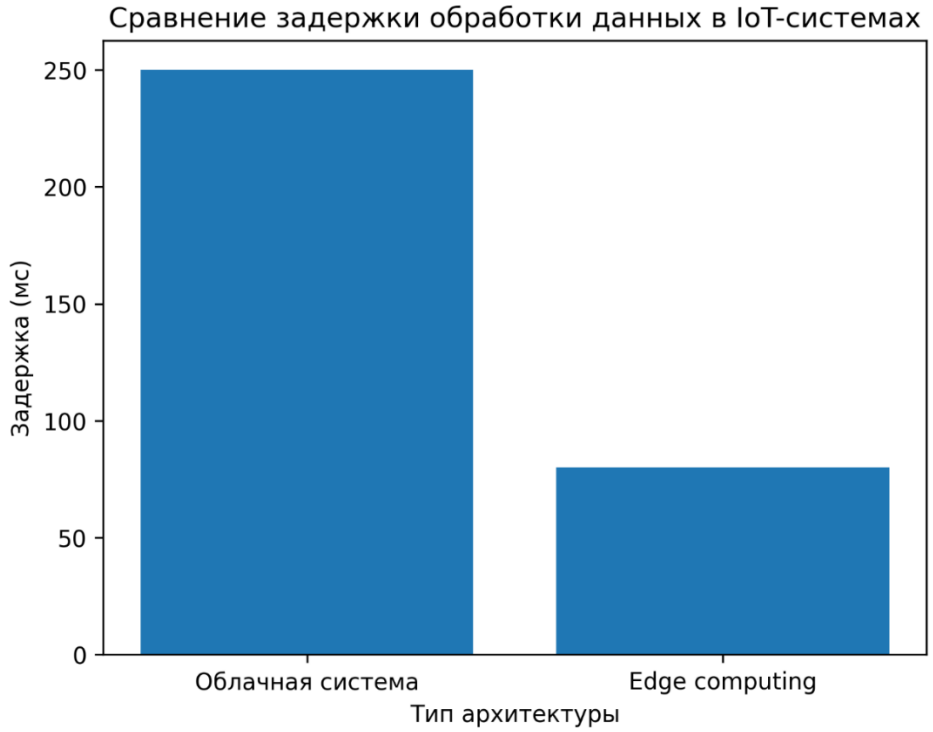

Рис.1. Гистограмма сравнения задержки двух архитектур

Результаты исследования подтверждают, что использование edge computing значительно повышает эффективность IoT-систем. Снижение задержек особенно важно для приложений реального времени, где требуется мгновенная реакция системы. Повышение точности обнаружения аномалий свидетельствует о возможности более раннего выявления угроз.

Кроме того, распределённая архитектура снижает зависимость от центральных узлов и повышает устойчивость системы к сбоям и атакам.

В работе предложена архитектура безопасной IoT-системы с использованием edge computing. Проведённый анализ показал, что данный подход позволяет существенно снизить задержки обработки данных, уменьшить нагрузку на сеть и повысить уровень информационной безопасности.

Список использованной литературы

1. Abbasi N., Soltanaghaei M., Zamani Boroujeni F. Anomaly detection in IoT edge computing using deep learning. Journal of Supercomputing, 2024.

2. Yu X., Yang X., Tan Q. An edge computing-based anomaly detection method in IoT. Applied Soft Computing, 2022.

3. Sicari S., Rizzardi A., Grieco L.A. Security, privacy and trust in Internet of Things. Computer Networks, 2015.

4. Karimov B., Turaev S. IoT tizimlarida axborot xavfsizligini ta’minlash usullari // Axborot texnologiyalari va boshqaruv, 2021.