МИКРОСЕРВИСЫ И ОБЛАКА В РАЗРЕЗЕ IoT

Басов Д.А., Жук Д.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Селезнёв И.Л. – к.т.н.,доцент

Устройства, составляющие инфраструктуру IoT управляют и собирают всевозможные форматы данных, что существенно повышает сложность разработки, поддержки и расширяемости решений в данной области. Возможным вариантом выхода из данной ситуации является преобразование данных IoT в базу данных пользователей и обеспечить выполнение запросов к ней с помощью микросервисов. Это решение позволяет эффективно проводить проверку подлинности данных от контроллеров IoT и проводить аналитику в формате больших данных.

Интернет вещей (IoT), который соединяет и обеспечивает связь между обширной сетью датчиков, приборов и объектов, является сегодня одной из самых перспективных ИТ концепций. IoT на настоящее время производит революцию во многих сферах, от автоматизации вождения автомобилей до личных помощников. Бизнес рассматривает IoT как возможность подключить миллиарды новых устройств к Интернету и генерировать большие суммы доходов.

Эти аргументы заставляют задать фундаментальный вопрос, что же на самом деле означает IoT? Большинство принимает этот термин дословно, полагая, что он просто подразумевает подключение датчиков на различных устройствах и сами машины непосредственно к сети Интернет. Тем не менее, эта модель создает потенциальные проблемы. Если IoT датчики и элементы управления находятся в сети Интернет, они могут быть подвержены атакам из любой точки всемирной паутины.

В то же время, сегодня уже миллиарды датчиков и элементов управления размещены как в домах, так и в офисах – и они не просто подключены к Интернет. Линии питания и подключения большинства современных датчиков и элементов управления обеспечивают их связь с единым контроллером, который интерпретирует полученные данные и действует на основе результатов их обработки. В последнее время эти контроллеры получили возможность подключения к сети Интернет, и большинство систем «Умный дом» использует именно эту модель.

В модели контроллера владелец дома или бизнеса устанавливает датчики и контрольные точки, обеспечивающие связь с контроллером. Контрольная точка осуществляет основные функции управления, а также может отправлять данные на мобильное устройство для удаленного управления. Контроллер должен быть подключен к сети Интернет и обеспечивать гарантии безопасности. Данная модель контроллера может решить многие вопросы безопасности IoT для пользователей. Тем не менее, другие проблемы остаются, например, неопределенность с протоколированием и сертификацией форматов данных, задача поиска и аутентификации датчика. Решение этих вопросов может привести к внедрению значительных изменений для облачной среды организации.

Переосмысление подхода к IoT. Сенсорные устройства управляют и собирают различные форматы данных. Пользователи, подключающиеся к датчику IoT, вряд ли знают формат данных обмена, кроме случая, когда они стандартизированы. Не зная формата данных, интерпретировать их и осуществлять управление невозможно. Развитая инфраструктура IoT предполагает большое количество датчиков и множество их мест размещения. Данные, поступающие от одного типа сенсоров ситуативны и отражают условия непосредственно в зоне своего охвата.

Одним из решений является преобразование данных IoT в базу данных пользователей, обеспечение выполнения запроса к которой можно осуществлять с помощью микросервисов. Аналитики могут извлечь данные по запросу -- не только на текущий период, но также и за прошлые периоды, если проверку подлинности данных от контроллеров IoT собирать в удобном формате больших данных. Процесс хранения может помочь согласовать форматы данных от разных датчиков в общий слой и идентифицировать данные по местоположению или множеству других факторов, которые облегчают к ним доступ и их использование.

Предлагаемая модель базы данных переносит IoT из локальной сети в облако (рисунок 1). Пользователям по-прежнему необходимо собирать данные от устройств IoT, но также идентифицировать и хранить их, чтобы обеспечить легкость доступа. Эта модель также требует, чтобы решения безопасности IoT организации перешли на уровень облачных сред, а не оставались на уровне сети. Облачные активы, развивающиеся для использования через приложения без непосредственного участия приложений (как и активы IoT, поскольку датчики не являются частью пользовательских приложений) также требуют специального планирования для решения вопросов форматов данных и поддержки синхронизированного анализа данных от нескольких источников IoT. Если архитектура на основе контроллеров, может решить эту проблему, то масштабируемость приложений IoT может оказаться сложной задачей.

IoT подход на основе баз данных и микросервисов также предлагает улучшение поддержки конфиденциальности и политики безопасности. Так как шаблоны запросов непосредственно видны, IoT системы, основанные на микросервисах и запросах, легче обнаружить при попытке отслеживать местоположение человека.

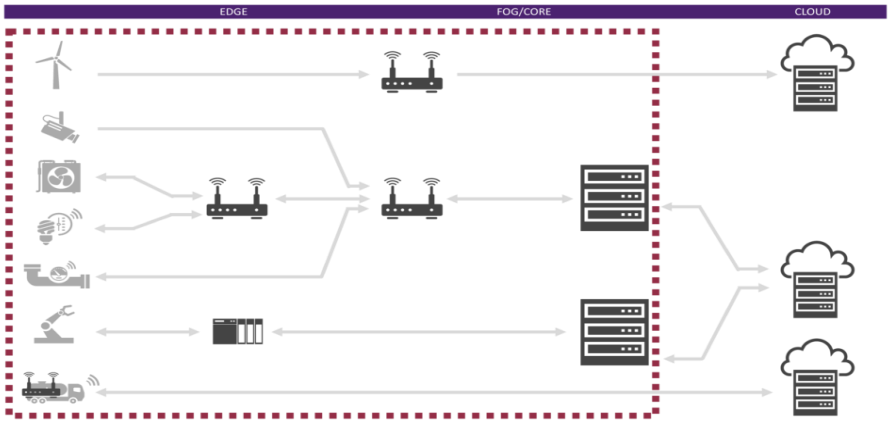

Рисунок 1 – Перенос IoT из локальной сети в облако

Миссия IoT состоит в подключении активов, обеспечивающих поступление ценной информации и влияющих на выполнение важных задач, но поток информации от этих активов является основой в инфраструктуре интернета вещей. Принятие подхода к IoT, основанного на базах данных, может предоставить всю необходимую нам информацию без потенциальных рисков и затрат.

Список использованных источников:

1. Building Microservices: Designing Fine-Grained Systems / Sam Newman // O'Reilly Media 2015 -- 280 s
2. Интернет вещей. Исследования и область применнения / Е. Зараменских, И. Артемьев // Инфра-М 2017 – 188 с.
3. Архитектура интернета вещей / Ли Перри // ДМК-Пресс, 2019 – 454 с.

ПРИМЕНЕНИЕ АЛГОРИТМА ОБРАТНОГО РАСПРОСТРАНЕНИЯ ОШИБКИ ДЛЯ КОЛОРИЗАЦИИ ИЗОБРАЖЕНИЙ

Беликова Т.О., Евсаев П.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лукашевич М.М. – к.т.н., доцент

Колоризация – любой процесс, в результате которого в последовательность изображений или в монохромное изображение добавляется цвет.

Алгоритм обратного распространения ошибки представляет собой распространение сигналов ошибки от выходов сети к её входам, применяя градиентные методы оптимизации и осуществляя подбор весов для многослойной сети [1]. Ключевым фактором здесь является целевая функция, которая формируется в виде квадратичной суммы разностей между полученными и требуемыми значениями выходных сигналов.

Для обучения сети нужны обучающая выборка и расчёт соответствующих значений сигналов нейронной сети, а также необходимо минимизировать значения целевой функции. Выборка будет состоять из цветных изображений, их полутоновых копий изображений локальных признаков, построенные для каждого полутонового изображения. Одним из способов обучения для непрерывной целевой функции является градиентные методы оптимизации.

Каждый цикл обучения состоит из следующих этапов [1]:

1) сгенерировать входные сигналы и вычислить производные значения функции активации каждого слоя, значения выходных слоёв (включая скрытый слой);

2) изменить направления сигналов и заменить функции активации на производные от них, подать разность между ожидаемым и полученным значением на новый вход сети и произвести расчёт значений требуемых обратных разностей;

3) на основе результатов, полученных в п.1 и 2, обучить оригинальную сеть и сеть обратного распространения ошибки;