GeekBrains

Кибернетика умных устройств

Архитектура IoT решений

Оглавление

Введение

На данном занятии мы рассмотрим архитектуру IoT решений, узнаем из чего состоит экосистема интернета вещей. Посмотрим, как вещи могут взаимодействовать между собой или с информационными системами.

Экосистема в IoT

Интернет вещей (Internet of Things, IoT) представляет собой концепцию вычислительной сети, включающей физические объекты, именуемые «вещами», в которых присутствуют технические приемо-передающие средства связи, обеспечивающие взаимодействие между вещами или между вещами и внешней средой.

С помощью «Интернета вещей» взаимодействие объектов, среды и людей будет во многом переплетено, что обещает сделать мир «умным» — более благоустроенным для человека.

Развитие IoT в целом связано не только с увеличением числа «подключенных» устройств, но и с формированием технологической экосистемы, представленной технологическими решениями, позволяющими собирать, передавать, агрегировать данные, а также платформы, обеспечивающей обработку данных и их использование при создании «умных» решений.

Далее, рассмотрим основные составляющие экосистемы:

Технологическая экосистема IoT

- **Датчики**: встроенные системы, операционные системы реального времени, источники бесперебойного питания, микроэлектромеханические системы (МЭМС);
- **Системы связи между датчиками**: зона охвата беспроводных персональных сетей составляет от нескольких сантиметров до нескольких километров. Для обмена данными между датчиками применяются низкоскоростные маломощные информационные каналы, которые часто построены не на протоколе IP;
- **Локальные вычислительные сети**: обычно это системы обмена данными на основе протокола IP, например, 802.11 Wi-Fi-сеть для быстрой радиосвязи, часто это пиринговые или звездообразные сети;
- **Агрегаторы, маршрутизаторы, шлюзы**: поставщики встроенных систем, самые бюджетные составляющие (процессоры, динамическая оперативная память и система хранения данных), производители модулей, производители пассивных компонентов, производители тонких клиентов, производители сотовых и беспроводных радиосистем, поставщики межплатформенного программного обеспечения, разработчики инфраструктуры туманных вычислений, инструментарий для граничной аналитики, безопасность граничных устройств, системы управления сертификатами;
- **Глобальная вычислительная сеть**: операторы сотовой связи, операторы спутниковой связи, операторы маломощных глобальных сетей (Low-Power Wide-Area Network, LPWAN). Обычно применяются транспортные протоколы интернета для IoT и сетевых устройств (MQTT, CoAP и даже HTTP);
- **Облако**: инфраструктура в качестве поставщика услуг, платформа в качестве поставщика услуг, разработчики баз данных, поставщики услуг потоковой и пакетной обработки данных, инструменты для анализа данных, программное обеспечение в качестве поставщика услуг, поставщики данных, операторы программно-определяемых сетей, сервисы машинного обучения;
- **Анализ данных**: огромные массивы информации передаются в облако. Работа с большими объемами данных и получение из них пользы – это задача, требующая комплексной обработки событий, аналитики и приемов машинного обучения;
- **Безопасность**: при сведении всех элементов архитектуры воедино встают вопросы безопасности. Безопасность касается каждого компонента: от датчиков физических величин до ЦПУ и цифрового

аппаратного обеспечения, систем радиосвязи и самих протоколов передачи данных. На каждом уровне необходимо обеспечить безопасность, достоверность и целостность. В этой цепи не должно быть слабых звеньев, поскольку интернет вещей станет главной мишенью для хакерских атак в мире.

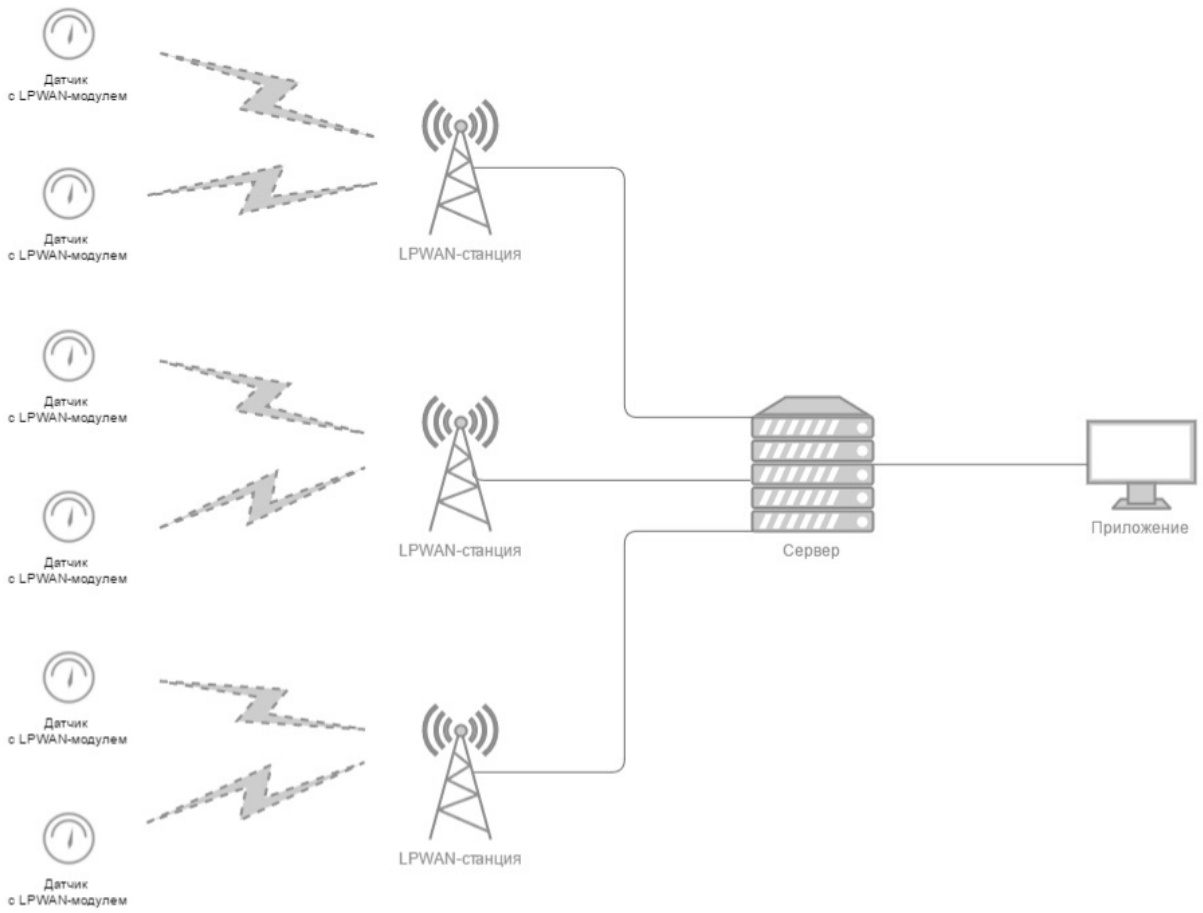
Как упоминалось на прошлом занятии, подобная экосистема вовлекает в себя огромное количество профессиональных сфер и специалистов из различных технических областей:

- **Физиков**, которые занимаются разработкой новые типы сенсорных устройств (датчиков), а также стремятся совершить революцию в сфере элементов питания, пытаясь продлить срок службы батареек на годы.
- **Инженеров-программистов** встраиваемых систем, которые работают над инновационными устройствами.
- **Сетевых инженеров**, умеющие работать с персональными сетями и глобальной вычислительной сетью, а также с программно-конфигурируемыми сетями.
- **Специалистов по работе с данными**, работающие над новейшими схемами машинного обучения на граничных устройствах и в облаке.
- **DevOps-инженеры**, которые успешно реализуют облачные решения различных масштабов.

Интернет вещей всегда будет нуждаться в поставщиках услуг, например, компаниях, занимающихся реализацией проектов, системных интеграторах, поставщиках комплексных систем и изготовителях комплектного оборудования.

Архитектура LPWAN сетей

Технологической основой интернета вещей является LPWAN. LPWAN (Low-power Wide-area Network – «энергоэффективная сеть дальнего радиуса действия») – беспроводная технология передачи небольших по объёму данных на дальние расстояния, разработанная для распределённых сетей телеметрии, межмашинного взаимодействия и интернета вещей. LPWAN является лишь одной из беспроводных технологий, обеспечивающих среду сбора данных с различного оборудования: датчиков, счётчиков и сенсоров. Принцип работы LPWAN-сетей показан на рисунке ниже.



Принцип работы LPWAN-сетей (топология звезда)

В основе принципа передачи данных по технологии LPWAN лежит физическое свойство радиосистем – повышение энергетики сообщений, означающее, что при уменьшении скорости передачи данных – увеличивается дальность связи. Чем ниже битовая скорость передачи, тем больше энергии вкладывается в каждый бит и тем легче выделить его на фоне шумов в приёмной части системы. Таким образом, низкая скорость передачи данных позволяет добиться большей дальности

распространения радиосигнала, и, как следствие, увеличения радиуса действия принимающей станции.

Стоит отметить, что существующие технологии коммуникаций через сотовую сеть не оптимизированы под требования устройств с низким энергопотреблением и малыми объемами данных, поэтому основной рост IoT будет связан с совершенствованием существующих сотовых сетей и массовым распространением LPWAN сетей, таких как LoRaWAN.

Распределение технологий среди беспроводных устройств можно увидеть на рисунке ниже.

	ЛОКАЛЬНАЯ СЕТЬ Ближний радиус действия	LPWAN Интернет вещей	СОТОВАЯ СЕТЬ M2M
	40%	45%	15%
+	Наличие стандартных протоколов	Низкое энергопотребление Низкая стоимость позиционирования	Существующее покрытие Высокая скорость передачи данных
-	Работа батареи Стоимость сети	Низкая скорость передачи данных	Автономность Общая стоимость владения
	ZigBee, Wi-Fi	LoRa	GSM, 3G+, H+, 4G

Распределение технологий среди беспроводных устройств

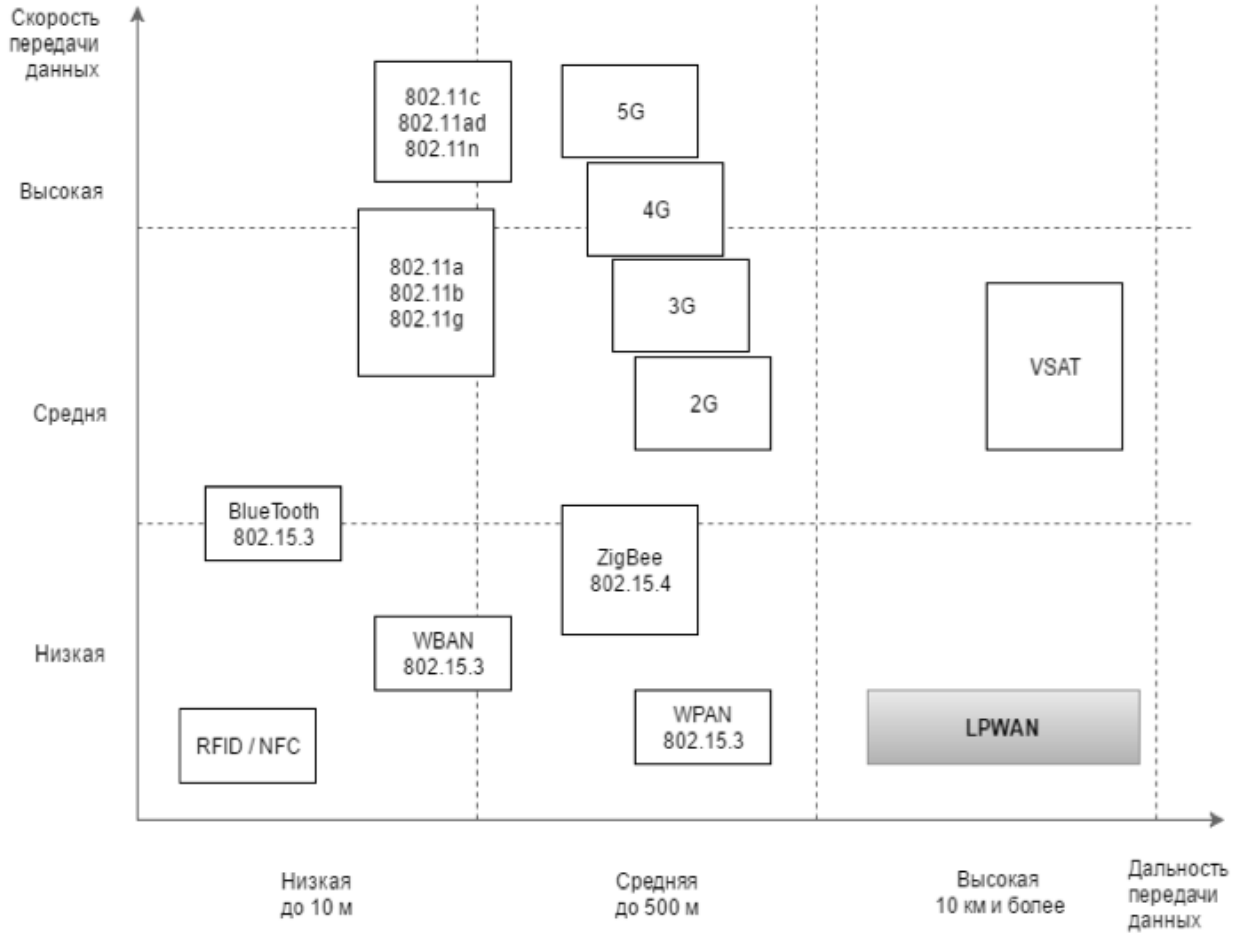
Подход, который используется для построения LPWAN-сети, схож с принципом работы сетей мобильной связи. LPWAN-сеть использует топологию «звезда», (на рисунке выше) в которой каждое устройство взаимодействует напрямую с базовой станцией. Сети городского или регионального масштаба строятся с использованием конфигурации «звезда из звезд».

Устройство или модем с LPWAN-модулем осуществляет передачу данных по радиоканалу на базовую станцию. Базовая станция принимает сигналы от о всех устройств в радиусе покрытия (своего действия), оцифровывает и передает на удаленный сервер, используя доступный канал связи: Ethernet, сотовая 3G/4G связь.

Полученные на сервере данные используются для отображения, анализа, построения отчетов и принятия решений.

Управление устройствами и обновление программного обеспечения происходит с использованием обратного канала связи.

Для передачи данных по радиоканалу, как правило, применяется не лицензируемый спектр частот, разрешенных к свободному использованию в регионе построения сети: 169 МГц, 433 МГц, 868/915 МГц, 2,4 ГГц. Место LPWAN-сетей в общем стеке различных технологий показана на рисунке ниже.



Распределение различных сетей по скорости и дальности передачи данных

На данный схеме сгруппированы технологии передачи данных в зависимости от скорости передачи данных и дальности передачи данных. Соответственно по схеме видно что первая технология RFID или NFC сочетает в себе низкую пропускную способность и довольно малый радиус действия. Следующая технология Bluetooth, которая часто используется в IoT, Позволяет передавать данные с чуть большей скоростью но на не очень большие расстояния. Далее можно выделить группу стандартов Wi-Fi 802.11 которые представляют собой различные стандарты протокола Wi-Fi которые в процессе эволюции значительно увеличивает скорость передачи данных и немного увеличивает дальность за счет более сложного кодирования передаваемых сигналов. Далее идёт группа стандартов сотовых сетей которые как мы знаем постоянно стремятся увеличить скорость, однако за счёт роста используемых частот дальность или радиус покрытия более новых стандартов сетей становится меньше. Отдельно можно выделить стандарт ZigBee, Который во многом схож со технологии Wi-Fi однако имеет другую

топологию (схему построения) сети, Ведущего позволяет передавать данные на относительно среднее расстояние с достаточной для этого скоростью. Также особняком стоит технология спутниковой передачи данных VSAT, которая является довольно дорогой, но способная обеспечивать передачу данных из отдалённых районов на большие расстояния при помощи спутников. Наконец отдельно можно выделить технология LPWAN, которая позволяет передавать данные на значительно дальние расстояния (в среднем около 10 км), что достигается за счёт снижения скорости передачи данных.

Технология LPWAN обладает рядом преимуществ, в том числе:

1. Большая дальность радиопередачи по сравнению с другими беспроводными технологиями, такими как GPRS или ZigBee, - до 10-15 км.
2. Низкое энергопотребление конечных устройств благодаря минимальной мощности, необходимой для передачи небольших пакетов данных.
3. Высокое проникновение радиосигнала в городских районах при использовании субгигагерцовых частот (например, 433 и 868 МГц).
4. Высокая масштабируемость сети на больших территориях.
5. Отсутствие необходимости получать разрешение на использование частот или платить за использование радиочастотного спектра, поскольку используются нелицензированные частоты.

LPWAN, как и любая другая технология передачи данных, имеет свои ограничения. К ним относятся:

1. Низкая пропускная способность: это связано с использованием низкочастотного радиоканала. Фактическая пропускная способность зависит от технологии передачи, используемой на физическом уровне, и составляет от нескольких сотен бит в секунду до десятков кбит в секунду.
2. Задержка передачи данных: Время, необходимое для передачи радиосигналов от датчика к конечному приложению, может привести к задержкам от нескольких секунд до десятков секунд.
3. Отсутствие единого стандарта: Не существует единого стандарта, определяющего физический уровень и контроль доступа к среде для беспроводных сетей LPWAN.

Таким образом, технология LPWAN ориентирована на приложения, требующие гарантированной передачи небольшого объема данных, возможности длительной работы сетевых устройств от автономных источников питания, большого территориального охвата беспроводной сетью.

Основными областями применения технологии LPWAN являются беспроводные сенсорные сети, автоматизация сбора показаний приборов учета, системы промышленного мониторинга и управления

Семейство технологий LPWAN является важным компонентом экосистемы Интернета вещей (IoT), поскольку она обеспечивает беспрепятственное подключение устройств с низким энергопотреблением и низкой пропускной способностью к Интернету через беспроводные сети дальнего радиуса действия, что может помочь предприятиям получить ценные сведения, повысить эффективность работы и стимулировать рост.

Каковы плюсы и минусы IoT?

Интернет вещей (IoT) имеет свои преимущества и недостатки, которые заключаются в следующем.

Преимущества

- Обеспечивает доступ к информации с любого устройства в любое время и в любом месте.
- Облегчает коммуникацию между подключенными электронными устройствами.
- Обеспечивает передачу пакетов данных по подключенной сети, что приводит к экономии времени и средств.
- Автоматизирует задачи, повышая тем самым качество услуг предприятия и снижая необходимость вмешательства человека.

Недостатки:

- По мере увеличения количества подключенных устройств и обмена информацией между ними возрастает вероятность кражи конфиденциальной информации хакерами.
- Управление и сбор данных с миллионов устройств IoT будет сложной задачей для предприятий.
- Системная ошибка может повредить каждое подключенное устройство.
- Для IoT не существует международного стандарта функциональной совместимости, что затрудняет взаимодействие устройств разных производителей друг с другом.

При этом существует множество проблем, мешающих внедрению IoT в больших масштабах. В основном они связаны с конструкцией современного интернета и прерывистой связью современных сетей. Существует несколько

аспектов, применимых к системам IoT, которые влияют на их архитектуру и реализацию, а именно:

1. **Масштабируемость**: масштабируемость для IoT-систем выражается в количестве датчиков и исполнительных устройств, подключенных к системе, в количестве сетей, которые соединяют их вместе, в количестве данных, связанных с системой, и скорости их перемещения, а также в количестве требуемой вычислительной мощности.
2. **Большие данные**: многие более продвинутые системы IoT зависят от анализа огромных объемов данных. Например, существует необходимость извлечения закономерностей из исторических данных, которые могут быть использованы для принятия решений о будущих действиях (например, предиктивное обслуживание). Извлечение полезной информации из сложных данных, таких как видео, – еще один пример анализа, требующего больших объемов обработки. Способность добывать существующие данные для получения новой информации и необходимость объединять различные наборы данных новыми способами — это характеристики, которые являются частью системы IoT. Таким образом, системы IoT часто являются классическими примерами обработки "больших данных".
3. **Облачные вычисления**: Системы IoT часто предполагают использование облачных вычислительных платформ. Облачные вычислительные платформы предлагают возможность использования большого количества ресурсов, как в плане хранения данных, так и в плане возможности предоставления гибких и масштабируемых ресурсов обработки для анализа данных. Системы IoT требуют использования разнообразного программного обеспечения для обработки данных, и адаптивность облачных сервисов, которые необходимы для того, чтобы справляться с новыми требованиями, обновлениями прошивки или системы и иметь возможность предлагать новые возможности с течением времени и меняющимися требования индустрии.
4. **Реальное время**: Системы IoT часто функционируют в режиме реального времени; данные о происходящих событиях поступают непрерывно, и может возникнуть необходимость в своевременной реакции на этот поток событий. Для этого может потребоваться обработка потока данных; действие на данные о событиях по мере их поступления, сравнение их с предыдущими событиями, а также со статическими данными, чтобы реагировать наиболее подходящим образом. Параллельно необходимо обеспечить обнаружение и предотвращение использования поврежденных данных – будь то в результате неисправности датчиков

или злонамеренных действий – поскольку использование поврежденных данных может нанести вред и ущерб людям, оборудованию и окружающей среде.

5. **Высокая распределенность**: Системы IoT могут охватывать целые здания, целые города и даже земной шар. Распределенность может также относиться к обработке данных – часть обработки происходит централизованно (в облачных сервисах), но обработка может происходить на границе сети, либо в шлюзах IoT, либо даже внутри (более мощных типов) датчиков и исполнительных устройств. Сегодня в мире официально больше мобильных устройств, чем людей.
6. **Гетерогенные системы**: Системы IoT часто строятся с использованием очень разнородного набора технологий. Это относится не только к датчикам и исполнительным механизмам, но и к типам задействованных сетей и разнообразию обрабатывающих компонентов. Обычно датчики представляют собой маломощные устройства, и часто эти устройства используют для связи специализированные локальные сети. Чтобы обеспечить доступ к подобным устройствам в масштабах Интернета, используется шлюз IoT.
7. **Безопасность и конфиденциальность**: Вопрос безопасности и надежности распределенных гетерогенных систем IoT является сложной проблемой, решения которой должны масштабироваться и развиваться вместе с системами. Получение гарантий того, что эти системы безопасны, надежны, устойчивы и оправдывают ожидания заинтересованных сторон в отношении конфиденциальности, является довольно сложной задачей.
8. **Соответствие требованиям**: Обеспечение уверенности в работе этих IoT-систем необходимо как в связи с нормативными требованиями конкретных отраслей, секторов и вертикалей, так и в связи с нормами и ожиданиями заинтересованных сторон IoT-систем.
9. **Интеграция**: Системы IoT не существуют сами по себе, но должны быть подключены к существующим операционным технологическим системам, таким как заводские системы, системы управления зданиями и другие типы систем управления физическими объектами, а также к существующим корпоративным системам, включая корпоративные приложения и корпоративные базы данных.

Стандарты совместимости IoT

Когда речь идет о сетевых устройствах Интернета вещей (IoT), две характеристики вызывают наиболее серьезные проблемы: маломощные устройства, предназначенные для работы в течение месяцев или даже лет без подзарядки, и частый обмен данными по сетям, в которых происходит потеря пакетов. К сожалению, существующие стандартные интернет-протоколы не являются оптимальными в таких условиях, что ведет к необходимости тщательного продумывания всего IoT решения

В более широком смысле имеет место дисбаланс между огромным количеством устройств, генерирующих данные с бешеной скоростью в разных местах, и использованием сетевых технологий. Эти сложности требуют определенных возможностей от сетевых протоколов во всей архитектуре сети от физического уровня к прикладному.

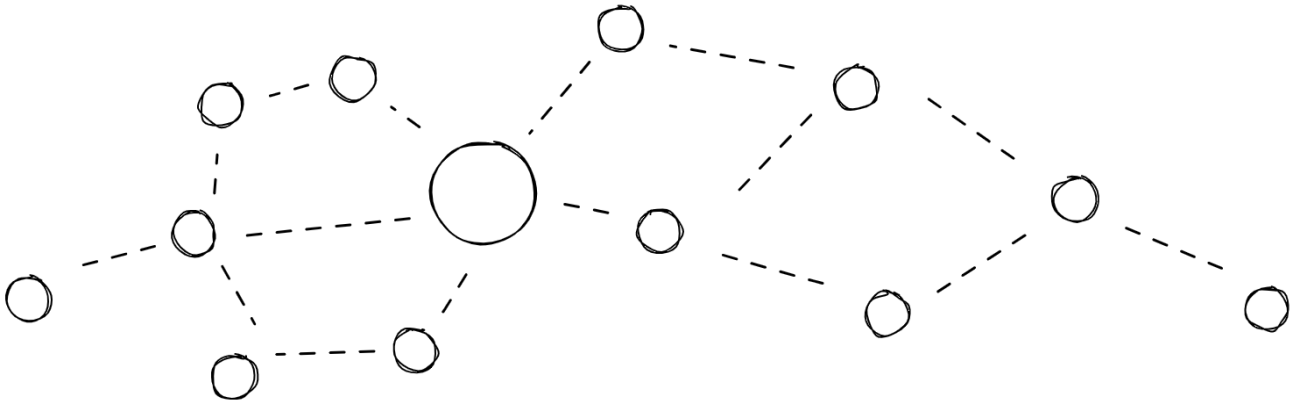
Всегда приходится выбирать, поэтому не забываем про диаграмму:

Интернет вещей и межмашинное (M2M) взаимодействие

Далее, поговорим о том, что же такое межмашинное взаимодействие или M2M (Machine to Machine). Потому что перед тем, как сформировался интернет вещей в том понимании, о котором мы говорим, изначально машины могли взаимодействовать лишь между собой.

Что же из себя представляет межмашинное взаимодействие (или M2M)? Эта концепция подразумевает, что устройство обменивается данными напрямую с другим устройством в рамках какой-либо локальной (закрытой, без доступа в интернет) сети. При этом M2M взаимодействие – это автономное взаимодействие: подразумевается возможность узла (одной из машин) инициировать сессию передачи данных и передачу этих самых данных от себя к какому-либо другому оборудованию (другому узлу или машине), при этом без участия человека. Важно понимать, что при M2M взаимодействии устройства очень ограничены, потому что они не имеют выхода в интернет и способны обмениваться информацией лишь между себе подобными устройствами, образуя своеобразную закрытую экосистему.

Схема M2M взаимодействия выглядит примерно следующим образом:



Логическим шагом развития данного подхода стала реализация функции доступа устройствам в интернет.

Каким же образом межмашинное взаимодействие может стать частью IoT? Достаточно просто, если в архитектуре сети заложен какой-то, граничный либо промежуточной маршрутизатор/концентратор (представьте себе аналог роутера с промежуточной обработкой), являющийся конечной точкой в общении между устройствами, и имеющий выход в интернет, занимаясь передачей данных во внешние системы для дальнейших их обработки.

Существует также альтернативный подход, в котором сбор и агрегирование данных с других устройств происходит на каком-то почти аналогичном устройстве, но с более мощной «начинкой» и с возможностью работы по сети.

В независимости от того, где и как происходит выход в интернет, отличительной чертой IoT-систем является то, что тем или иным образом они всегда имеют доступ к сети.

Благодаря возможности передачи полезной информации с умных устройств в сеть интернет, появляется возможность подсоединить простейшие устройства к облачной инфраструктуре различных сервис-провайдеров. Потому что до того, как, стандарты связи и облачные технологии перестали быть дорогостоящими и стали частью повседневной реальности, у умных устройств отсутствовал способ за короткий промежуток времени отправить данные другим устройствам, хранить информацию сколь угодно долго и анализировать данные, чтобы выявлять тенденции и шаблоны. По мере развития облачных технологий беспроводные системы связи стали повсеместными, появились современные эффективные и экономичные элементы питания, такие как литий-ионные аккумуляторы, в связи с чем устройства обрели рентабельность, а модели машинного обучения нашли новые направления практического применения. Это сильно укрепило позиции интернета вещей. Если бы все эти технологии не сошлись воедино именно в тот самый момент, когда это произошло, мы до сих пор жили бы в мире M2M.

M2M (Machine-to-Machine) взаимодействие имеет несколько основных недостатков или проблем:

- **Безопасность**: M2M соединения могут быть уязвимы для взлома, что может привести к компрометации данных или управления системой.
- **Ограниченность связи**: Некоторые типы M2M устройств могут иметь ограниченную дальность связи или быть зависимыми от доступности инфраструктуры, такой как покрытие сети.
- **Совместимость**: не все M2M устройства могут работать вместе, и может потребоваться дополнительная конфигурация или программирование для их интеграции при подключении новых устройств.
- **Нестабильность**: M2M соединения могут быть нестабильными из-за помех или других факторов окружающей среды, которые могут привести к потере данных или отключению соединения.
- **Сложность настройки и управления**: M2M системы могут быть сложными для настройки и управления, особенно если они состоят из множества разнородных устройств и протоколов.
- **Необходимость в поддержке**: M2M системы требуют регулярной обслуживания и поддержки для обеспечения их надежной работы.

- **Цена**: Конфигурация и установка M2M систем может быть дороже, чем стандартные методы коммуникации и управления.
- **Проблемы с доступностью данных**: из-за особенностей M2M взаимодействия, некоторые системы могут иметь проблемы с доступностью данных, когда информация не может быть получена в реальном времени или отсутствует на момент запроса.

Некоторые основные достоинства и преимущества M2M включают:

- **Автоматизация**: M2M системы позволяют автоматизировать процессы и обмен данными между устройствами, что может увеличить эффективность и снизить затраты.
- **Реальное время**: Многие M2M системы позволяют обмениваться данными в реальном времени, что может помочь принимать быстрые и обоснованные решения.
- **Удаленное контролирование**: M2M системы могут позволять удаленно контролировать и управлять устройствами и процессами, что может помочь снизить затраты на обслуживание и увеличить мобильность.
- **Сбор данных**: M2M системы могут позволять собирать и анализировать большое количество данных, что может помочь в принятии обоснованных решений и улучшить эффективность бизнес-процессов.
- **Связь между различными системами**: M2M системы могут позволять обмениваться данными между различными системами, что может помочь в решении задач и оптимизации бизнес-процессов.
- **Увеличение безопасности**: M2M системы могут помочь увеличить безопасность путем мониторинга и управления устройствами и процессами удаленно.
- **Снижение затрат**: M2M системы могут снизить затраты на обслуживание и оборудование, а также улучшить эффективность бизнес-процессов.
- **Инновационные приложения**: M2M технологии открывают множество новых возможностей для создания инновационных приложений и сервисов.
- **Масштабируемость**: M2M системы могут быть легко расширены и масштабированы в зависимости от потребностей бизнеса.
- **Удаленное управление**: M2M системы позволяют удаленно контролировать и управлять устройствами и процессами, что может снизить необходимость в постоянной наличии оператора или инженера на месте.
- **Автоматизация и оптимизация процессов**: M2M системы могут автоматизировать и оптимизировать различные бизнес-процессы,

например, мониторинг и управление запасами, мониторинг и управление энергоресурсами, мониторинг и управление транспортными средствами.

Погружение в архитектуру интернета вещей

Так как архитектура интернета вещей охватывает большое количество различных технологий и протоколов то архитекторы подобных решений должны комплексно подходить к созданию подобных решений: он должен понимать как вся система должна работать в целом и какие изменения понесёт в себе система в связи с изменением хотя бы одного из элементов этой системы. Вся эта сложность и многогранность интернета вещей связана с тем, что это сфера очень комплексная и она намного шире, чем любые традиционные технологии. Её отличает довольно большой масштаб и сочетание различных типов архитектур, которые в обычных сферах между собой могут быть не связаны.

В сфере интернета вещей существует огромное количество IoT-провайдеров, поставщиков облачных услуг, облачных платформ, систем управления, систем безопасности, платформ обработки и анализа данных, систем мониторинга, контроля и управления.

Определённую сложность сюда вносит довольно большое количество различных протоколов и типов сетей, глобальных, локальных, персональных, которые активно развиваются и меняются, но при этом имеют свои региональные ограничения.

Ошибка в выборе протокола при построении сети точно приведёт к ошибкам или проблемам в обмене данных между устройствами, возможно к снижению качества сигнала. Если решение имеет риск столкнуться с подобными проблемами, то необходимо учитывать возможность масштабирование решения в контексте сети. А еще необходимо учитывать интерференции и коллизии в различных типах сетей.

В таких решениях важно понимать каким образом данные снимаются с оконечного оборудования и с какой периодичностью передаются в интернет ввиду чего необходимо уделять достаточное время проработки алгоритмов работы умных устройств.

Необходимо учитывать риски по отказу системы как целиком, так и частично. Учитывать сроки и стратегии восстановления системы и проработать алгоритм работы в случае частичной потери данных или их временной недоступности.

Необходимо выбрать не только технологии передачи данных и построить архитектуру решения необходимо также выбрать необходимый интернет-протоколов, например MQTT*, либо CoAP*, AMPQ*, при помощи которых будет осуществляться передача данных от устройств на платформу.

💡 ***MQTT**: легкий протокол обмена сообщениями с публикацией и подпиской, используемый в IoT для обеспечения связи между устройствами и серверами.

💡 ***CoAP**: специализированный веб-протокол передачи данных, используемый в устройствах IoT с ограниченными ресурсами для обеспечения связи с Интернетом.

💡 ***AMQP**: протокол обмена сообщениями открытого стандарта, используемый для надежного обмена сообщениями между приложениями и системами в корпоративном и IoT контекстах.

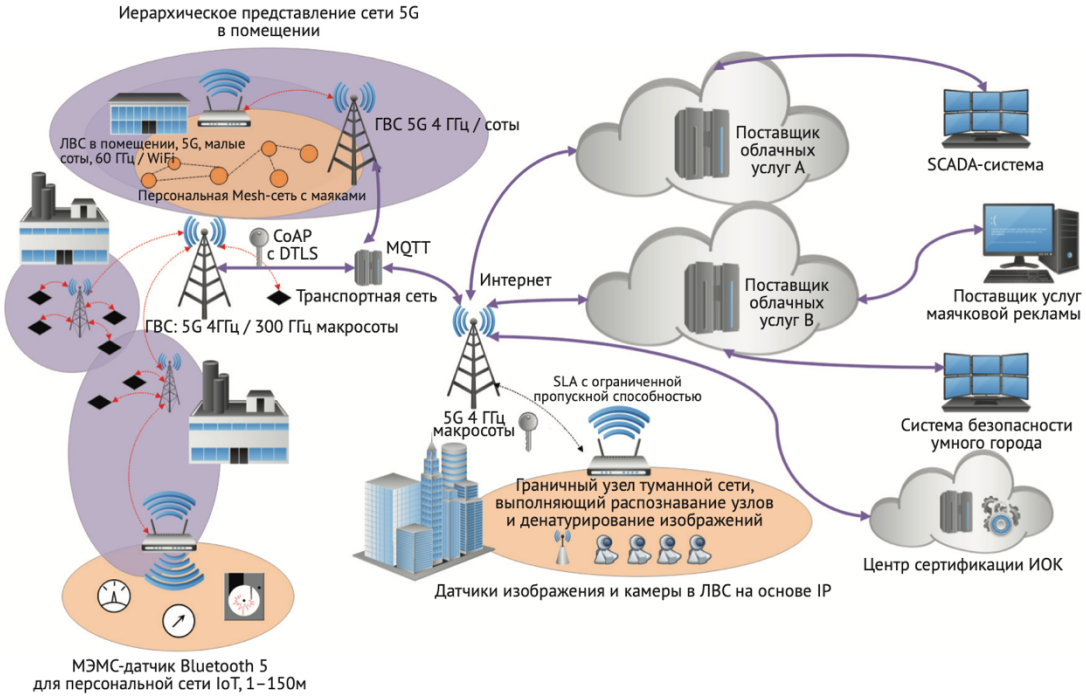
(более подробно данные протоколы будут рассмотрены на 5 занятии)

Необходимо предусмотреть возможность миграции на других поставщиков или других вендоров, что особенно актуально сейчас, т.е. решение должно быть изначально мульти-вендорным, либо достаточно гибким, чтобы можно было этого вендора сменить.

Далее необходимо определиться с точкой обработки данных, будь то пограничные вычисления, туманные вычисления или обработка данных на платформе. В случае с пограничными и туманными вычислениями данные будут обрабатываться на самих устройствах или элементах сетевой инфраструктуры, т.е. в непосредственной близости от источника данных, что помогает снизить задержку в принятии каких-либо решений после обработки полученных данных, а также внедрить промежуточно обработку информации, чтобы оптимизировать количество и качество передаваемых метрик далее по сети. В случае с обработкой данных на платформе важно уделить внимание работе с данными и возможностям аналитики, так как в случае с неподходящим инструментом могут возникнуть захламления системы избыточными данными или возникнет необходимость в применении более сложных и ресурсо-затратных алгоритмов.

Ещё очень важный момент — это проработка энергопотребления оконечного оборудования, на которое влияет логика работы и технологии которые применяются в решении. Так как многие устройства обладают батарейным питанием расчет данного показателя является критически важным для построения решений интернета вещей. Хотя устройство позволяет использовать питание постоянных источников питания это может вносить определенные ограничения в решении виду того, что данные источники сильно снижают мобильность и гибкость IoT решений в некоторых сферах.

В дополнение ко всему вышесказанному необходимо отметить вопросы по безопасности передаваемых и используемых данных, которые необходимо решать на всем пути следовании данных.



Варианты IoT-решений. Полный спектр различных вариантов на всех уровнях IoT-архитектуры: от датчика до облака, и наоборот.

Датчики и питание

Интернет вещей берет свое начало с оконечного оборудования с сенсорным устройством, которое снимает необходимые метрики из окружающей среды. Это может быть срабатывание датчика движения, периодические данные температуры какой-то установки, или геркон, определяющий, закрыта ли дверь. IoT очень связан с физическим действием или событием, позволяя выдавать реакцию на какой-то фактор реального мира. И объемы данных здесь очень различны: от нескольких байт, где необходимо передать, например телеметрию окружающей среды, до нескольких сотен мегабайт данных, поступающих с какого-нибудь промышленного контроллера или установки. Благодаря все тому же технологическому прогрессу стало возможно очень сильно уменьшить измерительные приборы/датчики, что позволило не только уменьшить решение по габаритам, но и значительно его удешевить. По сути, это один из ключевых факторов благодаря которому интернет вещей приобрёл, приобретает и будет приобретать популярность и объемы, которые фигурируют в многочисленных исследованиях. В который раз стоит отметить вопрос с питанием устройств: нельзя считать, что оконечные устройства снабжаются энергией по умолчанию.

Передача Данных

Следующим не менее важным элементом интернета вещей является технологии передачи данных, которые позволяют из самых удалённых неблагоприятных зон отчислять передачу собранных данных с умных устройств. В словосочетание интернета вещей не просто так содержится слово интернет, потому что вопросы, которые касаются сетевых технологий обмена данными теории сигналов кодирования, контрольных сумм – все это является важной частью в контексте связи в интернете вещей. На самом деле фундаментом интернета вещей являются не датчики и не приложение, а именно возможность установить соединение и обмениваться данными по сети. Как уже было сказано ранее при проектировании подобных решений в сфере интернета вещей необходимо учитывать все сложные и неочевидные нюансы в различном сетевом взаимодействии всех элементов системы. Здесь пригодятся компетенции по проектированию систем, по расчёту и моделированию зон покрытия радиосигнала и качеству такого покрытия, в зависимости от применяемой радио-технологии. Эти инструменты включают в себя динамические характеристики радиосигнала, такие как анализ спектра и электропитания, отношение сигнал/шум, потери в тракте передачи и интерференция. Важно знать основы теории информации и ограничения, которые влияют на общую пропускную способность и качество данных. Кроме того, спектр частот сигнала беспроводной связи также не безграничен и распределяется между несколькими устройствами, а архитектор, разрабатывающий широкомасштабную IoT-систему, должен понимать, как и каким образом распределяется спектр.

Интернет-маршрутизация и протоколы

Для передачи данных от датчиков в интернет-пространство необходимы две технологии: маршрутизатор-шлюз и опорные интернет-протоколы, обеспечивающие эффективность обмена данными. Маршрутизатор особенно важен в таких аспектах, как безопасность, управление и направление данных. Граничные маршрутизаторы управляют и следят за состоянием соответствующих mesh-сетей, а также выравнивают и поддерживают качество данных. Также огромное значение принадлежит конфиденциальности и безопасности данных.

Интернет вещей открыл дорогу новым IoT-протоколам, которые выходят на один уровень с традиционными протоколами HTTP и SNMP, применяющимися уже несколько десятков лет. Для передачи IoT-данных требуются эффективные, энергосберегающие протоколы с малой задержкой, способные легко и безопасно отправлять данные в облако и из него.

Существуют различные протоколы и стандарты, которые используются для связи между устройствами и инфраструктурой IoT. Некоторые из самых распространенных протоколов включают:

MQTT: протокол сообщений для маломощных устройств, который обеспечивает низкое потребление энергии и низкую задержку передачи данных.

CoAP: протокол для обмена данными в Интернете объектов, который похож на HTTP, но оптимизирован для использования с низкопотребляющими устройствами.

Zigbee: беспроводной сетевой протокол, который используется для связи между устройствами в маломасштабных домашних сетях.

Туманные и граничные вычисления, аналитика и машинное обучение

Для обработки потока данных, поступающих в облачную службу с пограничного узла, необходимо рассмотреть различные аспекты архитектуры облачных систем, такие как модели SaaS*, IaaS* и PaaS*. Архитектор должен иметь четкое представление о потоке данных и типичных схемах проектирования облачных сервисов, а также о влиянии задержки на систему IoT. Возможно, нет необходимости отправлять все данные IoT в облако, поскольку стоимость может быть снижена за счет обработки данных на границе сети или через облачный сервис с пограничным маршрутизатором.

💡 ***SaaS**: Software as a Service - Программное обеспечение как услуга, модель облачных вычислений, которая позволяет пользователям получать доступ к программным приложениям через Интернет без необходимости установки или обслуживания.

💡 ***PaaS**: Platform as a Service - Платформа как услуга, модель облачных вычислений, которая предоставляет разработчикам платформу для создания и развертывания приложений, не заботясь о настройке и управлении инфраструктурой.

💡 ***IaaS**: Infrastructure as a Service - Инфраструктура как услуга, модель облачных вычислений, которая предоставляет виртуализированные вычислительные ресурсы через Интернет, включая серверы, хранилища и сети, которые пользователи могут использовать для создания и управления собственными приложениями и услугами.

Данные, полученные от физических воздействий, преобразованные в цифровые сигналы, могут быть крайне разнообразными и требуют использования аналитических инструментов и процессоров правил IoT. Сложность реализации системы IoT варьируется в зависимости от разрабатываемого решения. Например, простые алгоритмы правил могут быть установлены на граничном маршрутизаторе для мониторинга скачков температуры, а сложные модели, такие как рекуррентная нейронная сеть в сочетании с анализом коррелированных по времени сигналов, могут потребоваться для передачи в реальном времени больших объемов

структурированных и неструктурированных данных в облачное хранилище данных для предиктивной аналитики и долгосрочного прогнозирования.

В архитектуре IoT также важна роль облачных компьютерных систем, которые обеспечивают хранение и обработку больших объемов данных, а также предоставляют доступ к этим данным различным приложениям и сервисам. Таким образом, облачные системы служат как мост между устройствами IoT и приложениями, которые могут использовать эти данные. В некоторых случаях, облачные системы также могут использовать машинное обучение и искусственный интеллект для анализа и обработки данных, чтобы обеспечить более интеллектуальное и автоматизированное управление устройствами IoT.

Платформы – это программное обеспечение, которое обеспечивает контроль, мониторинг и управление устройствами IoT. Они могут включать в себя функции для анализа данных, обработки и хранения информации.

Приложения – это программы, которые используют данные, собранные устройствами IoT, для предоставления полезной информации пользователям. Например, приложение для домашней автоматизации может использовать данные с датчиков температуры и влажности для регулирования климата в доме.

Угроза и безопасность в интернете вещей

IoT подвержена различным формам взлома из-за ее широкого распространения в различных местах, включая общественные места, удаленные районы и движущиеся транспортные средства. Это представляет собой значительный риск для безопасности, поскольку IoT является крупной и привлекательной целью для киберпреступников. Поэтому в архитектуре IoT необходимо учитывать меры безопасности, такие как шифрование и аутентификация, для защиты данных и устройств от несанкционированного доступа. Также важно обеспечить обновление и поддержку устройств, чтобы исправлять найденные уязвимости и обеспечивать их защиту.

Вывод:

В заключение, можно сказать, что архитектура Интернета вещей является достаточно сложной и многослойной, и включает в себя множество различных компонентов, каждый из которых имеет свою роль в работе системы в целом. Но с правильно построенной архитектурой и использованием современных технологий, Интернет вещей может обеспечить множество преимуществ и новых возможностей для бизнеса и общества в целом.

Важно отметить, что архитектура Интернета вещей постоянно развивается и меняется с ростом инновационных технологий и расширением ее применения в различных областях.

Эталонная модель Всемирного форума IoT

Всемирный форум IoT (IoT World Forum, IWF) – спонсируемое отраслью ежегодное событие, объединяющее представителей бизнеса, госструктур и вузовской науки с целью продвижения IoT на рынок. Комитет по архитектуре Всемирного форума IoT, составленный из лидеров индустрии, включая IBM, Intel и Cisco, в октябре 2014 года опубликовал эталонную модель IoT. Эта модель служит общей структурой, призванной помочь отрасли ускорить развертывание IoT. Модель предназначена для того, чтобы стимулировать сотрудничество и способствовать созданию повторяемых моделей внедрения.

Эта эталонная модель является полезным дополнением к модели МСЭ-Т. Документы МСЭ-Т делают упор на уровнях устройства и шлюза, описывая верхние уровни лишь в общих чертах. Наибольшее внимание рекомендации серии Y.206x уделяют определению концепции для поддержки разработки стандартов взаимодействия с устройствами IoT.

IWF озабочен более масштабным вопросом разработки приложений, промежуточного ПО и функций поддержки для корпоративного интернета вещей. Предложенная семиуровневая модель изображена на рисунке ниже.

Эталонная модель Всемирного форума IoT

Документальное описание модели IWF, опубликованное Cisco, указывает, что разработанная модель отличается следующими характеристиками:

- **упрощает**: помогает разбить сложные системы на части так, чтобы каждая из этих частей стала понятнее;
- **проясняет**: предоставляет дополнительные сведения для точной идентификации уровней IoT и выработки общей терминологии;
- **идентифицирует**: идентифицирует аспекты, в которых те или иные типы обработки оптимизированы в различных частях системы;
- **стандартизирует**: представляет собой первый шаг к тому, чтобы поставщики могли создавать продукты IoT, способные взаимодействовать друг с другом;
- **организует**: делает IoT реальным и доступным, а не просто абстрактной концепцией.

Эталонная модель Всемирного форума IoT представляет собой систему классификации компонентов Интернета вещей (IoT).

Уровень 1 модели состоит из физических устройств и контроллеров, которые используются для взаимодействия с физическими объектами, такими как датчики и исполнительные механизмы. Эти устройства могут выполнять такие задачи, как генерация данных и преобразование аналоговых и цифровых сигналов, а также поддерживать удаленный опрос и управление. Логически этот уровень облегчает связь между устройствами и обеспечивает низкоуровневую обработку на уровне 3. С физической точки зрения, этот уровень состоит из сетевых устройств, таких как маршрутизаторы, коммутаторы, шлюзы и брандмауэры, которые используются для подключения устройств к Интернету и создания локальных и глобальных сетей. Этот уровень позволяет устройствам взаимодействовать друг с другом и с прикладными платформами, такими как компьютеры, смартфоны и устройства дистанционного управления.

Уровень 2 модели относится к шлюзам, которые представляют собой сетевые и коммуникационные устройства.

Уровень 3 в IoT по IWF связан с управлением огромными объемами данных, генерируемых распределенной сетью датчиков. Например, нефтяные месторождения и нефтеперерабатывающие заводы могут генерировать терабайты данных каждый день, а самолет может генерировать аналогичный объем данных в час. Вместо того чтобы хранить все эти данные в централизованном хранилище для легкого доступа приложений IoT, более практично обрабатывать как можно больше данных как можно ближе к датчикам. Именно здесь вступает в дело пограничный вычислительный уровень - он преобразует сетевые данные в пригодную для использования информацию, которую можно обрабатывать и хранить. Элементы обработки на этом уровне способны обрабатывать большие объемы данных и

преобразовывать их в более управляемую форму, что сокращает объем данных, которые необходимо хранить.

Периферийный вычислительный уровень модели IWF включает следующие операции:

- **Анализ данных**: принятие решения о необходимости обработки данных на более высоком уровне на основе определенных критериев.
- **Форматирование**: изменение формата данных для единообразной обработки на более высоких уровнях.
- **Разрхивирование/декодирование**: обработка зашифрованных данных с добавлением контекста, например, их источника.
- **Сокращение**: обобщение данных для уменьшения их влияния на объем и трафик сети.
- **Оценка**: определение того, представляют ли данные сигнал тревоги или пороговое значение, и возможная пересылка их дополнительным получателям.

Элементы обработки на уровне граничных вычислений располагаются рядом с устройствами, генерирующими данные, такими как датчики в сети IoT. Благодаря локальной обработке части данных уменьшается объем данных, хранимых и обрабатываемых централизованными приложениями IoT. Этот тип обработки известен как "туманные вычисления", которые отличаются от традиционных "облачных вычислений". Облачные вычисления основаны на централизованных ресурсах, доступ к которым имеет небольшое количество пользователей, в то время как туманные вычисления распределяют ресурсы и обработку данных между отдельными интеллектуальными устройствами в сети IoT. Туманные вычисления решают такие проблемы, как безопасность, конфиденциальность, ограниченная пропускная способность сети и задержка в больших сетях IoT. Название "туманные вычисления" используется потому, что они расположены ближе к земле, по сравнению с "облачными вычислениями", которые находятся выше, как бы в небе.

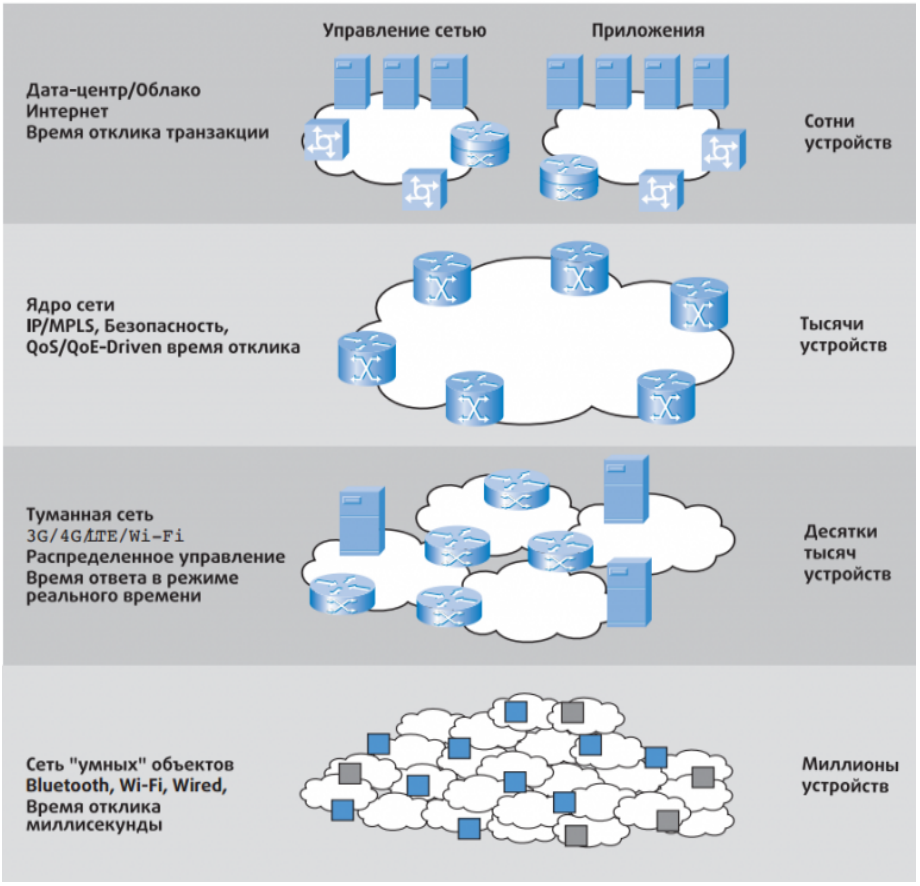


Рис. Туманные вычисления

На **уровне 4**, уровне накопления данных, информация, собранная и обработанная на уровне граничных вычислений, хранится, что делает ее доступной для дальнейшего анализа. Этот уровень значительно отличается от низкоуровневых (туман) и высокоуровневых (облако) вычислений по своей конструкции, требованиям и методам обработки.

Поток данных через сеть называется "данные в движении" и определяется скоростью и организацией устройств, генерирующих данные. Данные генерируются на основе событий и должны собираться и обрабатываться в режиме реального времени. Однако многие приложения не требуют обработки с той же скоростью, с какой генерируются данные, а облачная сеть и платформы приложений не могут справиться с огромным объемом данных от устройств IoT. Таким образом, приложения работают с "данными в состоянии покоя", хранящимися данными, доступ к которым можно получить по мере необходимости или вне реального времени. Верхние уровни обрабатывают транзакции, а нижние - события.

Ниже перечислены операции, выполняемые на уровне накопления данных:

- преобразование «данных в движении» в «данные в покое»;
- преобразование формата из сетевых пакетов в реляционные таблицы БД;
- переход от вычислений по событиям к вычислениям по запросу;

- значительное снижение объема данных за счет фильтрации и выборочного хранения.

Уровень накопления данных служит для разделения информационных технологий и операционных технологий. ИТ относится к ряду технологий, участвующих в обработке информации, включая аппаратное и программное обеспечение, коммуникационные технологии и сопутствующие услуги. В то же время ОТ относится к аппаратному и программному обеспечению, которое контролирует или управляет физическими устройствами, процессами и событиями на предприятии.

На этом уровне хранятся большие объемы данных без модификации для конкретных приложений. Данные могут поступать из различных источников и в различных форматах, но **уровень 5** абстракции данных поможет организовать и отформатировать данные для облегчения доступа и использования приложениями.

Задачи, которые могут быть выполнены на уровне накопления данных, включают в себя:

- Объединение данных из различных источников и обеспечение согласованного формата данных.
- Выполнение преобразований для обеспечения того, чтобы данные из разных источников имели единый смысл.
- Помещение отформатированных данных в базу данных соответствующего типа, например, в систему больших данных типа Hadoop для повторяющихся данных или в реляционную базу данных для данных о событиях.
- Уведомление приложений более высокого уровня, когда данные заполнены или достигли определенного уровня.
- Консолидация данных в одном месте или предоставление приложениям доступа к нескольким источникам данных с помощью виртуализации данных.
- Обеспечение защиты данных с помощью аутентификации и авторизации.
- Нормализация или денормализация данных и их индексирование для облегчения доступа к ним приложений.

Уровень 6 эталонной модели IoT состоит из различных приложений, которые используют данные IoT или управляют устройствами IoT. Эти приложения обычно работают с данными, хранящимися на Уровне 5, и им не нужно работать на скорости сети. Чтобы облегчить работу приложений, для них должен существовать упрощенный способ взаимодействия непосредственно с Уровнем 3 или даже Уровнем 2, минуя промежуточные уровни.

Уровень 7, взаимодействие и процесс, важен, поскольку он признает, что для того, чтобы IoT была полезной, люди должны иметь возможность взаимодействовать с ней. Этот уровень может включать множество приложений и обмен информацией или управление через Интернет или корпоративную сеть.

Эталонная модель IoT служит основой для стандартизации концепций и терминологии IoT и описывает необходимые функции и вопросы, которые должны быть решены до внедрения решения IoT.

Заключение

На данном занятии мы изучили архитектуру IoT решений, узнали из чего состоит экосистема интернета вещей. Посмотрели, как вещи могут взаимодействовать между собой или с информационными системами.

Домашнее задание

1. Попробуйте составить верхнеуровневое описание какого-нибудь интересного вам IoT решения, которое должно в себя включать: схему основных компонентов системы, их связь между собой, используемые протоколы, а также потоки данных.