DESCRIÇÃO

Introdução, conceituação e visão geral sobre Internet das Coisas e seus principais componentes.

PROPÓSITO

Compreender os conceitos básicos relacionados à Internet das Coisas, os componentes de sua arquitetura, a mudança de paradigma de sua implantação e o impacto nas redes de internet no dia a dia da sociedade, tanto para o reconhecimento das tendências, quanto para a discussão e a proposição de possíveis caminhos evolutivos dessa nova tecnologia.

OBJETIVOS

MÓDULO 1

Descrever os principais elementos de uma arquitetura de IoT e suas aplicações

MÓDULO 2

Reconhecer os esforços de padronização e os principais protocolos usados para o estabelecimento da conectividade em uma rede de IoT

MÓDULO 3

Identificar as plataformas de IoT disponíveis no mercado e seus principais serviços

INTRODUÇÃO

O que significa a internet das coisas? Por que fala-se tanto sobre o assunto não apenas na comunidade científica, mas também na mídia em geral? O potencial dela é gigantesco, podendo ser inferido pelos benefícios que a IoT já vem entregando para a sociedade.

Enquanto esta seção é escrita, milhares de dispositivos de IoT estão sendo instalados, conectados e operacionalizados para otimizar o trabalho até em fazendas. Estações meteorológicas autônomas, câmeras de vigilância inteligentes e sensores dos mais diversos inclusive permitem o autorreparo de máquinas e sistemas na indústria, além de muitas outras possiblidades.

É bem verdade que houve muita ansiedade nos últimos anos a respeito do tema. Especialistas chegaram a prever que a IoT poderia sobrecarregar e até mesmo derrubar a internet antes do ano de 2021. Entretanto, apesar da consistente adoção em massa da tecnologia e do crescente volume de investimento no setor, isso ainda não aconteceu.

Mas ainda há dúvidas à frente: o que são os dispositivos de IoT? Quais seriam as vantagens, as desvantagens e os riscos da massificação deles? E, por fim, quais são as preocupações inerentes à segurança e à privacidade das pessoas?

Este tema pretende apresentar o assunto para você e responder às indagações acima. O objetivo é que tal estudo possa construir, em seu processo educacional, os alicerces necessários para entender a discussão, o impacto e as mudanças que essa tecnologia já está provocando.

Em seguida, descreveremos os componentes e os conceitos de uma rede baseada em IoT em dois níveis: básico e intermediário. Com isso, você já poderá se credenciar para leituras mais profundas e complexas. Ainda veremos, por fim, por que a Internet das Coisas é o novo Big Data.

MÓDULO 1

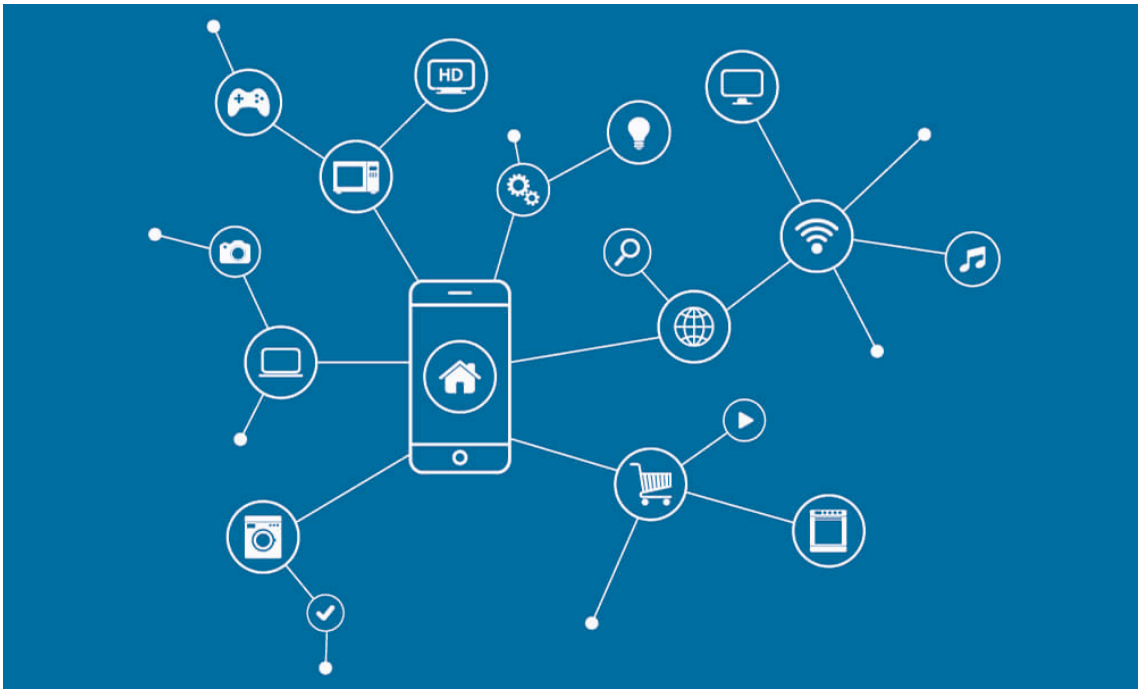
- **Descrever os principais elementos de uma arquitetura de IoT e suas aplicações**

PRIMEIRAS PALAVRAS

Neste módulo, apresentaremos o conceito de internet das coisas (IoT) e contaremos um pouco de sua história.

Falaremos ainda sobre os componentes básicos da tecnologia, principalmente o hardware, cuja escolha pode determinar o desenvolvimento da aplicação de IoT. No final, fecharemos o módulo com exemplos de aplicações baseados em casos de uso reais.

IOT



Fonte: Shutterstock.com

A internet das coisas (IoT, cuja sigla deriva da expressão em inglês *Internet of Things*) se refere a um ecossistema composto de vários elementos que trocam informações e realizam serviços dos mais diversos por meio da internet.

Nessa acepção mais abrangente, o termo é usado para se referir a redes compostas por milhares e até milhões de hardwares especializados com software embarcado. Mesmo geograficamente dispersos, eles estão conectados a uma plataforma de gestão e suporte paga em servidores remotos.

EVOLUÇÃO E HISTÓRIA

A rede de IoT cumpre tarefas específicas de forma autônoma usando funcionalidades distribuídas na nuvem.

Essa rede, portanto, é composta de várias coisas (*things*) que possuem muitos tipos.

★ EXEMPLO

Algumas dessas *things* são: eletrodomésticos, câmeras, smartphones, tablets, termostatos, equipamentos industriais, atenuadores e sensores dos mais diversos até veículos e aeronaves

não tripuladas.

Atribui-se a criação do termo IoT a Kevin Aston.

Executivo e diretor do laboratório Auto-ID Labs do MIT em 1999, Aston buscava soluções de otimização para as cadeias de suprimento. Entusiasmado com a tecnologia RFID, ele cunhou o termo após apresentar uma solução de gestão de estoque de cosméticos na qual era possível gerenciar cada tipo de produto, otimizando a logística de controle do inventário (Kevin Aston).

❓ VOCÊ SABIA

No entanto, outros autores afirmam que o conceito foi pensado anos antes. Em 1990, cientistas conectaram uma torradeira e uma máquina de café a uma câmera acoplada usando o protocolo TCP/IP. Fotos eram enviadas regularmente a um computador no qual os pesquisadores podiam ver se a jarra de café estava cheia ou vazia sem se deslocar ao local.

Alguns estudiosos ainda citam ainda que, na década de 1980, um estudante da universidade Carnegie Mellon teria sido o precursor da tecnologia IoT. Ele conectou a máquina de vendas de Coca-Cola do dormitório da faculdade à internet local. A ideia era, diretamente do conforto dos seus quartos, saber se havia refrigerantes e se eles estavam gelados.

Independentemente de qual tenha sido a primeira máquina (thing) conectada, o potencial da tecnologia é enorme. Segundo a empresa de consultoria McKinsey & Company (2017), a IoT terá um papel revolucionário na sociedade, impactando diversos segmentos.

Listaremos alguns deles a seguir:

Fonte: Shutterstock.com.

INDÚSTRIA

Fonte: Shutterstock.com.

CIDADES

Fonte: Shutterstock.com.

AUTOMÓVEIS

Fonte: Shutterstock.com.

VAREJO

Fonte: Shutterstock.com.

AGRICULTURA

Fonte: Shutterstock.com.

SAÚDE

No mesmo relatório, a empresa (2017) afirma que a tecnologia pode gerar um valor de mercado entre US$4 a 11 trilhões até 2025, porém sua adoção tem sido mais lenta que o

previsto.

A consultoria IDC esperava que, já em 2020, o mercado de IoT alcançaria a cifra de US$1,7 trilhão. Já a Gartner previa que 25 bilhões de dispositivos estariam conectados no mesmo ano.

O fato é que ainda não alcançamos tais números, mas a demanda por dispositivos e plataformas de IoT, assim como por softwares embarcados e serviços de valor agregado baseados nessa tecnologia, continua aquecida – e sua tendência é aumentar consideravelmente nos próximos anos.

BIG DATA E INTERNET

O número de dispositivos de IoT conectados à internet vem crescendo vertiginosamente a cada ano.

Em breve, haverá dezenas, centenas ou talvez milhares de bilhões de dispositivos conectados a ela – e todos gerando telemetria.

Isso significa a existência de bilhões de fontes de dados conectadas trabalhando simultaneamente e em tempo real.

Por isso, muitos especialistas projetam que a internet, como temos hoje em dia, estará sobrecarregada em poucos anos. Eles afirmam que a comunicação é um gargalo crítico que precisa ser resolvido rapidamente. Além disso, esses bilhões de dispositivos de IoT serão como *datacenters* distribuídos globalmente, o que leva muitos estudiosos a afirmarem que a IoT será o novo Big Data.

O volume, a velocidade de atualização, a variedade e a distribuição dessas fontes de dados serão maiores do que quaisquer estrutura de Big Data existente hoje em dia. Consultorias especializadas estimam que já existem atualmente cerca de 20 bilhões de dispositivos de IoT operando no mundo.

💬 COMENTÁRIO

O consumo de banda, a produção gigantesca de dados e uma necessidade de velocidade de processamento cada vez maior vêm direcionando a forma como a internet deverá evoluir nos

próximos anos.

PRINCIPAIS ELEMENTOS

ARQUITETURA

A troca de informações entre os dispositivos em uma rede IoT é feita por meio de uma arquitetura distribuída que é composta por vários elementos. Essa rede de comunicação permite não somente que os dispositivos se comuniquem entre si quando necessário, mas também que eles consumam serviços normalmente hospedados na *cloud* (nuvem) por meio da internet.

Fonte:Shutterstock.com

Diversos protocolos de comunicação podem ser usados para suportar uma IoT.

Protocolos de transporte (wi-fi, GSM e Bluetooth) e de comunicação de dados (o MQTT e o HTTP estabelecem as condições em que os dados são enviados dos dispositivos para os servidores).

O diagrama de componentes na figura a seguir mostra, de forma básica, a relação entre os elementos de uma arquitetura baseada na internet das coisas.

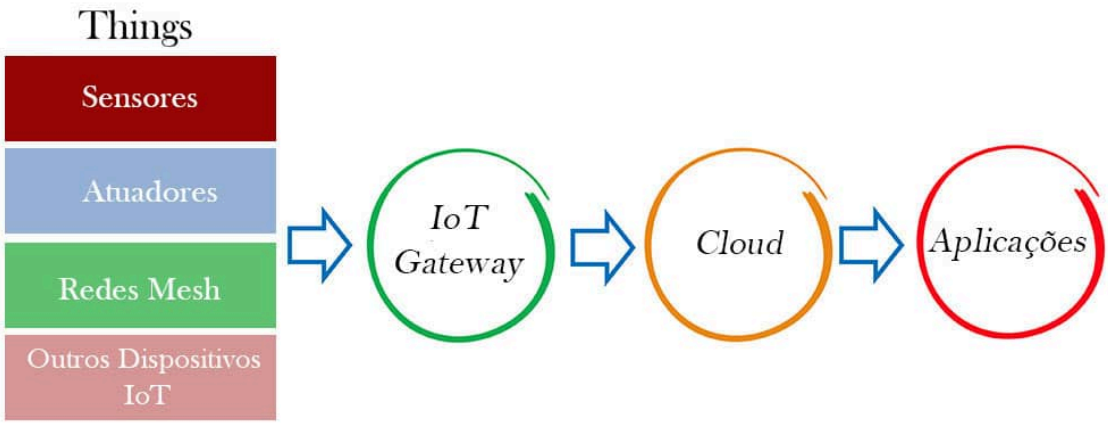


Imagem: Shutterstock.com, adaptado por Heloise Godinho.

Diagrama ilustrativo de uma arquitetura baseada na internet das coisas.

Vemos nela os dispositivos (*things*) conectados – que podem somar milhares ou milhões de unidades – comunicando-se com serviços na nuvem por intermédio de um servidor *gateway* adicional.

O *gateway* encontra-se posicionado geograficamente próximo dos dispositivos para a reduzir a latência de rede, viabilizando serviços críticos que necessitam de respostas quase em tempo real, como, por exemplo, os carros autônomos e as cirurgias remotas. Esse *gateway* implementa outra tecnologia usada denominada *edge computing* (ou computação de borda), que viabiliza esses serviços críticos.

SAIBA MAIS

A latência experimentada em uma torre de telefonia celular convencional LTE é de cerca de 40 milissegundos. Já carros autônomos precisam de menos de 10 milissegundos para serem considerados seguros.

A nuvem no diagrama representa uma plataforma de IoT baseada em *cloud*. Falaremos mais sobre *cloud* nos próximos módulos. A “linguagem” (protocolos de comunicação) que os componentes dessa arquitetura usam para se comunicar pode variar bastante.

HTTP/HTTPS e MQTT são as mais comuns.

Os dispositivos podem estar conectados entre si e com o *gateway edge* através de diversas topologias de rede.

A estrela é a mais comum delas, mas existem implementações nas quais as redes de IoT podem possuir diversas configurações:

ANEL (*RING*)

BARRAMENTO (*BUS*)

ÁRVORE (*TREE*)

COMPLETAMENTE CONECTADOS (*FULLY CONNECTED*)

No caso de *fully connected*, os elementos fazem simultaneamente a coordenação entre si e com o *gateway*.

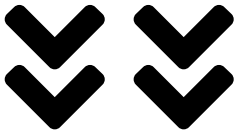
DISPOSITIVOS

No diagrama acima, vimos que a arquitetura é composta por muitos dispositivos (*things*) interligados. Cada um deles consiste em um software embutido em um hardware ultraespecializado (normalmente de tamanho pequeno) e conectado à internet.

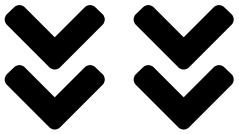
Sua função pode ser apenas a de coletar dados. No entanto, esse hardware também é capaz de reagir a eles e processá-los, emitindo alarmes, classificando elementos ou identificando animais e pessoas.

Mas precisamos, em primeiro lugar, conceituar esses dispositivos. *Things* são dispositivos desenhados para fins específicos. Eles são capazes de:

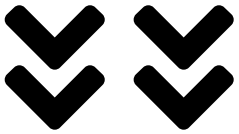
COLETAR DADOS DO AMBIENTE EM QUE SE ENCONTRAM.



REALIZAR ALGUM PROCESSAMENTO.



TRANSMITIR TAIS DADOS PELA INTERNET.



ESTABELECER UMA COMUNICAÇÃO ENTRE SI E COM SERVIDORES (CHAMADOS DE *GATEWAYS* OU *BROKERS*).

Portanto, qualquer aparelho conectado capaz de minimamente coletar e transmitir dados, trabalhando de forma independente ou em sincronia com outros aparelhos, é considerado um dispositivo de IoT.

Os dispositivos IoT também proveem interfaces diretas para o gerenciamento e o *troubleshooting* (solução de problemas). Eles podem estar:

Imagem: Shutterstock.com

Nas fábricas

Imagem: Shutterstock.com

No ambiente de trabalho

Imagem: Shutterstock.com

No campo

Imagem: Shutterstock.com

Nas residências

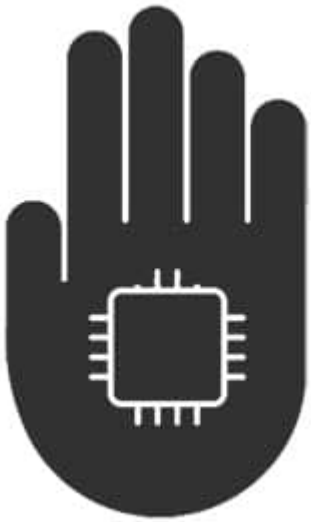


Imagem: Shutterstock.com

Inseridos sob a pele (na forma de microchips) ou nas vestimentas das pessoas

O último caso permite que elas utilizem roupas e acessórios “inteligentes”. Os dispositivos, neste caso, podem assumir a forma de:

Medidores de pressão em uma linha de montagem.

Termômetros em um refrigerador industrial.

Localizadores em um contêiner de carga.

Câmeras de vigilância térmicas em fornos de produção de aço.

Sensores sísmicos em contato com o solo de regiões próximo de atividades vulcânicas ou de placas tectônicas.

HARDWARE

Existem basicamente dois tipos de hardware (ou placas) para IoT comercializados atualmente.

PLACA DE CIRCUITO BASEADO EM UM MICROCONTROLADOR

O Arduino é um exemplo típico. Ele não tem sistema operacional, sendo carregado apenas com um conjunto de instruções no firmware ou na memória para desempenhar uma função bem específica.

Placas baseadas em microcontroladores funcionam muito bem para:

- Controlar outros dispositivos.
- Servir como hub intermediário de comunicação.
- Coletar dados por meio de sensores.
- Realizar cálculos simples que não requeiram muita memória (sendo normalmente sua maior limitação).

COMPUTADOR COMPLETO QUE NECESSITA DE UM SISTEMA OPERACIONAL

Esse tipo de hardware – cujo exemplo típico é o Raspberry Pi – consiste em um computador completo que necessita de um sistema operacional, normalmente o Linux, para funcionar.

COMPONENTES BÁSICOS COMUNS A AMBOS

Um hardware destinado à IoT precisa conter:

- Módulo de processamento central responsável pelo esforço computacional e pelo armazenamento dos dados.
- Fonte de força.
- Um ou mais conversores analógico-digitais.
- Módulos de interfaces periféricos e de comunicação, que podem (ou não) estar embutidos em um único chip.

Na placa, sensores dos mais diversos tipos podem ser conectados diretamente nas portas de entrada ou de saída ou receber módulos extensores, como, por exemplo, os *shields* do Arduino.

Entretanto, as placas são genéricas. Elas dificilmente já vêm de fábrica com os acessórios para serem utilizados em aplicações práticas. Eles, portanto, precisam ser estimados e adquiridos à parte.

📢 ATENÇÃO

O importante é ter atenção na documentação da placa escolhida para identificar corretamente os componentes e as funcionalidades nativas e verificar se o fabricante disponibiliza separadamente os recursos de hardware e software necessários para implementar o que se deseja.

SENSORES

Sensores são dispositivos sofisticados usados para a aquisição de dados em tempo real. Eles convertem uma **medição física** em sinais elétricos digitais ou analógicos que podem ser interpretados e manipulados.

MEDIÇÃO FÍSICA

A temperatura de um corpo, a pressão atmosférica, a aceleração de um carro ou a altitude de um drone.

Há diversos sensores disponíveis no mercado. Listaremos alguns deles a seguir:

- De movimento
- De deslocamento indutivo
- De nível

De intensidade luminosa

Sensíveis à cor

Escolher o sensor certo para determinada aplicação pode ser um trabalho difícil. Há muitos parâmetros e especificações que devem ser levados em consideração para uma tomada de decisão.

Contudo, podemos citar os mais comuns ou relevantes:

CUSTO

ALCANCE

PRECISÃO

CALIBRAGEM

CUSTO

O preço de aquisição pode ter pouca variação entre um fabricante e outro, porém, quando se leva em conta a implementação de milhares de unidades IoT, pequenas diferenças podem ser significativas no final do processo.

ALCANCE

Sensores que irradiam ondas eletromagnéticas, por exemplo, já vêm de fábrica com uma alanca pré-definido.

PRECISÃO

É preciso verificar se a variação na medição atende aos requisitos do projeto.

CALIBRAGEM

As condições do ambiente podem interferir na leitura do sensor; por isso, é importante que ele seja calibrável para garantir a conformidade do resultado.

Não existe IoT sem sensores e aquisição de dados.

PLACAS COMERCIAIS

Existem placas que vêm sendo usadas para prototipar e até mesmo implementar em produção os dispositivos de IoT. As mais comuns para prototipação são as da família Arduino e Raspberry Pi.

Obviamente, as grandes fabricantes criam os próprios hardwares proprietários e customizados. Eles costumam ser embutidos em outros aparelhos, criando, assim, geladeiras, televisores, bicicletas inteligentes, além de muitos outros produtos, embora também haja muitas aplicações comerciais baseadas em Arduino e Raspberry Pi.

Uma das características dos dispositivos IoT é o baixo consumo de eletricidade. Alguns, como o ESP8266, ilustrado na figura ao lado, possuem modos de economia de energia (*sleep mode*), enquanto outros usam um hardware de baixo consumo tanto para a unidade de processamento central (MCU) quanto para o módulo que implementa os protocolos de transporte sem fio, como, por exemplo, ZigBee, Bluetooth ou a própria rede de telefonia celular: LTE, 3G, 4G etc. Eles são altamente eficientes no consumo energético.

Fonte: Shutterstock.com.

Apontaremos no próximo módulo as placas mais comuns para a prototipação e o aprendizado, bem como seus principais componentes e subsistemas.

Escolher o hardware adequado para prototipar um dispositivo de IoT é fundamental e pode economizar muita dor de cabeça durante a execução do projeto.

Essa escolha implica a análise de:

CAPACIDADE DE PROCESSAMENTO

REQUERIMENTOS DE CONSUMO DE ENERGIA

QUANTIDADE DE MEMÓRIA

ACESSÓRIOS E MÓDULOS DE EXPANSÃO DISPONÍVEIS

QUANTIDADE DE PORTAS DE ENTRADA/SAÍDA

AMBIENTE E LINGUAGEM DE DESENVOLVIMENTO REQUERIDOS

É preciso também ter uma visão da evolução do dispositivo que se quer construir. Deve-se levar em consideração a escalabilidade, a modularidade, o custo e o desempenho do hardware escolhido.

Por fim, escrever um código para os dispositivos de IoT não é tarefa fácil. Desse modo, o custo de desenvolvimento e as linguagens de programação suportadas também precisam ser levadas em consideração.

PLATAFORMAS DE PROTOTIPAÇÃO

Falaremos agora sobre cada plataforma de prototipação atualmente disponível no mercado. No entanto, essa indústria está em constante evolução: **a todo momento surgem novidades**.

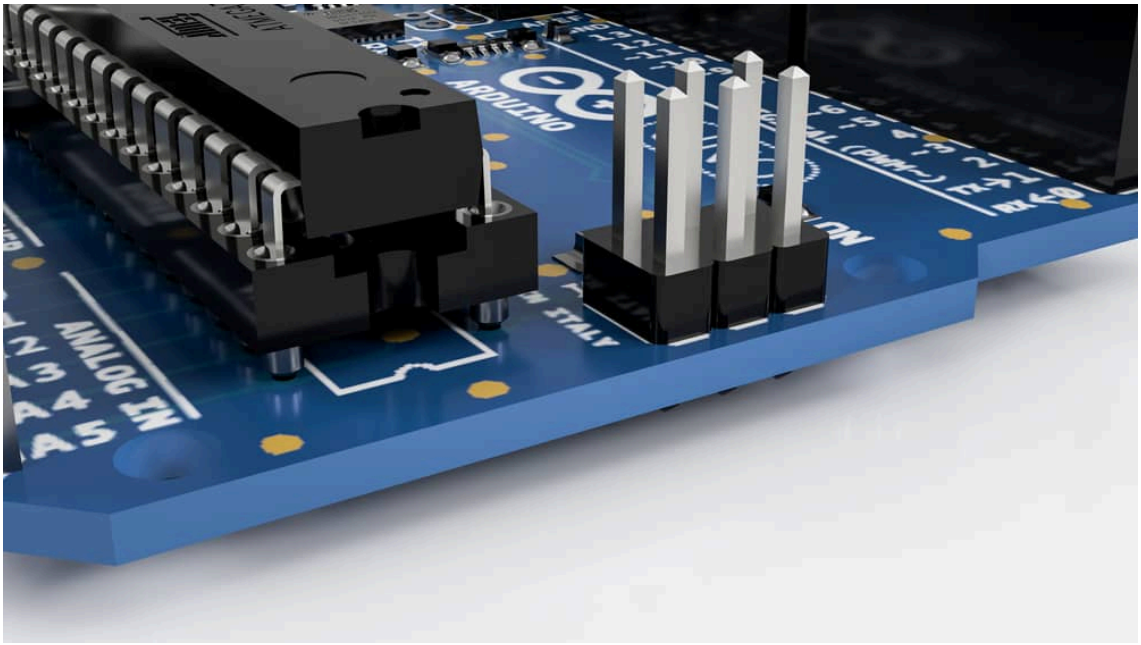
Placas tidas como muito boas podem passar a ser consideradas obsoletas do dia para a noite. Diversas placas de circuito foram descontinuadas em anos recentes.

Você está avisado(a): nada impede que uma rede inteira de elementos IoT se torne ultrapassada repentinamente.

ARDUINO

Compreende uma família de placas de circuito de código aberto. Elas estão baseadas em microprocessadores de baixo custo com software embarcado que devem ser programados em C/C++.

Existe uma grande variedade de Arduinos (apelidados de micro, nano, mega, Leonardo e diversos outros nomes), sendo a mais popular o Arduino Uno. A maior parte requer módulos de expansão (chamados de *shields*) para implementar a capacidade de comunicação em rede e outras funcionalidades. Esses módulos são muito simples, funcionando praticamente no modo *plug and play.*



Fonte: Shutterstock.com.

Atualmente, a plataforma Arduino é uma das mais conhecidas e maduras do mercado, sendo largamente usada para desenvolver dispositivos conectados.

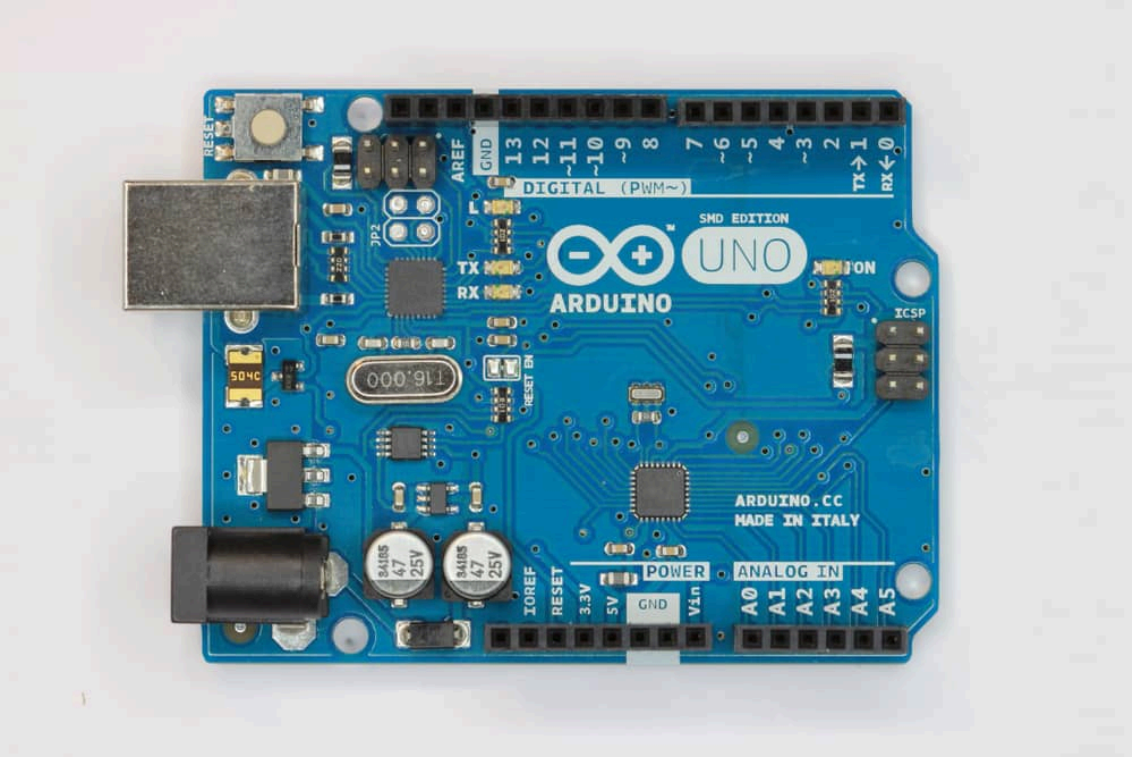
COMENTÁRIO

Uma de suas restrições costuma ser a pequena quantidade de memória disponível: ela normalmente possui 256KB, sendo que 8KB já são usados pelo *bootloader*. Isso limita bastante o desenvolvimento de aplicações mais pesadas.

Ele é indicado, portanto, para atividades de coleta de dados e pequenos processamentos. Cabe aos serviços hospedados na nuvem realizar o processamento robusto, demandando ações do dispositivo apenas quando é necessário. **Por causa do custo baixo, a plataforma permite uma grande escala**.

Com a massificação e a alta demanda da internet das coisas, o fabricante passou a disponibilizar uma linha de placas desenhadas especificamente para aplicações IoT. Elas já saem da fábrica com módulos de comunicação embutidos e diversas funcionalidades.

O mais básico é o Arduino NANO 33 IoT. Usando o processador Arm Cortex-M0 32-bit SAMD21, ele vem com um módulo de conectividade para wi-fi e Bluetooth nativo, além do modulo de criptografia denominado Microchip ECC608 Crypto Chip, que garante a segurança das comunicações.



Fonte: Shutterstock.com

Arduino.

O Arduino é facilmente programável. Para isso, basta:

Conectá-lo via porta USB a um computador no qual sua **IDE** esteja instalada.

Escrever o código.

Sincronizá-lo com o hardware.

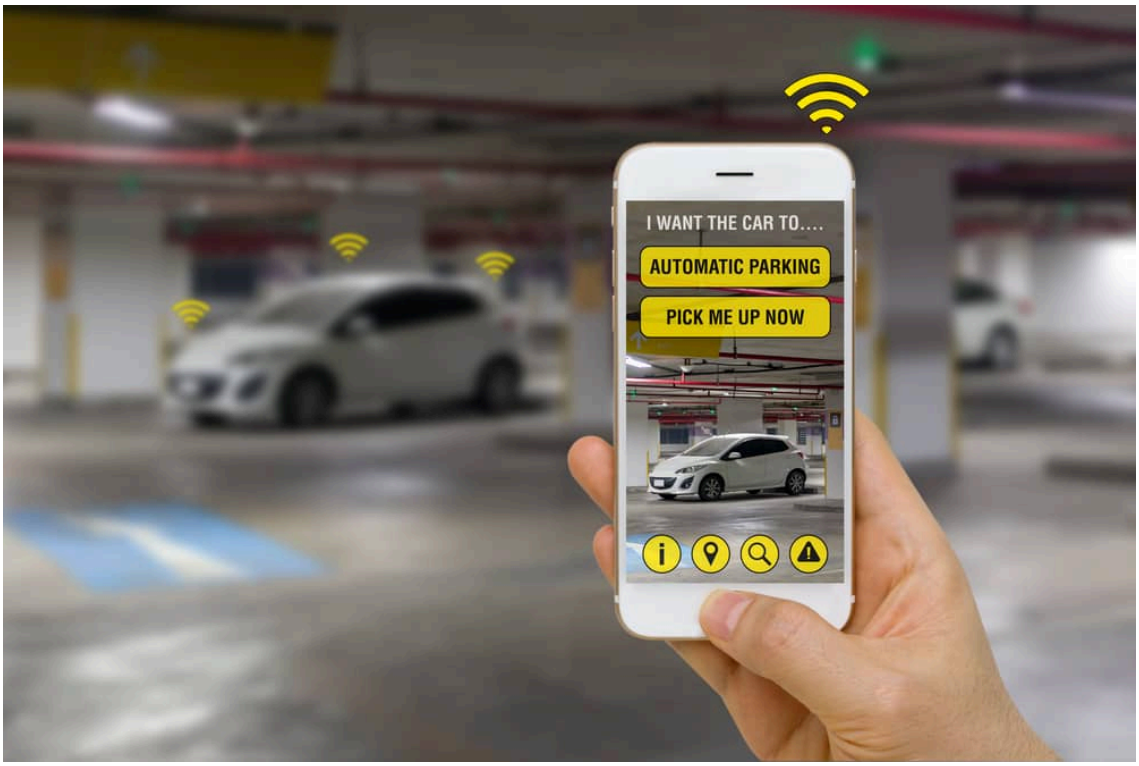
IDE

Sigla em inglês para a expressão traduzida como “ambiente de desenvolvimento integrado”

A IDE automaticamente compila, *linka* e carrega o código binário dentro da placa.

O fabricante também oferece um serviço de internet chamado de Arduino Cloud para integrar os dispositivos por meio de serviços na nuvem.

As aplicações de IoT mais comuns que empregam o Arduino incluem sistemas para:



Fonte: Shutterstock.com.

Registro de estacionamento de carros

Fonte: Shutterstock.com.

Estações meteorológicas

Fonte: Shutterstock.com.

Sistema de regulação de temperatura automáticos

Fonte: Shutterstock.com.

Sistemas de monitoramento de poluição sonora e atmosférica

Muitos fabricantes de dispositivos de IoT usam as placas Arduino diretamente nos seus produtos por considerarem que o hardware tem maturidade e estabilidade suficiente para funcionar em produção – e não apenas durante a prototipação.

Existem muitas cópias piratas das placas Arduino fabricadas na China e vendidas como se fossem originais. Muitas delas até podem ter um desempenho similar. É preciso ficar atento na hora de comprar.

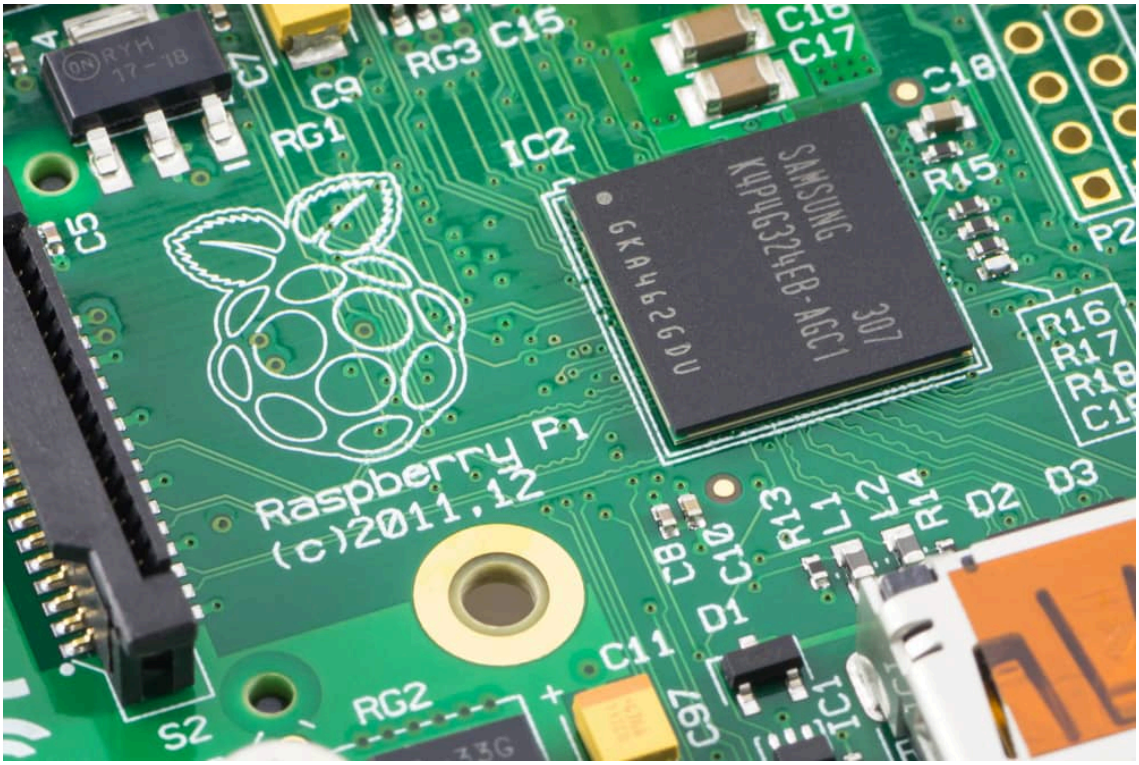
RASPBERRY PI

Enquanto o Arduino constitui uma placa de circuito que contém uma unidade processadora com módulos periféricos que o complementam, o Raspberry Pi é um computador completo com Linux embutido como sistema operacional.

Ele pode ser conectado diretamente a um monitor e funcionar exatamente como um PC convencional.

O Raspberry Pi foi inicialmente concebido pela fundação de mesmo nome para ser uma plataforma educacional barata para ensinar programação e computação às pessoas.

Entretanto, seu uso foi além disso: o dispositivo já vem sendo usado de diversas outras maneiras, por exemplo, como base para prototipação e aplicações comerciais (desde automação residencial até aplicações industriais).



Fonte:Shutterstock.com

Similar ao Arduino, o Raspberry Pi é baseado em *open-source* (código aberto), porque utiliza o sistema operacional Linux, que é aberto, embora sua placa não seja. Ele possui um módulo de processamento central e portas de entrada e saída onde os sensores são conectados.

A última versão lançada durante a redação deste tema foi o Raspberry Pi 4 Model B.

Esse hardware conta com:

- Quatro portas USB
- Uma porta gigabit ethernet
- Uma porta de áudio estéreo
- Duas portas micro HDMI
- Módulos de wi-fi\Bluetooth

Um processador Broadcom BCM2711

Quad core Cortex-A72 (ARM v8) 64-bit SoC de 1.5GHz

Memória RAM de até 8Gb

Slot para cartão de memória Micro SD

Fonte: Shutterstock.com.

Raspberry Pi.

Obviamente, o Raspberry Pi é mais robusto e poderoso que o Arduino, sendo capaz de realizar processamentos mais complexos. Contudo, ele consome mais energia, o que inviabiliza o seu uso para determinadas aplicações.

Para essas aplicações, a versão mais simples (chamada de Raspberry Pi Zero W) talvez seja indicada. O fabricante também disponibiliza uma série de acessórios e periféricos, embora os módulos de conectividade LoRa – além de outros – precisem ser adquiridos de outros fornecedores. De qualquer forma, não há limitações para a utilização do Raspberry Pi como dispositivo de IoT.

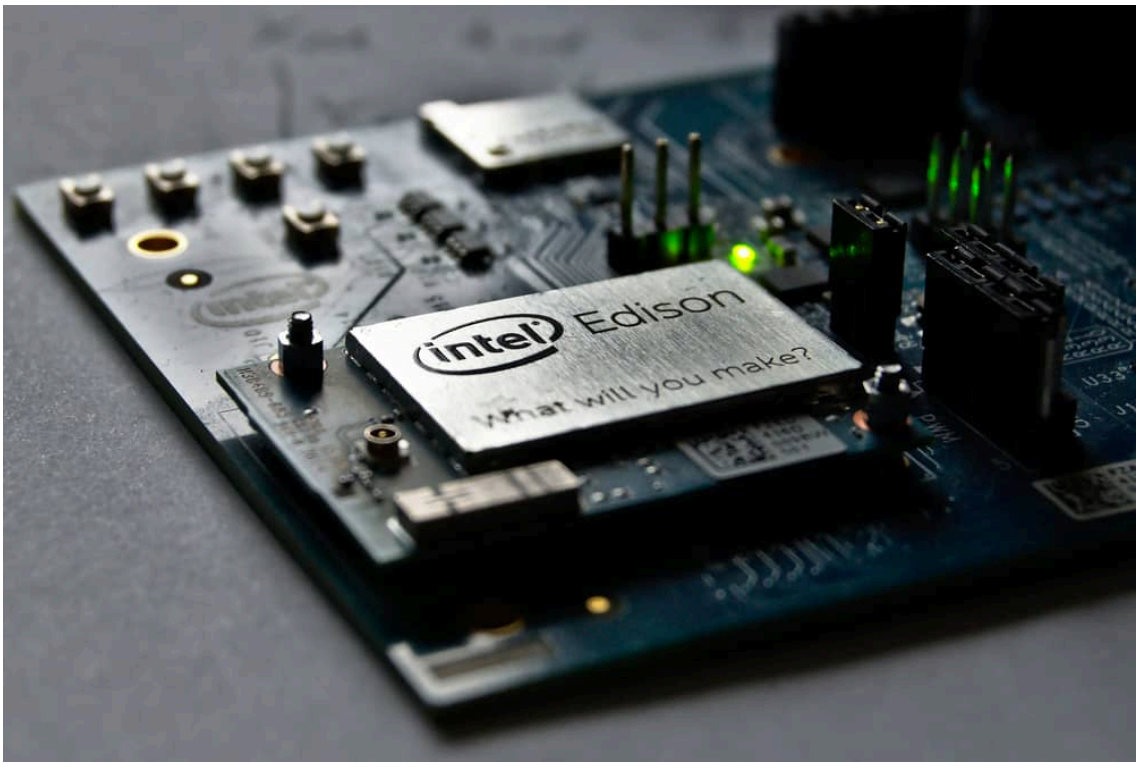
INTEL EDISON

O chip Intel Edison é fabricado pela gigante Intel. Seu grande diferencial está no tamanho reduzido. Suas medidas são modestas: comprimento (35,5mm), largura (25mm), altura (3,9mm) e peso (5,3g).

Esse chip foi idealizado para ser usado especificamente em:

IoT

Roupas inteligentes (*wearable*), dado o seu tamanho reduzido.



Fonte:Shutterstock

O Intel Edison é um computador que roda o Yocto Linux como OS, sendo análogo ao Raspberry Pi. No entanto, todos os seus módulos foram consolidados em um chip único, que custa mais caro.

Ele não pode ser conectado diretamente ao computador para ser configurado, como o Arduino e o Raspberry Pi; por isso, é preciso comprar separadamente o kit de desenvolvimento na forma de uma placa secundária de configuração (*breakout board*). O chip será encaixado nessa placa através de um conector Hirose DF40 de 70 pinos para receber as configurações e o código compilado.

Essa placa é compatível com Arduino e pode receber diversos *shields*. O código-fonte pode ser escrito em C/C++ mediante o emprego de:

IDE do Arduino

Node.js

Python (se o ambiente de desenvolvimento é MCU SDK ou mesmo Eclipse).

SAIBA MAIS

Quando o Edison estiver configurado, será possível acessá-lo via SSH com Putty por meio da rede wi-fi. Sua versão mais recente possui:

Conectividade wi-fi\Bluetooth 4.0

1GB de memória RAM

4GB de memória

MMC (*storage*)

Interface para SD-Card

Porta USB

Total de quarenta portas de entrada/saída de uso geral

O modelo de processamento central é composto por um Intel Atom Dual Core de 500MHz e um microcontrolador Intel Quark de 100MHz.

Uma de suas desvantagens é que ele ainda não atingiu uma massa crítica como os outros. A comunidade que desenvolve e publica o código para o Intel Edison ainda é muito reduzida, o que torna a curva de aprendizado mais difícil para os iniciantes.

Além disso, tanto ele quanto o Raspberry Pi, por serem computadores completos (e não apenas uma placa com microcontrolador), são mais difíceis de se utilizar. Contudo, é possível construir aplicações poderosas com o Intel Edison. Um exemplo são aplicações que usam a

visão computacional para rastrear objetos ou classificá-los, ou para acoplar o dispositivo em um drone a fim de transmitir dados ou imagens para o controle de terra.

Infelizmente, essa placa, ao lado do Intel Galileo e do Joule, foi recentemente descontinuada pela Intel.

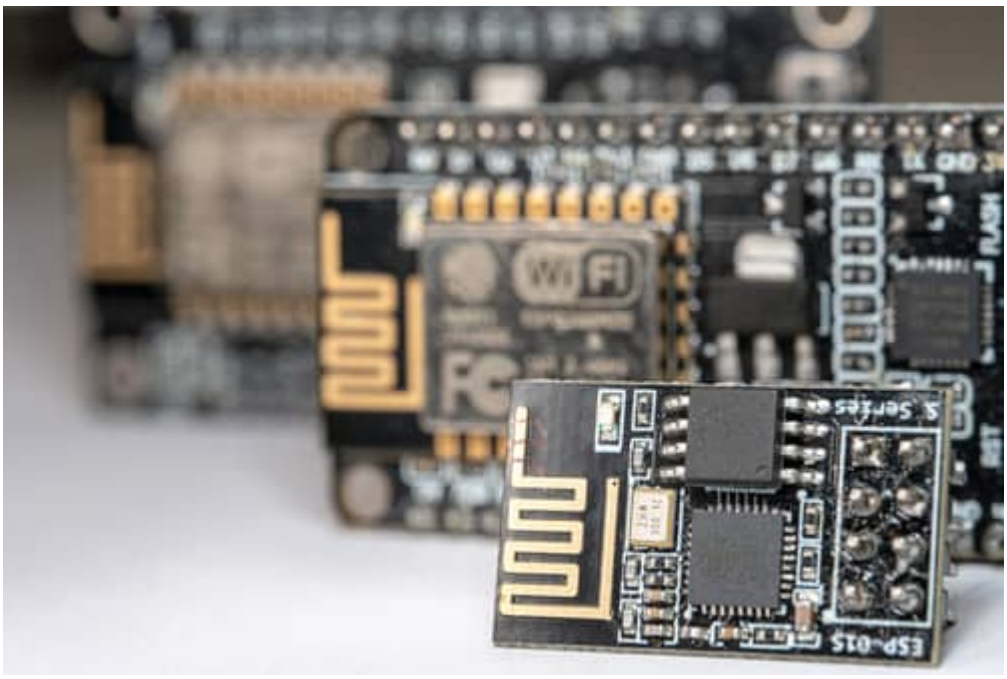
No entanto, ainda existem milhares de placas em funcionamento suportando as mais diversas aplicações.

ESP8266

A família de chips ESP8266 foi lançada em 2014 na China.

Inicialmente, não ela despertou muito interesse, principalmente porque havia apenas documentação em chinês e pouco código disponível. Porém, com o tempo, o ESP8266 passou a ser largamente usado em protótipos e provas de conceito para IoT. Atualmente existe uma grande comunidade suportando-o.

O chip possui capacidade de comunicação wi-fi nativa e tem uma relação custo-benefício muito boa, sendo vendido por menos de US$5. Como o Intel Edison, ele é muito pequeno: o chip foi desenhado para ser usado como dispositivo IoT, inclusive para aplicações vestíveis (*wearable*).



Fonte: Shutterstock.com.

O ESP8266 foi dotado com um processador RISC de 23 bits chamado de Tensilica. Ele pode atingir até 160MHz de Clock e conta com um conversor analógico-digital de 10 bits.

Podendo funcionar como módulo de comunicação wi-fi para outros microcontroladores ou de forma independente, o ESP8266 pode:

Ter até dezessete portas de entrada/saída para uso geral.

Ser acessado via Putty (dependendo da versão e se estiver configurado e conectado à rede wi-fi) graças aos comandos SSH.

Quando vem com o firmware AT embutido, pode ser programado por meio de um Arduino, em que este funciona como uma breakout board.

Neste último caso, a placa Arduino funciona como uma breakout board.

Apesar de o ESP8266 ainda ser comercializado, versões novas já foram lançadas. Fabricante do chip, a Espressif Systems lançou a versão ESP8285, que tem praticamente as mesmas funcionalidades do ESP8266, embora possua dimensões mais reduzidas.

Sua evolução surgiu por conta do lançamento da placa ESP32. Ela possui:

4MB de memória.

Wi-fi e Bluetooth embutidos.

Controle remoto IR.

Trinta e duas portas de entrada e saída de uso geral.

O menor consumo de energia no modo *deep sleep*: apenas 5µA. O ESP8266 e o ESP8285 consomem cerca de 20µA no mesmo modo.

A MCU é o processador Tensilica Xtensa LX6 Dual-Core 32-bit processor. Seu relógio é de 240MHz e o conversor analógico-digital, de 12 bits (maior resolução).

Sua escala de temperatura de operação oscila de -40 graus Celsius até +125 graus Celsius, permitindo o desenvolvimento de dispositivos capazes de operar em situações críticas.

EXEMPLOS DE APLICAÇÕES

Fonte: Shutterstock.com.

Projetar e implementar uma aplicação baseada em IoT é uma tarefa multidisciplinar que envolve a escolha da placa e o dimensionamento de diversos fatores tanto de software como de hardware. É o caso, por exemplo, de sensores.

Apresentaremos a seguir duas aplicações desenvolvidas pelo autor em parceria com uma empresa de tecnologia israelense. A ideia é que você observe uma aplicação concreta de IoT baseada no mundo real. Nomes e valores foram alterados para fins educacionais.

CASO DE USO 1

A FoodX é uma das maiores empresas agropecuárias do Brasil. Seu faturamento de R$8,2 bilhões em 2019 posicionou a companhia na 22ª posição entre as 40 maiores empresas de agronegócio brasileiro. Com sede na cidade de Curitiba, a empresa atua no mercado nacional há 40 anos e está presente em 120 países, sendo que, em 2019, as exportações representaram 55% das suas vendas totais.

A organização emprega cerca de 19 mil pessoas e possui diversas fábricas, centros de distribuição, armazéns, fazendas de plantio ou de pecuária bovina, totalizando cerca de 170 unidades distribuídas em 16 estados brasileiros.

IMPLEMENTAÇÕES

Há alguns anos, a FoodX vem modernizando suas operações. Ela tem progressivamente instalado estações meteorológicas dedicadas à telemetria e ao gerenciamento remoto em suas fazendas de plantio de soja e de outros grãos.

Esses dispositivos de IoT são capazes de medir:

- Condições do solo
- Precipitação de chuva
- Velocidade e direção do vento
- Radiação solar
- Temperatura e umidade relativa do ar
- Umidade do solo
- Nível e vazão de rios e lagos
- Pressão atmosférica
- Qualidade do ar e da água usada na irrigação

A empresa também vem investindo na otimização do uso do maquinário. Dispositivos de IoT foram instalados nos tratores e em outras máquinas agrícolas para monitorar o consumo de combustível, implementar a manutenção preventiva e automatizar o controle do maquinário em tempo real.

Em suas fazendas de gado, a FoodX implementou dispositivos de IoT com funções analíticas de inteligência artificial (IA) para desenvolver técnicas de agropecuária de precisão com o objetivo de otimizar a capacidade reprodutiva do gado e fazer um melhor uso do pasto.

Foram instalados sistemas inteligentes que recebem dados dos dispositivos de IoT para dar suporte à tomada de decisão. Os novos sistemas são capazes de otimizar o lucro do pecuarista, indicando o ponto ótimo de negociação (PON) e otimizando o ROI.

A solução funciona ao monitorar a eficiência da operação de confinamento e de engorda do gado, acompanhando o desempenho de cada animal individualmente ao mesmo tempo em que busca dados de mercado na internet.

Além disso, a FoodX vem investindo em segurança. Os seguintes itens foram comprados e estão sendo instalados nos parques industriais:

Milhares de câmeras de monitoramento

Imageamento térmico

Sensores de movimento

Alarmes e fechaduras inteligentes

Ao final, toda essa modernização se traduz em milhares de dispositivos instalados em todos os locais da companhia.

Para viabilizar a operação de IoT, a FoodX também contratou serviços de internet dos quatro maiores provedores brasileiros para conectar sua rede de *things* com dezenas de centros de monitoramento espalhados pelo país.

Consequentemente, ela precisa administrar diversos contratos de prestação de serviço de internet para seus milhares de dispositivos de IoT. Eles usam, entre outros tipos, a tecnologia de transmissão 3G/4G, LTE, wi-fi e Bluetooth.

Atualmente, a organização estuda o emprego das tecnologias *narrow band* IoT (NB-IoT) *e long term evolution for machines* (LTE-M) para operar a próxima geração de dispositivos IoT que vão ser incorporados ao *grid*. Para isso, novos contratos com diversos SLAs (sigla de *service level agreement*), contendo diferentes sensibilidades à latência, precisam ser feitos com as operadoras.

PROBLEMA

Constantes falhas e interrupções no fornecimento de internet para os dispositivos tem gerado atualmente perdas de milhares de dólares na operação do *grid* IoT.

O problema consiste na:

Complexidade de gerenciar dezenas de centrais de monitoramento (cada uma com milhares de dispositivos conectados);

Dificuldade em identificar quando e onde o problema ocorre

Falta de meios para aferir se os SLAs e a banda contratados estão sendo devidamente entregues pelas operadoras.

Além disso, os sistemas de monitoramento dos fabricantes dos dispositivos só emitem alertas quando tais dispositivos já estão desconectados (offline). Eles não monitoram a degradação do serviço. Tampouco existe uma troca de informação entre sistemas de gerenciamento de diferentes fabricantes.

Também não há como aferir o cumprimento da banda e dos SLAs contratados das operadoras de telecomunicação. As falhas reportadas geram muitas tarefas manuais para investigação e correção dos problemas, introduzindo ineficiência na operação e gerando um custo extra significativo à companhia.

SOLUÇÃO

A empresa decidiu integrar todos os seus centros de monitoramento em um único. Para isso, ela migrou todos os seus dispositivos de internet das coisas para umas das três maiores plataformas de IoT presentes no Brasil.

Com isso, os serviços nativos contratados permitem que se reporte em tempo real os dados gerais de conexão dos dispositivos e dos canais de comunicação fornecidos pelas operadoras contratadas, além de gerar análises e métricas diversas.

Além disso, outro programa desenvolvido pelo departamento de TI da empresa diretamente na *cloud* da plataforma de IoT contratada correlaciona falhas entre os dispositivos de fabricantes diferentes, otimizando o tempo de resolução de problemas.

A solução ainda monitora a degradação da internet, sendo capaz de prever em grande medida quando vai ocorrer uma falha. Ela dispara alarmes que cadastram pedidos de manutenção

preventiva e registram as interrupções e as velocidades experimentadas para a comparação com o contratado, acionando as operadoras quando necessário.

CASO DE USO 2

A TelecomInc Brazil é uma subsidiária de uma empresa norte-americana com sede em Miami. Operando infraestrutura de telecomunicações para rede celular, ela possui escritórios em 20 países.

Em novembro de 2019, a TelecomInc ativou sua rede **LoRaWAN** para internet das coisas em diversas capitais brasileiras com o objetivo de suportar a adoção de tecnologias para cidades inteligentes.

LORAWAN

LoRaWAN é um protocolo de rede de baixa potência e de longa distância (LPWA) projetado para conectar “coisas” operadas por bateria sem fio à internet em redes regionais, nacionais ou globais. Ele tem como alvo os principais requisitos da internet das coisas (IoT), como, por exemplo, serviços de comunicação bidirecional, segurança ponta a ponta, mobilidade e localização.

IMPLEMENTAÇÕES

Tendo comprado ativos de uma operadora brasileira dois anos atrás, a empresa afirma que já tem 350 mil dispositivos IoT conectados usando sua infraestrutura de rede LoRaWAN. Ela conecta seus clientes à internet por intermédio de redes de transporte de grandes operadoras brasileiras.

Entre seus clientes, a TelecomInc tem diversas empresas de segurança que empregam sensores de presença, dispositivos de monitoramento residencial, dispositivos para gestão de frotas e câmeras das mais diversas com IoT. Outros clientes incluem companhias que operam medidores de energia elétrica inteligentes, automação industrial, sistemas de rastreamento e logística.

O maior desafio dessa organização é garantir a satisfação do cliente e uma boa experiência no uso de sua infraestrutura. Ela precisa fornecer serviços com valores agressivos de SLA, banda, latência e disponibilidade de rede em torno de 99.99% para suportar as tecnologias emergentes que seus clientes estão adotando.

A empresa tem como meta para os próximos cinco anos cobrir 120 cidades brasileiras com sua infraestrutura de rede LoRaWAN, incluindo todas as capitais. Até o final de 2025, ela espera ter 5 milhões de dispositivos IoT conectados em sua infraestrutura.

Diante do crescente aumento no uso da rede e do emprego massivo de dispositivos IoT, além de estar ciente da relevância em priorizar a experiência do usuário, a TelecomInc decidiu utilizar as plataformas de gerenciamento de cada fabricante para fazer o monitoramento das falhas e da performance de suas antenas.

PROBLEMA

A TelecomInc controla e monitora a performance e a utilização da rede LoraWan de forma descentralizada e manual. Ela é incapaz de:

Correlacionar alarmes.

Agir preventivamente para evitar falhas ou diagnosticar em tempo real a degradação dos serviços contratados.

A empresa constatou um aumento do registro de reclamações em seu *call center* e teme que a taxa de cancelamento de clientes possa tornar-se crítica.

SOLUÇÃO

Diante do crescente aumento de uso da rede LoraWan e dos agressivos SLAs que os clientes exigem, e querendo priorizar a experiência do usuário, a TelecomInc decidiu centralizar a gestão dos seus dispositivos em uma única plataforma de IoT robusta. Nessa plataforma, a empresa realiza o gerenciamento de falhas e o monitoramento de performance cruzando os alarmes recebidos.

Seus funcionários monitoraram o status dos dispositivos de IoT e das *leased lines* contratadas todos os dias (24 horas por dia e 7 dias por semana). O objetivo é garantir a aderência aos SLAs contratados e que a experiência do usuário esteja de acordo com a expectativa dos clientes, evitando, assim, o risco de multas contratuais e penalidades do agente regulador.

O sistema também ajuda a TelecomInc a verificar se está recebendo a banda contratada das operadoras de telecomunicações.

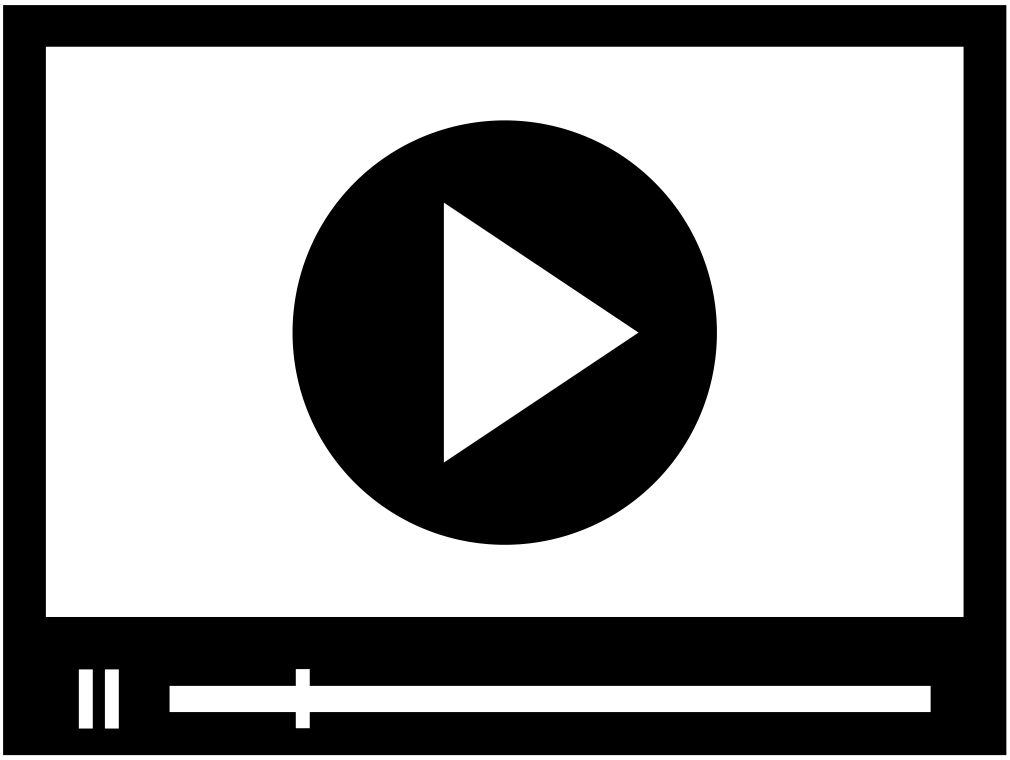
PERSPECTIVAS E PROJEÇÕES

Em 2019, o presidente da República assinou o Decreto Nº 9.854, que versa sobre a internet das coisas. Esse decreto define:

[A IOT É UMA] “INFRAESTRUTURA QUE INTEGRA A PRESTAÇÃO DE SERVIÇOS DE VALOR ADICIONADO COM CAPACIDADES DE CONEXÃO FÍSICA OU VIRTUAL DE COISAS COM DISPOSITIVOS BASEADOS EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO EXISTENTES E NAS SUAS EVOLUÇÕES, COM INTEROPERABILIDADE”.

BRASIL, 2019

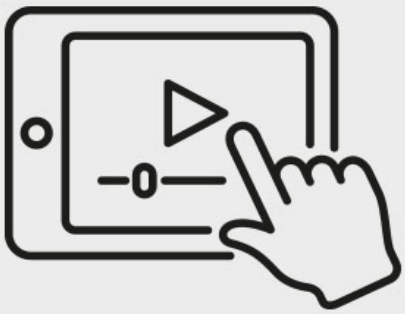
A expectativa é que os serviços de IoT não pagarão os altos impostos setoriais que poderiam afetar o seu crescimento no país. Essa notícia, portanto, aqueceu o mercado. As consultorias especializadas projetaram para cima suas previsões de investimento no setor.



A INTERNET DAS COISAS

O especialista Michel Medeiros apresenta o conceito da internet das coisas (IoT), seu histórico, arquitetura e os tipos de dispositivos que podem ser utilizados.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



VERIFICANDO O APRENDIZADO

1. UMA ARQUITETURA DE IOT É COMPOSTA POR ELEMENTOS BÁSICOS. QUAL ALTERNATIVA APRESENTA OS ELEMENTOS CORRETOS?

A) Gateway Backhaul, dispositivos CDN, *cloud* e aplicações.

B) Gateway Edge, camada de apresentação, *cloud* e aplicações.

C) Gateway Edge, dispositivos IOT, *cloud* e aplicações.

D) Servidor de internet, *things*, *cloud storage* e *caching service*.

E) Servidor DNS, dispositivos CDN, *cloud* e aplicações.

2. ASSINALE A ALTERNATIVA QUE CONCEITUA CORRETAMENTE OS DISPOSITIVOS DE IOT:

A) O dispositivo de IoT é um hardware que gera alarmes com os dados coletados, armazenando-os em sua memória sem transmiti-los.

B) O dispositivo de IoT é composto por um hardware e software que se conecta à internet exclusivamente para receber dados coletados pela nuvem.

C) O dispositivo de IoT é um software que se conecta à internet para transmitir dados coletados.

D) O dispositivo de IoT é composto por hardware e *software* que se conecta à internet para transmitir dados coletados.

E) O dispositivo de IoT é composto por hardware e software que se conecta à internet para verificar o funcionamento da cloud.

GABARITO

1. Uma arquitetura de IoT é composta por elementos básicos. Qual alternativa apresenta os elementos corretos?

A alternativa **"C "** está correta.

Para que seja possível a comunicação entre os diversos tipos de dispositivos IoT, como, por exemplo, sensores e atuadores, entre outros, é necessário o emprego de uma arquitetura distribuída que contenha não apenas os dispositivos, mas também os *gateways*. Para reduzir a latência da rede, a *cloud* em que fica essa plataforma integra as informações e, por fim, as aplicações.

2. Assinale a alternativa que conceitua corretamente os dispositivos de IoT:

A alternativa **"D "** está correta.

Os diversos tipos de dispositivos IoT são formados por uma combinação de hardware ultraespecializado e software embarcado, os quais, juntos, permitem a coleta de dados e seu envio por meio da internet, além de, em alguns casos, realizar o processamento deles e reagir a algum evento.

MÓDULO 2

⊙ **Reconhecer os esforços de padronização e os principais protocolos usados para o estabelecimento da conectividade em uma rede de IoT**

PRIMEIRAS PALAVRAS

O módulo anterior nos deu uma ideia geral do conceito de IoT, de seus elementos e de sua arquitetura, além de estabelecer um breve histórico. Vimos também as principais placas utilizadas para prototipação e aplicações comerciais.

O objetivo deste módulo, por sua vez, é dar a você uma visão geral dos esforços de padronização em curso e apresentar os principais protocolos de comunicação utilizados em implementações de IoT: MQTT e HTTPS.

ESFORÇOS DE PADRONIZAÇÃO

DELINEANDO PROBLEMAS E LIMITAÇÕES

Fonte: Shutterstock.com.

O mercado de IoT experimentou um crescimento vertiginoso nos últimos anos, com o aparecimento de diversos fabricantes de hardware, software e plataformas de IoT. São inúmeras as opções de placas e protocolos disponíveis para se desenvolver uma aplicação de internet das coisas.

Dessa forma, distintos fabricantes fizeram escolhas diferentes baseados em seus objetivos comerciais e em requerimentos técnicos, combinando as tecnologias disponíveis de acordo com as conveniências do momento para alcançar seus objetivos de negócios.

Criou-se, assim, uma miríade de soluções proprietárias.

Não houve esforços para a criação de uma interoperabilidade. Além disso, tais soluções são fracamente acopláveis entre si, quando não completamente incompatíveis. Alguns fabricantes inclusive implementam esse tipo de estratégia intencionalmente para travar o cliente nos seus ambientes, criando uma barreira tecnológica e de custo que o força a continuar comprando seus produtos e serviços.

COMENTÁRIO

Obviamente, um mercado fechado é bastante desvantajoso para a comunidade. Ele retarda a evolução e a adoção de tecnologias por dispersar esforços e investimentos, além de inibir a criação de padrões largamente aceitos.

O esforço de desenvolver soluções completas fim a fim reduz o número de competidores no mercado, levando à concentração, ao monopólio e ao alto custo de desenvolvimento.

Um mercado aberto e baseado em padrões da indústria, entretanto, reorganiza as prioridades de investimento, empreendendo esforços no estabelecimento de consensos tecnológicos e padrões interoperáveis.

Isso permite que fabricantes especializem suas competências nas áreas em que são melhores, criando vantagens competitivas baseadas no mérito. Desse modo, os usuários podem facilmente mudar de fabricantes ou operar soluções heterogêneas sem maiores dificuldades.

É interesse dos governos, das agências reguladoras e até mesmo dos fabricantes que padrões sejam definidos, uma vez que eles simplificam e barateiam o custo do desenvolvimento de aplicações baseadas em IoT. Eles também aceleram a evolução da internet das coisas ao permitir que novos competidores se estabeleçam em nichos de mercado, imprimindo mais competição, além de proporcionar maior flexibilidade de escolha aos clientes.

EXEMPLO

Um dos grandes problemas de interconectividade experimentados atualmente pelos gestores de soluções de IoT é a forte dependência de sensores e atuadores dos seus sistemas de administração e interfaces de processamento proprietários.

Isso torna extremamente complicada a consolidação dos dados transmitidos, assim como dificulta especialmente a gestão dos hardwares, exigindo a criação de camadas com interfaces adicionais. Entretanto, a qualidade de gestão de uma rede heterogênea dessa forma dificilmente é uniforme.

Há, portanto, a necessidade de se criar uma camada aberta e padronizada para unificar a operação remota de sensores e outros hardwares de diferentes fabricantes, facilitando a

entrega dos dados para as funções distribuídas e hospedadas na nuvem, bem como para permitir a gestão integrada dos sensores por intermédio do envio de comandos.

Outros benefícios da adoção de padrões para a tecnologia IoT incluem a redução dos custos de propriedade (TCO, sigla de *total cost of ownership*) e a interoperabilidade dos multifabricantes.

=

Padrões são definidos após longos debates nos quais diversos interesses são levados em consideração, incluindo políticas governamentais de inclusão e proteção ao meio ambiente; no entanto, leva algum tempo para se atingir tal maturidade.

CONSÓRCIOS FORMADOS

Vários deles foram formados para propor padronizações para IoT. Elencaremos alguns deles a seguir:

ONEM2M CONSORTIUM

Criado para desenvolver uma camada M2M (*machine to machine*) que possa ser usada em hardwares e softwares novos e antigos.

Ele possui atualmente 227 participantes – entre eles, gigantes como as empresas AT&T, China Mobile e Vodafone.

OCF (OPEN CONNECTIVITY FOUNDATION)

Consórcio que reúne mais de 300 membros do naipe de Microsoft, Samsung, LG e Electrolux. O objetivo é criar um padrão que permita uma interoperabilidade entre os novos e antigos dispositivos de IoT.

IEEE P2413 WORKING GROUP

Grupo de estudos formado por especialistas membros do Institute of Electrical and Electronics Engineers (**IEEE**). Ele visa à criação de um framework padrão para a arquitetura de IoT.

IEEE

Organização profissional sem fins lucrativos dedicada ao avanço da tecnologia. Um de seus papéis mais importantes é o estabelecimento de padrões para uso em computadores e diversos dispositivos.

IIC (INDUSTRIAL INTERNET CONSORTIUM)

Organização sem fins lucrativos que reúne 258 empresas – entre elas, DELL, Huawei e GE – com o propósito de acelerar a adoção e a difusão das melhores práticas para a aceleração do crescimento de IoT para a indústria.

IETF (INTERNET ENGINEERING TASK FORCE)

Organização cujo objetivo é revisar diversas tecnologias para equipamentos de baixo consumo de energia (6LoWPAN) em diversas áreas, como, por exemplo, segurança, roteamento e camada de acesso.

THINGSTORE

A comunidade cientifica e empresarial vem discutindo uma possível solução que pode funcionar como um padrão para o futuro da IoT: a ThingStore.

Ela implementa o conceito de serviço inteligente e funciona da seguinte maneira: o trabalho de desenvolvimento de sistemas complexos para IoT – tanto o embarcado quanto aquele na nuvem – fica a cargo de especialistas.

Uma empresa especializada em visão computacional cria os softwares e os carrega em uma loja virtual chamada de ThingStore. Outra empresa que maneja *things* em forma de câmeras de vigilância pode optar por assinar ou comprar o serviço, carregando-os em sua nuvem a fim de que seus dispositivos o utilizem.

Dessa forma, teríamos dispositivos de IoT genéricos que foram projetados para enviar telemetria na forma de dados brutos segundo padrões e especificações da indústria de IoT.

Não haveria preocupação com o software embarcado: ele se comunicaria com o serviço complexo existente na nuvem (plataforma de IoT), que faria todo o processamento pesado.

A ThingStore, portanto, contribuiria para a racionalização do uso da internet (somente o dado bruto trafega) e permitiria o compartilhamento da infraestrutura de IoT, já que as interfaces seriam do modo padrão, e não proprietárias. Além disso, ela simplificaria o desenvolvimento e promoveria o reuso do software.

Não é objetivo deste módulo entrar em detalhes acerca do progresso das discussões sobre a padronização para IoT, até porque alguns vão conseguir se estabelecer e outros, não. Torna-se difícil, nesse momento, prever o que irá acontecer.

O importante é você saber o seguinte:

Os esforços na busca pelas padronizações e pelas melhores práticas de IoT estão ocorrendo; dessa maneira, futuros padrões poderão emergir de um ou de vários dos consórcios existentes.

PROTOCOLOS DE COMUNICAÇÃO DE DADOS USADOS EM IOT

Um sistema baseado em IoT pode implementar até quatro formas diferentes de comunicação entre seus componentes:

Os dispositivos podem se comunicar entre si diretamente (*device to device*) ou podem se comunicar com o *gateway* (*device to gateway*). Os *gateways*, por sua vez, falam com os sistemas de dados (*gateway to data systems*), enquanto os próprios sistemas de dados podem conversar entre si para realizar tarefas, como, por exemplo, a de sincronizar suas partições (*data system to data system*).

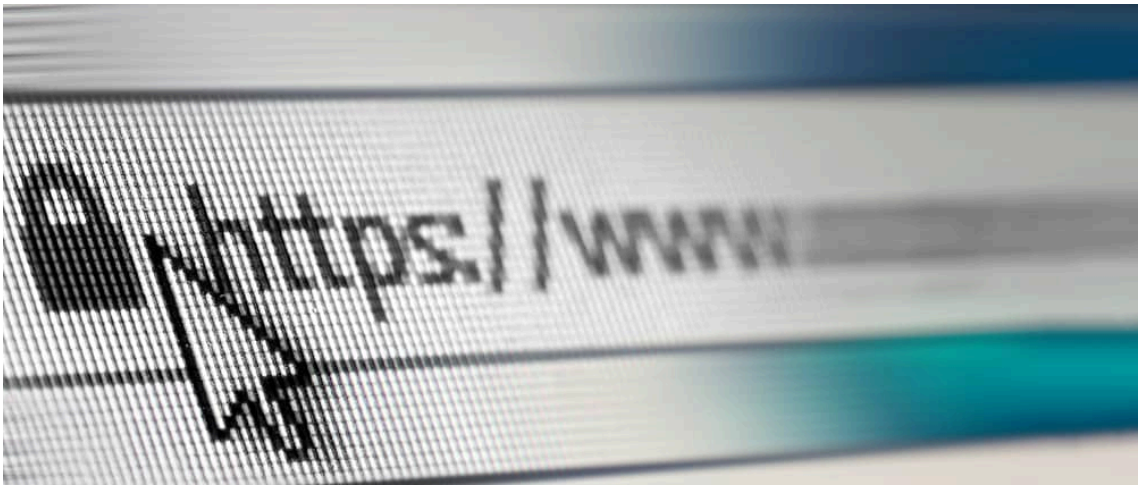
Essa capacidade de comunicação permite que toda a rede atinja um estado consistente e esteja “consciente” acerca do que está acontecendo com os outros membros da rede. Ela é conhecida como **cura automática** (ou *self healing*).

★ EXEMPLO

Em uma rede de energia elétrica, medidores e concentradores inteligentes podem, por ação ou omissão, fazer o *gateway* entender que existe um blecaute de energia em determinados nós dela e que ações automáticas podem ser tomadas para isolar os elementos em risco ou danificados e até mesmo rotear o fluxo de energia elétrica através de outros transformadores por caminhos alternativos.

Apresentaremos a seguir dois protocolos de comunicação de dados:

PROTOCOLO HTTP/HTTPS



Fonte: Shutterstock.com.

O protocolo HTTP (hypertext transfer protocol) é bem conhecido entre os desenvolvedores e os profissionais de tecnologia de informação (TI) por ter sido criado nos primórdios da internet para suportar a comunicação entre páginas (sites) e navegadores. Ele implementa código legível no formato de texto ASCII.

Ele funciona por meio de requisições e respostas *(requests, responses*) sobre o protocolo TCP. O TCP é um protocolo orientado à conexão, isto é, o servidor abre uma sessão de comunicação com o cliente, que fará a requisição e a manterá aberta enquanto houver a troca de dados, fechando-a logo após o encerramento dessa troca.

O HTTPS (Hypertext Transfer Protocol Secure) é uma extensão de segurança do bem conhecido protocolo HTTP.

📢 ATENÇÃO

O HTTP, portanto, é inseguro e extremamente não recomendado para a implementação da transmissão de dados em aplicações comerciais, devendo, para isso, ser usado o HTTPS, que é bastante seguro.

Ele emprega a criptografia para impedir que dados trocados sejam lidos e verifica a identidade do servidor e do software com que se está comunicando. Além disso, é simples e bastante intuitivo de se usar, tendo sido criado para naturalmente passar por cima de *firewalls* e *proxies* ou para evitá-los.

Citaremos três deles adiante:

SENTIDO ÚNICO DO TRÁFEGO DE DADOS

O sentido da comunicação, isto é, o tráfego de dados ocorre apenas em um sentido: do cliente para o servidor. A IoT, contudo, requer comunicação bidirecional.

Alguns evangelistas da internet das coisas advogam que isso, na verdade, aumenta a segurança, pois impede que estranhos enviem pedidos de conexão para o dispositivo. Contudo, em redes modernas de IoT, é preciso configurar ou atualizar milhares de dispositivos simultaneamente – e, para isso, eles precisam aceitar requisições de conexão.

TRAVAMENTO

O HTTPS é síncrono e, portanto, trava a *thread* enquanto espera a resposta do servidor, desperdiçando recursos preciosos, como, por exemplo, o tempo de processador. Ele, afinal, foi projetado para estabelecer a comunicação apenas entre dois agentes: o cliente e o servidor.

Além disso, criar e manter a sessão TCP consome muitos recursos valiosos e pode se tornar bastante ineficiente tanto em consumo de energia quanto em recursos computacionais. Caso haja milhares de requisições simultâneas, isso pode até derrubar o servidor.

O HTTPS também divide enormes quantidades de dados para transferi-los em pequenos pacotes, o que tem o potencial de gerar picos de grande consumo de banda e retardos na rede devido ao *overhead* dos pacotes.

NÃO GUARDAR ESTADOS

Outra desvantagem é o fato de não guardar estados (*stateless communication*). Sempre que um dispositivo precisa enviar telemetria, é preciso solicitar uma conexão e fazer a autenticação,

o que, aliás, também gera bastante *overhead* durante o *handshake*.

PROTOCOLO MQTT

Nesta seção, conheceremos o protocolo MQTT de padrão aberto. Ele resolve algumas das limitações do HTTP/HTTPS.

A) HISTÓRICO E CONCEITUAÇÃO

MQTT é a sigla desta expressão em inglês: *message queuing telemetry transport*. Adaptando-a para o português, isso significa transporte de telemetria de enfileiramento de mensagens.

Ele foi criado em 1999 pela IBM especificamente para:

Suportar a comunicação M2M (machine to machine).

Implementar uma arquitetura cliente-servidor orientada a mensagens.

B) COMANDOS

Os dados trocados entre os dispositivos de IoT (clientes) e o servidor, que normalmente é chamado de *broker*, são subscritas por tópicos hierárquicos.

Isso é conhecido como protocolo de mensagens *publish/subscribe*, na qual fluxos de dados são enviados para serem consumidos de acordo com os tópicos que assinam.

Pode-se subscrever para um ou mais tópicos. Isso possibilita a comunicação de um para um, de um para muitos e de muitos para um.

★ EXEMPLO

Quatro dispositivos IoT estão conectados ao mesmo *broker*. Todos eles assinam a mesma fila específica; assim, quando um deles publica um dado nessa fila, todos os outros consomem a informação, podendo responder ao valor publicado. O pacote que o MQTT trafega ocupa 2 bytes e tem um cabeçalho menor que o do HTTPS. Enquanto os comandos do HTTP seguem o formato texto e emitem palavras legíveis aos humanos, eles, no MQTT, são curtos, menos complexos e seguem o formato binário, gerando, portanto, menos *overhead* e a economia da banda.

O MQTT é, portanto, ideal para as redes cuja internet seja custosa e limitada. Seu vocabulário de comandos também é muito simples.

De modo geral, seus principais comandos funcionam da seguinte forma:

CONNECT E *CONNACK*

O *connect* é enviado para requisitar a abertura de uma conexão. O iniciador recebe um *connack* (*connection acknowledge*) de resposta.

SUBSCRIBE E *UNSUBSCRIBE*

O comando *subscribe* inscreve o dispositivo em determinada fila. Já o *unsubscribe* produz o efeito contrário.

PUBLISH E *PUBACK*

O *publish* é enviado quando se quer publicar dados em fila específica de acordo com o tópico, recebendo um *puback* de volta.

C) QOS

Ao enviar uma mensagem, pode-se escolher entre três distintos níveis de QOS (quality of service), que serão os responsáveis por estabelecer os contratos entre o remetente e o destinatário dos dados.

1

MODO QOS 0

QoS 0 é o modo mais rápido, pois estabelece que nenhuma das pontas da comunicação (cliente e o servidor) receberá a confirmação (*acknowledge*) de que o dado foi recebido.

Obviamente, esse modo é o mais propenso para haver uma perda de mensagens. Ele é chamado, por isso, de “disparar e esquecer” (*fire and forget*).

MODO QOS 1

No modo QoS 1 (chamado de *at least once*), o cliente e o servidor confirmam o recebimento dos dados. Caso alguma das pontas não envie o ACK de confirmação ou ele se perca, o remetente reenviará a mensagem após determinado período.

2

3

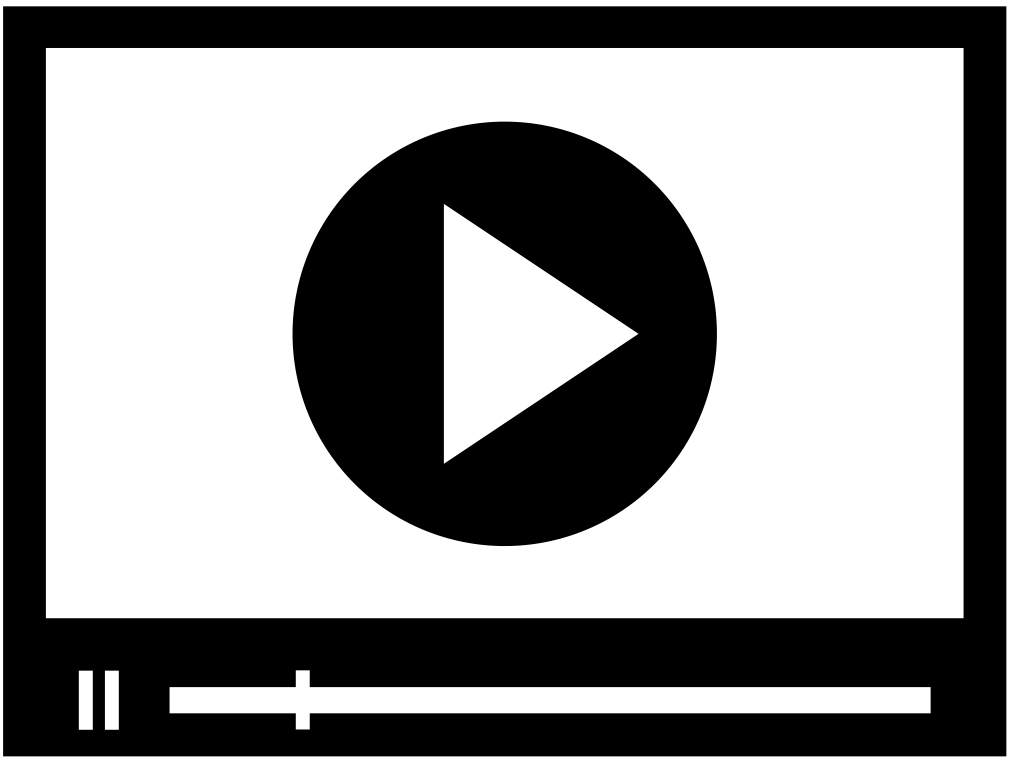
MODO QOS 2

No QoS 2 (*exactly once*), o MQTT implementa um pequeno *handshake* para garantir que a mensagem seja entregue apenas uma vez. Esse protocolo é altamente confiável, uma vez que

as mensagens podem ser persistidas no servidor até que o dispositivo esteja online e possa recebê-las.

O *handshake* do MQTT armazena o estado da comunicação (diz que ele é *statefull*). Desse modo, é possível reusar uma conexão aberta para enviar mais telemetria, simplificando a operação e consumindo menor banda.

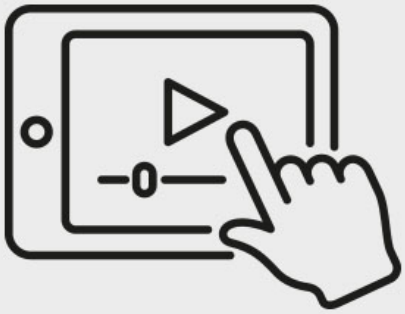
Um dos aspectos mais interessantes do MQTT – e que comumente passa despercebido – é saber que ele pode funcionar sem internet. Após o MQTT usar o protocolo TCP para enviar as mensagens, é necessário haver apenas o IP do cliente e do servidor para ocorrer uma troca de informações entre as pontas.



MODELOS DE COMUNICAÇÃO PARA IOT

O especialista Michel Medeiros apresenta os principais protocolos de comunicação para IoT.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.



VERIFICANDO O APRENDIZADO

1. APONTE OS DOIS PROTOCOLOS DE COMUNICAÇÃO MAIS USADOS EM IOT:

A) AMQP e MQTT

B) HTTPS e AMQP

C) HTTP e AMQP

D) HTTPS e MQTT

E) HTTP e HTTPS

2. MARQUE A OPÇÃO COM UMA CARACTERÍSTICA CORRETA DO PROTOCOLO MQTT:

A) Criado pela AT&T, ele implementa a arquitetura de mensageria por subscrição em filas de tópicos.

B) Orientado à conexão, ele depende do protocolo UDR para o transporte dos dados.

C) Ele foi criado no início da internet para suportar a comunicação entre sites e navegadores.

D) Criado pela IBM, ele implementa a arquitetura cliente-servidor e é orientado à mensageria.

E) Os pacotes possuem cabeçalhos grandes no formato texto e introduzem bastante *overhead*.

GABARITO

1. Aponte os dois protocolos de comunicação mais usados em IoT:

A alternativa **"D "** está correta.

Os dois protocolos de comunicação mais usados em IoT são o HTTPS e o MQTT. Aquele é utilizado largamente nas aplicações web, mas não é suficiente para o emprego nos dispositivos IoT, enquanto este é o protocolo que tem atendido às necessidades para tais dispositivos.

2. Marque a opção com uma característica correta do protocolo MQTT:

A alternativa **"D "** está correta.

O MQTT foi criado pela IBM e utiliza uma arquitetura cliente-servidor. Ele emprega o conceito de filas baseadas em tópicos: os clientes se inscrevem, ou melhor, assinam aquele tópico para que possam receber as informações necessárias.

MÓDULO 3

⦿ **Identificar as plataformas de IoT disponíveis no mercado e seus principais serviços**

PRIMEIRAS PALAVRAS

Segundo as metodologias modernas de desenvolvimento de software, os requisitos de um sistema se dividem em vários tipos de requerimentos:

De negócio

De sistema

De desempenho

Funcionais

Não funcionais

Os sistemas baseados em IoT são especificados com classificações adicionais devido à natureza intensa do tráfego de dados.

Existem, portanto, requerimentos de gerenciamentos de dados que especificam como eles devem ser recebidos e tratados.

Esses requerimentos possuem quatro tipos:

INGESTÃO

Trata do modo como os dados serão recebidos e tratados pelo sistema.

ANALYTICS

Específica os requisitos de modelos preditivos, de IA e afins.

COMUNICAÇÃO

Versa sobre a comunicação entre os módulos do sistema, incluindo alarmes e mensageria.

PERSISTÊNCIA

Fala de políticas e técnicas de retenção dos dados no servidor.

Tendo isso em vista, conheceremos agora os requisitos não funcionais da IoT e a arquitetura de referência para a internet das coisas.

REQUISITOS NÃO FUNCIONAIS DA IOT

Desenvolver uma aplicação de IoT é uma tarefa multidisciplinar que envolve hardware, software e muito planejamento.

A etapa de levantamento de requisitos busca determinar as funcionalidades que o sistema precisa ter para atingir os objetivos de negócios.

É nesse momento que são definidos os requisitos não funcionais. Eles especificam as limitações e as restrições (ou capacidades), podendo ser de vários tipos:

DISPONIBILIDADE

É preciso especificar o tempo de atividade do serviço. A maioria dos sistemas de IoT funciona 24 horas por dia e 7 dias por semana.

CONFIABILIDADE

O projetista especifica o tempo de execução que o sistema deve apresentar sem incorrer em falhas ou erros. As IoT são aplicações críticas e não admitem falhas, sob pena de haver a geração de falsos alarmes.

RECUPERAÇÃO DE DESASTRE (*DISASTER RECOVERY*)

Determina os recursos que precisam existir e como eles devem funcionar para que o sistema se recupere de uma falha catastrófica.

★ EXEMPLO

Um terremoto em um dos *datacenters* que servem um sistema ou outro sistema de monitoramento meteorológico que utilize um *datacenter* na cidade A. Em caso de falha nessa localidade, os serviços devem migrar rapidamente para a cidade B, que é geograficamente distante.

SEGURANÇA, PROTEÇÃO DE DADOS E BACKUP

A especificação do sistema precisa estabelecer que meios de segurança devem ser usados para autenticar e autorizar usuários, além de garantir a proteção tanto dos dados coletados e analisados quanto dos comandos enviados. Regras e recursos destinados a criar redundância de dados também têm de ser especificados.

ESCALABILIDADE

O sistema deve ser resiliente ao aumento de demanda, seja ele progressivo ou repentino.

As melhores plataformas de IoT:

- Suportam adoção rápida de novos dispositivos.
- Permitem *upgrades* automáticos nos recursos computacionais em nuvem para atender aos picos de demanda.

Utilizam-se técnicas de *load balancing* para uma melhor divisão da carga entre os nós de processamento. É necessário ser transparente para os dispositivos.

ARQUITETURAS DE REFERÊNCIA PARA IOT

Decidir qual arquitetura usar para suportar uma rede de IoT não é tarefa fácil: isso envolve, afinal, custos crescentes (e, muitas vezes, escondidos), que podem subir muito de acordo com o tamanho da rede. Para que os dispositivos troquem informações de forma adequada e – em muitos casos – executem ações coordenadas, é necessário haver um meio em comum.

Tendo isso em vista, diversos fabricantes desenvolveram plataformas a fim de que os dispositivos de IoT possam ser integrados e gerenciados de forma simples e eficiente da melhor maneira possível.

Listaremos abaixo as principais plataformas. Antes disso, porém, devemos observar que muitos provedores de peso (*big techs*) já criaram os próprios ambientes de IoT nos quais disponibilizam diversos serviços de valor agregado.

- Amazon AWS IoT Core
- Microsoft Azure IoT Suite
- Google Cloud’s IoT Platform
- Cisca IoT Cloud Connect
- Oracle IoT Platform

Salesforce IoT Cloud

IBM Watson IoT Platform

Thingspeak IoT Platform

IRI Voracity

Kaa IoT Platform

Thingworx 8 IoT Platform

Cloud Arduino

Nesta seção, apresentamos uma visão geral das principais plataformas de IoT disponíveis no mercado, descrevendo, para isso, seus principais serviços. A ideia é que você obtenha uma noção geral acerca das opções existentes no mercado.

Nosso foco serão as três maiores plataformas em circulação:

Amazon AWS IoT

Microsoft Azure IoT Suite

Google Cloud IoT

SAIBA MAIS

Líder de mercado, a AWS possui a maior variedade de oferta de serviços, mas tem preços mais elevados que os de suas principais concorrentes: Azure IoT e Google IoT Core. Ambas ocupam respectivamente a segunda e a terceira posição.

AMAZON AWS IOT

O AWS IoT é o ambiente na nuvem que a Amazon disponibiliza para integrar os dispositivos de IoT.

Após a conexão de cada um deles à nuvem IoT AWS, ela garante que tais dispositivos possam:

Trocar informações entre si.

Consumir **serviços especializados** que são disponibilizados no formato SaaS (Do inglês software as a service.) .

SERVIÇOS ESPECIALIZADOS

Eles podem ser tanto serviços específicos do tipo AWS IoT Core quanto serviços AWS puramente genéricos.

O AWS IoT suporta os protocolos de comunicação MQTT, HTTP/HTTPS e TLS.

Para usar todas as funcionalidades, é preciso ter uma conta AWS.

Conectar um dispositivo à sua nuvem é bastante simples, demorando de 15 a 20 minutos. Observe o passo a passo:

1

Usando o console AWS IoT, o usuário precisa, primeiro lugar, selecionar o sistema operacional (Linux ou Windows). Ele o usará para:

Executar os comandos de configuração do dispositivo.

Escolher o ambiente de desenvolvimento (SDK) entre Java, Python e Node.js

Em seguida, o usuário registrará o dispositivo, escolhendo um nome único que não pode ser alterado. O sistema gera um certificado, a política de autorização e o script com o propósito de interagir e carregar a SDK no dispositivo.

Esse procedimento pode ser executado num computador, o qual, por sua vez, será usado depois para carregar e configurar os arquivos no dispositivo IoT. Caso o dispositivo suporte um navegador, o procedimento também pode ser executado diretamente nele: é só salvar os arquivos em seu *file system*.

2

3

Ao final, quando o dispositivo IoT estiver configurado, basta testá-lo e explorar as possibilidades de serviços oferecidas pela plataforma AWS IoT.

Os serviços AWS Core IoT que a plataforma oferece servem para:

Conectar o dispositivo à nuvem.

Permitir que ele consuma serviços diversos.

Para que isso seja possível, diversos módulos trabalham juntos.

A arquitetura do sistema é composta basicamente por **quatro módulos**:

MESSAGE BROKER

O ponto de entrada é o módulo responsável por manejar a comunicação entre os dispositivos inscritos nele e a nuvem AWS IoT.

DEVICE SHADOW

Ele garante que os dados de aplicações destinados ao dispositivo sejam entregues mesmo se ele estiver offline, sincronizando-os assim que o aparelho reconectar.

RULES ENGINE

Este módulo guarda expressões e dados que ditam o comportamento do dispositivo. Por meio dele, é possível invocar funções lambda para atender a uma demanda específica.

SECURITY AND IDENTITY

A segurança fica a cargo deste módulo, que utiliza protocolos baseados no certificado x.509 para garantir a autenticação e as devidas autorizações do dispositivo requerente. Ele se comunica periodicamente com os outros módulos mencionados ou sempre que uma requisição é iniciada.

RESUMINDO

Uma rede de dispositivos de IoT geograficamente distribuídos pode ser conectada à plataforma AWS para que ela coordene a comunicação entre eles. Além disso, não é necessário que cada dispositivo processe completamente os dados adquiridos; em vez disso, serviços inteligentes hospedados na nuvem AWS podem fazer esse trabalho mais pesado de processamento, sincronizando o resultado quando os dispositivos estiverem online.

MICROSOFT AZURE IOT SUITE

A solução da Microsoft para integrar dispositivos de IoT é chamada de Azure IoT.

Ela é baseada em um *software open source* e oferece basicamente os mesmos serviços da Amazon AWS IoT; entretanto, a arquitetura que a suporta é bem diferente.

O gateway de conexão de entrada, que recebe os dados e as requisições dos dispositivos, é denominado IoT Hub. Ele é responsável por receber a gigantesca quantidade de dados que é enviada por milhares de *things*. A IoT Hub suporta os protocolos de comunicação MQTT, HTTP/HTTPS e AMQP.

Os fluxos de dados passam então pelo módulo de *analytics* do sistema, cujo nome é *stream analytics.*

Nele, é possível:

Configurar regras.

Definir ações e *thresholds* por dispositivo ou por grupo de dispositivos.

Processar e visualizar os dados quase em tempo real.

Armazenados em *blobs* (*storage blobs*), esses dados podem ser repassados pelo *event hub* para diversos serviços, como, por exemplo, web jobs ou web apps.

O módulo DocumentDB armazena os metadados, enquanto o módulo LogicApp faz a integração com os sistemas de *backend*. A plataforma também é rica em painéis para a visualização de dados (*dashboards*) bastante customizáveis, fazendo o uso do Power BI.

Pode-se observar diversos gráficos relacionados a fluxos de dados entrantes, análises e computação realizadas, histórico de alarmes etc. Também é possível gerenciar e enviar comandos (telecomandos) manualmente para os dispositivos a partir do *dashboard*.

DICA

No caso de uma rede com muitos dispositivos, o desenvolvedor precisa usar as APIs para implementar comandos em lote ou implementar automações.

A autenticação e autorização são feitos pelo módulo *active directory*. O sistema permite a implantação e a orquestração de diversos serviços complexos, sendo bastante escalável e projetado para ser agnóstico em relação ao sistema operacional dos dispositivos de IoT ou equivalente no caso dos microprocessadores.

Desse modo, o Azure IoT pode conectar virtualmente qualquer tipo de aparelho.

O registro dos dispositivos – tal qual no AWS IoT – toma apenas alguns minutos e requer a criação de uma conta, embora o usuário também tenha a opção de criar dispositivos virtuais (*virtual devices*) para realizar simulações e testes.

SAIBA MAIS

A Microsoft disponibiliza opcionalmente um ambiente de desenvolvimento (SDK) muito rico em bibliotecas; contendo muitos exemplos de código, ele pode ser usado em qualquer dispositivo.

Existem muitos casos indicados para se usar Azure IoT, como o de gerenciamento de ativos, gerenciamento de frota e o de manutenção preventiva, mas o caso de emprego mais comum e bastante enfatizado pela empresa é o de monitoramento industrial remoto. Diversos *things* acoplados às máquinas e conectados à plataforma enviam suas telemetrias para a IoT Hub. Os serviços de *analytics* então recebem os dados, sendo capazes de determinar se uma máquina não está funcionando corretamente, se requer algum tipo de intervenção ou até mesmo se precisa de manutenção. A plataforma pode então abrir um chamado no sistema de *trouble ticket* no *backend* do cliente ou gerar outros alertas automaticamente para os gestores da área.

O objetivo final, portanto, é integrar a tecnologia IoT como parte de um processo de negócios.

ATENÇÃO

É importante mencionar também que toda a comunicação entre a plataforma e os dispositivos é criptografada. O Azure IoT usa o certificado X.509 e *tokens* de segurança para validar cada dispositivo conectado.

GOOGLE CLOUD IOT

A solução da Google para integrar dispositivos de IoT é similar às duas mostradas anteriormente (AWS e Azure IoT). Baseadas em serviços gerenciáveis, todas elas oferecem um portal para o gerenciamento da rede de equipamentos na administração da rede de IoTs.

Para iniciar o serviço, é preciso criar uma conta, registrar os dispositivos e configurar os serviços que vão tratar os dados – e assim por diante.

O processo de adoção dos equipamentos até que ele esteja pronto para uso recebe o nome de **provisionamento**.

SAIBA MAIS

O usuário precisa carregar no dispositivo um código específico, além de um conjunto de metadados, um *token* ou uma chave de acesso, para autorizá-lo na nuvem da Google. Essa

nuvem é específica por serviço.

A porta de entrada para os dados na plataforma de IoT da Google é chamada de *communication broker*. Ela suporta os protocolos de comunicação MQTT e HTTPS e funciona como um *endpoint* global: o dispositivo é associado ao *datacenter* geograficamente mais próximo, reduzindo ao mínimo a latência experimentada.

Por meio do *broker*, a telemetria é injetada na plataforma através do *protocol bridge* diretamente para o *data broker*, o qual, por sua vez, envia os dados para o módulo *cloud* Pub/Sub. Ele persiste as mensagens e é baseado no sistema de tópicos de subscrição. Cada *stream de dados* recebido é associado (assinado) a um tópico. Isso permite que eles sejam tratados de forma diferente, invocando distintos serviços.

O *stream*, portanto, publica e consome de filas separadas de acordo com os tópicos que assina. Ele se conecta de forma nativa a diversos outros módulos do Google Cloud.

Eis três exemplos:

CLOUD ML ENGINE

Oferece serviços de aprendizado de máquina, como treinamento e execução de modelos.

CLOUD DATA FLOW

Realiza serviços de *analytics*.

BIG QUERY

Provê serviços de armazenamento de dados Big Data.

O usuário pode rodar *queries* (ANSI SQL) sobre grandes quantidades de dados sem sobrecarregar o sistema. O *cloud* Pub/Sub é inteligente, sendo capaz de escalar automaticamente de acordo com o aumento das mensagens (caso diversos dispositivos IoT respondam simultaneamente a um evento no mundo real que provoque um pico de demanda).

O usuário tem a opção de redirecionar os dados para a ferramenta de *log* do sistema conhecida como *cloud logging*. Ela armazena os dados de telemetria e de eventos relacionados aos dispositivos para fins de gestão, monitoramento e de auditoria.

É possível gerar métricas, gráficos e relatórios detalhados sobre o funcionamento da rede em tempo real. A ferramenta também permite a criação de alertas.

A plataforma ainda provê um *load balance* automático e suporte a dispositivos virtuais caso o cliente queira testar os serviços antes de empregá-los em produção nos dispositivos físicos.

Ela disponibiliza um ambiente de desenvolvimento chamado de *firebase*, que usa uma SDK nativa que suporta IOS, Android e C++. Além disso, disponibiliza uma API para suportar:

Desenvolvimento de aplicações

Execução de comandos em lote, como o registro de grupos de Dispositivos IoT e **automação**.

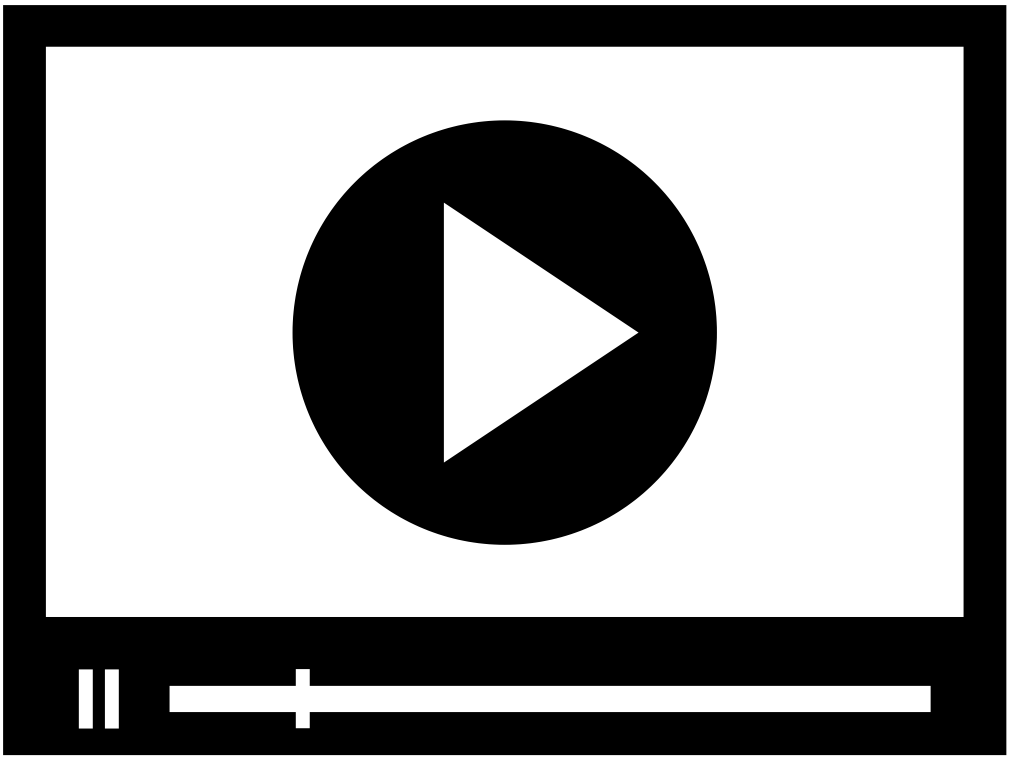
DISPOSITIVOS IOT E AUTOMAÇÃO

Caso das atualizações OTA (over the air).

Essas atualizações permitem ao usuário, em um *push* único, atualizar toda uma rede de dispositivos remotamente.

Havendo a necessidade de um serviço mais robusto e que requeira uma latência mínima, tendo uma comunicação quase em tempo real, é possível contratar o Google Cloud IoT Edge. Ele complementa as funcionalidades de IoT, permitindo que os dispositivos respondam quase em tempo real aos dados injetados nos *streams*.

Quanto à segurança, toda a comunicação com os dispositivos é criptografada. O Google IoT Core permite a criação de perfis de usuário de acordo com o nível de acesso.



ARQUITETURA DE REFERÊNCIA PARA IOT

O especialista Michel Medeiros apresenta as principais arquiteturas de referência para IoT.

Para assistir a um vídeo sobre o assunto, acesse a versão online deste conteúdo.

VERIFICANDO O APRENDIZADO

1. O VOLUME DE DADOS GERADO PELOS DISPOSITIVOS É IMENSO E REQUER RECURSOS COMPUTACIONAIS QUE PERMITAM O PROCESSAMENTO DAQUELES GERADOS E COLETADOS.

PARA ISSO, SÃO UTILIZADAS PLATAFORMAS DE INTEGRAÇÃO QUE PERMITEM O TRATAMENTO DESSE VOLUME DE INFORMAÇÕES. AS TRÊS MAIORES PLATAFORMAS DE IOT SÃO...

A) Salesforce, Azure e Google IoT

B) Watson, Azure e Google IoT

C) AWS, Cisco e Google IoT

D) AWS, Azure e Google IoT

E) AWS, Azure e Cloud Arduino

2. AS PLATAFORMAS DE INTEGRAÇÃO PARA DISPOSITIVOS IOT POSSUEM DIVERSOS MÓDULOS PARA GARANTIR A COMUNICAÇÃO E A CORRETA TROCA DE DADOS. ENTRE ESSES MÓDULOS, EXISTE O *CLOUD* PUB/SUB, QUE RECEBE A TELEMETRIA DOS DISPOSITIVOS E PERMITE A ASSOCIAÇÃO POR TÓPICOS. ESSE MÓDULO PERTENCE À QUAL PLATAFORMA DE IOT?

A) Microsoft Azure IoT

B) Oracle IoT

C) Google Cloud IoT

D) Amazon AWS IoT

E) Arduino Cloud IoT

GABARITO

1. O volume de dados gerado pelos dispositivos é imenso e requer recursos computacionais que permitam o processamento daqueles gerados e coletados.

Para isso, são utilizadas plataformas de integração que permitem o tratamento desse volume de informações. As três maiores plataformas de IoT são...

A alternativa **"D "** está correta.

Apesar de outros provedores terem soluções para a integração de dispositivos IoT, as três plataformas detentoras do maior *market share* do segmento são estas: AWS, Azure e Google IoT, sendo a AWS a mais utilizada.

2. As plataformas de integração para dispositivos IoT possuem diversos módulos para garantir a comunicação e a correta troca de dados. Entre esses módulos, existe o *cloud* Pub/Sub, que recebe a telemetria dos dispositivos e permite a associação por tópicos. Esse módulo pertence à qual plataforma de IoT?

A alternativa **"C "** está correta.

A plataforma Google Cloud IoT recebe os dados por meio do *communication broker*, que pode ser considerado a porta de entrada da plataforma. Através do *broker*, os dados de telemetria são enviados para o *data broke*r por meio do protocol bridge, que, em seguida, envia os dados para o módulo *cloud* Pub/Sub.

CONCLUSÃO

CONSIDERAÇÕES FINAIS

A tecnologia IoT é caracterizada por um ambiente extremamente heterogêneo e complexo que mistura software e hardware nos seus limites. Neste tema, introduzimos os principais conceitos e componentes para que você compreenda e esteja familiarizado com essa nova e excitante área.

No primeiro módulo, apresentamos a arquitetura e conceituamos a tecnologia. Também delineamos brevemente alguns conceitos, os quais, nos dois módulos seguintes, foram detalhados, como, por exemplo, os dispositivos e as plataformas de IoT.

Você agora já consegue identificar os principais componentes disponíveis no mercado, compará-los e escolher a plataforma mais adequada para sua solução.

Para ouvir um *podcast* sobre o assunto, acesse a versão online deste conteúdo.

AVALIAÇÃO DO TEMA

REFERÊNCIAS

AKPNAR, K.; HUA, K. A. **ThingStore** - an internet of things management system. *In*: 2017 IEEE Third International Conference on Multimedia Big Data. Laguna Hills. 2017. p. 354-361. Consultado em meio eletrônico em: 9 fev. 2021.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Consultado em meio eletrônico em: 9 fev. 2021.

INTEL. **Intel Edison development platform**. Consultado em meio eletrônico em: 25 fev. 2021.

INTERNATIONAL TELECOMMUNICATION UNION. **Unleashing the potential of the internet of things**. 2016. Consultado em meio eletrônico em: 9 fev. 2021.

MQTT. **MQTT**: The standard for IoT messaging. Consultado em meio eletrônico em: 25 fev. 2021.

PATEL, M.; SHANGKUAN, J.; THOMAS, J. **What's new with the internet of things?**. *In*: McKinsey & Company. Publicado em: 10 maio 2017.

PROJECT HUB. 221 **IOT projects**. Consultado em meio eletrônico em: 25 fev. 2021.

RASPBERRY PI. **Raspberry Pi**. Consultado em meio eletrônico em: 25 fev. 2021.

EXPLORE+

Acesse o site das plataformas de IoT apresentadas neste tema para verificar as características dos serviços oferecidos por cada uma:

Amazon AWS IoT

Microsoft Azure IoT

Google IoT

CONTEUDISTA

Michel Souza Medeiros

🔗 CURRÍCULO LATTES