# Internet of Things: Arquiteturas e Tecnologias

Hugo Manuel Cunha, Marcos Daniel Teixeira da Silva, Susana Vitória Sá Silva Marques

Universidade do Minho, Departamento de Informática, 4710-057 Braga, Portugal
Email:{a84656,a78566,a84167} @alunos.uminho.pt

**Abstract.** Há milhões de dispositivos tecnológicos em lares, fábricas, poços de petróleo, hospitais, carros e outros lugares. Com o crescimento e abundância destes, tem-se necessidade cada vez mais de soluções para conectá-los, armazenar e analisar dados dos mesmos. O termo "Internet of Things" descreve o grande e cada vez maior conjunto de dispositivos digitais que operam entre redes de escala global.

## 1 Introdução

A Internet Society define Internet of Things(IoT) em sentido amplo como a "extensão da conetividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores." Ao contrário da Internet que todos utilizamos, a IoT é composta apenas por sensores e outros dispositivos inteligentes. Entre os seus usos estão a captação de dados operacionais de sensores remotos em plataformas de petróleo, o seu benefício em dados climáticos e o controle de termostatos inteligentes. A IoT oferece novas e inovadoras maneiras para as organizações gerenciarem e monitorizarem operações remotas.

## 2 Arquiteturas IoT

Não existe qualquer arquitetura para IoT consensual, isto é universalmente aceite. A mais básica é composta por três camadas, tal como mostra a fig.1. Esta foi introduzida nas fases inicias de investigação nesta área.

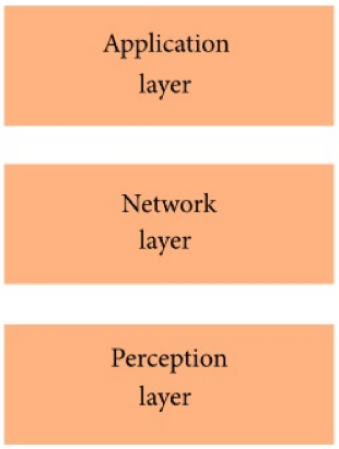


**Fig. 1.** Arquitetura 3-layer

**Application Layer** – Responsável por entregar o serviço especificado ao utilizador. Esta define as diversas aplicações nas quais a IoT pode ser aplicada, tais como, smart cities e smart homes;
**Network Layer** – Trata da conexão entre os diferentes aparelhos. As suas features são também usadas na transmissão e processamento de dados;
**Perception Layer** – É a camada física que contém sensores para a recolha de informação. [1].

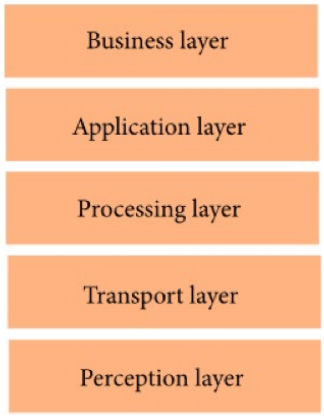


**Fig. 2.** Arquitetura 5-layer

A arquitetura de 3 camadas define a ideia principal de IoT da conexão entre os diferentes dispositivos, mas revelou se insuficiente na transferência de informação na IoT, uma vez que esta se foca em aspetos mais delicados. Para colmatar esta lacuna foi criada a arquitetura de 5 camadas, nas quais a Application Layer e Perception Layer possuem a mesma função desempenhada na arquitetura explicada previamente.
**Business Layer** – Gere todo o sistema IoT, incluindo aplicações e modelos de negócio;
**Processing Layer** – Também conhecida como middleware layer. Esta guarda, analisa e processa uma quantidade enorme de dados provenientes da Transport Layer. Fornece um conjunto de serviços ás camadas inferiores;
**Transport Layer** – Transfere os dados da perception layer para a processing layer (e vice versa), através de redes como 3G, LAN, Wireless, Bluetooth [1].

## 2.1 OpenIoT – The Open Source Internet of Things

OpenIoT é um projeto open source, disponível em (https://github.com/OpenIotOrg/openiot/), usado para obter a informação reservada nas clouds dos sensores. Esta usa formas eficientes de descobrir e gerir ambientes cloud para IoT e seus recursos, tais como sensores ou smart devices. Passamos agora à análise e explicação sucinta de duas arquiteturas propostas designadas de cloud and fog computing, respetivamente.

### Cloud OpenIoT

A arquitetura OpenIoT é composta por 7 elementos principais, divididos em 3 planos distintos:

**- Application**
**- Virtualized**
**- Physical**

Application é composto por 3 vertentes:

**Request Definition** - Possibilita especificações on-the-fly de pedidos de serviço para a plataforma OpenIoT. Este abrange um conjunto de serviços para especificação e formulação dos pedidos, enquanto os envia para o **Scheduler**;
**Configuration and Monitoring** - Gera e configura as funcionalidades dos sensores presentes na plataforma;
**Request Presentation** - Componente responsável pela visualização dos outputs de um serviço, selecionando mash-ups de uma biblioteca apropriada de forma a facilitar a apresentação do mesmo;

Tal como em Application, o plano Virtualized possui também 3 componentes:

**Cloud and Data Storage** - Comporta-se como uma base de dados, permitindo assim o armazenamento dos dados provenientes do Sensor Middleware;
**Scheduler** - Processa os pedidos recebidos da Request Definiton, assegurando o seu acesso apropriado aos recursos que os mesmos requerem;
**Service Delivery** - Combina o fluxo de dados como indicado pelo fluxo de trabalho do serviço dentro do sistema OpenIoT, de modo a que seja entregue o serviço pedido;

Por último, temos o plano Physical que é composto pelo **Sensor Middleware**, sendo que, este coleciona, filtra e combina o fluxo de dados de sensores virtuais ou dispositivos físicos.

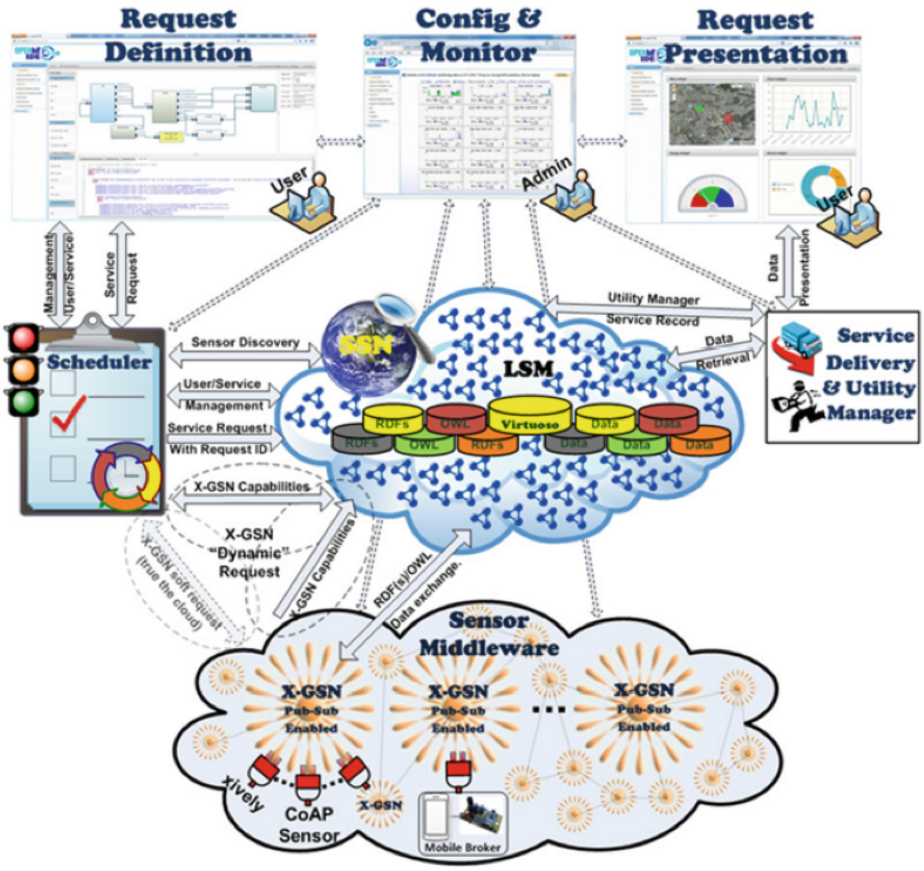


**Fig. 3.** Uma visão global da arquitetura OpenIoT

**Fog Computing**

Sistema que facilita a operação de serviços de computação, armazenamento e rede entre end devices e bases de dados da cloud computing.

A sua arquitetura é dividida em 6 camadas:

**Transport Layer** - Faz o upload dos dados preprocessados para a Cloud;
**Security Layer** - Responsável pela encriptação/decriptação, privacidade e integridade dos dados;
**Storage Layer** - Trata não só do armazenamento dos dados, como também da sua replicação e distribuição;
**Preprocessing Layer** - Camada encarregue da análise, filtragem e reconstrução de dados;
**Monitoring Layer** - Gere os recursos, poder, respostas e serviços;
**Physical Layer** - Onde se localizam os sensores

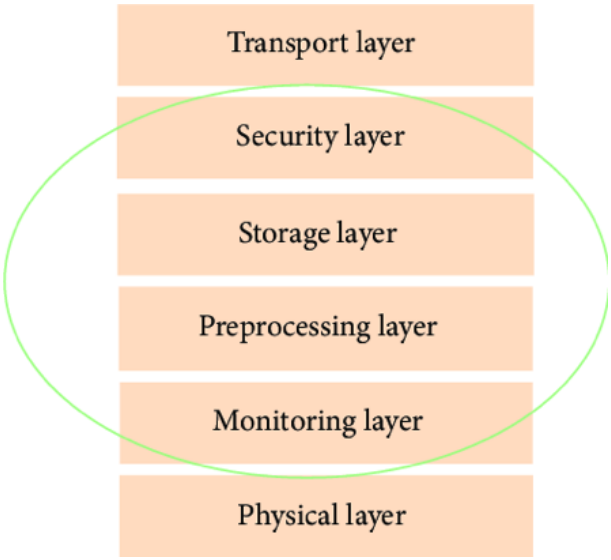


**Fig. 4.** Camadas da Arquitetura Fog

## 3 Tecnologias- Elementos da IoT

### 3.1 Introdução

Cada vez mais, o número de aparelhos com ligação à Internet atinge novos níveis, sendo que vários destes aparelhos conectam-se para fazer parte de um sistema maior. Para se conectar todos estes aparelhos e ter um objetivo

concreto, existem e estão a ser criadas tecnologias que permitem um melhor uso das arquiteturas vistas anteriormente. Para se perceber melhor o significado e o contexto em que a IoT se encontra, discutiremos a seguir 4 dos seus maiores elementos que ajudam à sua funcionalidade.

### Sensing

Controlar múltiplos aparelhos requer uma capacidade de atuação física bem como mecanismos sensíveis de deteção. Milhares de variáveis a rastrear implicam centenas de sensores e atuadores de tipos variados de baixo consumo energético o que leva a criação de um fluxo de dados grande do ponto de vista exterior á rede IoT. Sensores de proximidade e de abertura de portas para detetar a presença de uma pessoa numa dada sala podem ser associados ao evento de ligar as luzes ou sistemas HVAC criando um dos mais simples exemplos de pares sensor-atuador apenas sustentado por tecnologias IoT. [2].


**Fig. 5.** Diagrama de Internet of Things que mostra as aplicações finais com base nos dados recolhidos

**Comunicação**

Exemplos de protocolos de comunicação usados para IoT são RFID, NFC, Bluetooth, Wifi, Zwave e Zigbee.

**RFID:** RFID ou identificação por rádio frequência é um método de identificação automática através de sinais de rádio que recupera e armazena dados remotos através de tags.
Uma tag RFID é um pequeno objeto que pode ser colocado numa pessoa, animal ou equipamento. O sistema contém também um chip(reader) e antena que lhe permite responder aos sinais de rádio enviados por uma base transmissora.
**Controlador de RFID** - É o dispositivo de interface que controla todo o sistema periférico de RFID (antena e tag) para além da comunicação com o resto do sistema.
Estes sistemas podes ser definidos pela faixa de frequência em que operam:
**Sistemas de Média e Alta Frequência** - Para curtas distâncias de leituras e baixos custos; normalmente utilizados para a localização e identificação em smartphones.
**Sistemas de Ultra Frequência** - Para leituras em médias ou longas distâncias e em alta velocidade. Normalmente utilizados em veículos ou recolha automática de dados numa sequência de objetos em movimento. Um exemplo de aplicação é a via verde das autoestradas, ou para abrir/fechar as cancelas dos parques de estacionamento.

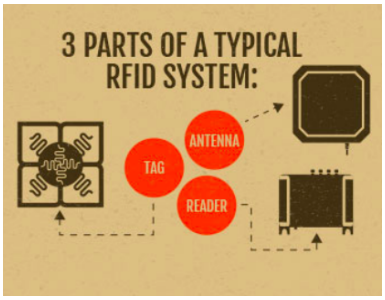


**Fig. 6.** Composição do sistema RFID

**NFC:** NFC ou comunicação por campo de proximidade é uma tecnologia que permite a troca de informações sem fio de forma segura entre dispositivos compatíveis que estejam próximos um do outro e que funcionem a 13.56 MHz. Ou seja, logo que os dispositivos estejam suficientemente próximos, a comunicação é estabelecida automaticamente, sem a necessidade de configurações adicionais.

NFC é uma especialização da tecnologia RFID. Assim as bases da NFC são as mesmas que as da RFID e operam à mesma frequência. Algo que as distingue é o facto da NFC conseguir agir tanto como um reader como uma tag, sendo uma das vantagens destes aparelhos serem obrigados a uma proximidade entre eles (não mais que alguns centímetros) para poderem funcionar.
Assim tem-se tornado uma escolha segura entre os dispositivos dos consumidores tais como o telemóvel, pois permite o pagamento contactless, ou os andantes de comboio e metro onde atualmente apenas é necessário aproximar o cartão à plataforma para os validar.


**Fig. 7.** Pagamento via NFC em máquina de refrigerantes

**Wi-Fi:** A conexão Wi-Fi é representada por todo tipo de conexão que obedece ao padrão IEEE 802.11 e todas as suas variantes. Basicamente, esse é o padrão que foi definido para que as conexões de internet fossem possíveis pelos dispositivos. A conexão através dela acontece a partir de um ponto onde existe uma conexão com a internet tradicional, cabeada, e esse ponto é conectado a um transmissor que envia um sinal de internet pelo ar em determinado raio de efetividade. A difusão desse sinal pode ser feita de forma aberta ou fechada com o uso de senhas ou endereços físicos, também conhecidos por MAC para o acesso.

**Bluetooth:** O Bluetooth é uma tecnologia de comunicação sem fio que permite que computadores, smartphones, tablets e afins troquem dados entre si e se conectem a mouses, teclados, fones de ouvido, impressoras, caixas de som e outros acessórios a partir de ondas de rádio. A ideia consiste em possibilitar que dispositivos se interliguem de maneira rápida, descomplicada e sem uso de cabos, bastando que um esteja próximo do outro.

**Fig. 8.** Bluetooth

**ZigBee e Zwave:** Atualmente, ZigBee e Zwave são as dois maiores rivais de low-powered mesh networking, esta tecnologia fomentada pela introdução de IoT tem sido continuamente refinada pelo que podemos encontrar múltiplas versões do mesmo equipamento com especificações diferentes, neste artigo focamos nas mais abundantes.
Zwave utiliza frequências de rádio na banda dos 800 MHz, que em contraste com ZigBee na banda 2.4GHz, permite maior tempo de utilização, tendo alguns equipamentos a capacidade de operar durante anos sem necessidade de fontes de alimentação, fator crucial em equipamentos IoT, perdendo a vantagem na taxa de dados sendo limitado a 40Kb/s contra os 250Kb/s do seu rival. O alcance de 90 metros de Zwave salvaguarda o seu lugar em redes mais pequenas sendo possível existir um máximo de 232 aparelhos conectados contra o muito superior limite de 65000 de ZigBee que ultrapassa a dificuldade de ter um alcance máximo registado de 75 metros. É necessário ter em consideração a latência visto que Zwave perde por uma ordem de magnitude e o facto da mobilidade ser um problema para a performance desta tecnologia, como também perceber que Zwave ganha na segurança e na interoperabilidade sendo apenas necessário certificar equipamentos com Zwave ao contrário de ZigBee que está por trás de patentes custosas.
Cada uma destas tecnologias está adaptada a situações que variam com a área, divisões do edifício a equipar e o número de equipamentos pelo que deve ser tomada uma decisão na conceção da rede. [3]. [4]. [5].

### Computação

Faz parte do modelo IoT o processamento de dados o que necessita da capacidade de computação. Computação ao longo de uma mesh-network é um desafio, com a quantidade de dados a processar, são utilizados meios extremos como o modelo de Fog computing que necessitam de processadores mais evoluídos do que a quantidade de energia disponível permite, este paradoxo é facilmente resolvido ao introduzir nodos de maior capacidade de computação com intuito de localizar intrinsecamente o processamento na rede. [6].

### Semântica

Semântica na IoT refere-se à capacidade de extrair conhecimento de forma inteligente por diferentes máquinas para fornecer os serviços necessários. A extração de conhecimento inclui a descoberta e o uso de recursos e informações de modelagem. Além disso, inclui o reconhecimento e a análise de dados para dar sentido à decisão correta de fornecer o serviço exato. Assim, a semântica representa o cérebro da IoT enviando exigências para o recurso certo. Esse requisito é suportado por tecnologias da Web Semântica, como o RDF (Resource Description Framework) e o Web Ontology Language (OWL). Em 2011, adotou-se o formato Efficient XML Interchange (EXI) como recomendação. O EXI é importante no contexto da IoT porque reduz as necessidades de largura de banda sem afetar os recursos relacionados, como a vida útil da bateria, o tamanho do código, a energia consumida no processamento e o tamanho da memória. O EXI converte mensagens XML em binárias para reduzir a largura de banda necessária e minimizar o tamanho de armazenamento necessário. [7].

## 4 Tecnologias- Protocolos

**MQTT e CoAP:** Quando estamos a falar de IoT todos os problemas resumem-se à necessidade de alta eficiência energética, extensa quantidade de equipamentos e grandes quantidades de dados dispersos. Protocolos de comunicação implementam de maneiras diferentes soluções para estes problemas, no caso de MQTT, este é um dos mais antigos, criado para ligar linhas de petróleo por redes de satélites falaciosas, acaba por ser útil em IoT pela sua capacidade de estabelecer diferentes níveis de qualidade de serviço (QoS) usando pouca energia. Do nível 0, lançar mensagem, até ao nível 3, estabelecer uma única conecção responsiva com outros equipamentos, este protocolo tem a capacidade de transmitir diferentes tipos de dados com diferentes tamanhos e prioridades. O MQTT usa o padrão publicador / subscritor para ligar as partes interessadas. Isso é feito dissociando o remetente (editor) do recetor (assinante) através de um broker. O editor envia uma mensagem para o broker sobre um tópico, vários assinantes aguardam a receção de mensagens. Os editores e assinantes são autónomos, o que significa que não precisam saber da existência um do outro.

Usando técnicas parecidas com HTTP encontramos CoAP, este protocolo baseado em request/response envia mensagens Confirmáveis ou não confirmáveis para uma entidade que serve de servidor e este responde com a informação necessária caso seja possível. Graças às parecenças com HTTP, CoAP é capaz de utilizar um proxy para comunicar com aparelhos da Internet. Feito com ideia em IoT, este protocolo está otimizado com headers mais pequenos que permitem maior fluidez da informação entre maquinas ao evitar buffers largos com latência alta.
Entre estes dois podemos observar que MQTT está melhor equipado para rápidas alterações, eventos mas CoAP ganha na capacidade de transferir maiores quantidades de dados.

**AMQP:** O AMQP (Advanced Message Queuing Protocol) é um protocolo que pertence à camada de aplicação já anteriormente mencionada. Permite o envio e a receção de mensagens de forma assíncrona, ou seja, quando enviamos uma mensagem não esperamos uma resposta imediata - independente do hardware, sistema operacional e linguagem de programação.
De forma bastante genérica, o AMQP é um protocolo onde um cliente é capaz de comunicar-se com um broker.
O broker é uma entidade que recebe mensagens de publishers- ou seja, clientes que produzem mensagens e encaminha mensagens a consumers, que são clientes que recebem mensagens. Assim, o AMQP é um protocolo bi-direcional onde um cliente pode enviar e receber mensagens de outros clientes através do broker.
Ao publicar uma mensagem, o cliente **publisher** encaminha esta mensagem a outra entidade denominada **exchange**, que de acordo com regras específicas denominadas **bindings** as encaminha para filas **(queues)** que, por sua vez, podem estar sendo utilizadas por outro cliente, o **consumer**.

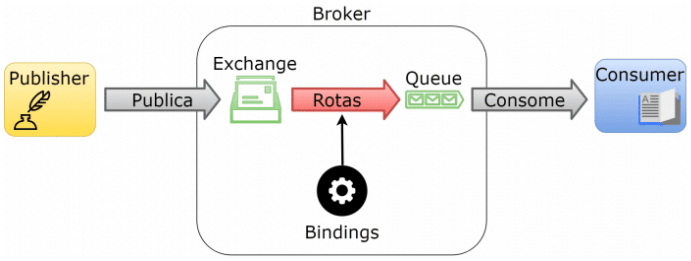


**Fig. 9.** Diagrama do Funcionamento do Exchange no AMQP.

## 5 Conclusão

A IoT tem o potencial de aumentar drasticamente a disponibilidade de informações e transformar empresas e organizações em todos os setores do mundo.

Como tal, espera-se encontrar maneiras de impulsionar o poder da IoT nos objetivos estratégicos da maioria das empresas de tecnologia, independentemente do seu foco no setor.
O número de diferentes tecnologias necessárias para apoiar a implantação e maior crescimento da IoT resulta em amplos esforços para desenvolver normas e especificações técnicas compatíveis com a comunicação entre os seus dispositivos e componentes. Neste artigo, apresentou-se modelos de arquiteturas para um uso eficaz e correto de um sistema IoT e mencionamos várias tecnologias e protocolos que usam as arquiteturas descritas em cima de forma a desenvolver dispositivos tecnológicos que poderão estar relacionados nas áreas mais versátis tais como a saúde, os transportes e a comunicação.

## References


1. Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applica- tions," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. doi:10.1155/2017/9324035
2. Gubbi,Rajkumar Buyya,Slaven Marusic,Marimuthu Palaniswami,"Internet of Things (IoT): A vision, architectural elements, and future directions",in Future Generation Computer Systems, Elsevier, September 2013
3. IET,"How safe is Zwave?", in Computing Control Engineering Journal ( Volume: 17 , Issue: 6,Dec.-Jan. 2006
4. Fouladi, Behrang and Sahand Ghanoun, "Security Evaluation of the Z-Wave Wireless Protocol.",2013
5. Kresimir Malaric, Stanislav Safaric, "ZigBee Wireless Standard", Faculty of Electrical Engineering and Computing,2004
6. Aykut Kanyilmaz, "Fog Based Architecture Design for IoT with Private Nodes: A Smart Home Application",in 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), April 2019
7. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications" in IEEE COMMUNICATION SURVEYS TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015, pp. 2352.