

CENTRO UNIVERSITÁRIO DO ESTADO DO PARÁ  
ESCOLA DE NEGÓCIOS, TECNOLOGIA E INOVAÇÃO  
BACHARELADO EM ENGENHARIA DA COMPUTAÇÃO

CAIO HENRIQUE ESQUINA LIMÃO  
RAFAEL RIBEIRO FERREIRA BERNARDO  
VINICIOS KOJI YAMAMOTO

**IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA EM UM AMBIENTE DE IOT**

Belém

2019

CAIO HENRIQUE ESQUINA LIMÃO  
RAFAEL RIBEIRO FERREIRA BERNARDO  
VINICIOS KOJI YAMAMOTO

## **IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA EM UM AMBIENTE DE IOT**

Trabalho de Curso na modalidade Monografia, apresentado como requisito parcial para obtenção do grau de Bacharelado em Engenharia de Computação do Centro Universitário do Estado do Pará – CESUPA, sob orientação da professora MSc. Michelle Bitar Lelis dos Santos.

Belém  
2019

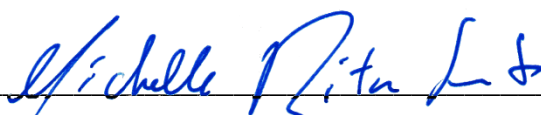
CAIO HENRIQUE ESQUINA LIMÃO  
RAFAEL RIBEIRO FERREIRA BERNARDO  
VINICIOS KOJI YAMAMOTO

## IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA EM UM AMBIENTE DE IOT

**Trabalho de Curso na modalidade Monografia** apresentado como requisito parcial para obtenção do grau de Bacharelado em Engenharia de Computação do Centro Universitário do Estado do Pará – CESUPA.

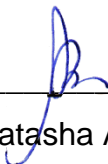
**Data da Defesa: 12/06/2019**

### Banca Examinadora:



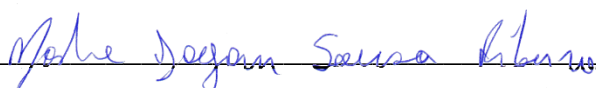
---

Prof. MSc. Michelle Bitar Lelis dos Santos – Orientadora  
Centro Universitário do Estado do Pará – CESUPA



---

Prof. MSc. Alessandra Natasha Alcantara Barreiros Baganha – Membro  
Centro Universitário do Estado do Pará – CESUPA



---

Prof. MSc. Moshe Dayan Sousa Ribeiro – Membro  
Centro Universitário do Estado do Pará – CESUPA

## **AGRADECIMENTOS**

Agradeço primeiramente à Deus pelo dom da vida, misericórdia, sabedoria, proteção e por estar sempre ao meu lado me ajudando a levantar.

Em segundo lugar eu gostaria de deixar os meus mais sinceros agradecimentos à minha mãe pelo amor, carinho, cuidado, companheirismo, pelos valores e princípios que me foram passados. Pela sua dedicação em cuidar e sustentar a nossa família muitas vezes abdicando de si mesma, enfim, pelo exemplo de mulher que ela é e que me faz querer melhorar como pessoa cada vez mais.

Em terceiro lugar eu gostaria de agradecer aos meus irmãos Carlos e Luiza, minha avó Esther, e ao restante da minha família pelo cuidado e por estarem sempre presentes quando necessário.

Também agradeço ao meu grande amigo Lucas por todas as conversas, momentos compartilhados e conselhos que espero levar para a vida toda, assim como a sua amizade.

Em seguida eu agradeço às amigadas da faculdade que espero levar para o resto da vida, em especial ao Sérgio, Rafael, Vinícios e Vitor, pelo conhecimento, experiências e momentos compartilhados durante o curso.

Gostaria de agradecer em especial a minha orientadora Michelle pelo auxílio, puxões de orelha, sabedoria e exemplo. Pela sua grande influência na minha formação profissional e amadurecimento pessoal assim como participação essencial no desenvolvimento deste trabalho.

**Caio Henrique Esquina oLimão**

## **AGRADECIMENTOS**

Agradeço primeiramente aos meus pais, Fernando e Conceição por me servirem de inspiração em todos os momentos, me apoiar, proporcionar tudo que eu precisei para chegar aonde estou e ao seu imensurável carinho.

Agradeço aos meus familiares, Luciano, Socorro, Barbara, Beatriz e Eddie por sempre me ajudar a todo momento, me aconselhar em muitas ocasiões e estar sempre presentes.

Agradeço aos meus grandes amigos Adran, Bruna e Mateus por sempre compartilharem dos melhores momentos de gratidão e companheirismo até hoje.

Agradeço a minha orientadora Michelle pelo seu auxílio, seu conhecimento compartilhado ao longo do curso e a sua influência para a escolha da minha futura carreira.

**Rafael Ribeiro Ferreira Bernardo**

## **AGRADECIMENTOS**

Aos meus pais, Kayuri e Geraldo, por sempre terem lutado para me proporcionar as melhores condições de estudo e por terem apoiado todas as minhas decisões.

À Isabella, pelo apoio, paciência, amor, compreensão e todos os instantes que tivemos juntos até este momento.

À minha família, por todo o apoio concebido e por estarem sempre ao meu lado, partilhando todos os momentos.

Aos meus filhos de quatro patas que me trazem paz e felicidade com um simples olhar e um abanar de suas caudas.

Aos meus amados amigos que sempre se demonstraram disponíveis para me ajudar e deixar de lado todas as preocupações.

À minha querida orientadora, Michelle, por ser uma fonte de inspiração e pela disponibilidade, dedicação e todo o conhecimento partilhado durante o desenvolvimento deste trabalho.

Aos docentes do Centro Universitário do Estado do Pará que estiveram presentes neste percurso acadêmico e a instituição pelas condições proporcionadas.

**Vinicios Koji Yamamoto**

*“A experiência é uma lanterna  
dependurada nas costas que apenas  
ilumina o caminho já percorrido.”*

Confúcio

## RESUMO

O avanço tecnológico reflete em uma demanda de conexão cada vez maior, requerendo que a Internet se adapte ao cenário que está por vir. Logo, o próximo passo para suportar esta quantidade de conexões, dispositivos e novas aplicações, é a integração da Internet a tecnologias específicas como *Big Data*, computação em nuvem, 5G e inteligência artificial. Este novo cenário nada mais é do que a Internet das Coisas, uma rede global capaz de suportar e interconectar todos os serviços atuais e futuros. Para que estes serviços atendam às necessidades dos clientes da melhor maneira possível, é necessária a coleta de uma grande quantidade de dados, precisando-se identificar todos os dispositivos da rede. É justamente nesse ponto que o RFID se torna essencial para o funcionamento da Internet das Coisas, pois a partir do momento que as diferentes camadas da rede conseguem se enxergar, novas soluções se tornam possíveis, como os carros autônomos. Assim, para exemplificar o cenário descrito acima, esta monografia propõe um protótipo de um sistema de controle de acesso imersa em um ambiente de Internet das Coisas, destacando o papel do RFID como identificador de objetos e pessoas.

**Palavras-chave:** Internet das Coisas. RFID.



## **ABSTRACT**

Technological advancement reflects on an ever-increasing demand for connection, requiring the Internet to adapt to the scenario that is coming. So, the next step in supporting this amount of connections, devices, and new applications is the integration of the Internet with specific technologies such as Big Data, cloud computing, 5G, and artificial intelligence. This new scenario is nothing more than the Internet of Things, a global network capable of supporting and interconnecting all current and future services. For these services to meet customer needs in the best possible way, it is necessary to collect a large amount of data, needing to identify all the devices in the network. It is precisely at this point that RFID becomes essential to the functioning of the Internet of Things, because as soon as the different layers of the network can see themselves, new solutions become possible, such as autonomous cars. Thus, to exemplify the scenario described above, this monograph proposes a prototype of an access control system immersed in an Internet of Things environment, highlighting the role of RFID as an identifier of objects and people.

**Keywords:** Internet of Things. RFID.

## LISTA DE FIGURAS

Figura 1 – A evolução da Internet .....	19
Figura 2 – Ciclo de tendências .....	20
Figura 3 – Modelo de referência ITU-T .....	23
Figura 4 – Tecnologias essenciais para IoT .....	29
Figura 5 – Recursos do 5G .....	30
Figura 6 – Distribuição de rádios 4G x 5G .....	30
Figura 7 – Arquitetura SDN .....	31
Figura 8 – Crescimento global de dados.....	33
Figura 9 – Sistema RFID.....	37
Figura 10 – Classificação dos sistemas RFID.....	38
Figura 11 – Representação da transmissão FDX, HDX, e Sequencial .....	39
Figura 12 – Tipos de tecnologias de auto identificação.....	44
Figura 13 – Ataques à sistemas RFID.....	46
Figura 14 – <i>Raspberry Pi 3 Model B</i> .....	51
Figura 15 – NodeMCU .....	52
Figura 16 – Leitor RFID MFRC522.....	52
Figura 17 – <i>Tags</i> do leitor RFID MFRC522 .....	53
Figura 18 – Protocolo MQTT .....	53
Figura 19 – Funcionamento do protocolo MQTT.....	54
Figura 20 – Serviços da plataforma Firebase.....	55
Figura 21 – Plataforma Firebase .....	55
Figura 22 – Esquemático do protótipo.....	56
Figura 23 – Controle do MFRC522 .....	57
Figura 24 – Firebase Realtime Database.....	58
Figura 25 – Raspberry Pi 3 utilizando o MQTT .....	58
Figura 26 – Controle de acesso .....	59
Figura 27 – Leitura das <i>tags</i> .....	60
Figura 28 – Recursos computacionais do Raspberry Pi 3.....	61
Figura 29 – <i>Tags</i> aprovadas e negadas.....	61

## LISTA DE QUADROS

Quadro 1 – Descrição técnica do Raspberry Pi 3.....	51
Quadro 2 – Descrição técnica do NodeMCU .....	52

## LISTA DE SIGLAS

4G	Quarta Geração de Redes Móveis
5G	Quinta Geração de Redes Móveis
AAA	<i>Authentication, Authorization and Accounting</i>
DOS	<i>Denial of Service</i>
EAS	<i>Electronic Article Surveillance</i>
FDX	<i>Full-Duplex</i>
GSMA	<i>Global System for Mobile Communications</i>
HDX	<i>Half-Duplex</i>
HF	<i>High Frequency</i>
IA	Inteligência Artificial
IBM	<i>International Business Machines</i>
ID	<i>Identity</i>
IERC	<i>IoT European Research Cluster</i>
IOT	<i>Internet of Things</i>
IPV4	<i>Internet Protocol version 4</i>
IPV6	<i>Internet Protocol version 6</i>
ISM	<i>Industrial-Scientific-Medical</i>
ITU	<i>International Telecommunication Union</i>
JSON	<i>Java Script Object Notation</i>
LAN	<i>Local Area Network</i>
LF	<i>Low Frequency</i>
M2M	<i>Machine to Machine</i>
MQTT	<i>Message Queuing Telemetry Transport</i>
MWC	<i>Mobile World Congress</i>
OCR	<i>Optical Character Recognition</i>
ONU	Organização das Nações Unidas
OTA	<i>Over the Air</i>
QOS	<i>Quality of Service</i>
RFID	<i>Radio-Frequency Identification</i>
SAAS	<i>Software as a Service</i>
SDN	<i>Software Defined Networking</i>

TCP	<i>Transmission Control Protocol</i>
TIC	Tecnologia da Informação e Comunicação
UHF	<i>Ultra High Frequency</i>
WAN	<i>Wide Area Network</i>

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>15</b>
1.1	OBJETIVOS	16
1.1.1	Objetivo geral	16
1.1.2	Objetivos específicos	17
1.2	JUSTIFICATIVA	17
1.3	METODOLOGIA	18
1.4	ESTRUTURA DO TRABALHO	18
<b>2</b>	<b>INTERNET DAS COISAS</b>	<b>19</b>
2.1	ÁREAS DE APLICAÇÃO	21
2.2	MODELOS DE REFERÊNCIA PARA IOT	22
2.2.1	Arquitetura ITU-T	23
2.3	PROTOCOLOS DE COMUNICAÇÃO	26
2.3.1	Zigbee	26
2.3.2	LoRaWAN	27
2.3.3	Sigfox	27
2.3.4	Wi-Fi	27
2.3.5	MQTT	27
2.3.6	Bluetooth	28
2.4	TECNOLOGIAS ESSENCIAIS PARA IOT	28
2.4.1	Rede móvel 5G	29
2.4.2	Big Data	32
2.4.3	Inteligência artificial	33
2.4.4	Computação em nuvem	34
<b>3</b>	<b>IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA</b>	<b>37</b>
3.1	PRINCÍPIOS DE FUNCIONAMENTO	38
3.2	COMPONENTES DA TECNOLOGIA RFID	40
3.2.1	Tag RFID	40
3.2.2	Leitor RFID	42
3.2.3	Antena RFID	42
3.2.4	Controlador	42
3.3	FAIXA DE OPERAÇÃO	43

3.4	TECNOLOGIAS SEMELHANTES.....	43
3.5	RFID EM UM AMBIENTE DE IOT.....	44
3.6	SEGURANÇA E PRIVACIDADE.....	45
3.6.1	Problemas de segurança.....	46
3.6.2	Soluções para os problemas de segurança.....	48
<b>4</b>	<b>DESENVOLVIMENTO DO PROTÓTIPO.....</b>	<b>50</b>
4.1	HARDWARE E SOFTWARE UTILIZADOS.....	50
4.1.1	Raspberry Pi.....	50
4.1.2	NodeMCU.....	51
4.1.3	Leitor RFID MFRC522.....	52
4.1.4	Tag RFID.....	53
4.1.5	MQTT.....	53
4.1.6	Firebase.....	54
4.2	METODO DE DESENVOLVIMENTO.....	56
<b>5</b>	<b>RESULTADOS E DISCUSSÕES.....</b>	<b>60</b>
<b>6</b>	<b>CONCLUSÃO.....</b>	<b>62</b>
6.1	DIFICULDADES ENCONTRADAS.....	62
6.2	TRABALHOS FUTUROS.....	63
	<b>REFERÊNCIAS.....</b>	<b>64</b>

## 1 INTRODUÇÃO

Nos últimos anos, a viabilidade de conectar pessoas e objetos inteligentes através de uma única infraestrutura, a Internet, tem sido o foco de muitas pesquisas em Tecnologia da Informação e Comunicação (TIC). Esse novo comportamento é intitulado como IoT (*Internet of Things*), ou Internet das Coisas, termo que foi utilizado pela primeira vez por Kevin Ashton em 1999. A IoT é definida pelo IERC (*IoT European Research Cluster*) como uma infraestrutura de rede dinâmica e global com capacidade de autoconfiguração, baseada em protocolos de comunicação padronizados e interoperáveis, nos quais as coisas têm identidades, atributos físicos, personalidades virtuais, interfaces inteligentes e são completamente integradas na rede de informação (ASHTON, 2009; IERC, 2014).

Através da combinação de diversas tecnologias, a Internet das Coisas tem monitorado e gerenciado processos de forma crescente nos últimos anos, e possibilitará a conexão de cerca de 28 bilhões de dispositivos até 2021 (ERICSSON, 2016). Desta maneira, a IoT possibilita um ambiente que traz inovações tecnológicas nunca antes imaginadas e pode ser aplicada em diversos ramos. Por exemplo, em áreas e setores como: cidades inteligentes, carros autônomos, *e-health* e agricultura. Portanto, futuramente poderá influenciar a forma de como as pessoas interagem com o mundo físico (JI; GANCHEV; ODROMA, 2014).

Neste cenário, espera-se que os dispositivos de Internet das Coisas sejam responsáveis por mais de 75% do tráfego de dados na rede mundial de computadores. Deste modo, a rede de acesso precisa lidar de forma eficiente com a comunicação M2M (*Machine to Machine*), ou Máquina a Máquina, que requer uma alta capacidade de conexão de dispositivos, alta largura de banda, latência significativamente reduzida e baixo consumo de energia. Condições atendidas pela quinta geração de redes móveis (5G) que já nasce com o pensamento de rede voltada para a IoT (BORKAR; PANDE, 2016).

Segundo Dias (2018), durante a palestra “*The 5G enabler of massive IoT deployment*” na Furukawa Summit 2018, o coordenador geral de vendas da Intracom Telecom, Panagiotis Dallas, afirmou que o 5G não é somente uma rede de acesso com alta velocidade, é um guarda-chuva que engloba várias tecnologias onde o acesso é apenas uma parte do modelo, impulsionando novos serviços como a Internet das coisas.



Cada vez mais, observa-se em diversos setores do mercado a adoção de novas tecnologias, com o propósito de aumentar a receita das empresas e proporcionar o crescimento das mesmas. Por exemplo, o novo sistema de IoT adotado pela Disney, é uma pulseira com chip RFID (*Radio-Frequency Identification*), ou identificação por radiofrequência, que atua como chaves de hotel, bilhetes e cartões de crédito, essas pulseiras se comunicam com milhares de sensores e transmitem dados em tempo real, todos estes dados são analisados, contribuindo para que a empresa proporcione uma melhor experiência para o cliente (MARR, 2017).

A identificação por radiofrequência é considerada fundamental para a IoT, pois, a RFID tem o potencial de permitir que as máquinas identifiquem objetos, compreendam seu status e adotem ações, se necessário. Para uma infraestrutura de Internet das Coisas, há quatro necessidades básicas que devem ser atendidas: a necessidade de interações automáticas, a necessidade de identificação, a necessidade de captura de dados e a necessidade de troca de dados. A IoT exigirá o desenvolvimento de uma infraestrutura global e de objetos inteligentes atendendo essas necessidades (KHOO, 2011).

Neste contexto, será desenvolvido um protótipo de um sistema de controle de acesso utilizando RFID, inserido em um ambiente de Internet das Coisas, com a finalidade de permitir o acesso a um grupo específico de usuários. Dado que a identificação dos usuários será feita através da tecnologia RFID, a solução se tornará de baixo custo, mais confiável e eficiente que as demais soluções encontradas no mercado. Este protótipo tem como objetivo responder o questionamento — Qual a relevância da identificação por rádio frequência em um ambiente de Internet das Coisas? Que justificará a escolha do RFID como tecnologia integradora das mais variadas aplicações de IoT.

## 1.1 OBJETIVOS

Os objetivos deste estudo são divididos em geral e específicos, de acordo com os tópicos abaixo.

### 1.1.1 Objetivo geral

Este trabalho tem como objetivo geral analisar o papel da identificação por radiofrequência (RFID) em um ambiente de Internet das Coisas (IoT).

### 1.1.2 Objetivos específicos

São objetivos específicos deste trabalho:

- Compreender o conceito de Internet das Coisas (IoT);
- Compreender a tecnologia de identificação por radiofrequência (RFID);
- Compreender o uso do RFID em um ambiente de IoT;
- Prototipar a utilização do RFID para controle de acesso em um ambiente de Internet das Coisas.

## 1.2 JUSTIFICATIVA

A Internet das Coisas possui grande importância para diversos setores, tais como: varejo, logística, agricultura e indústria automobilística. Dados antes nunca obtidos, agora são coletados e tratados por soluções que possibilitam a visualização, exploração e construção sofisticada da análise dos dados, garantindo sempre uma resposta confiável e em tempo real à medida que diversos eventos ocorrem no ambiente proposto (AWS, 2018).

As tecnologias 5G e a Internet das Coisas estão entre as principais tecnologias que moldarão o futuro da Internet nos próximos anos. Ao oferecer menor custo, menor consumo de energia e suporte para um número enorme de dispositivos, o 5G, além de facilitador, é essencial para a implantação completa da IoT, ampliando e possibilitando o desenvolvimento de novos serviços (PALATTELLA *et al.*, 2016).

Espera-se que a IoT impulse novos modelos de negócio ao longo dos próximos oito anos, movimentando mais de US\$ 200 bilhões em negócios somente no Brasil, com previsões de que ao redor do mundo este número some cerca de 11 trilhões de dólares em soluções de Internet das Coisas neste mesmo intervalo de tempo (MARTINS, 2017).

Cada vez mais, observam-se no mercado, oportunidades de implantação e aperfeiçoamento de aplicações para IoT em diversos setores. Na área de controle de acesso, por exemplo, o RFID pode ser utilizado em ingressos de eventos, dificultando a falsificação dos mesmos devido à sua identificação única no sistema.

Tais prospecções e constantes afirmações de empresas e pesquisadores do cenário mundial motivaram o desenvolvimento deste trabalho, que visa mostrar o espaço que o RFID ainda tem no mercado mesmo diante de tantas outras tecnologias

que surgiram desde a sua criação, visto que esta ainda é essencial para o controle de acesso em um ambiente de IoT.

### 1.3 METODOLOGIA

Esta será uma pesquisa bibliográfica referente ao uso de identificação por radiofrequência em Internet das Coisas. A metodologia que será adotada na pesquisa pode ser descrita como o processo de coleta de informações relevantes e confiáveis a respeito do assunto, tais como: artigos científicos, monografias e sites especializados em tecnologias ligados ao assunto.

Com base no entendimento do estudo feito a respeito do uso de identificação por radiofrequência em Internet das coisas, um protótipo com RFID será desenvolvido, analisando suas respectivas vantagens e relevância para a área de aplicação proposta no projeto.

### 1.4 ESTRUTURA DO TRABALHO

Além do capítulo introdutório previamente apresentado, o trabalho é organizado da seguinte forma:

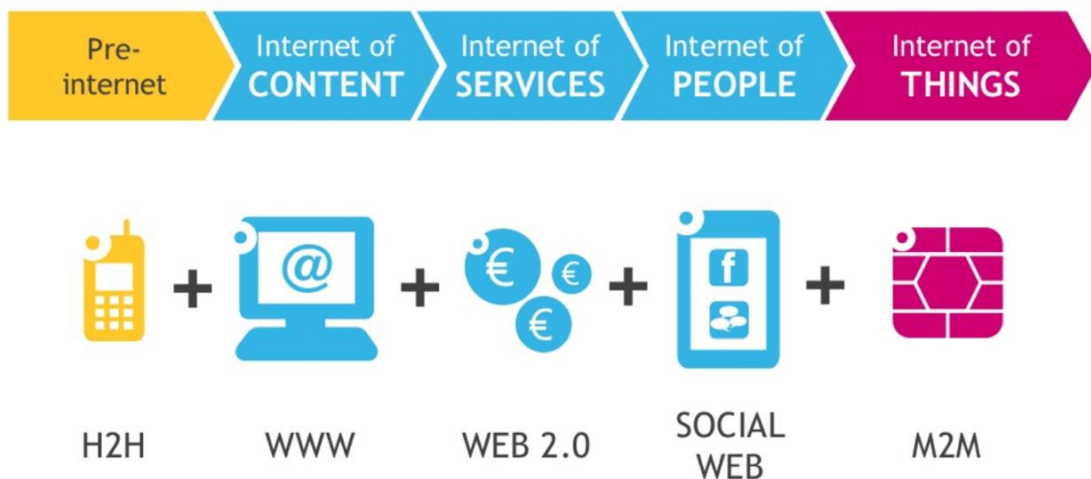
- Capítulo 2 – apresenta um detalhamento sobre a Internet das Coisas, expondo seu conceito, modelos de referência, protocolos e principais tecnologias.
- Capítulo 3 – apresenta o funcionamento da identificação por rádio frequência, destacando os principais componentes deste sistema, além de expor a utilização da tecnologia RFID em IoT e problemas de segurança e suas soluções.
- Capítulo 4 – apresenta as tecnologias e o método de desenvolvimento do protótipo de um sistema de controle de acesso utilizando RFID que se encontra inserido em um ambiente de IoT.
- Capítulo 5 – neste capítulo são apresentadas as análises e resultados obtidos a partir do protótipo.
- Capítulo 6 – neste capítulo são apresentadas as considerações finais da pesquisa, dificuldades encontradas e trabalhos futuros.

## 2 INTERNET DAS COISAS

A Internet das Coisas pode ser definida como uma rede que interconecta coisas ou objetos. Esta Infraestrutura necessita realizar iterações automáticas, possuir identificação única dos objetos, realizar a captura de dados e efetuar troca de dados. Pois, através da interconexão das coisas, visa controlar e monitorar processos de forma autônoma, podendo otimizar nosso dia a dia, já que cada dispositivo passa a agir como se fosse um único objeto inteligente e se torna parte de um sistema totalmente conectado. Isto gera dados a serem analisados para melhor tomada de decisões e gestão de negócios (KHOO, 2011; SANTOS *et al.*, 2016).

Porém, nem sempre foi possível esta conexão entre objetos inteligentes. Na figura 1 é possível verificar a evolução da Internet. Primeiro, a Internet conectou pessoas aos conteúdos. Então, conectou pessoas a serviços. Posteriormente, conectou pessoas a pessoas. Agora, está conectando coisas com coisas.

Figura 1 – A evolução da Internet



Fonte: Jadoul (2013)

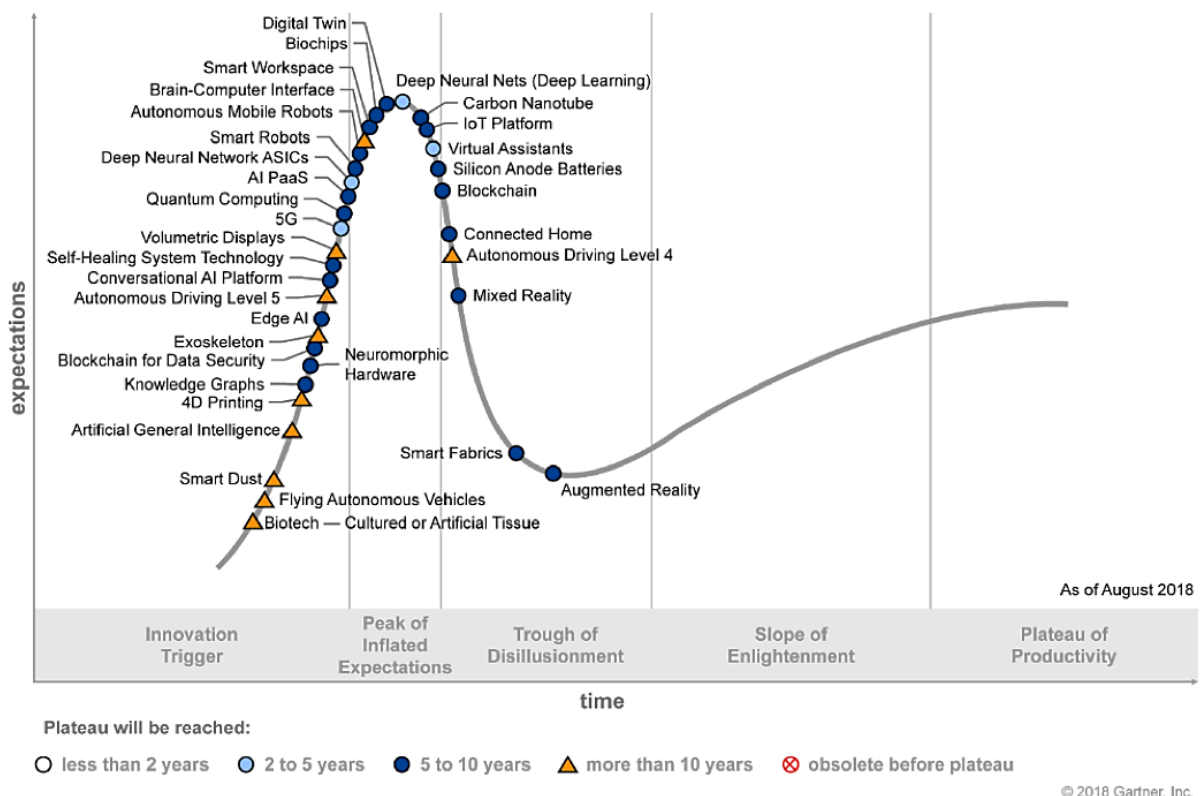
No atual cenário da Internet, a Internet das Coisas é considerada uma nova revolução da Internet e tem realizado a combinação de diversas tecnologias, com propósito de coletar, transmitir, processar e analisar dados. É evidente que para atingir este objetivo, a quantidade de dispositivos conectados à rede mundial de computadores irá se ampliar (SANTOS *et al.*, 2016).

Segundo Ericsson (2016), haverá cerca de 28 bilhões de dispositivos conectados até 2021, número muito além do suportado pelo IPv4 (*Internet Protocol version 4*), protocolo de interconexão de rede que possibilita uma conexão de quase 3,7 bilhões de endereços válidos na rede. Para a solução deste problema, a

implementação do IPv6 (*Internet Protocol version 6*), é de suma importância para o avanço da IoT, pois será possível conectar mais de 340 undecilhões de dispositivos, uma capacidade de endereçamento quase ilimitada.

Como toda tecnologia emergente, a IoT também está sujeita ao *Hype Cycle*, que consiste em uma representação gráfica dos estágios do ciclo de vida de uma tecnologia desde a sua concepção até a maturidade e adoção generalizada, como mostra a figura abaixo:

Figura 2 – Ciclo de tendências



Fonte: Gartner (2018)

A Gartner realiza periodicamente pesquisas de tendências de tecnologias do mercado. A figura 2 apresenta este estudo feito em 2018, onde é possível concluir que a plataforma da tecnologia IoT está localizada na zona de pico de expectativas. A figura também demonstra o tempo estimado para que a IoT esteja um grau de maturidade suficiente para que tenha um impacto significativo no mercado, que seria em torno de 5 a 10 anos.

## 2.1 ÁREAS DE APLICAÇÃO

É perceptível que as expectativas e demandas para projetos de IoT são crescentes em nível global, entretanto, alguns setores destacam-se dentre os que estão sujeitos a esta tecnologia, seja pelo fator inovação ou até mesmo pelos investimentos previstos nestas áreas, sendo estes os setores de agronegócio, cidades inteligentes, indústrias 4.0, varejo e saúde.

O agronegócio é uma das áreas mais importantes para o mercado brasileiro, tendo em vista que, há produtores dos mais variados tipos. Além disso, nota-se uma grande deficiência neste ramo pelo fato dos produtores de pequeno e médio porte ainda não possuírem aparato tecnológico e infraestrutura adequada. A IoT entra neste ramo para acabar com suas limitações, proporcionando inovações como o monitoramento do plantio e controle de pragas através de aplicativos especializados (GONÇALVES, 2018), controle de microrganismo e germinação, sempre visando dados cada vez mais precisos para uma melhor produção (WOLLINGER, 2018).

As cidades inteligentes, não se limitam apenas às relações transacionais entre serviços públicos e o cidadão, essa ideia é ampla e visa principalmente transformar uma cidade em um local mais confortável, tornando os serviços oferecidos cada vez mais eficazes, através de tecnologias que promovam uma infraestrutura inteligente, como por exemplo soluções que façam com que o transporte público seja mais pontual (COELHO, 2015). Para que esta ideia seja uma realidade, a IoT surge como chave principal para a criação das cidades inteligentes, visto que a mesma possui uma vasta diversidade de aplicações para esta área. Dentre estas aplicações é possível destacar: monitoramento da estrutura de prédios, detecção de latas de lixo cheias, semáforos inteligentes, iluminação pública com detecção de presença e o monitoramento do uso de energia elétrica e água em casas (KON; ZAMBOM, 2016).

No cenário de produção, onde o assunto com maior destaque atualmente é a respeito da quarta revolução industrial, conhecida como indústrias 4.0, a maior característica se baseia no oferecimento de serviços em tempo real, focando diretamente em obter, registrar e tratar o ambiente industrial de forma instantânea, para que isso aconteça, as indústrias terão que adotar sistemas *cyber-físicos*. O maior impacto da IoT nestas indústrias é a capacidade da comunicação *machine to machine* sem a intervenção humana, assim proporcionando mais eficiência de produção, segurança, corte de custos, diminuição de tempo (BORLIDO, 2017), monitoramento

integrado a acontecimentos das máquinas da indústria, tomadas de decisões melhores em virtude dos dados processados e novos serviços oferecidos via aplicativos ou *online* (ROMANO, 2017).

As vendas em varejo, como são conhecidas de forma tradicional para consumidores realizarem suas compras cotidianas, tendem a ser uma área drasticamente afetada pela IoT, mais especificamente no setor terciário das redes de varejo, o qual sofrerá as maiores mudanças. A IoT traz inúmeros benefícios para esse ramo, tais como, comparação de preços em tempo real, busca de produtos similares e compras automáticas (EGIDIO; UKEI, 2015). Além disto, as tecnologias utilizadas nesta área facilitam a adaptação dos varejistas às preferências do seu público-alvo, atendendo melhor as ofertas de mercado, o que implica em uma maior qualidade de serviço e satisfação (GOLD, 2018).

No campo da saúde, a IoT também se mostra em crescente desenvolvimento, tendo em vista o auxílio a hospitais, pacientes, médicos e demais profissionais da área tanto em rotinas diárias quanto em funções mais complexas. Destacam-se como principais pontos de aprimoramento: criações de históricos de perfis dos pacientes, portabilidade de prontuários, acionamentos de unidade de emergência e alertas nutricionais (EGIDIO; UKEI, 2015). Dentre os setores objeto de inovações se destacam o monitoramento de pacientes remotamente, através de *wearables* e utilizando Big Data aliado a inteligência artificial para analisar estes dados coletados remotamente, gerando possíveis diagnósticos baseados na literatura médica (REIS, 2018).

## 2.2 MODELOS DE REFERÊNCIA PARA IOT

Um modelo de referência pode ser utilizado como uma forma de padronização, facilitando e permitindo a interoperabilidade entre tecnologias baseadas na mesma arquitetura. Entretanto, a falta de normatização é algo frequente, que muitas vezes permite a integração somente com dispositivos do mesmo fabricante ou marca, que é o detentor da tecnologia.

Segundo Khan *et al.* (2012), é evidente a presença de diversos modelos e arquiteturas de referências para a Internet das Coisas, pois, cada empresa ou grupo expõe o seu, que muitas vezes torna a tarefa de padronização mais complexa, porém,

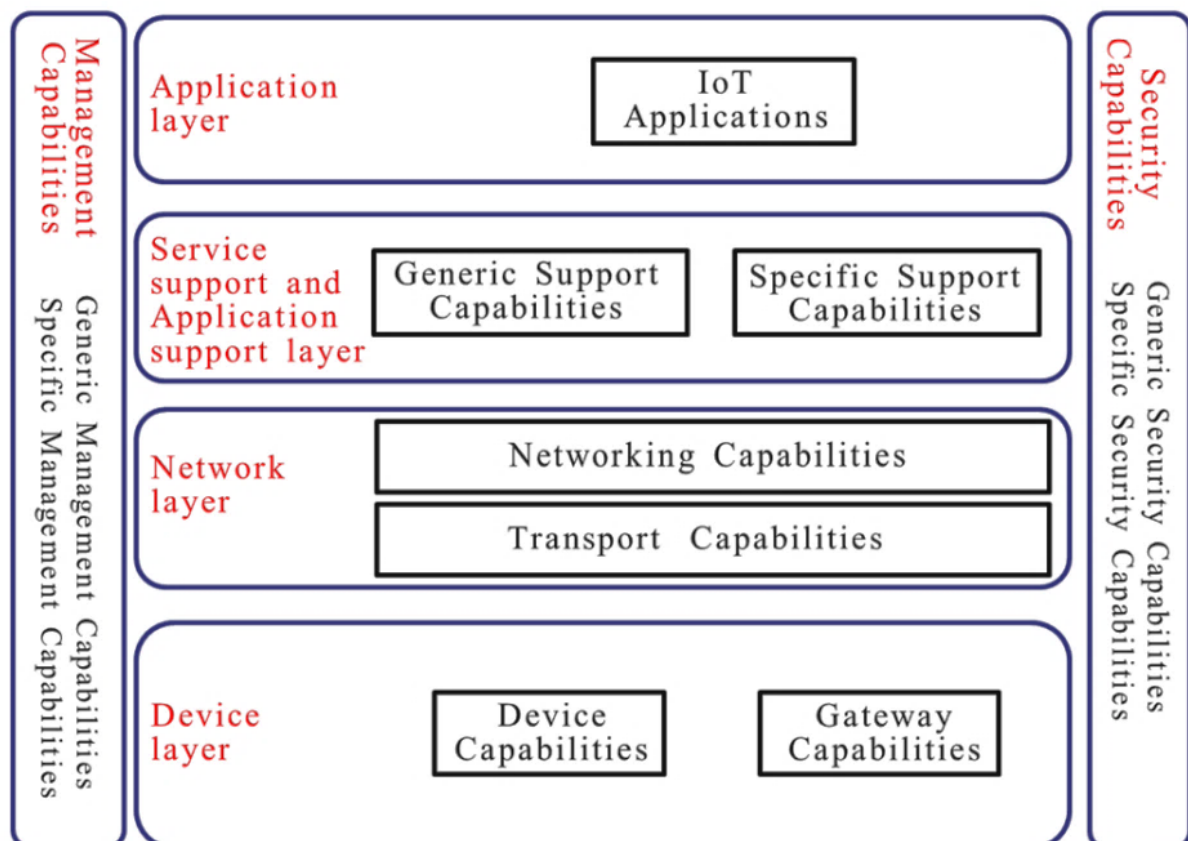
segundo o autor, existem algumas camadas que formam um modelo básico de arquitetura, os quais seriam: a camada de aplicação, rede e dispositivos.

### 2.2.1 Arquitetura ITU-T

Apesar da falta de uma normatização específica para IoT, a ITU (*International Telecommunication Union*) da ONU (*Organização das Nações Unidas*), agência responsável pela padronização na área de telecomunicações, possui um modelo de arquitetura de referência, que pode ser observado na figura 3.

Segundo a ITU-T (2012), a arquitetura de um sistema IoT é composta por quatro camadas horizontais, passando desde a coleta dos dados até a entrega do serviço ao usuário, além de possuir duas camadas verticais, que proporcionam uma capacidade de gerenciamento de funcionalidades e segurança, para colaborar com suas finalidades.

Figura 3 – Modelo de referência ITU-T



Fonte: ITU-T (2012, online)

Segundo especificações da ITU-T (2012), sua arquitetura é composta pelas seguintes camadas:



### **Camada de aplicação**

Camada responsável por disponibilizar uma abstração de alto nível, possibilitando a utilização de informações coletadas para integração com as aplicações ou sistemas de Internet das Coisas.

### **Serviço de suporte e camada de suporte da aplicação**

Camada responsável por fornecer os recursos necessários para as aplicações de Internet das Coisas. E estes recursos possuem diferentes tipos de funcionalidades, desde a coleta e armazenamento ao processamento de dados. Esta camada possui dois grupos de funcionalidades:

- Recursos genéricos de suporte: responsável pelos recursos comuns que podem ser usados por diferentes aplicações de IoT, por exemplo processamento e armazenamento de dados.
- Recursos específicos de suporte: responsável pelos recursos de suporte mais específicos e particulares dos sistemas de IoT, consistem em agrupamentos de requisitos e podem ser criados mais de um grupo de recursos específicos de suporte para diferentes funções de diferentes aplicações ou sistemas de IoT.

### **Camada de rede**

Camada responsável pela comunicação, uma das camadas mais importantes do modelo, pois é através dela que todos os dados são transmitidos, portando requer atenção com princípios de segurança. Esta camada possui dois grupos de funcionalidades:

- Recursos de rede: responsável por fornecer funções de controle de conectividade de rede, como acesso, transporte, gerenciamento móvel, autenticação, autorização e contabilidade (*Authentication, Authorization and Accounting - AAA*).
- Recursos de transporte: responsável pelo fornecimento de conectividade para o transporte do serviço IoT e informações de dados específicos da aplicação, bem como o transporte de informações de controle e gerenciamento relacionadas ao IoT.

## Camada do dispositivo

Camada responsável pelos elementos físicos, ou seja, são os objetos conectados, que podem ser desde sensores até câmeras. Camada que pode ser dividida em dois tipos de funcionalidades:

- Recursos do dispositivo: responsável, mas não estão limitados à interação direta com a rede de comunicação, coletando e carregando informações diretamente (sem usar recurso de *gateway*) para a rede de comunicação e pode receber diretamente informações (por exemplo, comandos) da rede de comunicação; interação indireta com a rede de comunicação, quando os próprios dispositivos são capazes de coletar e fazer o *upload* de informações diretamente para a rede de comunicação, ou seja, através de recursos de *gateway*; rede Ad-hoc, quando os dispositivos podem ser capazes de construir redes de forma Ad-hoc em alguns cenários que precisam de maior escalabilidade e implantação rápida; e por fim, *sleeping* e *waking-up*, quando os recursos do dispositivo podem suportar mecanismos para economizar energia.
- Recursos de *gateway*: responsável, mas estão limitados à suporte a várias interfaces; quando na camada de dispositivo, os recursos de *gateway* suportam dispositivos conectados através de diferentes tipos de tecnologias com fio ou sem fio; conversão de protocolo, quando as comunicações na camada do dispositivo usam diferentes protocolos de camada de dispositivo e quando comunicações envolvendo camada de dispositivo e camada de rede usam protocolos diferentes.

## Recurso de gerenciamento

A camada de gerenciamento, é responsável por gerir as demais camadas, considerando o gerenciamento de falhas, configurações, contabilidade, desempenho e segurança. Esta camada está dividida em dois grupos de funcionalidades:

- Recursos genéricos: suas funcionalidades incluem o gerenciamento de dispositivos, como a ativação e desativação remota de dispositivos, diagnóstico, atualização de *firmware* e/ou atualização de *software*, gerenciamento de status de funcionamento do dispositivo; gestão de topologia de rede local; gerenciamento de tráfego e congestionamento,

como a detecção de condições de transbordamento de rede e a implementação de reserva de recursos para fluxos de dados críticos.

- Recursos de gerenciamento específicos: estão intimamente associadas aos requisitos específicos da aplicação, por exemplo, requisitos de monitoramento da linha de transmissão de energia da rede inteligente.

### **Recurso de segurança**

A camada de segurança é responsável pelos critérios e padrões de segurança de todas as camadas. Porém, esses critérios não são definidos no documento apresentado pelo ITU. Existem dois grupos de funcionalidades de segurança:

- Recursos genéricos de segurança: são independentes dos aplicativos e atuam na camada de aplicação com autorização, autenticação, confidencialidade de dados do aplicativo e proteção de integridade, proteção de privacidade, auditoria de segurança e antivírus; na camada de rede com autorização, autenticação, uso de dados e confidencialidade de dados de sinalização e proteção de integridade de sinalização; na camada do dispositivo com autenticação, autorização, validação de integridade do dispositivo, controle de acesso, confidencialidade de dados e proteção de integridade.
- Recursos de segurança específicos: estão intimamente associados aos requisitos específicos da aplicação, por exemplo, requisitos de segurança para pagamento móvel.

## **2.3 PROTOCOLOS DE COMUNICAÇÃO**

A Internet das Coisas necessitará que as atuais tecnologias de comunicação se adaptem e criem soluções com suporte a todos os seus requisitos, tais como: baixo consumo de energia, poder de processamento e comportar todos os objetos da rede. Tendo isso em mente, serão descritos os protocolos de comunicação mais relevantes, que podem vir a ser utilizados juntamente como a Internet das Coisas.

### **2.3.1 Zigbee**

O Zigbee é um dos protocolos mais utilizados em ambientes industriais e casas inteligentes, sendo baseado no padrão IEEE 802.15.4. Suas aplicações geralmente

não requerem muitas mudanças na taxa de transmissão, e seu alcance varia de 10 a 100 metros com transmissão máxima de 250 Kb/s. Além disso, esse protocolo abrange as camadas de Internet, transporte e aplicação (VIDAL, 2017; ROTTA; CHARÃO; DANTAS, 2017).

### **2.3.2 LoRaWAN**

Focado em aplicações para redes WAN (*Wide Area Network*), o LoRa foi desenvolvido para prover comunicação de baixo consumo energético e oferecer recursos voltados para segurança e comunicação *machine to machine*. Mantido pela LoRa Alliance, suporta redes amplas com milhões de dispositivos e velocidade entre 0.3 Kb/s e 50 Kb/s, sendo um dos protocolos mais populares para IoT (VIDAL, 2017).

### **2.3.3 Sigfox**

Sendo focado principalmente em aplicações de *machine to machine* que trabalham com equipamentos que necessitam de pouca bateria e baixos níveis de transferência de dados, o Sigfox é uma tentativa de criação de rede intermediária entre Wi-Fi e redes móveis (4G, 5G), visto que o Wi-Fi não tem alcance suficiente para realizar a comunicação com todos os objetos e as redes móveis. A Sigfox possui taxas de 10 b/s e 1.000 bit/s com alcance de 30 a 50 Km (VIDAL, 2017).

### **2.3.4 Wi-Fi**

Já muito presente no nosso dia-a-dia, este protocolo é tido como opção óbvia para muitos projetistas. Sendo um protocolo LAN (*Local Area Network*) com alcance de aproximadamente 50 metros e capacidade de tratar grande quantidade de dados com altas taxas de transmissão, na casa das centenas de megabit por segundo e chegando até 1300 Mb/s com o padrão 802.11ac. Por outro lado, o seu consumo energético é tido como um grande obstáculo para a sua utilização em aplicações IoT, além de estar sujeito a interferências (VIDAL, 2017).

### **2.3.5 MQTT**

Criado para projetos de comunicação entre satélites e equipamentos de extração de óleo, possui alta confiabilidade e baixo custo de implementação, sua simplicidade o torna muito versátil para aplicações de IoT. Utiliza modelo

“*Publish/Subscribe*” ou seja, publicar e subscrever que necessita exclusivamente de um *broker* para gerenciar e retornar as mensagens enviadas pelos dispositivos na rede. A grande vantagem do MQTT (*Message Queuing Telemetry Transport*) é sua eficiência energética e segurança, visto que está atrelado ao protocolo TCP. Pelo fato de utilizar *broker* para comunicação, esse protocolo se torna uma boa opção para comunicação remota/*cloud*, pelo fato do servidor *cloud* atuar como *broker* entre os dispositivos e outros serviços (ROTTA; CHARÃO; DANTAS, 2017).

### 2.3.6 Bluetooth

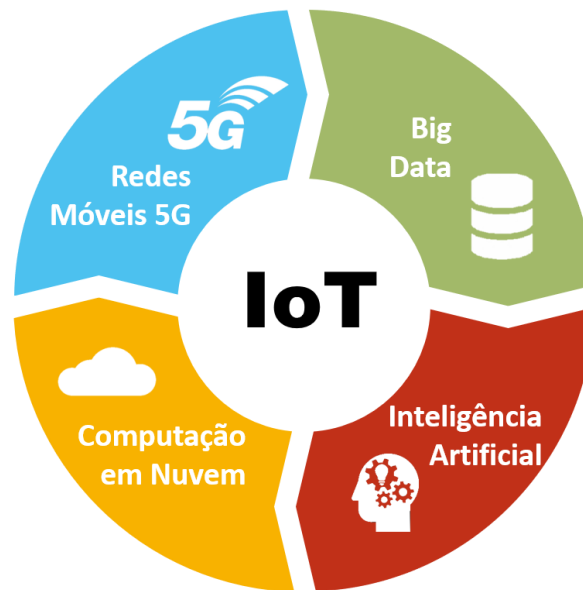
Sendo amplamente utilizado há muitos anos, este protocolo só entrou na disputa pelas aplicações de IoT com a sua versão 4.0 (*Bluetooth Low Energy*) e a mais recente, 5.0, que possibilita um menor consumo energético. É mantido pela Bluetooth SIG (*Special Interest Group*), possuindo extensa documentação e exemplos de aplicações disponíveis, o que facilita muito a sua integração com demais soluções, o tornando perfeito para automação residencial, comercial e produtos eletrônicos em geral (VIDAL, 2017).

Seu alcance varia de acordo com a classe utilizada, a classe 1 alcança até 100 metros e tem 100 mW de potência, a classe 2 alcança até 10 metros e tem uma potência de 2,5 mW e a classe 3 alcança até 1 metro e possui uma dissipação máxima de 1 mW. Vale destacar que o Bluetooth 5.0, em sua versão mais recente, alcança até 240 metros com uma taxa de transmissão de 50 Mb/s (VIDAL, 2017).

## 2.4 TECNOLOGIAS ESSENCIAIS PARA IOT

Ao decorrer da abertura do MWC 2019 (*Mobile World Congress*), Mats Granryd, diretor geral da GSMA, afirmou que a combinação de 5G, inteligência artificial (IA), Internet das Coisas (IoT) e Big Data (figura 4) mudará o mundo e criará infinitas possibilidades. Pois segundo o executivo, algumas iniciativas traçarão o futuro, dentre elas: IA em carros autônomos e a utilização de dados para prever epidemias (OLIVEIRA, 2019).

Figura 4 – Tecnologias essenciais para IoT



Fonte: Autores (2019)

Sabe-se que os avanços tecnológicos previstos para os próximos anos trazem muitas promessas, visto que a IoT tem como principal objetivo conectar objetos com objetos, possibilitando uma melhor experiência para o usuário. Para atingir este objetivo, algumas tecnologias são essenciais, para possibilitar o seu pleno funcionamento, tais como:

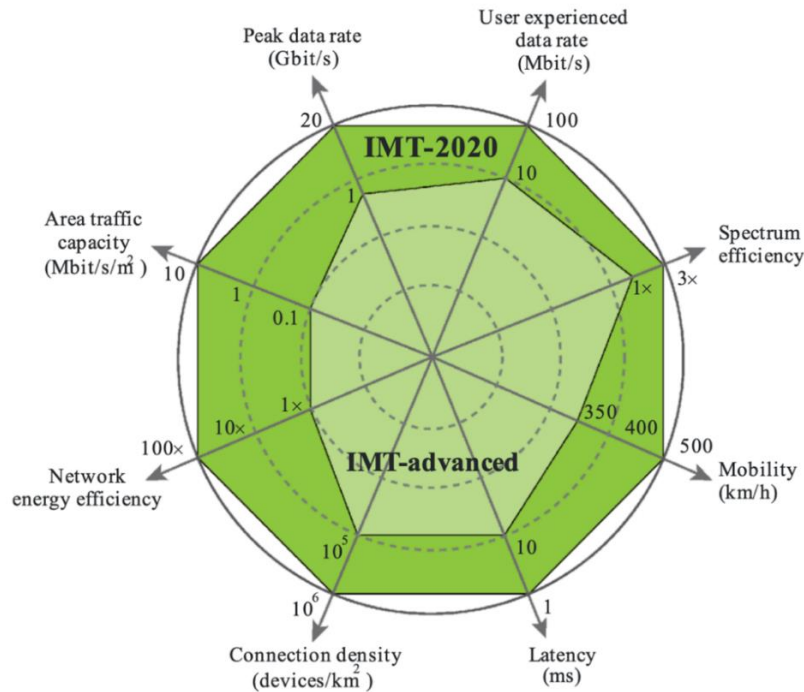
#### 2.4.1 Rede móvel 5G

A quinta geração de redes móveis (5G) é muito mais que um novo padrão de comunicação. É considerada como a evolução da comunicação de dados sem fio, pois, sua combinação de conectividade de alta velocidade e redução significativa no atraso de transmissão de dados, oferecerá suporte a aplicações de Internet das Coisas, como carros autônomos, onde o atraso de uma fração de segundo pode afetar sua resposta de frenagem (COLLELA, 2017).

De acordo com a ITU (2015), as redes 5G devem permitir uma taxa de transferência de dados de 100 Mb/s para cada usuário conectado, esta rede pode conectar até 1 milhão de dispositivos por metro quadrado, enquanto sua conectividade deve permanecer utilizável com velocidades de até 500 Km/h. Além disso, a latência, sob condições ideais, deve atingir no máximo 1 milissegundo e a rede deve prover uma eficiência energética 100 vezes maior que a quarta geração de redes móveis

(4G). A figura 5 compara os padrões IMT-2020 (5G) e IMT-advanced (4G), ressaltando a grande diferença entre os recursos oferecidos por cada tecnologia.

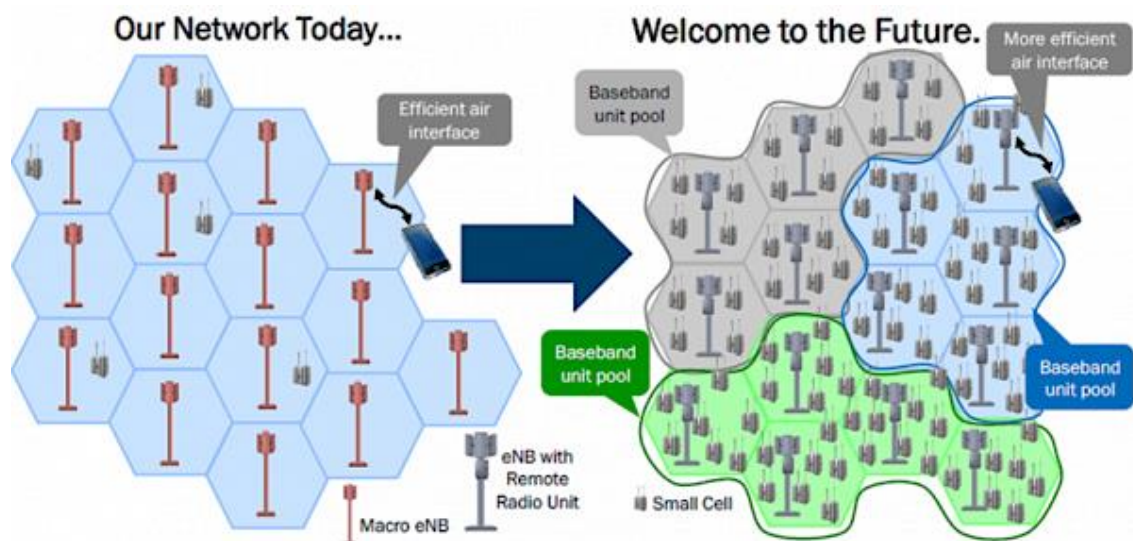
Figura 5 – Recursos do 5G



Fonte: ITU (2015)

Uma das chaves para o sucesso do 5G está no planejamento de espectro. Para a 5G Américas, as bandas de espectro móvel abaixo de 6 GHz serão importantes para a integração entre 4G e 5G, enquanto que as bandas mais elevadas necessitam de novas soluções de rádio (COMSTOR, 2018).

Figura 6 – Distribuição de rádios 4G x 5G

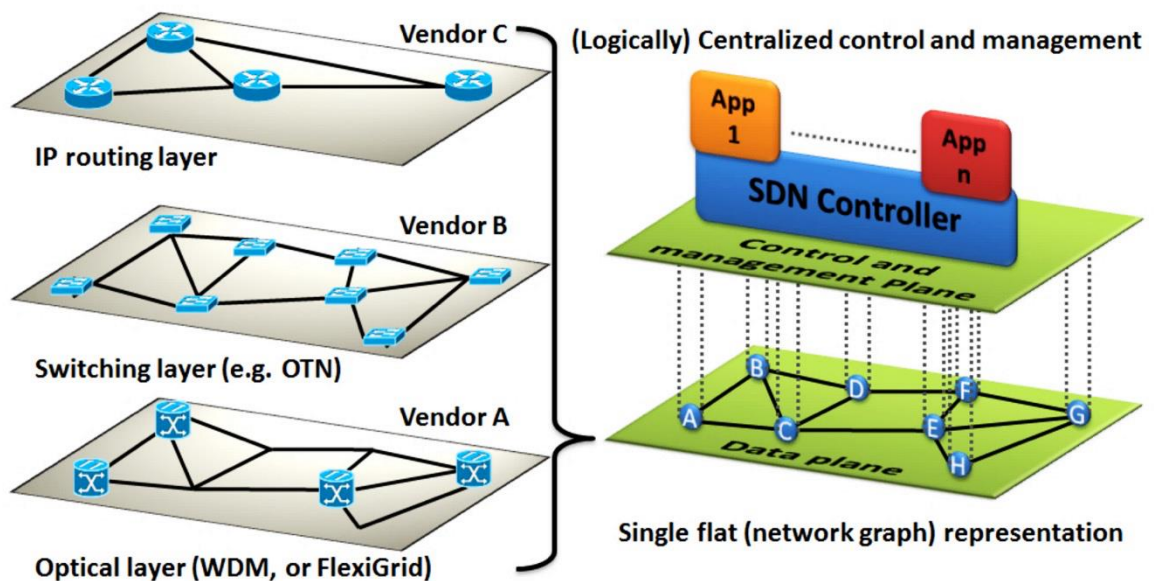


Fonte: Apeksha Telecom (2018)

Estas novas soluções, oferecem alguns problemas técnicos, pois, quanto maior a frequência de operação, menor será o comprimento de onda, por consequência, maior será a sua dificuldade de penetrar ou contornar obstáculos (ELGAN, 2018). Desta maneira, é possível verificar na figura 6, que as estações de rádio do 5G terão que estar mais próximas umas das outras, resultando em uma maior quantidade de rádios ao comparar com a tecnologia 4G, podendo trazer impactos estéticos para diversas cidades.

Outro fator importante está ligado ao fato de que as novas redes precisam lidar com a Internet das Coisas e seus bilhões de dispositivos. Os novos serviços de 5G terão um grande impacto na infraestrutura das operadoras, onde simplesmente realizar uma atualização do *hardware* e *software* não será o suficiente. Com a utilização da rede definida por *software* (SDN – *Software Defined Networking*), na estrutura do 5G, será possível oferecer maior escalabilidade para os novos dispositivos da rede de forma ágil e flexível (PRETZ, 2017).

Figura 7 – Arquitetura SDN



Fonte: Azodolmolky (2014)

A ideia do SDN é separar o plano de controle do plano de dados de uma forma mais inteligente (figura 7). Nesta estrutura de rede, as funções do plano de controle são atribuídas a um controlador SDN, responsável pela configuração do plano de dados dos dispositivos da rede. O controle de rede se torna programável, facilitando seu gerenciamento ao introduzir novos serviços. Por esta razão, a utilização do SDN permitirá um aumento da flexibilidade da rede 5G. Assim, esta rede virtualizada e



programável permitirá aos provedores inovar, tanto em suas operações, quanto em suas ofertas de serviços e expansões de rede (HAKIRI; BERTHOU, 2015).

Neste cenário, o 5G pode ser considerado como um facilitador para o desenvolvimento da Internet das Coisas. Pois, com sua perspectiva de prover comunicação em tempo real, confiável e escalável, será, fundamental para o avanço da Internet das Coisas.

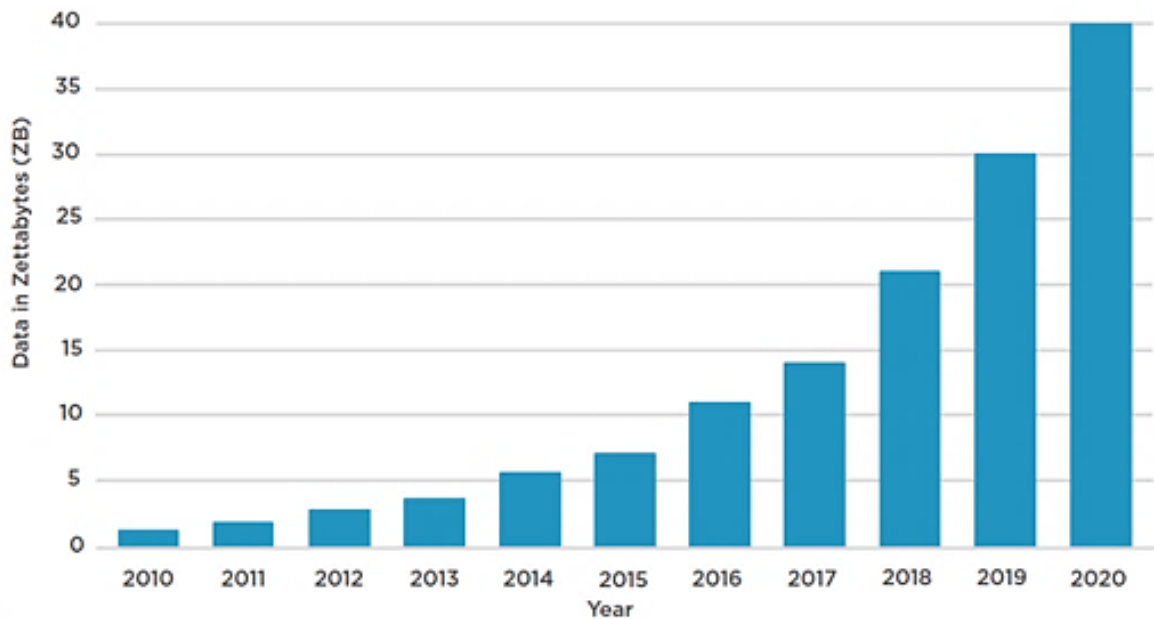
#### **2.4.2 Big Data**

Uma maneira simples de definir Big Data é destacar os seus V's, que discriminam, de modo geral, os objetivos e motivações da mesma (NASCIMENTO, 2017):

- Volume: compreende a crescente quantidade de dados a serem tratados;
- Variedade: ligado a diferentes tipos de dados que podem ser processados e analisados, sendo estes dados estruturados, semiestruturados e não estruturados;
- Velocidade: refere-se à agilidade para gerar, processar e analisar os dados;
- Veracidade: diz respeito à confiabilidade dos dados;
- Valor: reflete o quão valioso é um determinado dado, para realizar uma tomada de decisão.

Para um melhor entendimento da Big Data é preciso tomar ciência da crescente quantidade de dados que são gerados por sensores, aplicativos, carros, geladeiras e até mesmo redes sociais. Assim, esta tecnologia tem o objetivo de cruzar todos os dados extraídos de diversas fontes para obter tendências e padrões que possibilitem a tomada de decisões precisas, tendo em vista que há uma grande exigência dos consumidores e do próprio mercado por inovações (NASCIMENTO, 2017).

Figura 8 – Crescimento global de dados



Fonte: Felix (2018)

A expectativa do crescimento de dados no mundo, figura 8, se intensifica com a implementação da IoT. Por meio destes dados, a Big Data entra neste cenário com o objetivo de aproximar as empresas das necessidades dos seus clientes. Esta aproximação se torna possível devido à grande capacidade de processamento desta tecnologia, que aliada à coleta de dados em tempo real, poderá processá-los e apresentá-los de maneira mais acessível e simples, permitindo estratégias assertivas, refletindo em ações cada vez mais inteligentes.

### 2.4.3 Inteligência artificial

Para compreender este tema é necessário incorporar o termo “inteligência” à palavra “artificial”. O ser inteligente é aquele capaz de compreender, ser esperto e habilidoso. Além de que, inteligência é a capacidade de conhecer, aprender e compreender. A inteligência é o limiar que separa o homem de um animal. Sendo assim, pode-se caracterizar o termo inteligência artificial ou IA como um aglomerado de teorias práticas com o intuito de fazer máquinas ou *software* capazes de simular a inteligência humana (CUNHA, 2018).

Conforme o Teste de Turing, um computador só é inteligente se este for capaz de confundir o interrogador, fazendo com que ele não tenha certeza se quem o responde é humano ou máquina. Hoje em dia, a maioria dos sistemas não são

projetados para serem inteligentes, mas sim para realizarem funções específicas que são baseadas em métodos comportamentais humanos. A partir do desenvolvimento deste tipo de sistema é que surgem os conceitos de IA forte e IA fraca.

A IA forte se refere à computadores com consciência e capazes de escrever música e poesia, e não somente simular raciocínios. Já o conceito de IA fraca está ligado às máquinas que não são capazes de raciocinar por si mesmas, mas que são de certa forma “inteligentes”, um exemplo disso são os *chatbots*, que nada mais são do que *if-then* encadeados (JEAN, 2018).

Segundo o CEO da PayU Latam, José Velez, há cerca de 10 anos, poucas empresas estavam familiarizadas com a ideia de *Machine Learning* ou IA. Na atualidade estudo realizado pela Pega descobriu que 72% das pessoas já entendem o que é IA e apenas 28% se sentem desconfortáveis com a tecnologia, logo, não é nada surpreendente que muitas indústrias, empresas e mídia estejam focadas nisso (VELEZ, 2018).

A adoção de IA por organizações vem a ter um grande impacto financeiro, é esperado que ocorra reduções de custos operacionais, através da otimização e redução de erros humanos, através de ferramentas de auxílio a tomadas de decisões. Neste sentido, processos que envolvem um grande número de pessoas, passam a ocorrer com um número reduzido e de forma mais eficiente (VELEZ, 2018).

Tendo em vista o atual cenário do mercado, podemos dizer que a aplicação de IA aliada à Internet das Coisas, possibilita que empresas aprimorem os desenvolvimentos de seus produtos, criando assim, sistemas inovadores. Tais conceitos se interligam a partir do momento em que a IoT utiliza os dados apurados, gerados pelos sistemas de IA, de maneira otimizada. A Inteligência Artificial entra com o papel de assumir as ações humanas através de *software* cada dia mais sofisticados, onde essas ações serão aplicadas nos dispositivos através da IoT, afinal, de nada adianta capturar uma quantidade astronômica de volume de dados se os mesmos não forem interpretados e utilizados da maneira correta (MATOS, 2016).

#### **2.4.4 Computação em nuvem**

Segundo Puthal *et al.* (2015), a computação em nuvem oferece através da Internet um ambiente de recursos computacionais adaptável, ou seja, um conjunto de

serviços de rede, que proporciona escalabilidade e recursos computacionais sob demanda, que podem ser rapidamente fornecidos.

A computação em nuvem consiste no serviço de armazenamento e disponibilização de informação aos usuários em qualquer lugar, permitindo que a sua capacidade de processamento e armazenamento seja estendida sempre que for necessário, sem limites para seus servidores. Por isso as plataformas como *Internet banking* e de *e-mails* utilizam esta tecnologia, para que o cliente consiga acessar a sua conta por meio de qualquer dispositivo, seja este móvel ou não (VORTICE, 2017).

Porém, a computação em nuvem não fornece apenas dados de armazenamento, ela vai além, trazendo informações como a velocidade de comunicação do servidor com os usuários, potência de processamento e métrica sobre usuários. Isto faz com que processos e até mesmo áreas inteiras migrem para os sistemas automatizados e com informações em nuvem, inclusive possibilitando a manutenção desse ambiente. Por exemplo, as empresas não precisam mais instalar softwares para emitir notas fiscais, podem simplesmente migrar para ferramentas SaaS (*software as a service*) ou software como serviço, totalmente online, sem instalações e aquisições de licença, sem mídias físicas e com backups automáticos (VORTICE, 2017).

Apesar de seu funcionamento simples, existem diferentes modelos de computação em nuvem, que consistem em: privada, pública e híbrida. O primeiro se dá pela construção apenas para um usuário e de forma direcionada a ele na questão de armazenamento e segurança, ou seja, a nuvem e a infraestrutura do serviço são privadas e mantidas pelo próprio usuário e proprietário. Já o segundo modelo, o público, é como a maior parte da computação em nuvem funciona, neste modelo as aplicações são contratadas por diversas pessoas ou empresas, que compartilham todos os componentes ainda que utilizem individualmente e não tenham acesso à dados alheios. Por fim, a híbrida se dá quando mais de um tipo de serviço se faz presente, por exemplo, uma empresa pode manter sua rede privada (nuvem privada) e contar com a pública para momentos em que a capacidade precisar ser multiplicada (VORTICE, 2017).

Dessa forma, é notório que a computação em nuvem possui relevância no contexto da IoT. Visto que, é crescente a quantidade de dados gerados, necessita-se cada vez mais de processamento de grande armazenamento. Além do mais, as

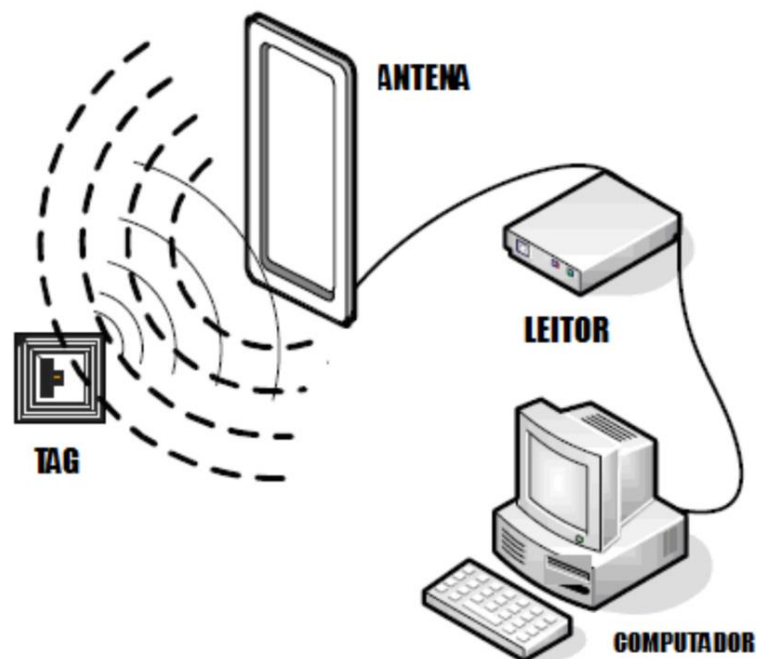
tecnologias em nuvem prometem garantir mais elasticidade para maior armazenamento de informações possíveis e flexibilidade para que usuários possam ter a capacidade de acessar serviços em qualquer lugar (SAPHIR, 2018).

### 3 IDENTIFICAÇÃO POR RÁDIO FREQUÊNCIA

A identificação por rádio frequência ou RFID (*Radio-Frequency Identification*), segundo Finkenzeller (2010), estabelece uma comunicação sem fio, utilizando ondas de radiofrequência para transmitir informações entre um leitor e um *transponder* (ou *tag*), geralmente anexado a um objeto, permitindo sua identificação. Sua primeira aplicação ocorreu no início da segunda guerra mundial, a tecnologia foi utilizada em sistemas de radares para identificação de aeronaves inimigas e aliadas, que respondiam ou não sinais de identificação por meio de ondas de rádio (LANDT, 2005).

O RFID é um tipo de tecnologia de identificação de objetos que possuam um *transponder* anexado em seu corpo, podendo ser identificado automaticamente, sem a necessidade de entrar em contato direto com um dispositivo leitor. O seu potencial de aplicação é amplo, desde a simples identificação de objetos até na área médica, logística e controle de acesso (PINHEIRO, 2006).

Figura 9 – Sistema RFID



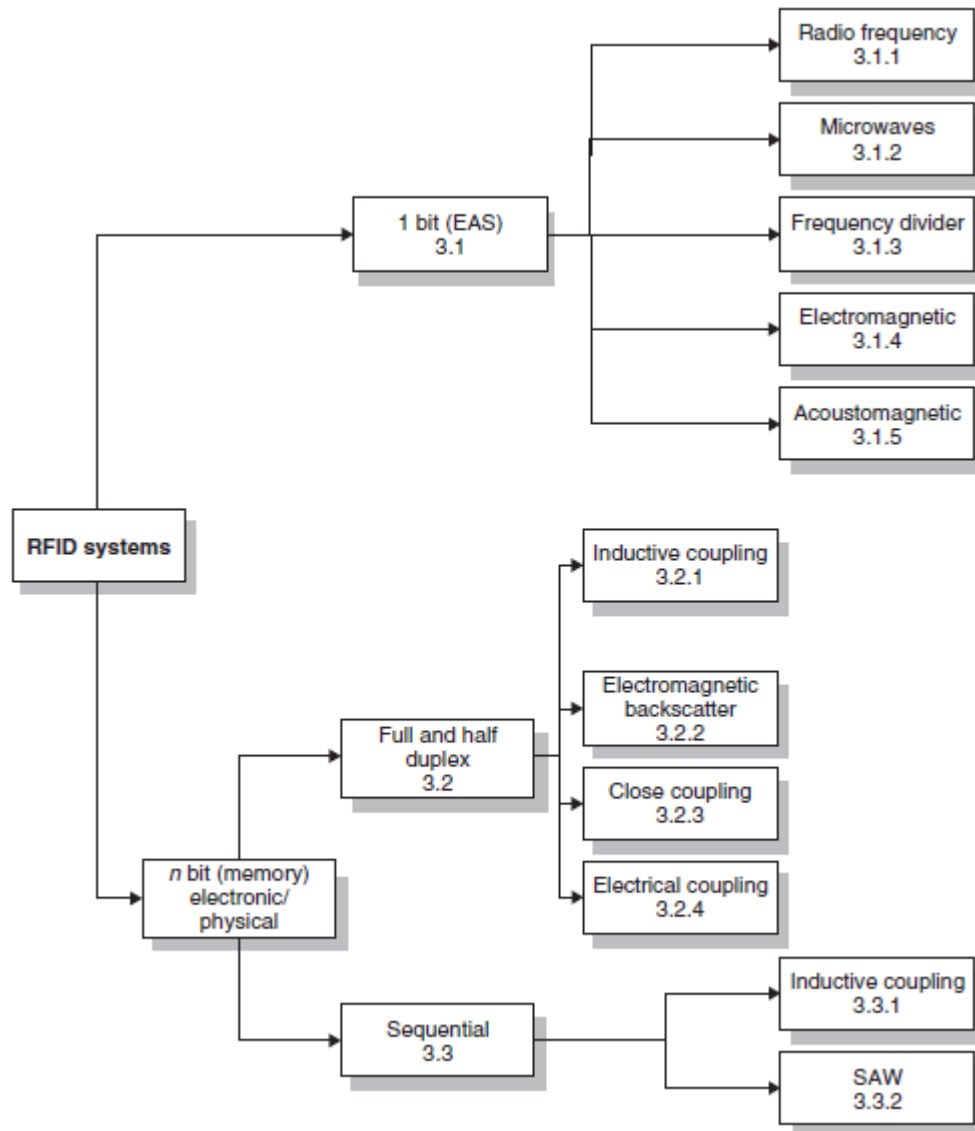
Fonte: Rodrigues; Borges; Barwaldt (2017)

O seu funcionamento é simples (figura 9), através de ondas de rádio é possível transmitir dados entre um leitor e uma *tag*, sem a necessidade de contato físico entre os dois. Posteriormente as informações são enviadas para um controlador, onde os dados são processados e analisados. Além disso, é possível efetuar múltiplas leituras de múltiplas *tags* permitindo a identificação de múltiplos objetos simultaneamente (FINKENZELLER, 2010).

### 3.1 PRINCÍPIOS DE FUNCIONAMENTO

Os sistemas RFID são classificados em duas categorias (figura 10): *1-bit transponder* e *n-bit transponder*. Estes sistemas apresentam diversas formas de comunicação entre o *transponder* e o leitor, além de especificar a transferência de energia e de dados (FINKENZELLER, 2010).

Figura 10 – Classificação dos sistemas RFID



Fonte: Finkenzeller (2010)

O sistema mais simples é o *1-bit transponder*, opera em apenas duas condições: “1” ou “0”. Quando se encontra no estado “1”, significa que a *tag* está localizado na região de leitura do leitor, e no estado “0”, a *tag* está fora da região de leitura. Devido à esta característica, sua aplicação é bastante comum em sistemas antifurto, presentes em lojas, que necessitam saber se o seu cliente está levando um

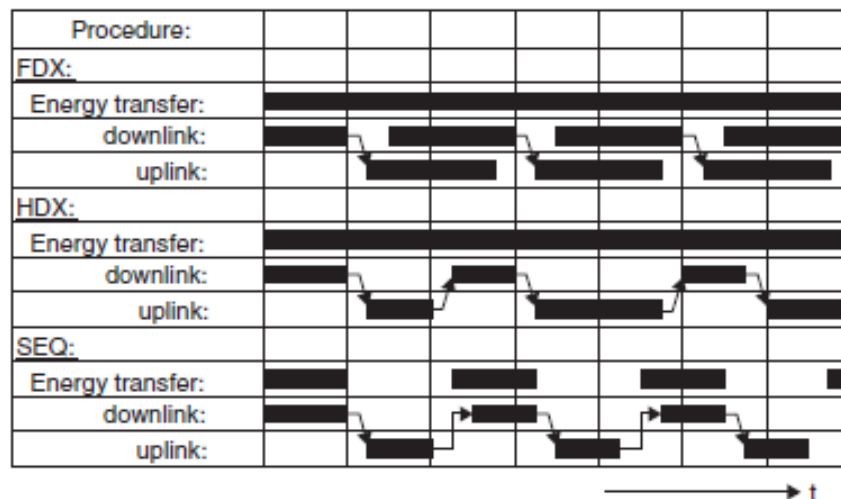
item que não teve sua compra efetivada. O sistema antifurto ou sistema EAS (*Electronic Article Surveillance*), é composto pelos seguintes componentes: a antena de um leitor, a *tag* e um dispositivo que realiza desativação da *tag* (colocando em estado “0”) após a confirmação da compra do cliente (FINKENZELLER, 2010).

Os sistemas *1-bit transponder* possuem um desempenho, determinado pela taxa de detecção em relação a máxima distância entre a *tag* e a antena do leitor. Diversos métodos são utilizados para realizar a detecção do *transponder* na zona de leitura do leitor, por radiofrequência, por micro-ondas, por divisão de frequência, por eletromagnetismo e por efeito acústico magnético (FINKENZELLER, 2010).

Para soluções mais complexas, os sistemas *n-bit transponder* possibilitam a comunicação e transmissão de dados entre o leitor e o *transponder*, assim como entre o *transponder* e o leitor. Esta comunicação pode ser através de *transponders* ativos ou passivos e a transmissão de dados entre eles pode ser do tipo *full-duplex* (FDX), *half-duplex* (HDX), ou sequencial (FINKENZELLER, 2010).

Na transmissão de dados *full-duplex*, a informação é enviada nos dois sentidos de forma simultânea, portanto, tanto a *tag* quanto o leitor enviam dados ao mesmo tempo. Na transmissão *half-duplex*, a informação é enviada nos dois sentidos, porém de forma não simultânea, sendo assim, a *tag* e o leitor intercalam o tempo de envio da informação. Em ambos procedimentos, o fornecimento de energia ao *transponder* é contínuo e não depende do fluxo de dados, diferente da sequencial, em que o fornecimento de energia e a transferência de informações ocorrem alternadamente, como pode ser visualizado na figura 11 (FINKENZELLER, 2010).

Figura 11 – Representação da transmissão FDX, HDX, e Sequencial



Fonte: Finkenzeller (2010)



Todas estas técnicas de transmissão apresentadas possuem diferentes métodos de comunicação sem fio, chamado de acoplamento, devido à variedade de métodos, será apresentado a seguir os dois principais métodos de acoplamento utilizados nos sistemas RFID, o acoplamento indutivo e eletromagnético.

Um *transponder* por acoplamento indutivo possui um microchip para armazenar os dados e uma bobina que funciona como antena. Em grande parte, são elementos passivos, ou seja, a energia necessária para o funcionamento é fornecida pelo dispositivo de leitura. Para seu funcionamento, um campo eletromagnético é gerado pelo dispositivo de leitura, que é recebido pela bobina do *transponder*. Desta forma, por indutância, é gerada uma tensão que é retificada, gerando energia para o microchip, que começa a transmitir um sinal que contém o código de identificação (ID) para o dispositivo de leitura (FINKENZELLER, 2010).

Os sistemas por acoplamento eletromagnético operam em altas frequências, nas faixas *ultra high frequency* (UHF) e micro-ondas. Desta maneira, a comunicação entre o *transponder* e o dispositivo de leitura pode ser realizado em longas distâncias e por operarem com comprimentos de onda curtas, possibilitam o uso de antenas pequenas e de boa eficiência. Para seu funcionamento, o dispositivo de leitura, começa uma transição de um sinal em rádio frequência através de sua antena. O campo elétrico gerado pelo sinal, gera um fluxo de corrente nos capacitores do *transponder*, resultando em uma diferença de potencial que alimenta o microchip do *transponder*, que por sua vez começa a transmitir um sinal contendo o código de identificação para o dispositivo de leitura (FINKENZELLER, 2010).

## 3.2 COMPONENTES DA TECNOLOGIA RFID

O sistema RFID geralmente é formado pelos seguintes componentes: *transponder* (ou *tag*), leitor, antena e controlador. O *transponder* possui uma antena e um microchip, utilizado para armazenar informações. O leitor realizando leitura e ou escrita na *tag*. A antena estabelece a comunicação. O controlador é responsável pelo processamento da informação obtida pelo leitor (FINKENZELLER, 2010).

### 3.2.1 Tag RFID

A *tag* ou *transponder* é um dos principais componentes de um sistema RFID, este dispositivo pode armazenar e transmitir dados para um leitor sem necessidade

de contato, utilizando ondas de rádio. Seu propósito é estar anexado fisicamente ao objeto, possibilitando sua identificação (FINKENZELLER, 2010). Sua classificação é dada pela sua energização e capacidade de gravação e ou escrita.

A classificação, de acordo com o tipo de energização, caracteriza as *tags* como ativas, semi-passivas e passivas. As *tags* ativas possuem a habilidade de iniciar sua comunicação com o leitor e outras *tags* de forma independente, pois, possuem uma fonte de energia. As semi-passivas possuem bateria, mas apenas podem responder sinais que cheguem até elas. Já as passivas não possuem uma fonte de energia, através de ondas eletromagnéticas ou micro-ondas geradas pelo leitor, produzem sua própria energia, possibilitando que seja enviado um sinal para o dispositivo leitor (FINKENZELLER, 2010).

A classificação que foi criada pela EPCglobal leva em conta a capacidade de poder se realizar gravação e leitura em *tags* (ROBERTI, 2010), as classes são as seguintes:

- Classe 0: não é possível realizar a gravação de um novo ID na *tag*, pois são pré-programadas permitindo somente a leitura.
- Classe 1: é permitida a gravação apenas uma vez, podendo realizar diversas leituras, ou seja, o usuário grava somente uma vez não podendo modificar a informação.
- Classe 2: permite leitura e gravação diversas vezes.
- Classe 3: possui a capacidade de leitura e gravação, além de possuir sensores acoplados, capazes de registrar pressão, temperatura e outros parâmetros.
- Classe 4: possui todos os recursos das classes anteriores, e na capacidade de iniciar a comunicação com outras *tags* e leitores.
- Classe 5: semelhante com as *tags* da classe 4, mas com funcionalidades adicionais, pode fornecer energia para outras *tags* e se comunicar com outros dispositivos além dos leitores.

As *tags* passivas, geralmente são classificadas na faixa de classe 0 a 3. A classe 4 descreve as *tags* ativas, que possuem uma fonte de energia interna. A classe 5 é reservada para leitores e *tags* ativas que podem ler dados de outras *tags* (FINKENZELLER, 2010).

### 3.2.2 Leitor RFID

O leitor é o equipamento responsável por orquestrar a comunicação com qualquer *tag* compatível, obter sua informação e em seguida, apresentar os dados da *tag* a uma aplicação que pode fazer uso de seus dados (FINKENZELLER, 2010).

Os leitores podem ser subdivididos em dois blocos funcionais: o sistema de controle e a interface de alta frequência. A interface de alta frequência é responsável por gerar o sinal para ativar o *transponder*, modular o sinal de transmissão para enviar dados ao *transponder* e realizar a recepção e demodulação dos sinais de alta frequência transmitidos por um *transponder*. O sistema de controle realiza funções relacionadas a gerência, como codificação e decodificação e controle da comunicação com as *tags* do sistema. Em sistemas mais complexos são executados algoritmos anticolisão, aplicações de desempenho e criptografia e descryptografia dos dados transferidos entre *tag* e leitor (JIA *et al.*, 2012).

### 3.2.3 Antena RFID

As antenas RFID podem ser divididas em duas classes: antena da *tag* e antena do leitor. A antena do leitor realiza a propagação e recepção do sinal enviado a *tag*, sendo ela interna ou externa ao leitor. Já a antena da *tag* encontra-se interna a *tag*, sendo responsável por gerar energia para ativar a *tag* passiva. Além de transmitir o sinal que transporta a informação armazenada na *tag* para o leitor (KALNOSKAS, 2017).

### 3.2.4 Controlador

O controlador possui dois elementos, um banco de dados e um *software* que é chamado de *middleware*. Ele se encontra entre os leitores e as aplicações, e é responsável pelo gerenciamento do fluxo de dados enviados por diversos leitores de uma rede. Além de exercer a função de processamento, eliminando dados errôneos, duplicados ou redundantes. Desta maneira, permite que os dados sejam manuseados mais próximos da borda da rede, o que diminui a carga de transmissão de dados e deixando de ser necessário um servidor central que exerceria a função de gerência e filtragem de dados importantes para a aplicação (HUNT; PUGLIA; PUGLIA, 2006).

### 3.3 FAIXA DE OPERAÇÃO

Sendo um dos parâmetros de maior importância, que determina o alcance de leitura, tipo de *tag* e leitor, a faixa de operação dos sistemas RFID dividem-se entre as seguintes categorias (JISK, 2006):

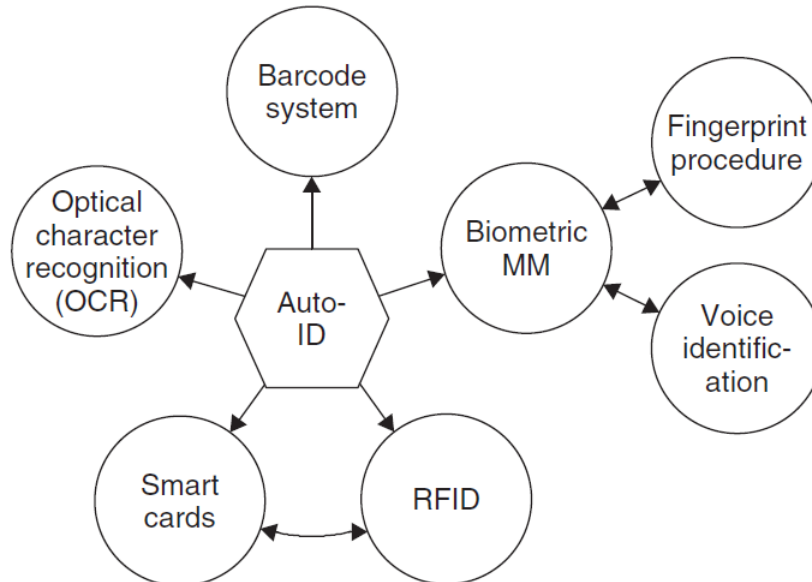
- Baixa frequência (LF – *Low Frequency*): sua operação, varia entre 125 KHz e 134 KHz. Possui baixo alcance, de no máximo 50 centímetros, sendo utilizado para aplicações, como por exemplo, identificação de animais.
- Alta frequência (HF – *High Frequency*): opera utilizando a faixa até 13,56 MHz. O alcance típico dessa frequência é de até 1,5 metros em condições ideais, comumente utilizado em aplicações de transmissão de dados e que não demandam um alcance muito grande, como por exemplo controle de acesso e segurança de passaporte.
- Ultra alta frequência (UHF – *Ultra High Frequency*): utiliza as frequências de 433 MHz atingindo até 100 metros ou 865 MHz a 960 MHz chegando até 5 metros. Esta faixa de operação é utilizada para aplicações que requerem um alcance superior, como rastreamento de ativos, controle de inventários em grandes fábricas e identificação de veículos.
- Micro-ondas: opera entre as frequências 2,45 GHz e 5,8 GHz. Também conhecida como ISM (*Industrial-Scientific-Medical*) este tipo de frequência é voltado para estudos e pesquisas das áreas industriais, científicas e médicas. Podendo ter um alcance de 10 metros e é utilizado em aplicações como em pedágios eletrônicos.

### 3.4 TECNOLOGIAS SEMELHANTES

A tecnologia RFID é uma ramificação das tecnologias de auto identificação e tornaram-se populares em setores que necessitam de procedimentos de identificação automática, com objetivo de obter informações sobre determinado produto, por exemplo. Os principais tipos de sistemas de auto identificação estão demonstrados na figura 12, são eles: código de barras, *smart cards*, reconhecimento óptico de caracteres (OCR - *Optical Character Recognition*), biométrico (impressão digital e

identificação de voz), cartões magnéticos, além do próprio sistema de identificação por rádio frequência (FINKENZELLER, 2010).

Figura 12 – Tipos de tecnologias de auto identificação



Fonte: Finkenzeller (2010)

Os sistemas de auto identificação que utilizam dispositivos ópticos para leitura da informação, como o código de barras, são os mais baratos e difundidos atualmente. Porém ele necessita de determinado ângulo entre a etiqueta e o leitor para realizar a leitura adequada da informação, tornando-o inapropriado para aplicações que não possuam intervenção humana, visto que há necessidade de ajuste no posicionamento dos objetos para poder identificá-los de maneira correta (FINKENZELLER, 2010).

Apesar do código de barras ser a tecnologia com menor custo, os sistemas RFID apresentam algumas vantagens, tais como: proporcionar a leitura da informação sem a necessidade de proximidade com o leitor, maior velocidade de leitura das etiquetas, possibilita a contagem de estoque de forma automática, entre outras vantagens. O RFID necessita de maior investimento quando comparado a soluções que utilizam código de barras, porém a sua utilização é justificada por estas vantagens destacadas. (MONTEIRO, 2018).

### 3.5 RFID EM UM AMBIENTE DE IOT

Com a necessidade de conectar todos os tipos de objetos, a Internet das Coisas pode encontrar no RFID uma solução para o desenvolvimento de suas aplicações. O RFID é capaz de identificar qualquer objeto, basta que um *transponder*

seja implantado em sua superfície ou em seu interior. Esta possibilidade de identificação poderá trazer diversas mudanças, visto que a rede se tornará capaz de coletar informações de maneira automática sobre todos os seus componentes, se tornando mais dinâmica e rica em informações (CHAMEKH *et al.*, 2018).

Desta maneira, este trabalho apresenta no capítulo 5 um protótipo demonstrando a utilização do RFID em um ambiente de IoT, em específico, uma situação de controle de acesso. O controle de acesso é utilizado para limitar ou restringir o ingresso de um indivíduo ou grupo de indivíduos a um ambiente. Portanto, um sistema RFID pode ser utilizado para realizar a identificação automática de pessoas através de um *transponder*. Além do que, algumas soluções que utilizam RFID podem prover uma identificação à distância, sem a necessidade de aproximar o *transponder* do leitor.

### 3.6 SEGURANÇA E PRIVACIDADE

A Internet das Coisas integra diversos objetos inteligentes, capazes de se comunicarem uns com os outros. Estes objetos inteligentes podem fornecer dados, acessá-los e utilizar recursos de processamento e armazenamento em nuvem. Problemas de segurança em relação à privacidade, comunicação e armazenamento são um significativo desafio para o ambiente de Internet das Coisas (CONTI *et al.*, 2018).

Para Kurose; Ross (2010), uma comunicação segura deve atender as seguintes características:

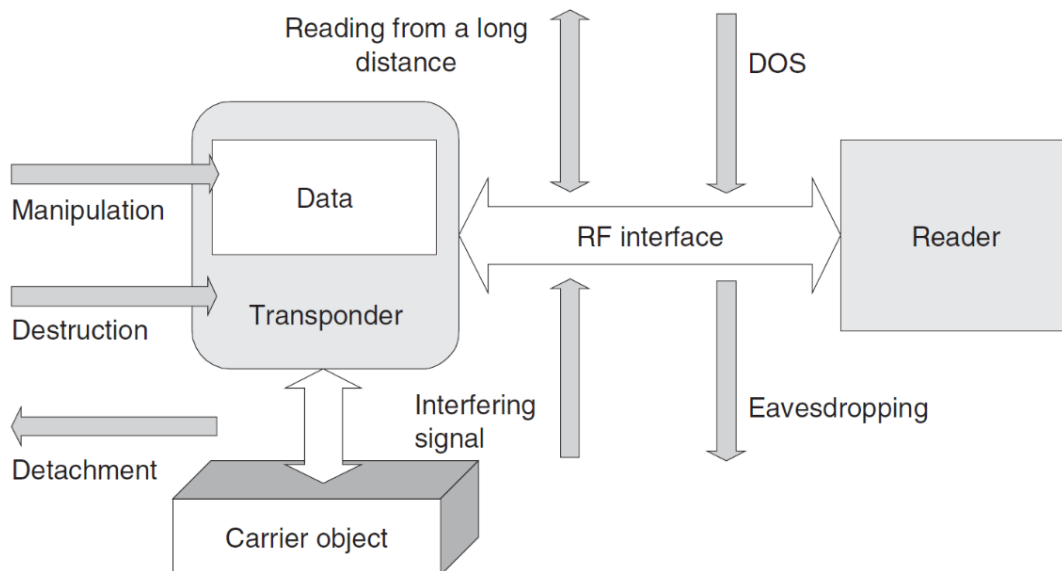
- **Confidencialidade:** é relacionada a privacidade dos dados. Tem o objetivo de transmitir a informação de modo que seu conteúdo não possa ser lido ou que não possa ser entendido.
- **Integridade:** é associada a imutabilidade da informação. Necessita garantir que a informação não foi modificada ou violada.
- **Autenticação:** é referente a autorização de acesso e a autenticidade da origem da informação. Tem que garantir que a informação seja acessada por apenas pessoas ou máquinas autorizadas, além de procurar garantir que a informação é proveniente da fonte desejada.
- **Disponibilidade:** é referente a garantia da disponibilidade da informação. Deve assegurar que a informação seja acessada em qualquer momento.

- Não repúdio: é a necessidade de provar que uma pessoa ou máquina fez algo. Ou seja, é a garantia que o emissor de uma informação é seu autor, não podendo negar este fato.
- Controle de acesso: é garantir que entidades que desejam acesso a recursos possam fazer se autorizadas, e realizem este acesso perante permissões bem definidas.

### 3.6.1 Problemas de segurança

Soluções de Internet das Coisas que utilizam RFID estão sujeitas a ataques em três pontos, assim como nas demais tecnologias sem fio, sendo estes: o meio de transmissão, o equipamento de transmissão e na recepção dos dados. A figura 13 exemplifica tipos básicos de ataques que afetam este tipo de sistema, em sua grande maioria sendo direcionados ao *transponder* ou à interface de rádio frequência que se encontra entre o *transponder* e o leitor (FINKENZELLER, 2010).

Figura 13 – Ataques à sistemas RFID



Fonte: Finkenzeller (2010)

Sendo o RFID um dos componentes de um ambiente de IoT, é de extrema importância que os dados cheguem ao seu destino mantendo sua integridade, além de ser necessário manter a privacidade da informação, que é tida como ponto crucial. Para entender como solucionar os problemas de segurança dos sistemas RFID, primeiramente, deve-se conhecê-los.

### **Clonagem e Spoofing**

São tipos de ataques que dependem um do outro. A clonagem consiste na cópia da *tag*, que pode ser feita através da acoplagem de um dispositivo de gravação junto ao de recepção ou através da cópia do serial de uma *tag read-only* (somente leitura), gerando uma *tag* idêntica a original. Já a técnica de *spoofing* baseia-se nos dados obtidos durante a clonagem para obter informações de autenticação e formato de dados, possibilitando a emulação de uma *tag* válida (FINKENZELLER, 2010).

A grande diferença entre essas duas técnicas de ataque é que na técnica de *spoofing* não é necessária uma *tag* igual à original, já que é possível gerar uma *tag* válida, pois se pode transmitir as mesmas características da *tag* original através de qualquer dispositivo de rádio frequência (FINKENZELLER, 2010).

### **Eavesdropping**

Esta técnica baseia-se na espionagem da transmissão de dados, onde um terceiro agente utiliza de uma das maiores ameaças à tecnologia RFID, a interceptação da comunicação entre o transmissor e o receptor. O alcance dos sistemas RFID varia da ordem de poucos centímetros a muitos metros, logo, os receptores de rádio do invasor só precisam de uma tensão de saída de antena que seja de ordem de grandeza suficiente para receber sinais úteis, desta forma, a espionagem se torna possível à uma distância muito maior que a da troca de informações (FINKENZELLER, 2010).

### **Denial of Service (DOS)**

Diferente dos outros tipos de ataque, um ataque DOS tem como objetivo causar confusão e impedir que a comunicação aconteça e caracteriza-se pela emulação de inúmeros *transponders*, ao redor do leitor. Todo receptor possui um número limite de *transponders* que podem ser identificados e validados ao mesmo tempo, e caso este número seja extrapolado, o sistema fica impedido de validar as informações recebidas e acaba deixando algumas informações e solicitações feitas a ele passarem sem checagem, que podem vir a comprometer o sistema. (FINKENZELLER, 2010).



### ***Jamming***

Esta técnica de ataque é bastante frequente nas transmissões de rádio frequência. O *Jamming*, consiste na interrupção da transmissão, seu objetivo é bloquear o meio de transmissão realizando uma nova transmissão ao mesmo tempo que a original, causando ruído e comprometendo a transmissão original de dados. Pode-se considerar esse tipo de ataque como sendo DOS, já que ele tem por finalidade inibir a efetivação do envio de dados (FINKENZELLER, 2010).

### ***Man-in-the-middle***

Este tipo de ataque ocorre entre o leitor e a *tag*, durante o processo de transmissão. O atacante controla a troca de dados entre o leitor e a *tag*, manipulando e modificando as informações que estão sendo transmitida, antes que chegue ao destino final. Deste modo, quando o leitor recebe os dados ele já não pode garantir a sua confidencialidade e integridade da informação (BASHIR; MIR, 2018).

### ***Relay Attack***

Este tipo de ataque tem como objetivo enganar o leitor e aumentar o alcance entre o leitor e a *tag* quase que deliberadamente, através da interposição de um transmissor. Para conseguir enganar o receptor, o usuário ataca alguma *tag* que esteja dentro do alcance de leitura e o utiliza para simular uma extensão do raio de leitura do leitor, de forma que seja possível permitir a leitura sem que o usuário esteja no ambiente. Este tipo de ataque é utilizado principalmente contra sistemas de controle de acesso, para liberar acesso privilegiado sem a necessidade de que a pessoa esteja no recinto (FINKENZELLER, 2010).

## **3.6.2 Soluções para os problemas de segurança**

Após apresentados os tipos de ataques mais comuns realizados contra sistemas RFID pode-se afirmar que as aplicações de RFID são sensíveis a falhas de segurança o bastante para que exista preocupação em determinados tipos de aplicações, principalmente nas de controle de acesso, que estão sujeitas à ataques iminentes (FINKENZELLER, 2010).

Logo, o grande ponto por trás das aplicações RFID é o equilíbrio entre o investimento necessário em soluções de segurança mais robustas e a viabilidade do

projeto, pois um dos motivos para a utilização de soluções em RFID é justamente a redução de custos. Para facilitar a análise de viabilidade das soluções de segurança comumente utilizadas, seguem os métodos de segurança mais comuns:

### **Criptografia**

Sendo um dos métodos mais eficazes para a proteção de dados, a criptografia também pode ser muito bem implementada em aplicações RFID, pois ao encriptar as informações contidas em uma *tag*, se garante a confidencialidade dos dados caso eles sejam interceptados por terceiros. Para se ter acesso aos dados encriptados é preciso que o usuário saiba as chaves necessárias para realizar a decodificação, sendo que a robustez da encriptação depende da técnica adotada (FINKENZELLER, 2010).

O tipo de encriptação escolhido deve estar de acordo com a aplicação em questão, por exemplo, em soluções que envolvam apenas a localização ou identificação de itens não valiosos não é necessária uma maior proteção, em outro caso, para um sistema que trate de informações sigilosas, como contas bancárias, aconselha-se um certo nível de proteção (FINKENZELLER, 2010).

### **Autenticação mútua**

Nesta técnica, todas as *tags* e leitores detêm a mesma chave criptográfica. Quando uma *tag* entra pela primeira vez na zona de leitura do dispositivo leitor, não se pode presumir que os dois possuem permissão para se comunicarem. Pois no ponto de vista da *tag*, é necessário proteger seus dados armazenados. Para o dispositivo leitor, existe a necessidade de proteger a aplicação contra informações falsas. Desta maneira, a troca de informações somente é estabelecida após a checagem das chaves criptográficas, que devem ser as mesmas para os dois dispositivos (FINKENZELLER, 2010).

### **Desativação**

Utilizada para proteger a privacidade do cliente, esta técnica permita a emissão de comandos que inutilizam a informação presente na *tag* RFID. Costuma ser utilizada em estabelecimentos comerciais após a venda do item (SPRUIT; WESTER, 2013).

## 4 DESENVOLVIMENTO DO PROTÓTIPO

Neste capítulo serão apresentados os materiais, tanto *hardware* quanto *software*, que foram utilizados para a elaboração do protótipo de um sistema de controle de acesso utilizando RFID, inserido em um ambiente de IoT. Além do método de desenvolvimento do protótipo utilizado para a obtenção do resultado desejado.

### 4.1 HARDWARE E SOFTWARE UTILIZADOS

Para o desenvolvimento deste protótipo foi utilizada a placa Raspberry Pi 3 Model B, como unidade responsável pelo processamento de dados. Nesta placa foram implementados todos os algoritmos responsáveis pelas regras de um sistema de controle de acesso e integração com o banco de dados em nuvem chamado Firebase. A escolha do Raspberry Pi 3 foi pelo fato de seu tamanho reduzido, baixo consumo de energia e capacidade de processamento compatível com as necessidades do protótipo.

Nesta placa, o sistema operacional utilizado foi o Raspbian, versão 4.9. Esta versão possui interface gráfica, para realizar a visualização e utilização do sistema operacional, foi utilizado o *software* VNC Viewer, que possibilita o acesso remoto da placa. Já para a programação do Raspberry Pi, foi utilizada a linguagem *Python*, versão 3.5.3, além da utilização das seguintes bibliotecas: paho-mqtt e pyrebase.

Para realizar a identificação de uma pessoa, foi utilizado a *tag* passiva e leitor RFID MFRC522, associados a um microcontrolador NodeMCU, que utiliza a rede Wi-Fi para se comunicar com o Raspberry Pi, através do protocolo MQTT.

#### 4.1.1 Raspberry Pi

O Raspberry Pi é um microcomputador que possui a capacidade de realizar as principais funções de um desktop. O modelo utilizado para este protótipo foi o Raspberry Pi 3 Model B. Suas características técnicas são de um computador completo, porém de baixo custo, sendo bastante utilizado nas mais diversas aplicações, projetos de automação, computação e redes (GARRETT, 2014).

Figura 14 – *Raspberry Pi 3 Model B*

Fonte: Raspberrypi (2016)

As especificações técnicas do Raspberry Pi 3 Model B são explicitadas o quadro abaixo:

Quadro 1 – Descrição técnica do Raspberry Pi 3

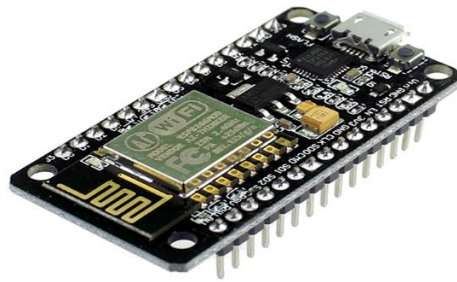
<b>Processador</b>	Quad Core 1.2GHz Broadcom BCM2837 64bit CPU
<b>Memória Ram</b>	1GB
<b>Adaptadores</b>	BCM43438 wireless LAN and Bluetooth Low Energy, 4 saídas áudio/vídeo estéreo e 100 Base Ethernet
<b>GPIOs</b>	40 pinos
<b>Entrada HDMI</b>	1 porta Full Size
<b>Entrada USB</b>	4 portas
<b>Portas para suporte</b>	Câmera CSI, display DSI e Micro SD

Fonte: Raspberrypi (2016)

#### 4.1.2 NodeMCU

O NodeMCU, é um sistema embarcado de código aberto da família de microcontroladores ESP8266. Criado para ser utilizado no desenvolvimento de projetos de IoT, pois além de possuir um controlador, é um equipamento de baixo custo, com suporte integrado a redes Wi-Fi, tamanho reduzido e baixo consumo de energia, justamente os principais pontos tratados pela IoT como essenciais em seus dispositivos de borda. Vale destacar que a sua programação pode ser feita via OTA (*Over the Air*), ou seja, através de Wi-Fi ou Bluetooth (OLIVEIRA, 2017).

Figura 15 – NodeMCU



Fonte: Oliveira (2017)

Além das características citadas acima, algumas das especificações técnicas relevantes da versão do microcontrolador NodeMCU utilizado neste protótipo, estão expostas no quadro 2.

Quadro 2 – Descrição técnica do NodeMCU

<b>Processador</b>	ESP8266-12E de operação 80/160mHz
<b>Arquitetura</b>	RISC de 32 bits
<b>Memória flash</b>	4 Mb
<b>Adaptador Wi-Fi</b>	Padrão 802.11b/g/n
<b>GPIOs</b>	30 pinos
<b>Modo de Operação</b>	Acess Point, Station ou AP+Station

Fonte: Oliveira (2017)

#### 4.1.3 Leitor RFID MFRC522

O leitor RFID, foi criado e desenvolvido pela empresa NXP, utiliza um chip MFRC522, que por sua vez, opera em uma frequência de 13,56 MHz e permite leitura e escrita sem necessitar de contato entre leitor e *tag*. Tem como recomendações operacionais do fabricante sua tenção de entrada entre 2,5V até 3,6V, sendo o ideal 3,3V (NXP, 2016).

Figura 16 – Leitor RFID MFRC522



Fonte: Gbur (2017)

#### 4.1.4 Tag RFID

A tecnologia RFID se baseia na leitura de *tags* ou cartões para ter uma finalidade, e a figura 17 ilustra estas *tags* e cartões passivos que são compatíveis com o leitor RFID MFRC522.

Figura 17 – Tags do leitor RFID MFRC522



Fonte: Gbur (2017)

#### 4.1.5 MQTT

A conexão à Internet é uma característica fundamental para o funcionamento dos dispositivos em um cenário de IoT, visto que a mesma permite e necessita da comunicação entre eles. O protocolo de rede no qual a Internet, como a conhecemos, opera é o TCP/IP. Contudo o MQTT (*Message Queue Telemetry Transport*) ganha destaque como um protocolo padrão para comunicações entre dispositivos em ambientes de IoT (YUAN, 2017).

Figura18 – Protocolo MQTT



Fonte: Weble (2018)

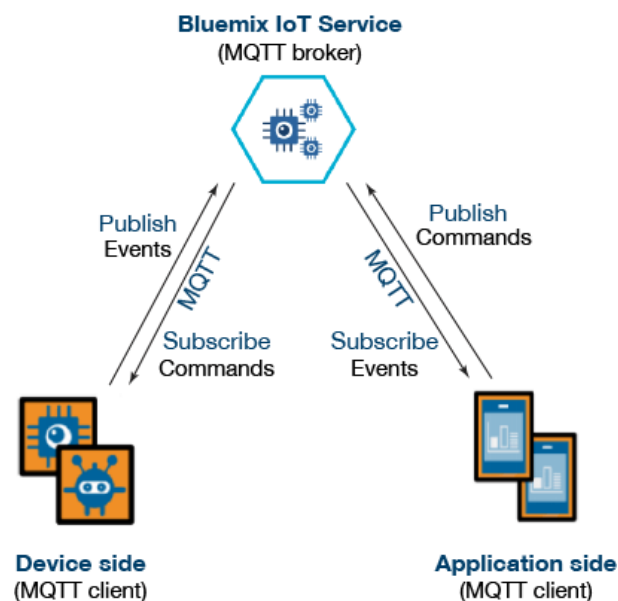
Criado pela IBM (*International Business Machines*) no final da década de 90, o MQTT foi desenvolvido, a priori, para efetuar o sensoriamento de petróleo feito por satélites. Este protocolo visa a comunicação através da troca de mensagens com suporte de forma assíncrona entre os dispositivos, ou seja, esta tecnologia retira o emissor e o receptor das mensagens do ambiente, por isso, este protocolo se torna escalável para projetos de rede (YUAN, 2017).

O MQTT possui o seu funcionamento resumido à dois tipos de entidades na rede, sendo eles, um *broker* e os clientes. O *broker* é definido como um servidor que

recebe as mensagens dos clientes e as armazena, já o cliente é caracterizado por qualquer dispositivo na rede, sejam eles sensores ou aplicativos que possuam a capacidade de interagir com o *broker* e receber mensagens (YUAN, 2017).

Como as mensagens do protocolo MQTT são classificadas por tópicos, o projeto ganha uma flexibilidade em especificar quais clientes devem possuir acesso para determinados tópicos, e consequentemente mensagens, tornando possível a aplicação de QoS (*Quality of Service*) ou qualidade de serviço por prioridade e acesso.

Figura 19 – Funcionamento do protocolo MQTT



Fonte: Tang (2015)

Para o melhor entendimento, as etapas de comunicação deste protocolo são expressas abaixo e mostradas na figura 19 (YUAN, 2017):

- 1º etapa: O cliente se conecta ao *broker* e pode assinar qualquer tópico de mensagem no *broker*.
- 2º etapa: O cliente publica as mensagens e as atribui a um tópico, enviando estas mensagens ao *broker*.
- 3º etapa: O *broker* encaminha todas as mensagens aos clientes que assinaram determinado tópico.

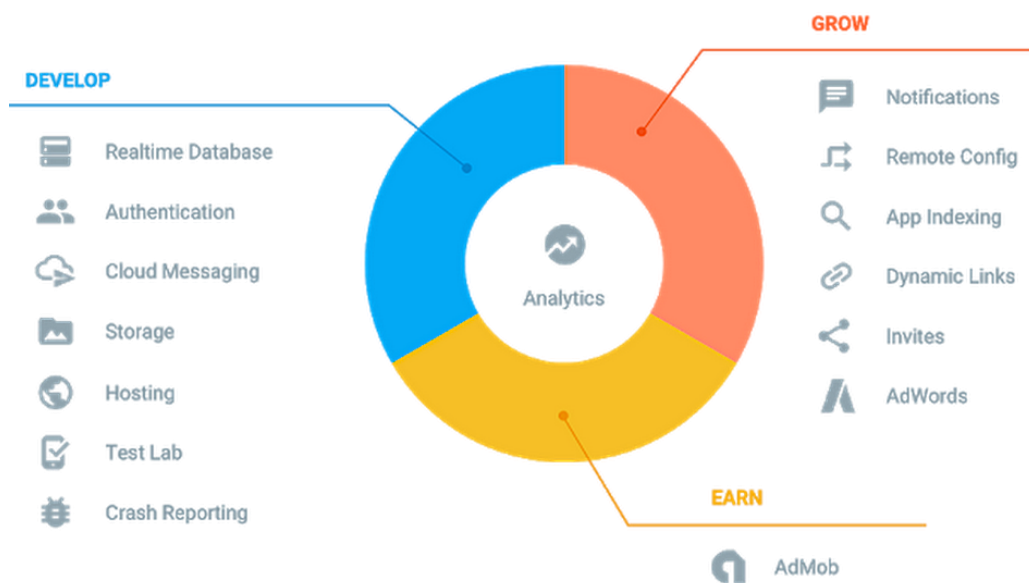
#### 4.1.6 Firebase

O Firebase é uma plataforma da Google que possui uma vasta gama de ferramentas para auxílio no desenvolvimento web e mobile com o intuito de prover

uma melhoria de qualidade e performance para essas soluções. A plataforma, como é mostrado na figura 20, foca em quatro serviços, sendo eles (VIANA, 2017):

- Analytics: visa gerar métricas da aplicação;
- Develop: tem a missão de fornecer a aplicação uma maior qualidade;
- Grow: consiste em recursos para o estímulo de conquistas do usuário para a aplicação;
- Earn: busca o lucro através das aplicações criadas e por meio de anúncios.

Figura 20 – Serviços da plataforma Firebase



Fonte: Fan (2016)

Apesar da plataforma Firebase oferecer tamanha diversidade de serviços para desenvolvimento prático de aplicações, o protótipo desta monografia em questão utiliza apenas a ferramenta Realtime Database, classificado no serviço de *development*.

Figura 21 – Plataforma Firebase



Fonte: Martínez (2018)

A plataforma Firebase Realtime Database é uma base de dados hospedada na nuvem. Os dados armazenados nesta base mantêm o formato JSON (*JavaScript*



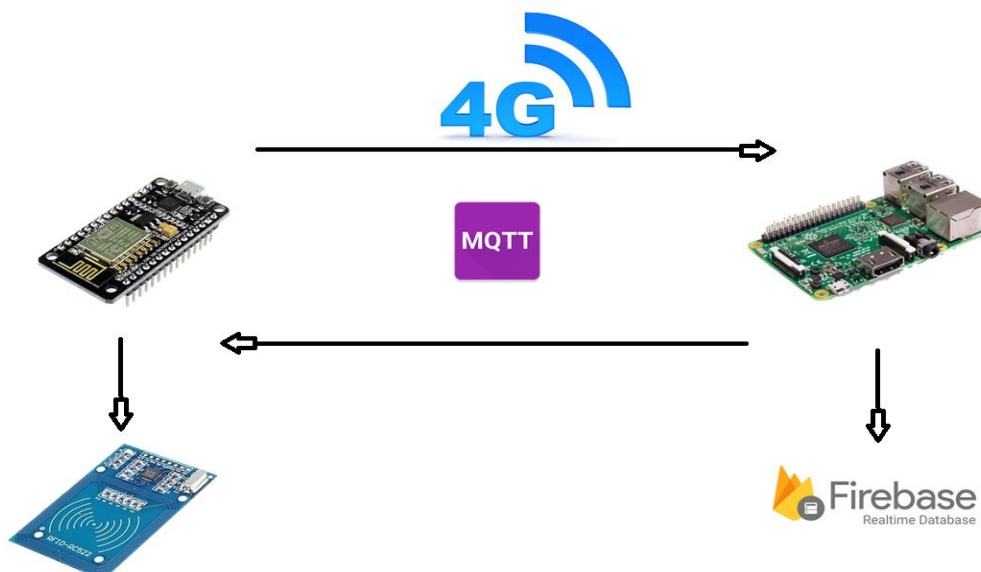
*Object Notation*) e são atualizados e sincronizados em tempo real para com os clientes. Além disso, todos os clientes que utilizam qualquer aplicação vinculada a esta ferramenta, compartilham instâncias e recebem automaticamente atualizações com dados mais recentes (GOOGLE, 2017).

O Firebase Realtime Database também pode ser classificado como um banco de dados NoSQL, ou seja, um modelo de banco de dados não relacional, e por isso conta com funcionalidades especiais. Sua interface de desenvolvimento permite apenas operações que possam ser executadas de forma rápida, melhorando a experiência dos usuários sem comprometer a capacidade de resposta em tempo real da aplicação (GOOGLE, 2017).

#### 4.2 METODO DE DESENVOLVIMENTO

O caso tratado neste tópico consiste em um protótipo de controle de acesso que utiliza o microcomputador Raspberry Pi 3 como principal nó da rede, onde ele recebe as informações dos leitores RFID MFRC522 distribuídos nos pontos desejados, por intermédio de microcontroladores do tipo NodeMcu ESP8266. A transmissão da informação realizada entre o microcontrolador e o microcomputador, utiliza o protocolo MQTT através do Wi-Fi, após a recepção da informação por parte do microcomputador, ele realiza uma consulta na base de dados em nuvem, Firebase, e analisa se o ID da *tag* consultada pelo sensor possui permissão de acesso para a área desejada.

Figura 22 – Esquemático do protótipo



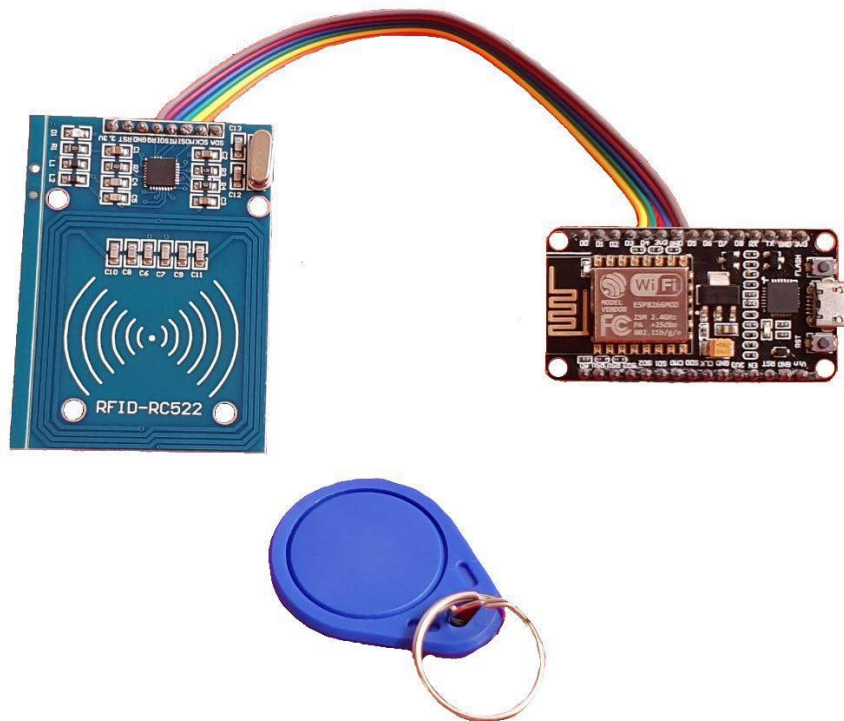
Fonte: Autores (2019)

A utilização da infraestrutura 4G para a comunicação com a rede mundial de computadores tem como objetivo aproximar o teste do protótipo com um cenário de IoT, que contará com a próxima geração de redes móveis 5G como solução de infraestrutura de comunicação.

Para melhor entendimento da prototipação tratada acima, segue a sequência de passos de seu funcionamento:

1. O módulo RFID MFRC522, controlado pelo NodeMcu ESP8266, recebe a leitura de alguma tag a qual tenha sido submetida;

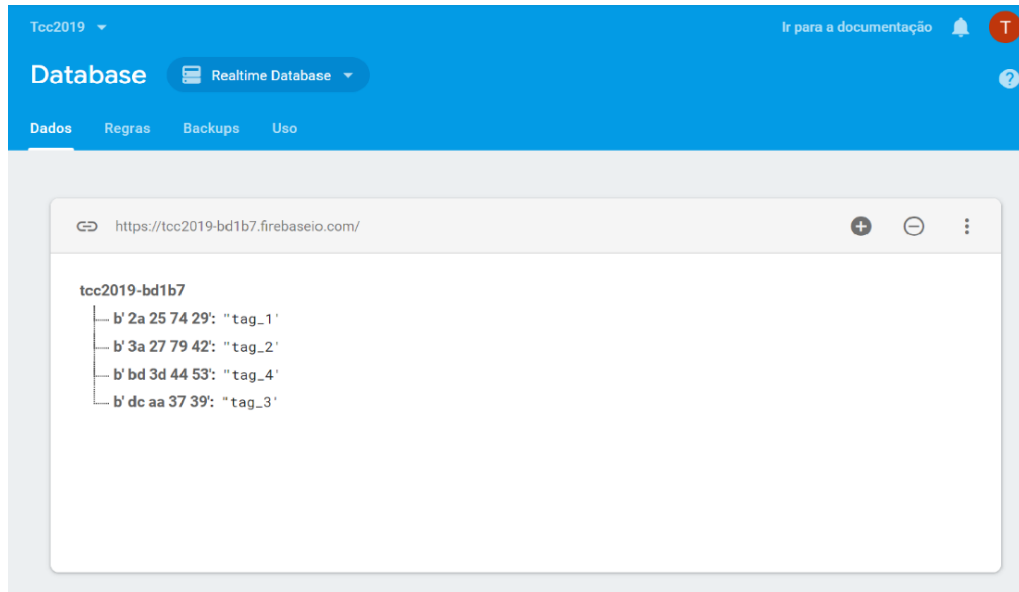
Figura 23 – Controle do MFRC522



**Fonte:** Autores (2019)

2. O NodeMcu ESP8266 por sua vez, utiliza o protocolo MQTT para publicar um tópico na rede, o conteúdo deste tópico é o ID da tag submetida anteriormente ao módulo RFID MFRC522;
3. O Raspberry Pi 3 utilizará o protocolo MQTT para subscrever o tópico que foi publicado na rede e ler seu conteúdo;
4. Depois da leitura do conteúdo do tópico, o Raspberry Pi 3 verifica na base de dados, criada pela ferramenta Firebase Realtime Database, se este ID se encontra presente;

Figura 24 – Firebase Realtime Database



Fonte: Autores (2019)

5. Após a verificação na base de dados, o Raspberry Pi 3 utiliza o protocolo MQTT para publicar um novo tópico a rede, o conteúdo deste tópico será uma resposta da existência do ID anteriormente buscado na base de dados;

Figura 25 – Raspberry Pi 3 utilizando o MQTT

The screenshot shows a terminal window titled '\*Python 3.5.3 Shell\*'. The terminal output is as follows:

```

Python 3.5.3 (default, Sep 27 2018, 17:25:39)
[GCC 6.3.0 20170516] on linux
Type "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: /home/pi/Desktop/linux_RFID_firestore.py =====
conectado!

pergunta Solicitação de Tag: b' 2a 25 74 29'
buscando....

b' 2a 25 74 29' : tag encontrada no banco
acesso autorizado

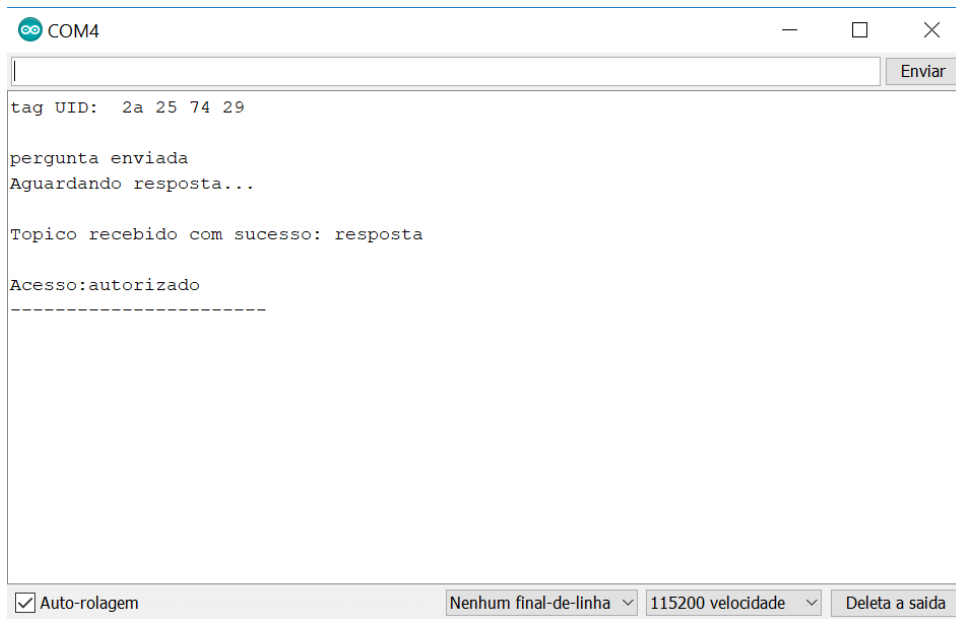
tempo de busca: 1.17
|

```

Fonte: Autores (2019)

6. Na sequência, o NodeMcu ESP8266 usa o protocolo MQTT para subscrever tópico que anteriormente foi publicado pelo Raspberry Pi 3;
7. Por fim, o NodeMcu ESP8266 lê o conteúdo deste último tópico e dependendo da resposta obtida, ele realizará o controle de acesso ou não.

Figura 26 – Controle de acesso



```
tag UID: 2a 25 74 29

pergunta enviada
Aguardando resposta...

Topico recebido com sucesso: resposta

Acesso: autorizado
-----
```

COM4

Enviar

Auto-rolagem    Nenhum final-de-linha    115200 velocidade    Deleta a saída

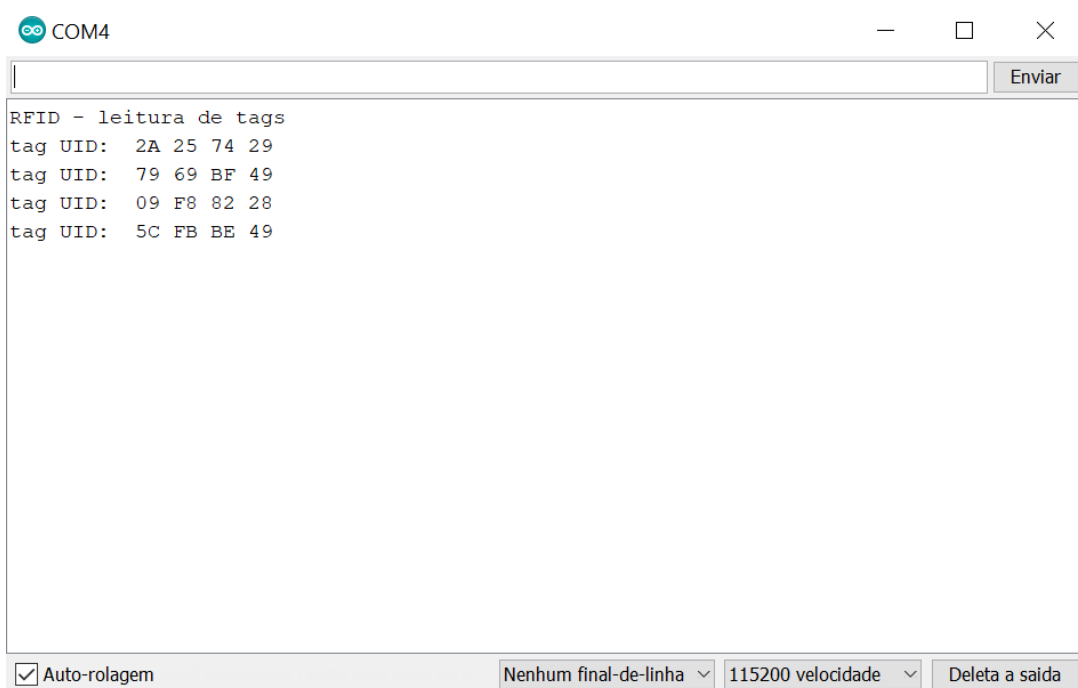
Fonte: Autores (2019)

## 5 RESULTADOS E DISCUSSÕES

Neste capítulo serão apresentados e discutidos os principais resultados obtidos durante a realização do protótipo de um sistema de controle de acesso utilizando RFID. O propósito deste protótipo consiste em autorizar a liberação de acesso de um determinado grupo de pessoas, mediante identificação por meio de *tags* RFID. Após a leitura da *tag* é realizada a verificação na base de dados se a pessoa está autorizada a ingressar no ambiente ou não.

Ao se realizar a leitura da *tag* pelo leitor RFID MFRC522, foi possível verificar que tanto para a leitura de uma *tag*, quanto para quatro *tags*, se obteve o sucesso de identificação da *tag* que se encontrava no raio de leitura, o registro destas leituras está apresentado na figura 27.

Figura 27 – Leitura das *tags*



Fonte: Autores (2019)

A comunicação entre o leitor e a placa Raspberry Pi 3, realizada por intermédio do NodeMCU, utilizou o protocolo de comunicação MQTT. Este protocolo, capaz de viabilizar a troca de informações entre estes sistemas embarcados, permite que ambos os dispositivos possam enviar e receber dados. Sua utilização se provou eficaz após a leitura de diversas *tags*, com a finalidade de enviar diversos tópicos entre o NodeMCU e o Raspberry Pi 3, onde não foram apresentadas falhas na comunicação.

Figura 28 – Recursos computacionais do Raspberry Pi 3

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
863	pi	20	0	58088	32840	12612	S	9.9	3.5	1:36.36	idle3
1714	pi	20	0	61612	33368	11368	S	3.9	3.5	0:09.07	python3
429	root	20	0	36516	25332	15876	S	2.6	2.7	1:33.36	vncserver -x11-c

Fonte: Autores (2019)

Já a utilização da placa Raspberry Pi 3, se mostrou apropriada para este protótipo. Pode-se verificar que durante a execução do protótipo, a utilização de recursos computacionais (memória RAM e processamento) se demonstrou baixa. Na figura 28 é possível ver que a utilização da memória RAM atingiu 3,5% e um processamento de 9,9% para a execução do script do protótipo.

Figura 29 – Tags aprovadas e negadas

```

COM4
tag UID: 09 f8 82 28

pergunta enviada
Aguardando resposta...

Topico recebido com sucesso: resposta

Acesso:autorizado
-----
tag UID: 5c fb be 49

pergunta enviada
Aguardando resposta...

Topico recebido com sucesso: resposta

Acesso:não autorizado
-----

```

Fonte: Autores (2019)

Para verificar a validação, o script utilizado pelo Raspberry PI 3 realizou consultas na base de dados criada através da ferramenta Firebase para verificar a autenticidade das *tags* submetidas. Após a validação, constatou-se que o protótipo como um todo conseguiu realizar a troca de mensagens via MQTT entre os sistemas embarcados e distinguir *tags* que estão cadastradas ou não. Entretanto, é importante ressaltar que ao se tratar da leitura de vários *tags* simultaneamente, o processo de retorno da informação para o NodeMCU apresenta um pequeno tempo de resposta, contudo, o sistema consegue funcionar adequadamente.

## 6 CONCLUSÃO

Este trabalho teve como objetivo compreender o papel da identificação por radiofrequência em um ambiente de Internet das Coisas. Para isso, foram estudados os conceitos da Internet das Coisas, assim como o funcionamento da tecnologia de identificação por rádio frequência. Além disso, analisou-se o papel do RFID dentro da Internet das Coisas através de um protótipo de um sistema de controle de acesso.

A IoT é um novo paradigma da Internet, que demanda conectividade em qualquer lugar, para qualquer pessoa e qualquer coisa. Foi possível verificar que esta nova etapa da Internet trará grandes mudanças, já que está focada na comunicação *machine to machine* e na conexão de milhares de sensores à rede, que irão produzir uma enorme quantidade de dados. Esta nova arquitetura precisa de uma infraestrutura capaz de transmitir dados em alta velocidade e de tecnologias capazes de tratá-los para transformá-los em informação. É justamente neste ponto que o 5G, Big Data, IA e computação em nuvem, responsáveis pela transmissão e o tratamento destes dados, são tidas como a base para a IoT, possibilitando o desenvolvimento de inúmeras soluções, em diversas áreas como varejo, agronegócio, saúde e indústrias.

Outra tecnologia que contribui com o avanço da Internet das Coisas é a identificação por rádio frequência. O RFID tem a capacidade de ser um identificador único para cada objeto, podendo ser lido à distância e permitindo a identificação automática e em tempo real, proporcionando assim, benefícios para diferentes situações que necessitam de uma informação precisa sobre a identificação de cada objeto.

O protótipo de um sistema de controle de acesso, demonstrou na prática, a real importância que a tecnologia RFID agrega ao cenário de Internet das Coisas. O uso das *tags* combinado ao leitor RFID para identificar pessoas, possibilitou que o protótipo alcançasse o controle de acesso com sucesso. Além do mais, a tecnologia de identificação por rádio frequência realizou leituras de forma rápida e precisa, fatores que proporcionam uma maior confiabilidade para a escolha desta tecnologia.

### 6.1 DIFICULDADES ENCONTRADAS

As dificuldades encontradas ao decorrer do desenvolvimento do trabalho foram relacionadas ao domínio de tecnologias, como o protocolo de comunicação MQTT e a ferramenta de computação em nuvem Firebase, utilizados para realizar o protótipo

de controle de acesso. Estas dificuldades foram superadas através da busca de materiais para auxílio no aprendizado sobre estas tecnologias.

## 6.2 TRABALHOS FUTUROS

Com o crescimento da Internet das Coisas, novos modelos de negócios surgirão, possibilitando o desenvolvimento de novas soluções de IoT. Os trabalhos futuros incluem estudos relativos à implantação de uma solução de controle de acesso em um ambiente real, como por exemplo, um dos prédios do CESUPA e ao desenvolvimento de um *software* para realizar o gerenciamento de *tags*, com a finalidade de proporcionar a exclusão, modificação e inclusão de novas *tags* em uma solução de controle de acesso.



## REFERÊNCIAS

- APEKSHA TELECOM. **Radio Network: 4G to 5G**. 2018. Disponível em: <<https://www.apekshatelecom.com/blog/radio-network-4g-to-5g>>. Acesso em 11 de março de 2019.
- ASHTON, Kevin. **That 'Internet of Things' Thing**. 2009. Disponível em: <<https://www.rfidjournal.com/articles/view?4986>>. Acesso em 01 de novembro de 2018.
- AWS. **The Internet of Things With AWS: Connecting the Physical World to the Cloud**. 2018. Disponível em: <<https://aws.amazon.com/pt/iot/>>. Acesso em 06 de novembro de 2018.
- AZODOLMOLKY, Siamak. **SONEP: A Software-Defined Optical Network Emulation Platform**. 2014. Disponível em: <[https://geant3plus.archive.geant.net/opencall/Optical/Documents/MoMOT\\_SONEP\\_SA\\_ONDM2014.pdf](https://geant3plus.archive.geant.net/opencall/Optical/Documents/MoMOT_SONEP_SA_ONDM2014.pdf)>. Acesso em 2 de maio de 2019
- BASHIR, Adil; MIR, Ajaz Hussain. Internet of Things Security Issues, Threats, Attacks and Counter Measures. **International Journal of Computing and Digital Systems**, v. 07, n. 02, p. 111–120, 2018. Disponível em: <<https://journal.uob.edu.bh/handle/123456789/206>>. Acesso em 02 de abril de 2019.
- BORKAR, Suresh; PANDE, Himangi. Application of 5G next generation network to Internet of Things. *In: 2016 International Conference on Internet of Things and Applications (IOTA)*. Pune, India: IEEE, 2016, p. 443–447. Disponível em: <<http://ieeexplore.ieee.org/document/7562769/>>. Acesso em 02 de novembro de 2018.
- BORLIDO, David José Araújo. **Indústria 4.0 – Aplicação a Sistemas de Manutenção**. 2017. Disponível em: <<https://repositorio-aberto.up.pt/bitstream/10216/102740/2/181981.pdf>>. Acesso em 05 de março de 2019.
- CHAMEKH, Marwa *et al.* Security of RFID Based Internet of Things Applications: Requirements and Open Issues. **2018 15th International Multi-conference On Systems, Signals & Devices (ssd)**, [s.l.], p.699-703. 2018. IEEE. Disponível em: <<https://ieeexplore.ieee.org/abstract/document/8570558>>. Acesso em 05 de abril de 2019.
- COELHO, Nuno. *et al.* **Cidades Inteligentes - “Smart Cities”** Infraestrutura tecnológica: caracterização, desafios e tendências. 2015. Disponível em: <[https://paginas.fe.up.pt/~projfeup/submit\\_14\\_15/uploads/relat\\_GI32.pdf](https://paginas.fe.up.pt/~projfeup/submit_14_15/uploads/relat_GI32.pdf)>. Acesso em 29 de março de 2019.
- COLLELA, Paolo. **5G and IoT: Ushering in a new era**. 2017. Disponível em: <<https://www.livemint.com/Opinion/SkctcUSRU6iMQ7BNUknwbFK/5G-and-IoT-Ushering-in-a-new-era.html>>. Acesso em 02 de maio de 2019.

COMSTOR. **Tecnologia 5g e iot: como essas tendências se relacionam?**. 2018. Disponível em: <<https://blogbrasil.comstor.com/tecnologia-5g-e-iot-como-essas-tendencias-se-relacionam>>. Acesso em 11 de março de 2019.

CONTI, Mauro *et al.* Internet of Things security and forensics: Challenges and opportunities. **Future Generation Computer Systems**, [s.l.], v. 78, p.544-546. 2018. Elsevier BV. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S0167739X17316667?via%3Dihub>>. Acesso em 03 de abril de 2019.

CUNHA, Welliton Sousa da. **Qual a relação entre o Big Data e o IoT?**. 2018. Disponível em: <<https://semanaacademica.org.br/artigo/estudo-da-inteligencia-artificial-aplicada-em-Internet-das-coisas-voltada-na-automacao>>. Acesso em 05 de março de 2019.

DIAS, Lia Ribeiro. **A 5G Ainda Não Está Madura, Diz Panos Dallas, da Intracom**. 2018. Disponível em: <<http://www.telesintese.com.br/a-5g-ainda-nao-esta-madura-diz-panos-dallas-da-intracom/>>. Acesso em 03 de novembro de 2018.

EGIDIO, Lucas; UKEI Tiago. **Internet das Coisas (IoT): Uma análise de aplicabilidade**. 2015. Disponível em: <[https://www.researchgate.net/publication/282854616\\_Internet\\_das\\_Coisas\\_IoT\\_Uma\\_analise\\_de\\_aplicabilidade](https://www.researchgate.net/publication/282854616_Internet_das_Coisas_IoT_Uma_analise_de_aplicabilidade)>. Acesso em 05 de março de 2019.

ELGAN, Mike. **Por que o 5G não será tão espetacular quanto parece**. 2018. Disponível em: <<https://computerworld.com.br/2018/10/02/por-que-o-5g-nao-sera-tao-espetacular-quanto-parece/>>. Acesso em 11 de março de 2019.

ERICSSON. **Cellular networks for massive IoT**. 2016. Disponível em: <<https://www.ericsson.com/en/white-papers/cellular-networks-for-massive-iot--enabling-low-power-wide-area-applications>>. Acessado em 08 abril de 2019.

FAN, Alex. **How Using Firebase Can Help You Earn More**. 2016. Disponível em: <<https://www.blog.google/products/admob/how-using-firebase-can-help-you-earn-more/>>. Acesso em 04 de abril de 2019.

FELIX, Waldyr. **Porque investir em Data Science em 2018**. 2018. Disponível em: <<https://waldyrfelix.com.br/porque-investir-em-data-science-em-2018-307da7c69a4>>. Acesso em 31 de março de 2019.

FINKENZELLER, Klaus. **RFID Handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication**. 3. ed. Chichester: Wiley, 2010. 462 p.

GARRETT, Filipe. **Como funciona o Raspberry Pi? Entenda a tecnologia e sua aplicabilidade**. 2014. Disponível em: <<https://www.techtudo.com.br/noticias/noticia/2014/11/como-funciona-o-raspberry-pi-entenda-tecnologia-e-sua-aplicabilidade.html>>. Acesso em 04 de abril de 2019.

GARTNER. **Gartner Identifies Five Emerging Technology Trends That Will Blur the Lines Between Human and Machine**. 2018. Disponível em: <<https://www.gartner.com/en/newsroom/press-releases/2018-08-20-gartner-identifies-five-emerging-technology-trends-that-will-blur-the-lines-between-human-and-machine>>. Acesso em 28 de fevereiro de 2019

GBUR, Felipe. **Módulo RFID RC522 mifare com arduino**. 2017. Disponível em: <<https://portal.vidadesilicio.com.br/modulo-rfid-rc522-mifare/>>. Acesso em 04 de abril de 2019.

GOLD, Jon. **IoT finalmente vai decolar no varejo em 2019?**. 2018. Disponível em: <<https://computerworld.com.br/2018/11/21/iot-finalmente-vai-decolar-no-varejo-em-2019/>>. Acesso em 07 de março de 2019.

GONÇALVES, Claudiana Freitas Botelho. *et al.* **Um estudo sobre a influência da iot no agronegócio a study on the influence of iot on agribusiness**. 2018. Disponível em: <<http://ojs.ciebe.com.br/index.php/GIE-METRO/article/view/2>>. Acesso em 05 de março de 2019.

GOOGLE. **Firestore Realtime Database**. 2017. Disponível em: <<https://firebase.google.com/docs/database/>>. Acesso em 04 de abril de 2019.

HAKIRI, Akram; BERTHOU, Pascal. **Leveraging SDN for The 5G Networks: Trends, Prospects and Challenges**. 2015. Disponível em: <<https://arxiv.org/abs/1506.02876v1>>. Acesso em 2 de maio de 2019

HUNT, V. Daniel; PUGLIA, Albert; PUGLIA, Mike. **RFID-A Guide to Radio Frequency Identification: Hunt/RFID**. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2006. Disponível em: <<http://doi.wiley.com/10.1002/0470112255>>. Acesso em 29 de março de 2019.

IERC. **Internet of Things**. 2014. Disponível em: <[http://www.Internet-of-things-research.eu/about\\_iiot.htm](http://www.Internet-of-things-research.eu/about_iiot.htm)>. Acesso em 01 de novembro de 2018.

ITU-T. **Overview of the Internet of things**. 2012. Disponível em: <<https://www.itu.int/rec/T-REC-Y.2060-201206-I/en>>. Acesso em 18 de março de 2019.

ITU. **IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond**. 2015. Disponível em: <[https://www.itu.int/dms\\_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf](https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf)>. Acesso em 02 de maio de 2019.

JADOUL, Marc. **The Internet of Things Is Human value created when machines talk?**. 2013. Disponível em: <<https://aws.amazon.com/pt/iiot/>>. Acesso em 26 de fevereiro de 2019.

JEAN, Martins. **IA: Conceitos de Inteligência Artificial (Turing, IA Fraca, IA Forte e Sala Chinesa)**. 2018. Disponível em: <<https://medium.com/@jeanfelpemartinsdacosta/ia-conceitos-de->

intelig%C3%A2ncia-artificial-turing-ia-frac-a-ia-forte-e-sala-chinesa-a149849b23a0>. Acesso em 05 de março de 2019.

Ji, Zhanlin; GANCHEV, I.; O'DROMA, M. A Generic IoT Architecture for Smart Cities. *In: 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies*. Limerick, Ireland: Institution of Engineering and Technology, 2014, p. 196–199. Disponível em: <<https://ieeexplore.ieee.org/document/6912755>>. Acesso em 01 novembro de 2018.

JIA, Xiaolin *et al.* RFID technology and its applications in Internet of Things (IoT). **2012 2nd International Conference On Consumer Electronics, Communications And Networks (cecnet)**, [s.l.], p.1282-1285. 2012. IEEE. Disponível em: <<https://ieeexplore.ieee.org/document/6201508>>. Acesso em 20 de março de 2019.

JISK. **RFID: Frequency, standards, adoption and innovation**. 2006. Disponível em: <<https://pdfs.semanticscholar.org/076e/f32f1b378cc92aa557e73058a88b5dda0aae.pdf>>. Acesso em 29 de março de 2019.

KALNOSKAS, Aimee. **How do RFID tags and reader antennas work?**. 2017. Disponível em: <<https://www.analogictips.com/rfid-tag-and-reader-antennas/>>. Acesso em 21 de março de 2019.

KHAN, R. *et al.* Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in: **2012 10th International Conference on Frontiers of Information Technology**, 2012, p. 257–260. Disponível em: <<https://ieeexplore.ieee.org/document/6424332>>. Acesso em 05 de março de 2019.

KHOO, Benjamin. RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. *In: 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. Dalian, China: IEEE, 2011, p. 709–712. Disponível em: <<http://ieeexplore.ieee.org/document/6142169/>>. Acesso em 03 de novembro de 2018.

KON, Fabio; ZAMBOM, Eduardo. Cidades Inteligentes: Tecnologias, Aplicações, Iniciativas e Desafios. In: MALDONADO, Jose Carlos *et al.* **Jornadas de Atualização em Informática 2016**. 1. ed. Porto Alegre: Sociedade Brasileira de Computação (sbc), 2016. Cap. 1. p. 13-60. Disponível em: <<https://doi.org/10.5753/sbc.6>>. Acesso em 05 de março de 2019.

KUROSE, Jim; ROSS, Keith. **Redes de computadores e a Internet: uma abordagem Top-Down**. 5 ed. São Paulo: Pearson, 2010. 614 p.

LANDT, Jeremy. The history of RFID. **IEEE Potentials**, [s.l.], v. 24, n. 4, p.8-11. 2005. IEEE. Institute of Electrical and Electronics Engineers (IEEE). Disponível em: <<https://ieeexplore.ieee.org/document/1549751>>. Acesso em 14 de março de 2019.

MARR, Bernard. **Disney Uses Big Data, IoT And Machine Learning To Boost Customer Experience**. 2017. Disponível em: <<https://www.forbes.com/sites/bernardmarr/2017/08/24/disney-uses-big-data-iot-and-machine-learning-to-boost-customer-experience/#7683405b3387>>. Acesso em 03 de novembro de 2018.

MARTÍNEZ, Pablo. **Lessons learnt (the hard way) using Firebase RealTime Database**. 2018. Disponível em: <<https://pamartinezandres.com/lessons-learnt-the-hard-way-using-firebase-realtime-database-c609b52b9afb>> Acesso em 04 de novembro de 2018.

MARTINS, Helena. **Governo Espera que Internet das Coisas Aporte US\$ 50 Bi na Economia**. 2017. Disponível em: <<http://agenciabrasil.ebc.com.br/pesquisa-e-inovacao/noticia/2017-09/governo-espera-que-Internet-das-coisas-aporte-us-50-bi-na>> Acesso em 04 de novembro de 2018.

MATOS, Lucio. **Quando a Inteligência Artificial se conecta à Internet das Coisas**. 2016. Disponível em: <<https://computerworld.com.br/2016/11/04/momento-da-intersecao-entre-inteligencia-artificial-e-Internet-das-coisas/>>. Acesso em 02 de março de 2019.

MONTEIRO, Ivan. **RFID: As vantagens e desvantagens dessa tecnologia**. 2018. Disponível em: <<http://www.gtpautomation.com/2018/07/31/rfid-as-vantagens-e-desvantagens-dessa-tecnologia/>>. Acesso em 17 de março de 2019.

NASCIMENTO, Rodrigo. **Afinal, o que é Big Data?**. 2017. Disponível em: <<http://marketingpordados.com/analise-de-dados/o-que-e-big-data-%F0%9F%A4%96/>>. Acesso em 31 de março de 2019.

NXP. **Standard performance MIFARE and NTAG frontend**. 2016. Disponível em: <<https://www.nxp.com/docs/en/data-sheet/MFRC522.pdf>>. Acesso em 04 de abril de 2019.

OLIVEIRA, Deborah. **Com AI, 5G, big data e IoT, possibilidades de conectividade são infinitas**. 2019. Disponível em: <<https://computerworld.com.br/2019/02/25/com-ai-5g-big-data-e-iot-possibilidades-de-conectividade-sao-infinitas/>>. Acesso em 11 de março de 2019.

OLIVEIRA, Greici. **NodeMCU – Uma plataforma com características singulares para o seu projeto IoT**. 2017. Disponível em: <<http://blogmasterwalkershop.com.br/embarcados/nodemcu/nodemcu-uma-plataforma-com-caracteristicas-singulares-para-o-seu-projeto-iot/>>. Acesso em 04 de abril de 2019.

PALATTELLA, Maria Rita. *et al.* Internet of Things in the 5G Era: Enablers, Architecture, and Business Models. **IEEE Journal on Selected Areas in Communications**, v. 34, n. 3, p. 510–527, 2016. Disponível em: <<https://ieeexplore.ieee.org/document/7397856/>>. Acesso em 03 de novembro de 2018.

PINHEIRO, José Mauricio dos Santos. **RFID: O fim das filas está próximo?**. 2006. Disponível em: <<http://www.teleco.com.br/tutoriais/tutorialrfid2/default.asp>>. Acesso em 20 de março de 2019.

PRETZ, Kathy. **5G: The Future of Communications Networks**. 2018. Disponível em: <<https://spectrum.ieee.org/the-institute/ieee-products-services/5g-the-future-of-communications-networks>>. Acesso em 02 de maio de 2019.

PUTHAL, D; *et al.* Cloud Computing Features, Issues, and Challenges: A Big Picture. In: **2015 International Conference on Computational Intelligence and Networks**. 2015, p. 116–123. Disponível em: <<https://ieeexplore.ieee.org/document/7053814>>. Acesso em 30 de março de 2019.

RASPBERRYPI. **Raspberry Pi 3 Model B**. 2016. Disponível em: <<https://www.raspberrypi.org/products/raspberry-pi-3-model-b/>>. Acesso em 04 de abril de 2019.

REIS, Carlos. **IoT na Saúde: o futuro já chegou**. 2018. Disponível em: <<https://www.revistaapolice.com.br/2018/12/iot-na-saude-o-futuro-ja-chegou/>>. Acesso em 07 de março de 2019.

ROBERTI, Mark. **Quais são as classes e geração de tags RFID?**. 2010. Disponível em: <<https://www.rfidjournal.com/blogs/experts/entry?8049>>. Acesso em 20 de março de 2019.

RODRIGUES, Alex; BORGES, Eduardo Nudes; BARWALDT, Regina. **Um estudo sobre o comportamento alimentar de frangos de corte utilizando a mineração de dados**. 2017. Disponível em: <<https://www.scienciaplena.org.br/sp/article/view/3733>>. Acesso em 20 de março de 2019.

ROMANO, Matheus. **Entenda o que é IoT na indústria 4.0 e porque isso é uma aposta que vai revolucionar o mercado industrial**. 2017. Disponível em: <<https://www.logiquesistemas.com.br/blog/iot-na-industria-4-0/>>. Acesso em 07 de março de 2019.

ROTTA, Giovanni; CHARÃO, Andrea; DANTAS, Mario. **Um Estudo sobre Protocolos de Comunicação para Ambientes ~ de Internet das Coisas**. 2017. Disponível em: <<http://www.lbd.dcc.ufmg.br/colecoes/erad/2017/091.pdf>>. Acesso em 17 de março de 2019.

SANTOS, Bruno P. *et al.* Internet das Coisas: da Teoria à Prática. In: SIQUEIRA, Frank Augusto *et al.* **Minicursos / XXXIV Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. 34. ed. Salvador: Sociedade Brasileira de Computação (sbc), 2016. Cap. 1. p. 1-50. Disponível em: <<https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/Internet-das-coisas.pdf>>. Acesso em 01 de novembro de 2018.

SAPHIR. **Internet das coisas e cloud computing: como se relacionam?**. 2018. Disponível em: <<https://blog.saphir.com.br/Internet-das-coisas-e-cloud-computing/>>. Acesso em 05 de março de 2019.

SPRUIT, Marco; WESTER, Wouter. **RFID Security and Privacy: Threats and Countermeasures**. 2013. Disponível em: <<http://www.cs.uu.nl/research/techreps/repo/CS-2013/2013-001.pdf>>. Acesso em 02 de abril de 2019.

TANG, Chun Bin. **Explore o MQTT e o serviço de Internet of Things no IBM Cloud**. 2015. Disponível em: <<https://www.ibm.com/developerworks/br/cloud/library/cl-mqtt-bluemix-iot-node-red-app/index.html>>. Acesso em 04 de abril de 2019.

VELEZ, Jose. **Como a IA e o machine learning estão moldando o cenário de pagamentos**. 2018. Disponível em: <<https://www.ecommercebrasil.com.br/artigos/inteligencia-artificial-e-machine-learning-moldando-os-pagamentos/>>. Acesso em 01 de março de 2019.

VIANA, Daniel. **Firebase: descubra no que esta plataforma pode te ajudar**. 2017. Disponível em: <<https://www.treinaweb.com.br/blog/firebase-descubra-no-que-esta-plataforma-pode-te-ajudar/>>. Acesso em 04 de abril de 2019.

VIDAL, Vitor. **10 protocolos de IoT que você deveria conhecer**. 2017. Disponível em: <<https://www.professionaisti.com.br/2017/11/10-protocolos-de-iot-que-voce-deveria-conhecer/>>. Acesso em 17 de março de 2019.

VORTICE. **Afinal, o que é e como funciona o Cloud Computing?**. 2017. Disponível em: <<http://blog.vortice.inf.br/afinal-o-que-e-e-como-funciona-o-cloud-computing/>>. Acesso em 05 de março de 2019.

WEBLE. **Licence MQTT**. 2018. Disponível em: <<https://www.weble.ch/produit/licence-mqtt/>> Acesso em 04 de novembro de 2018.

WOLLINGER, Leonardo Martins. **Monitoramento de grãos: uma aplicação de iot no agronegócio**. 2018. 82 f. TCC (Graduação) - Curso de Engenharia Elétrica e Eletrônica, Universidade Federal de Santa Catarina, Florianópolis, 2018. Disponível em: <<https://repositorio.ufsc.br/bitstream/handle/123456789/192684/TCC-Leonardo-Wollinger.pdf?sequence=1&isAllowed=y.com>>. Acesso em 07 de março de 2019.

YUAN, Michael. **Conhecendo o MQTT**. 2017. Disponível em: <<https://www.ibm.com/developerworks/br/library/iot-mqtt-why-good-for-iot/index.html>>. Acesso em 04 de abril de 2019.