UNIVERSIDADE FEDERAL DE OURO PRETO
ESCOLA DE MINAS
COLEGIADO DO CURSO DE ENGENHARIA DE CONTROLE E AUTOMAÇÃO - CECAU

DANIELLE SILVA CARDOSO

ASPECTOS ATUAIS DA IOT: CARACTERÍSTICAS E DESAFIOS

MONOGRAFIA DE GRADUAÇÃO EM ENGENHARIA DE CONTROLE E AUTOMAÇÃO

Ouro Preto, 2019

DANIELLE SILVA CARDOSO

ASPECTOS ATUAIS DA IOT: CARACTERÍSTICAS E DESAFIOS

Monografia apresentada ao Curso de Engenharia de Controle e Automação da Universidade Federal de Ouro Preto como parte dos requisitos para a obtenção do Grau de Engenheira de Controle e Automação.

Orientador: Prof. Dr. Agnaldo Jose da Rocha Reis.

FOLHA DE APROVAÇÃO

A comissão avaliadora constituída pelos professores Agnaldo José da Rocha Reis, Adrielle de Carvalho Santana e Alan Kardek Rego Segundo atesta que a monografia intitulada "Aspectos Atuais da IoT: Características e Desafios" foi defendida e aprovada em 19 de dezembro de 2019.

Prof. Dr. Agnaldo José da Rocha Reis – Orientador

Profa. Me. Adrielle de Carvalho Santana – Professora Convidada

Prof. Dr. Alan Kardek Rego Segundo – Professor Convidado

“Descobrir consiste em olhar para o que todo mundo está vendo e pensar uma coisa diferente”. (Roger Von Oech)

AGRADECIMENTOS

Chega ao fim de mais um ciclo da minha vida. Agradeço primeiramente a Deus pela vida e por sempre ter iluminado meu caminho. Aos meus pais Angela e Ronam, aos meus irmãos Maycon e Shayene pelo apoio e pelo incentivo durante todos esses anos.

Ao meu namorado Hélcio por toda paciência e ajuda durante a minha graduação. A todos os meus amigos que se fizeram presente nessa longa caminhada da minha vida.

A todos os professores, por todos os conselhos e ensinamentos durante o curso, principalmente ao meu professor orientador Agnaldo, por toda ajuda e empenho dedicado ao meu trabalho final.

Enfim, a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigada.

RESUMO

Atualmente estar conectado à Internet é muito mais do que uma simples conectividade e transporte de mensagens e dados. Com o rápido avanço da tecnologia, a Internet comum evolui para Internet das Coisas, tendo assim uma nova fase mais completa, inteligente e robusta. A Internet das Coisas é uma das áreas mais importantes na evolução da tecnologia, pois permite a interação de equipamentos com sensores e atuadores conectados na rede, tornando-os dispositivos inteligentes. Uma das melhores aplicações dentro dessa tecnologia é no setor residencial, conhecida por Automação Residencial ou Domótica, que deixa a casa conectada e o usuário consegue realizar o controle de dispositivos de qualquer lugar do mundo por meio de um smartphone, tablet ou similar, conectado ao aparelho e à Internet. Neste trabalho, além de se apresentar conceitos sobre Domótica e Internet das Coisas de forma simples e clara, trata-se também dos protocolos mais relevantes usados e apresenta as possíveis falhas desses sistemas, bem como os modos de prevenções contra os problemas encontrados.

Palavras-chaves: Internet das coisas. Domótica. Falhas. Proteção.

ABSTRACT

Today being connected to the Internet is much more than just connectivity and messaging and data transport. With the rapid advancement of technology, the common Internet evolves into the Internet of Things, thus having a new, more complete, intelligent and robust phase. The Internet of Things is one of the most important areas in the evolution of technology, as it allows equipment to interact with sensors and actuators connected to the network, making them intelligent devices. One of the best applications within this technology is in the residential sector, known as Home Automation or Home Automation, which leaves the home connected and the user can control devices from anywhere in the world through a smartphone, tablet or similar, connected to the home device and the Internet. In this paper, in addition to presenting concepts on Home Automation and Internet of Things in a simple and clear way, it is also the most relevant protocols used and presents the possible failures of these systems, as well as ways to prevent problems encountered.

Key-words: Internet of Things. Home Automation. Failures. Protection.

LISTAS DE ILUSTRAÇÕES

LISTAS DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

IoT - Internet of Things

CEBUS - Consumer Electronic Bus

EIA - Associação de Indústrias Eletrônicas

LON - Local Operating Network

EIB - European Installation Bus

EIBA - European Installation Bus Association

NIC. br - Núcleo de Informação e Coordenação do Ponto BR

IA - Inteligência Artificial

LoRaWAN - Long Range Wide Area Network

UNB - Ultra Narrow Band

SAS - Analytics Software & Solutions

VPN - Rede Virtual Privada

SUMÁRIO

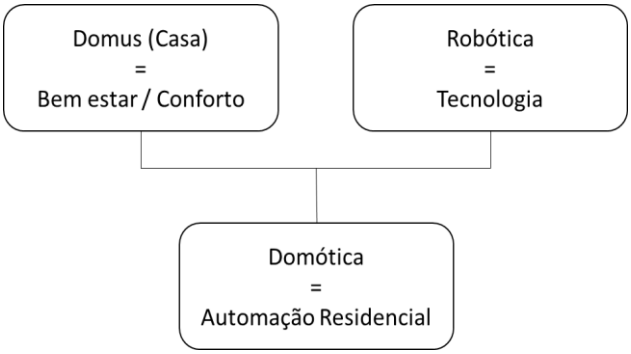
1 INTRODUÇÃO

Com o avanço da tecnologia, os sistemas automatizados de controle estão cada vez mais presentes no nosso dia-a-dia. Esses avanços tecnológicos, associados à procura por mais conforto e acessibilidade para os usuários, faz com que haja cada vez mais sistemas automáticos. Esses sistemas, por meio de sensores e comandos pré-estabelecidos, são capazes de detectar acontecimentos fora do padrão e realizar medidas para correção de maneira automática.

Muitas dessas tecnologias são desenvolvidas na Internet das Coisas (IoT – *Internet of Things*), onde uma rede de objetos físicos interligados por meio da internet adquire uma identidade no mundo digital. “A IoT representa a primeira evolução real da Internet, tendo um grande avanço na capacidade de coletar, analisar e distribuir dados. Ela representa um avanço que levará ao uso de aplicações revolucionárias.” (EVANS, 2011).

Com a evolução da internet na IoT, surgiram os sistemas de automação residencial, conhecida também como domótica, que é a derivação das palavras domus (casa) e robótica (controle automatizado). Na Figura 1, pode-se observar um esquema dessa derivação, na qual representa um processo que, obtendo diferentes soluções e equipamentos, possibilita ao usuário usufruir ao máximo a qualidade de vida em sua casa.

Figura1: Definição de Domótica



Entretanto, a maioria das pessoas ainda não acredita ou confia em uma residência que realiza ações automáticas, como por exemplo, as janelas se fecharem automaticamente quando está chovendo ou em cortinas que controlam a sua abertura de acordo com a

luminosidade do dia ou até mesmo a realização do controle de toda temperatura e luz por meio de um aplicativo, necessitando apenas de uma comunicação com a internet.

Apesar da aplicação da IoT na domótica trazer muitos benefícios para os usuários, facilitando o seu cotidiano, ainda existem muitas falhas dentro desse tipo de sistema. Dentre essas falhas, pode-se citar a vulnerabilidade no acesso, em que torna o acesso aos dados mais fáceis.

1.1 Objetivos gerais e específicos

O objetivo geral desta pesquisa é realizar um estudo sobre o avanço da tecnologia de aplicação da IoT, principalmente no setor da domótica, apontando as falhas de segurança ainda existentes nesse tipo de sistema, e possíveis conflitos que poderão surgir, de modo a apresentar o conteúdo de maneira simples e construtiva, agregando assim a utilização da IoT na domótica, minimizando o conflito de ideias existentes sobre o tema e demonstrando maneiras de prevenções ao uso dessa tecnologia.

Os objetivos específicos deste trabalho são:

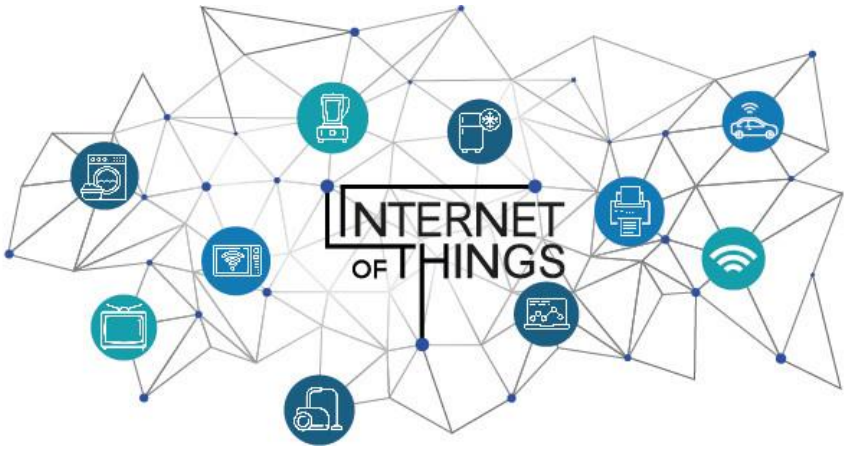
- Descrever os conceitos de Domótica e IoT, e suas aplicações;
- Mostrar o avanço da IoT em múltiplas áreas do cotidiano;
- Realizar o estudo dos riscos da aplicação da IoT dentro da Domótica;
- Apontar possíveis soluções para os problemas encontrados.

1.2 Justificativa do trabalho

A rápida melhoria na tecnologia pela busca de bem-estar e segurança com o uso da internet faz com que cada dia mais as casas e empresas tenham sistemas embarcados com funções automáticas. “Um dos objetivos da IoT é revolucionar a maneira como vivemos e trabalhamos, pois a evolução desses dispositivos está cada vez mais ligada as nossas rotinas” (RAZA; KULKARNI; SOORIYABANDARA, 2017). Muitos desses avanços tecnológicos acontecem principalmente na área da automação residencial.

No Brasil, o cenário da automação residencial está cada vez mais presente no dia a dia da sociedade, pois o cotidiano do brasileiro está se tornando cada vez mais corrido e com menos tempo para administrar os afazeres da casa. Sendo assim, a possibilidade de gerenciar determinadas atividades, como é apresentado na Figura 2, deixa de ser uma ostentação e passa a ser uma necessidade. Com a implantação da Domótica, o usuário consegue minimizar os custos residenciais e otimizar seu tempo com as tarefas a serem realizadas.

Figura2: Funções Domésticas com a IoT



Fonte: SEMPREUPDATE, 2019.

Apesar da Domótica trazer muitos benefícios e confortos aos usuários, ainda existem muitas falhas e conflitos nesse tipo de sistema, principalmente quando se é aplicada inteligência aos eletrodomésticos. Por ser um cenário complexo e possuir muitas opções, esse assunto faz jus de ter um estudo descritivo para informar aos leitores como esta tecnologia irá mudar suas vidas e como poderão se prevenir das falhas existentes nesse sistema.

1.3 Metodologia

Para o desenvolvimento do presente trabalho foram desenvolvidas as seguintes etapas:

- Levantamento Bibliográfico: Inicialmente foi realizado o levantamento teórico e análise bibliográfica. Para tanto, foram utilizados artigos, livros e monografias existentes sobre a

automação residencial e sobre a utilização da IoT. Após a compreensão sobre o tema, foi realizada a pesquisa sobre as falhas existentes nesses sistemas e possíveis soluções.

- Estudo dos Equipamentos e Aplicações na área: com ênfase nas aplicações oferecidas pela IoT, principalmente na área da Domótica.

- Montagem do trabalho: Por fim, a escrita do trabalho foi desenvolvida, de maneira clara, buscando deixar de fácil entendimento o assunto abordado. São apresentandas aplicações para o sistema, as falhas existentes e possíveis soluções para os problemas enfrentados.

1.4 Estrutura do trabalho

O presente trabalho está dividido em 5 capítulos, sendo:

Capítulo 1 – Introdução: exposição do tema, os objetivos gerais e específicos do trabalho, a justificativa da escolha do tema, os procedimentos metodológicos usados e a estrutura do trabalho.

Capítulo 2 – Revisão da Literatura: são apresentados os conceitos relevantes para a execução do trabalho, juntamente com um estudo teórico dos protocolos existentes. Assim como um estudo dos equipamentos existentes no mercado.

Capítulo 3 – Falhas Existentes na Domótica com a IoT: são abordadas as falhas existentes dentro da Domótica com a utilização da IoT.

Capítulo 4 – Soluções Para os Problemas Encontrados: tendo como base as falhas existentes no sistema. Neste capítulo foram desenvolvidas as possíveis soluções para os problemas encontrados.

Capítulo 5 – Considerações Finais: As análises finais do trabalho de conclusão de curso são apresentadas nesse capítulo.

2 REVISÃO DA LITERATURA

Neste capítulo é abordada a revisão dos principais conceitos relevantes para o entendimento das tecnologias relacionadas deste trabalho, sendo organizado em seções que mencionam cada conceito separadamente.

2.1 Domótica

De acordo com Adami (2014), o termo Domótica surgiu na França em meados do século passado, e por volta dos anos 80 deu-se início a utilização desse sistema nas construções dos edifícios, por busca de controle e interação das funções de iluminação, climatização e segurança dos novos prédios construídos. Dessa forma, podemos compreender a domótica como uma rede que toma ações de forma digital e autônoma, de maneira a acomodar as necessidades dos usuários.

O uso de sistemas embarcados, juntamente com a tecnologia, integrará e controlará múltiplos equipamentos de uma residência, tornando-a inteligente. Porém, para a instalação e aplicação de um sistema domótico será necessário à preparação de um projeto de automação residencial, no qual será realizado o levantamento de todos os pontos eletrônicos do lugar a ser implementado.

Para tais sistemas, de acordo com a empresa de integração dos sistemas Sislite (2019), podem-se fazer acessos de duas formas distintas:

- Domótica Passivo – no funcionamento passivo um elemento do sistema só será ativado se ocorrer uma interação de ordem. Esta ordem pode ser passada pelo usuário, por meio de um interruptor, ou por um comando, como é apresentado na Figura 3, podendo ser dada uma ou mais ordens instantâneas, utilizando-se de um aparelho ou de um aplicativo.

Figura3: Domótica Passivo

Fonte: SENTIDO DIGITAL, 2019.

- Domótica Automático - no funcionamento automático, que é um método mais avançado e tecnológico, o sistema é constituído por sensores que são capazes de interpretar parâmetros e reagir às circunstâncias passadas, de acordo com a transmissão de seu sinal do sensor. Como por exemplo, detectar que a temperatura da residência está abaixo do desejado, e automaticamente realizar o acionamento do aquecimento no cômodo desejado, ou então fazer o controle automático da iluminação da casa de acordo com a luminosidade passada pelas janelas. Na Figura 4 possui uma representação de tal funcionamento.

Figura4: Domótica Automática

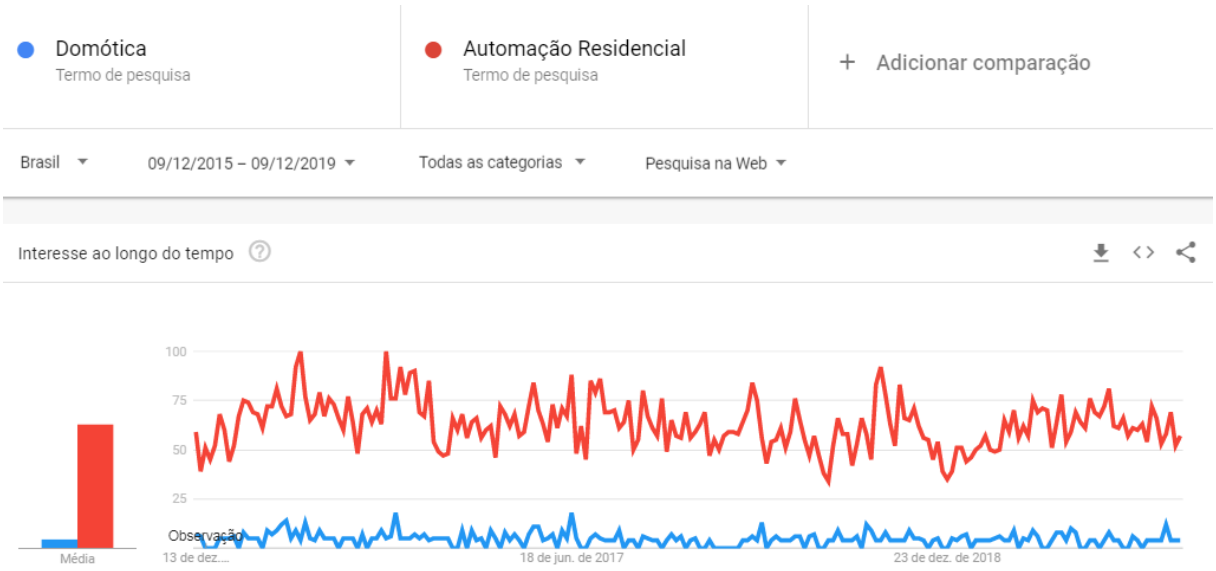
Fonte: SISLITE, 2019.

É possível perceber que a utilização da Domótica vem crescendo no mercado, principalmente no Brasil, pois cada dia mais os usuários buscam pelas soluções para automatizar as residências. Nas Figuras 5 e 6, poderá visualizar melhor esse crescimento pelas buscas da automatização pelo mundo e no Brasil, neste ano de 2019.

Figura 5: Crescimento da busca da automatização no mundo

Fonte: GOOGLE TRENDS, 2019.

Figura 6: Crescimento de busca da automatização no Brasil



Fonte: GOOGLE TRENDS, 2019.

2.1.1 Protocolos de Comunicação da Domótica

Com a constante evolução da domótica na sociedade, teve-se o desenvolvimento da comunicação entre controladores e dispositivos. Com esse avanço e para esse tipo de sistema, poderá dividir em três tipos as redes de comunicação, que segundo Mizusaki (2009).

- **Rede elétrica** – nesse tipo de comunicação, também conhecida como Powerline, é utilizada a própria instalação da casa para o funcionamento do sistema domótico, de maneira que tenha menor impacto na alteração física da instalação.
- **Rede Cabeada** – enquanto neste tipo de comunicação, assim como o nome sugere, para sua instalação será necessário cabos para o funcionamento do sistema de automação residencial. Por necessitar de cabos para realizar toda a ligação, esse tipo de comunicação se torna mais cara.
- **Rede sem fio** – mas conhecido como rede Wireless, esse tipo de comunicação consiste em uma transferência de dados de modo livre, sem o uso de um cabo conectado a ele, conectando a equipamentos de modo.

Na Figura 7, pode-se ver um sistema com a utilização das três redes com a Domótica, onde as linhas pontilhadas representam a rede elétrica, as linhas contínuas em cinza representam à rede cabeada e os sinais verdes a rede sem fio:

Figura 7: Utilização das redes com a Domótica

Fonte: PLCWIFI. NET, 2019.

Além dos três tipos de protocolos de rede apresentados, existe também a classificação por abertura em relação as suas comunicações, de acordo com Alves; Mota (2003):

- **Protocolos Fechados** – nesse tipo de protocolo os sistemas desenvolvidos pela empresa, são utilizados em regime exclusivo, ou seja, a venda dos equipamentos, serviços ofertados e o desenvolvimento podem ser realizados apenas pela entidade.

- **Protocolos Abertos** – no protocolo aberto, o desenvolvimento dos sistemas são realizados por diferentes entidades, tendo múltiplos fornecedores. Sendo assim, é mais fácil o avanço da tecnologia, pois permite que o desenvolvimento do protocolo seja por meio dos progressos realizados de cada fabricante.

A escolha de protocolos de comunicação é uma parte muito importante do projeto, pois determina o conjunto de regras, padrões e realiza a transmissão e o recebimento das informações do sistema. Existem diferentes protocolos de comunicação que se aplicam na automação residencial. No presente trabalho são apresentados os protocolos mais comercializados e vendidos atualmente, que conforme Gonçalves (2017) são:

- **X10** – criada em 1975, pela empresa Escocesa Pico Eletronics, é o protocolo mais antigo da área da domótica e um dos mais utilizados pela facilidade de instalação e pelo baixo custo de aquisição. O X10 é um protocolo de comunicação aberta, e realiza o controle dos aparelhos domésticos e da luz através da própria instalação elétrica da casa. Para seu funcionamento é usado um transmissor, que transmite comandos (liga / desliga), através do acionamento do botão que passa o controle a ser feito para um receptor, que será um módulo conectado na tomada (rede elétrica da residência) e por fim sensores receberão o comando, identificarão e ajustarão o comando solicitado, realizando assim a tarefa.

- **CEBUS** – o protocolo CEBUS (Consumer Electronic Bus) começou a ser desenvolvido em 1984 pela associação EIA (Associação de Indústrias Eletrônicas) e só se tornou um padrão internacional em 1995, consiste em uma arquitetura aberta e sua comunicação é realizada por meio de diversas redes. Podendo ser rede elétrica, rede cabeada e por comunicações infravermelhos e rádio frequência.

- **LONWORKS** – conhecido também por LON (Local Operating Network) foi desenvolvida na década de 90 pela empresa norte-americana Echelon Corp. Sua comunicação pode ser realizada por rede elétrica ou por rede cabeada, além de conseguir conexão com a internet. Por ter um custo alto de aquisição, não é recomendado à utilização para residências, tendo em vista que outros protocolos realizam as mesmas tarefas de forma mais barata. Seu funcionamento é feito por dispositivos de controle (microcontroladores) que comunicam entre si. Esses dispositivos interligados são sensores ligados nos sistemas e recebem o nome de nós. Esses nós recebem a transmissão do meio físico, através de uma interface que fica ligada nos dispositivos de entrada e saída (I/O), que é a representação dos aparelhos. O sinal recebido nesta ligação é transmitido ao atuador que realiza a ação da tarefa.

- **INSTEON –** Insteon é um protocolo feito para Domótica que consegue realizar o controle local e remoto, como: controle da iluminação, persianas, abertura de portas e portões, climatização, entre outros, esses são algumas de suas principais aplicações. Sua comunicação é feita através da rede elétrica ou via rádio. Esse protocolo possibilita o controlo de elaborados cenários para todo o tipo de aplicações domésticas.

- **EIB/KNX** – O protocolo EIB (European Installation) foi desenvolvido pela empresa European Installation Bus Association (EIBA), localizada em Bruxelas. O protocolo EIB realiza sua comunicação através da rede cabeada. Baseada numa arquitetura descentralizada o EIB define uma relação elemento a elemento entre os dispositivos, onde realiza a distribuição entre os sensores e atuadores instalados.

- **Z-WAVE –** O protocolo Z-WAVE foi desenvolvido pela empresa Dinamarquesa Zen-Sys, é um dos mais usados na automação residencial por controlar remotamente os aparelhos e equipamentos por meio de comunicação sem fio (*Wireless*), de maneira fácil e organizada. Não precisa de nenhum outro tipo de dispositivo para haver comunicação entre si, além de ter um preço acessível no mercado. Para o funcionamento do aparelho ou equipamento, basta apenas realizar a ligação dele no protocolo, pois ele já possui todas as ações pré-definidas no dispositivo.

- **ZIGBEE** – O protocolo ZigBee foi desenvolvido pela empresa Norte Americana ZigBee Alliance, é uma comunicação sem fio e um dos mais recentes protocolos criados. Ele permite que os dispositivos se comuniquem entre si sem o uso de um roteador,

compartilhando diretamente com o aparelho do protocolo. Com essa comunicação, ele permite o controle remoto de aparelhos domésticos extinguindo o uso de cabos, e com isso deixando a utilização mais prática desses equipamentos pelos usuários.

Na Tabela 1 é apresentado um comparativo entre os protocolos descritos, para demonstrar a diferença entre os preços dentro do mercado e a facilidade na sua instalação. O ícone "○" representa a facilidade e melhor preço para aquisição do protocolo em questão:

Tabela 1 – Comparativo dos Protocolos da Domótica

PROTOCOLO	INSTALAÇÃO	PREÇO
X – 10	○ ○ ○ ○ ○	○ ○ ○ ○ ○
CEBUS	○ ○	○ ○
LONWORKS	○ ○	○ ○
INSTEON	○ ○ ○ ○	○ ○ ○ ○
EIB / KNX	○ ○	○ ○
Z-WAVE	○ ○ ○ ○	○ ○ ○ ○
ZIGBEE	○ ○	○ ○ ○

Fonte: GONÇALVES, 2017

Com a finalidade de conseguir mais visualização e implementação dos sistemas de domótica, já existem projetos que conseguem usar simultaneamente dois tipos de protocolos de comunicação.

2.2 IoT – INTERNET OF THINGS

O termo Internet das Coisas vem da tradução de *Internet of Things*, também conhecida como internet dos objetos. Esse conceito surgiu com as melhorias de diversas áreas como sistemas embarcados, sensoriamento e microeletrônica. Essa tecnologia interliga equipamentos das rotinas diárias que estarão conectados na internet realizando a comunicação entre eles. "A Internet das Coisas é algo que obtemos quando conectamos as coisas, não operadas por seres humanos, à Internet" (WAHER, 2015).

Com essa crescente melhoria, é cada dia mais comum pesquisas sobre as novas tecnologias de comunicação, pode-se observar essa constante busca pela IoT na Figura 8:

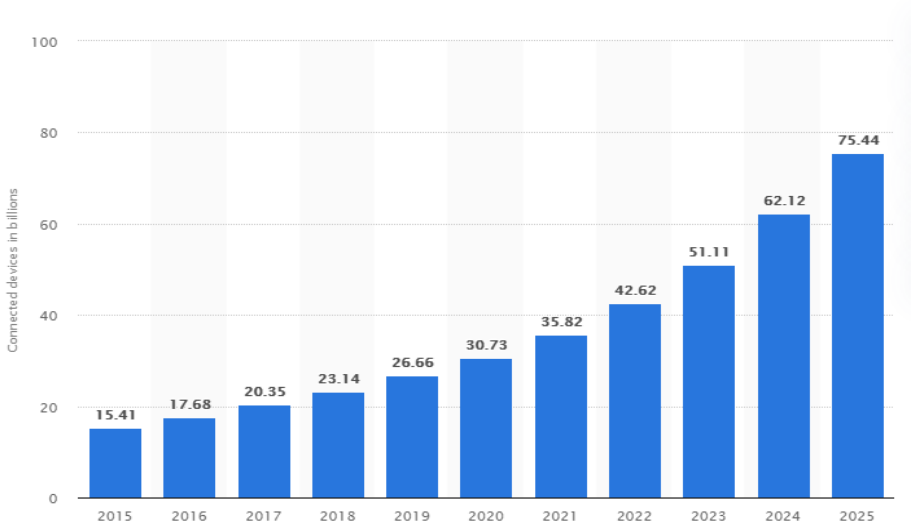
Figura 8: Pesquisas no mundo por IoT

Fonte: GOOGLE TRENDS, 2019.

A conexão na rede realizará o controle remoto dos equipamentos, permitindo o acesso deles com os provedores de serviços. De acordo com Elola (2019), a partir do ano de 2021 surgirá no Brasil à tecnologia de rede 5G que é a quinta geração da banda larga sem fio, entrando no mercado para substituir a 4G. Mas em alguns países como Estados Unidos e Coreia do Sul essa nova rede já é empregada. A utilização dessa tecnologia será considerado um grande passo para a permanência da IoT, pelo fato de ser mais potente, rápida e atender as necessidades dessa tecnologia. Essa inovação de rede, abrange um grande crescimento de oportunidades e desenvolvimentos para o mercado industrial e residencial, principalmente na parte da IoT na Domótica.

Na Figura 9, é apresentada a estatística segundo o portal online Alemão, Statista, dos dispositivos conectados à IoT pelo mundo entre os anos de 2015 até 2025.

Figura 9: Crescimento da utilização da IoT



Fonte: STATISTA, 2017.

Com esse brusco aumento de dispositivos conectados na rede, aumentou também o número de endereços IP's conectados. Em abril de 2014 a NIC.br (Núcleo de Informação e Coordenação do Ponto BR) (2014) divulgou uma nota com o esgotamento de blocos IPv4, que possuem espaço finito e são conjuntos numéricos de 32 bits, que possibilitam o endereçamento de até 4 bilhões de dispositivos. E em fevereiro de 2017, após três anos da primeira postagem, o NIC.br (2017) publicou um nota com o início da última fase disponível do estoque de endereços IPv4. Sistemas existentes na rede não poderiam solicitar mais endereços de IP na versão 4 para realizar conexões. Tendo assim uma carência de blocos IP para provedores de acesso e de conteúdo, como também para usuários de internet.

Esse esgotamento do IPv4 gerou um grande conflito para a utilização da IoT, tendo em vista que nesse tipo de sistema os dispositivos para realizar seu funcionamento necessitam de estarem conectados na rede. Então para solucionar esse conflito, em 2020, entrará em vigor a 6ª versão de endereços IP, que já existe há 10 anos, porém não eram utilizados, pois, estava em fase de teste. A nova versão será o IPv6, que possui endereçamento finito, e é composto por um conjunto numérico de 128 bits, aumentando assim a quantidade de dispositivos conectados na rede para 18 quintilhões.

Esse novo padrão de IPv6 possui várias características vantajosas, como: roteamento da internet mais competente; melhoria no processamento de pacotes de dados; configuração de rede simplificada; melhoria na segurança de transmissão. Além disso, de acordo com Alecrim (2019), ele faz parte de três categorias, que são apresentadas a seguir, permitindo melhorar a distribuição de endereços e possibilitando ter um acesso mais rápido de acordo com a necessidade.

- **Unicast** – o modelo Unicast, é aconselhado a ser utilizado em redes de ponto-a-ponto, pois determina apenas uma interface, de maneira que os pacotes de dados remetidos ao endereço sejam entregues somente a ele.
- **Multicast** – no modelo de multicast, os pacotes de dados podem ser remetidos a mais de um endereço, desde que todos eles pertençam a um mesmo grupo.
- **Anycast –** o funcionamento do Anycast é parecido ao do multicast, a diferença existente entre eles é que o pacote de dados remetido é entregue à interface do grupo que estiver mais perto.

Outra vantagem do IPv6, segundo Alecrim (2019), é que no seu desenvolvimento houve a cautela de corrigir as limitações de seguranças existentes nos endereçamentos anteriores. O principal mecanismo para essa limitação, foi a criação do IPSec (IP Security), que prevê funcionalidades de criptografia de pacotes de dados, garantindo assim, integridade, confidencialidade e autenticidade, nas transferências dos dados.

2.2.1 Protocolos da IoT

Para que um projeto de IoT seja bem sucedido e eficiente, é necessário ter dois elementos no projeto: possuir um objetivo de trabalho bem definido; obter um dispositivo inteligente, com sensores, atuadores, Inteligência Artificial (IA), um bom algoritmo e ter uma comunicação de protocolo adequada para o sistemas a ser desenvolvido.

Existem diversos protocolos usados na IoT, porém, no presente trabalho serão abordados quatro deles. De acordo com a Startup de solução em monitoramento de dispositivos, sistemas e micros serviços com foco em IoT – Damaton (2019), são os protocolos mais usados para

sistema com IoT, por permitirem a conexão de vários dispositivos simultaneamente e possuir um fácil acesso de comunicação.

- **Long Range Wide Area Network (LoRaWAN)** – neste protocolo a transmissão de dados é realizada por longas distâncias com consumo mínimo de energia, e o sinal transmitido consegue alcançar até 15km. Os aparelhos que utilizam essa comunicação de protocolo enviam e recebem os dados por meio de gateways (responsável por estabelecer a comunicação de protocolo entre duas redes - equipamento e internet), para depois serem enviados a servidores através de IP.

- **SigFox** - o protocolo SigFox foi desenvolvida pela empresa Francesa SigFox em 2009, com o intuito de fornecer uma conexão global para IoT, estabelecendo assim uma comunicação dos dados por meio da nuvem, via software, sem precisar da conexão com uma rede. Esse protocolo utiliza a técnica UNB (Ultra Narrow Band), por possuir sua largura de banda extensa e ter um longo alcance de transferência, sem perder os dados.

- **Zigbee –** neste protocolo é usada a rede sem fio (wireless), que utiliza sinais de radiofrequência para realizar as transmissões de dados. O Zigbee é mais utilizado na área industrial, por não necessitar de muitas mudanças na taxa de transmissão. Possui um pequeno alcance e um valor razoável de taxa de dados.

- **Wi-Fi e Bluetooth** – estes protocolos são os mais conhecidos no meio social, realizam a comunicação entre celulares, computadores, tv's, entre outros. O protocolo por Wi-Fi gerencia muitos dados com altas taxas de transmissão. O protocolo por Bluetooth foi desenvolvido pela empresa Ericsson em 1994, permite a troca de informações via wireless, possui uma taxa de transmissão de dados alta, porém menor do que a taxa do Wi-Fi.

Na Tabela 2, são apresentados os protocolos de comunicação da IoT, realizando um comparativo de suas características.

Tabela 2 – Comparativo dos Protocolos da IoT

PROTOCOLO	ALCANCE	TAXA DE DADOS
LoRaWAN	até 15 km	0,3 a 50 kbps
SIGFOX	30 a 50 km	100 bps
ZIGBEE	10 a 100 metros	250 kbps
WI-FI / BLUETOOTH	100 a 300 metros / 1 a 100 metros	11 a 54 Mbps / 1 Mbps

Fonte: DAMATON, 2019.

2.2.2 Aplicações da IoT

De acordo com a empresa SAS (Analytics Software & Solutions):

> A IoT está literalmente inundando a indústria com dados captados e transmitidos por sensores em linhas de produção, equipamentos financeiros, carros, eletroeletrônicos, dispositivos digitais, dispositivos comerciais e inúmeras áreas frequentadas por consumidores. Em 2020, o mercado da Internet das Coisas Industrial (IIoT) movimentará US$ 151 bilhões, crescendo a uma taxa anual composta de 8%. (ANALYTICS SOFTWARE & SOLUTIONS, 2019)

Com esse avanço e diversidade de aplicações, são apresentados a seguir algumas atuações da IoT de acordo com a empresa Totvs (2019) , em diferentes áreas de atuação:

- **Casas Inteligentes –** também conhecia por Smart Home, Automação Residencial ou Domótica, é o exemplo mais conhecido e procurado dentro da IoT, pois cada dia mais as pessoas buscam pelo conforto de realizar o monitoramento de sua casa durante uma viagem ou até mesmo enquanto trabalham. Outra aplicação é o poder de controlar o ar-condicionado de acordo com a necessidade do usuário, poder fazer o acionamento dele antes de chegar em casa, por um aplicativo no smartphone, para quando entrar a temperatura estar agradável, ou mesmo realizar o desligamento do aparelho quando não tiver ninguém dentro do ambiente. Mas, a automação residencial ainda é uma preocupação aos usuários em relação ao custo de aquisição e sua segurança perante o sistema.

- **Cidade Inteligente –** as cidades inteligentes ou apenas Smart City, são cidades que utilizam a tecnologia para apresentar melhoria na infraestrutura, trazendo soluções sustentáveis para toda a cidade. Essa busca vem com uma grande crescente nos governos em todo o mundo, está cada dia mais presente à necessidade por projetos de construção para transformar as áreas urbanas em cidades inteligentes. Com o uso da IoT nos projetos, é possível minimizar alguns problemas ambientais e sociais principalmente nas grandes cidades, tais como: o tráfego de carro, gerenciamento de energia e segurança pública. Por isso, esse tipo de tecnologia tende a crescer muito nos próximos anos.

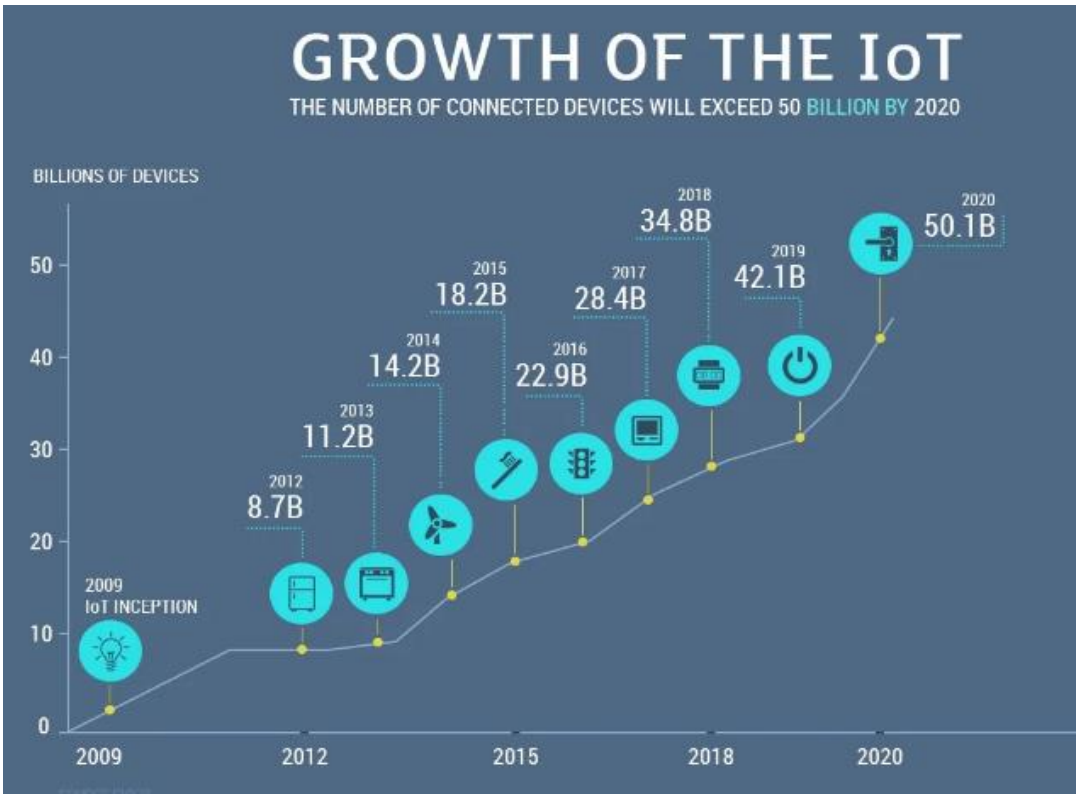
- **Carros Conectados –** os carros atuais são movidos por software e o pelo usuário, porém as indústrias automotivas estão na procura por carros mais inteligentes e capazes de tomar decisões autônomas. Por isso, surgiu o desenvolvimento dos carros conectados, que são automóveis que ofertam bem-estar e conforto aos usuários, por serem veículos que utilizam sensores internos, permitindo a conexão do veículo com outros meios. Uma vez que esses carros se conectam a IoT eles terão um universo de recursos para poder explorar, não havendo limites para funções a serem executadas.

- **Cuidados de Saúde –** no seguimento da saúde hospitais inteligentes é o novo conceito do sistema e o mais promissor para gerar impactos positivos dentro da sociedade. Tais hospitais irão cuidar da saúde dos pacientes de uma maneira completamente digital, com o auxílio dos aparelhos autônomos conectados à internet. Tornando assim, hospitais mais eficientes, qualificados e tecnológicos, melhorando o atendimento e eficiência dentro dos hospitais, reduzindo o tempo de espera e trazendo resultados ainda mais confiáveis para os pacientes.

- **Sensores industriais** – cada dia mais as empresas buscam pela Indústria 4.0 ou quarta geração industrial, que é o conceito que engloba todas as tecnologias desenvolvidas para facilitar os processos industriais. Vale destacar a automação de serviços e o controle de informações, que contarão com o uso da IoT em todo seu processo, melhorando os produtos desenvolvidos na empresa. Para esse processo acontecer será preciso colocar sensores nos equipamentos e maquinários das empresas. Essas mudanças deixarão as indústrias mais inteligentes e automatizadas.

Na Figura 10, pode-se observar o crescimento do uso da utilização da IoT, entre os anos de 2009 a 2020.

Figura 10: Crescimento de equipamentos com a utilização da IoT



Fonte: MOBIDEV, 2019.

2.2.3 IoT no Brasil

Apesar do uso da IoT aplicada na Domótica no Brasil não ter se expandido tanto, já encontramos alguns dispositivos conectados, deixando-os inteligentes. No mercado nacional tem algumas opções de dispositivos conectados à internet com o intuito de ajudar no dia a dia do usuário e deixar as coisas mais automatizadas.

A seguir, serão apresentados alguns desses dispositivos que podemos encontrar no Brasil:

- **Lâmpada inteligente** – a empresa Philips desenvolveu lâmpadas inteligentes, que são configuradas pelo aparelho Hue, apresentado na Figura 11, que por meio de uma conectividade a rede sem fio, consegue controlar até 50 lâmpadas conectar até 10 acessórios,

em que permitem ao usuário personalizar o acendimento da iluminação de toda a casa por meio de um smartphones, tablets ou por comando de voz.

Figura 11: Aparelho Hue

- Garantia: 2 anos pela fábrica
- Temperatura operacional: 0 °C a 40 °C
- Faixa de frequência: 2.400 - 2.483,5 MHz
- Número máximo de acessórios: 10
- Número máximo de lâmpadas: 50
- Consumo máximo de energia: 250mA

Fonte: PHILIPS, 2019.

- **Máquina de lavar conectada** – A empresa Samsung desenvolveu a máquina de lavar roupa inteligente Lava & Seca QDrive, apresentada na Figura 12. Este equipamento é fornecido com sistema de IA e possui conectividade com a rede Wireless. Com a conexão ao Wi-Fi é possível a fazer uma comunicação entre os equipamentos, o smartphone envia informações para a máquina, e o aparelho faz o processo conforme solicitado. De acordo com as orientações da empresa, a máquina QuickDrive reduz o tempo de lavagem em até 50% por fazer uso de dois motores e abaixa o consumo de energia em até 20%, isso sem afetar o desempenho de limpeza da roupa. Além de todas as vantagens citadas acima, o eletrodoméstico ainda conta com um recurso de aviso da hora correta de limpar o tambor e armazena os ciclos mais utilizados pelo usuário.

Figura 12: Máquina Lava & Seca QDrive

- Garantia da máquina: 1 ano
- Garantia do motor: 10 anos pela fábrica
- Capacidade de Lavagem: 10,2 kg
- Capacidade de Secagem: 6,0 kg
- Potência: 1100 W
- Programas de Lavagem: 14 programas

Fonte: SAMSUNG, 2019.

- **Ar-condicionado com Wi-Fi** – a Samsung desenvolveu o ar-condicionado mais silencioso e econômico, o Split Digital Inverter Frio Wind Free, apresentado na Figura 13. O ar-condicionado possibilita a conexão ao Wi-Fi, podendo realizar sua programação à distância, via aplicativo do smartphone. Outro benefício é o monitoramento em tempo real da temperatura ambiente e do consumo de energia gasto. De acordo com a empresa, o eletrodoméstico consegue economizar até 72% de energia em relação aos ares-condicionados tradicionais. A Samsung afirma ainda que o aparelho consegue reduzir as bactérias e os vírus em até 99%, capturando o pó contaminante do ambiente.

Figura 13: Ar-condicionado Split Digital Inverter Frio Wind Free

- Garantia da máquina: 1 ano
- Garantia do compressor: 10 anos
- Capacidade de Resfriamento: 3,52 KW
- Consumo Energético: 1080 W
- Corrente de Operação: 5,2 A

Fonte: SAMSUNG, 2019.

- **Câmera Smart** – uma opção de monitoramento da casa, escritório ou empresa é por meio de dispositivos móveis. A empresa D-link pensando nisso, desenvolveu a câmera Omna 180 Cam HD, apresentada na Figura 14, que de acordo com a empresa a Omna é derivação da palavra latina 'omnis', que significa todo-abrangente. Este dispositivo é compatível com a Apple HomeKit (ecossistema da Apple para casas inteligentes), e contém uma lente grande-angular de 180° com visão noturna, possui microfone e alto-falantes integrados para realizar uma comunicação de áudio bidirecional, além de filmar em resolução Full HD. O aparelho é equipado com sensor de movimento, na qual, quando detectado a câmera grava o movimento e emiti alertas para o smartphone do usuário.

Figura 14: Câmera Omna 180 Cam HD

- Garantia da máquina: 3 anos
- Tensão de Saída: 5 V
- Amperagem de Saída: 2 A
- Temperatura de operação: 0 a 40° C

Fonte: D-LINK, 2019.

- **Family Hub**: Family Hub, apresentada na Figura15, é a nova geladeira inteligente desenvolvida pela empresa Samsung. Além de conservar os alimentos frescos de maneira mais eficiência e possui um menor desperdício. O dispositivo conta com a conexão Wi-Fi, permitindo a interação da geladeira com o Smartphone. A nova geladeira da Samsung suporta comandos de voz, assistente virtual, tela interativa, que possibilita ouvir alguma música ou ler alguma noticia e uma câmera instalada em seu interior, permitindo o usuário ver quando o alimento chegou ao fim. Além disso, é possível sincronizar o dispositivo com lâmpadas smart e outros aparelhos inteligentes da casa.

Figura 15: Family Hub

- Garantia da geladeira: 1 ano
- Garantia do compressor: 10 anos
- Capacidade total: 582 litros
- Consumo Energético: 65 kWh/Mês
- Classificação INMETRO: A

Fonte: SAMSUNG, 2019.

2.3 IoT aplicada na Domótica

Daqui alguns anos, a utilização da IoT na Domótica ira causar um amplo impacto positivo no cotidiano dos seres humanos. Mediante o avanço dessa tecnologia, terá casas inteligentes, capazes de tomar ações automáticas, com equipamentos e aparelhos eletrônicos mais funcionais, objetivos e autossuficientes, trazendo melhorias para a residência e com isso mais conforto e bem estar no dia a dia dos usuários, na Tabela 3 pode-se observar algumas dessas aplicações.

Tabela 3 – Aplicações da IoT na Domótica

FUNÇÕES	EQUIPAMENTOS
Iluminação	• Controle da intensidade luz • Acionamento automático das lâmpadas
Hidráulico	• Monitoramento do nível dos reservatórios em tempo real • Medição da qualidade da água • Gerenciamento do consumo d'agua identificando vazamentos
Segurança	• Monitoramento remoto da casa • Controle das entradas, como portas e portões.
Climatização	• Controle automático da temperatura • Ar-condicionado inteligente
Elétrico	• Placas e aquecedores solares • Chuveiros Inteligentes

Nos dias atuais, já é possível encontrar muitos aparelhos com soluções que permitem deixar a residência automatizada, como foram apresentadas na Tabela 3. Essas tecnologias ainda precisam de mão de obra de instalação, porém esta realidade está mudando. No mercado hoje já existe equipamentos que permitem o próprio usuário realizar a instalação dos aparelhos, deixando a mão de obra mais barata e reduzindo os custos. Com isso, em pouco tempo terão casas inteligentes e com menos gastos.

Para a instalação da IoT na Domótica, será necessário apenas uma conexão adequada com à internet, realizando assim uma melhor comunicação entre os equipamentos da residência e os usuários. A IoT chegou para deixar ainda mais fácil a instalação e a maneira de uso dos equipamentos eletrodomésticos e eletrônicos da casa, deixando o valor mais acessível para as

pessoas que irão aderir e trazendo economia para a residência, pois com essa tecnologia será possível controlar vários sistemas remotamente.

A seguir são apresentadas algumas aplicações da IoT na Domótica:

- **Lâmpadas inteligentes** - as lâmpadas inteligentes, apresentada da Figura 16, são lâmpadas conectadas na rede, permitem a interação do usuário, podendo ser controladas através de aplicativos contidos no smartphone, ou deixá-las pré-programadas para seu acionamento/desligamento, mesmo estando distante. Permite também, a criação de várias combinações de iluminação, podendo brincar e deixando a imaginação fluir escolhendo qual cor e em qual intensidade a luz vai funcionar. Lâmpadas inteligentes, além de trazerem uma economia para a residência e aconchego, fornecerá também certa segurança, pois quando estiver em uma viagem, poderá realizar o acionamento da lâmpada em horários distintos, dando assim a impressão que tem alguém presente na casa.

Figura 16: Lâmpada Inteligente

Fonte: BANGGOOD, 2019.

- **Controle de acessos** - com a utilização da internet nos acessos de entrada e saída da casa, poderá programar as fechaduras das portas e dos portões para serem controladas remotamente por meio do celular, por leitura de impressão digital ou até mesmo por comando de voz. Outra vantagem desta aplicação é deixar uma autorização gravada no sistema, permitindo a entrada de pessoas do seu meio social, como amigos e familiares, deixando assim, uma maior segurança. Pois, caso alguma pessoa sem o acesso realizar alguma tentativa de entrada na casa, será encaminhado em tempo real uma alerta para o dono. A seguir é apresentado a uma fechadura inteligente da marca Wulian, que é capaz de realizar esse controle de acesso.

Figura 17: Controle de Acesso

Fonte: TECNEO, 2019.

- **Sistemas de segurança** – com todo o avanço, a segurança residencial também será mudada, com instalações de câmeras para realizar o monitoramento de acesso remoto na casa. Sensores de presença e sistemas de alarme em tempo real estarão interligados na câmera, em que na Figura 18 é apresentada uma câmera da marca Wulian, que conta com essa tecnologia. Os sensores presentes nos equipamentos poderão encaminhar avisos ao celular do dono da casa, de maneira que a pessoa possa analisar as notificações recebidas. Além da segurança externa, também abrirá espaço para a segurança interna do local, realizando instalações de câmeras com comunicação wireless, gerando relatórios online e encaminhando para smartphones, onde as câmeras internas poderão ser instaladas de modo portátil para serem usadas conforme a necessidade do usuário.

Figura 18: Sistema de Segurança

Fonte: TECNEO, 2019.

- **Eletrodomésticos** – com a utilização da IoT na Domótica, os eletrodomésticos também receberão mudanças, como máquinas de lavar, geladeiras, cafeteiras, tv's, aparelhos de som e fornos elétricos, como pode se observar na Figura 19. Através de aparelhos inteligentes, múltiplos eletrodomésticos poderão realizar as tarefas automaticamente, podendo ser programados remotamente e a distância, trazendo mais agilidade e conforto para o usuário, otimizando o tempo corrido da rotina. Outra aplicação interessante nesse segmento serão as compras de suprimentos da residência de forma online e automática. Uma lista de produtos será cadastrada e a cada saída de um desses produtos o mesmo será retirado do sistema, e assim que estiver em falta a própria geladeira da casa realiza o envio a lista dos produtos faltosos diretamente para o supermercado, que se encarregará de realizar a entrega.

Figura 19: Eletrodomésticos Inteligentes

Fonte: TECMUNDO, 2019.

- **Assistentes virtuais** – da mesma maneira que existem assistentes pessoais pelo celular, existem também assistentes virtuais, como apresentada na Figura 20, a Alexa que foi desenvolvida pela Amazon, para facilitar a vida. Tais assistentes irão contar com o auxílio da IoT para realizar as tarefas, como por exemplo, fazer as atualizações de planilhas e organizar seus compromissos de acordo com seu dia a dia. Também conseguirá realizar outras tarefas mais simples, trazendo mais comodidade para o usuário, como por exemplo, escolher alguma música para tocar sem precisar sair do lugar, ou até mesmo ligar e desligar aparelhos da casa como tv's, luz, entre outros. Todas essas tarefas poderão ser acionadas por um comando de voz ou apenas em um clique por aplicativo.

Figura 20: Assistente Virtual - Alexa

Fonte: AMAZON, 2019.

- **Telas multiuso** – as telas multiuso daqui alguns meses serão muito utilizadas no cotidiano, e você poderá escolher entre duas versões, uma mais simples ou uma mais complexa. Na versão simples, lembrará um smartphone ou smart tv, tendo a capacidade de apresentar vídeos e imagens, mostrar feed de notícias do mundo entre outras informações. Enquanto, na versão complexa, lembrará um Himirror e terá uma gama maior de funções, além do que é ofertado na versão básica, contara também com aplicativos avançados, como por exemplo, um aplicativo que realiza avaliações de como está o cuidado de sua pele e cabelo e apresentam dicas de como cuidar dele. Na Figura 21 é apresentada uma tela de multiuso da Himirror.

Figura 21: Tela Multiuso

Fonte: HIMIRROR, 2019.

- **Climatização e Persianas/Cortinas –** Conectando equipamentos como ar condicionado, cortinas e afins, como apresentada na Figura 22, o usuário conseguirá realizar o controle dos dispositivos de maneira fácil e ágil, através de um smartphone. Em relação à temperatura, é possível agendar horários definidos para o acionamento do ar-condicionado, ou deixá-lo de maneira autônomo de acordar com a temperatura da casa. Enquanto o controle da abertura e fechamento de persianas ou cortinas se dá de acordo com a luminosidade do lugar. Trazendo assim uma maior comodidade ao usuário.

Figura 22: Persianas e Cortinas Inteligentes

Fonte: OCCA, 2019.

3 FALHAS EXISTENTES NA DOMÓTICA COM A IoT

Nesta seção, são abordadas as presentes falhas encontradas nos sistemas de Domótica com a utilização da IoT, bem como os possíveis problemas que esse tipo de sistema pode causar nas redes e no mundo.

3.1 Desafio da segurança

De acordo com Buttler

> Muito em breve a IoT será incorporada em quase todos dispositivos móveis, medidores de estacionamento, termostatos, monitores cardíacos, estradas, prateleiras de supermercados e uma quantidade tão grande de dispositivos conectados com IoT que estarão propensos a uma enorme exploração de vulnerabilidades, problemas de privacidade e segurança. (BUTTLER, 2017).

O maior desafio encontrado no mundo da IoT está sendo o número de falhas nos sistemas que utilizam essa tecnologia. De acordo com a empresa de inteligência de software Dynatrace, “em todo o mundo, 52% de usuários de tecnologia utilizam dispositivos de Internet das Coisas (IoT), mas 64% desse universo já enfrentaram dificuldades de performance, de acordo com uma pesquisa global com 10 mil consumidores” (DYNATRACE, 2018).

Sendo assim, a preocupação com a segurança dos dados dentro da IoT está cada vez mais presente. De acordo com um estudo realizado pela empresa de consultoria Gartner, a preocupação com a segurança e privacidade dos dados no sistema são os maiores obstáculos encontrados. Esse estudo aponta que no ano de 2020, cerca de sessenta por cento (60%) dos orçamentos das empresas serão direcionadas para cyber segurança, para obter rápidas detecções de resposta contra as falhas existentes.

Por ser uma tecnologia computacional, todos os sistemas sempre estarão expostos a algum tipo de falha. As falhas de segurança mais comuns nos sistemas de IoT são apresentadas a seguir:

- **Vulnerabilidade** – atualmente, os sistemas de IoT ainda encontram-se com muitas vulnerabilidades, tornando-se assim um alvo para as falhas. Todo equipamento conectado a rede sem fio está propício a essas falhas de sistema. Os sistemas que estão vulneráveis a falhas possuem um acesso mais fácil aos hackeadores e malwares (vírus capazes de alterar e salvar dados). Dentro da domótica, os eletrodomésticos mais vulneráveis a uma falha de segurança são as smart tv's; que cada dia mais contam com novas tecnologias; sistemas que possui o controle de iluminação e som, equipamentos de climatização, entre outros que seguem esse segmento. Nesse tipo de eletrodomésticos as atualizações de firmware são limitadas, podendo assim apresentar falhas na criptografia (codificação e decodificação dos dados) e autenticação do usuário.

- **Fraude de dados** - nesse tipo de falha os hackers conseguem acessar o sistema de maneira a conseguir a identidade do usuário, como nome completo, endereço, número de telefone e algumas das vezes número do cartão de crédito. Isso é possível através de estratégias de coleta de dados e por meio das contas conectadas que fornecem diversas informações na rede. Tais informações podem ser encontradas dentro dos dispositivos inteligentes da pessoa, páginas gravadas no navegador ou até mesmo nos aplicativos instalados.

- **Ransomware** – também conhecido por sequestro virtual, esse tipo de falha está se tornando comum na internet. O sequestrador acessa os equipamentos inteligentes da pessoa, como computadores e dispositivos móveis, realizam bloqueios e alterações de senhas, conseguindo realizar todo o controle do equipamento, de maneira que o dono não consiga acessar o seu aparelho. Esse tipo de cibercrimosos realiza esse tipo de procedimento com o intuito de pedir um resgate.

- **WI-FI livre** – nos dias atuais está cada vez mais comum ter as redes livres de internet pública nos lugares, que nada mais é do que uma rede que libera acesso para navegação à internet de modo livre, sem necessitar de uma senha para navegar. Porém, esse tipo de zona livre requer cuidados a serem tomados, pois pode ser apenas uma armadilha para o hacker obter acesso aos seus dados de navegação, de modo malicioso.

3.2 Ataques Cibernéticos

A maioria dos dispositivos que estão conectados na IoT, para realizarem seu perfeito funcionamento necessitam de uma boa comunicação a um servidor de hospedagem de gerenciamento. Servidores ou páginas web podem conter falhas no escopo do seu código, possibilitando assim, um ataque cibernético no sistema por pessoas maliciosas, que buscam informações ou dados de alguma pessoa, empresa ou para se hospedar em sites de maneira incorreta.

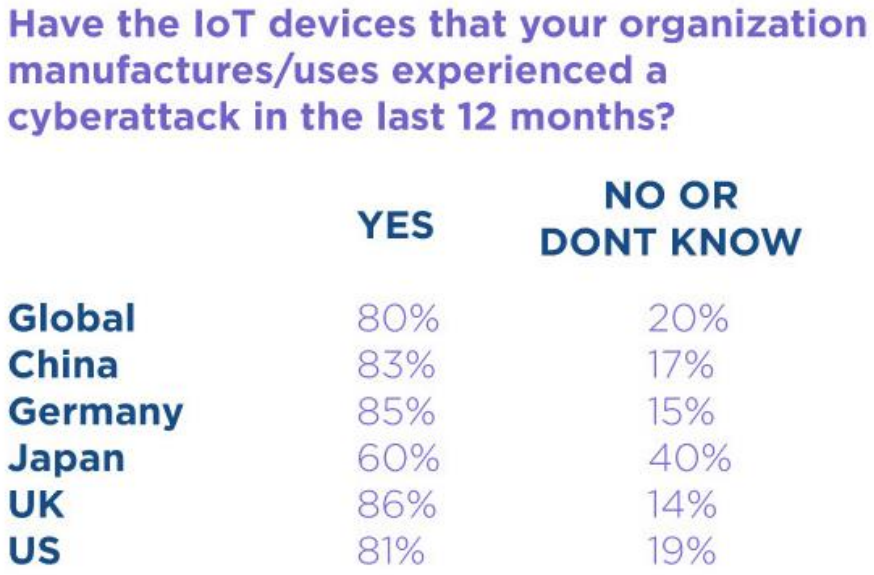
De acordo com uma pesquisa realizada em maio de 2019 pela empresa que realiza proteção de plataformas e aplicativos para indústrias de entretenimento – Irdeto (2019) “Oito em dez organizações vivenciaram um ataque cibernético em seus dispositivos de IoT (Internet das Coisas) nos últimos 12 meses”, um exemplo desse tipo de ataque foi a invasão de uma câmera de segurança da empresa Ring, pertencente a Amazon, que foi instalada no quarto em uma casa localizada em Mississipi nos Estados Unidos. O acontecimento ocorreu em dezembro de 2019, em que, um hacker conseguiu acessar o controle da câmera de segurança instalada, obtendo as imagens do quarto, na Figura 23 pode-se observar a imagem que o hacker conseguiu acesso, além da imagem obtida, o hacker conseguiu ainda se comunicar com uma criança de oito anos que se encontrava no quarto no momento.

Figura 23: Imagens da Câmera ao ser invadida

Fonte: Portal FolhaPE, 2019.

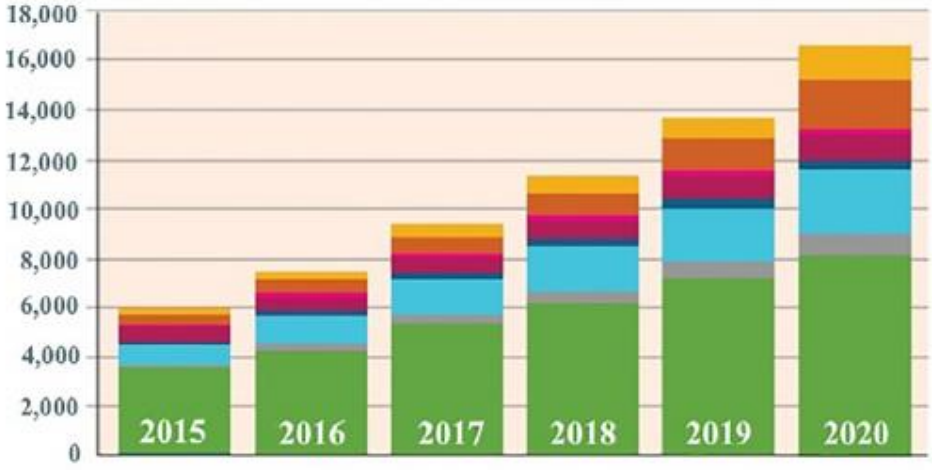
Na Figura 24 pode-se observar o percentual da pesquisa realizada pela empresa Irdeto, enquanto na Figura 25 é apresentada uma estatística dos números de ataques entre os anos de 2015 a 2020.

Figura 24: Percentual de ataques em um ano



Fonte: IRDETO, 2019.

Figura 25: Estatística dos Ataques Cibernéticos



Fonte: JUNIPER RESEARCH, 2017.

Com isso, pode-se observar o grande crescimento dos ataques. Isso ocorreu devido ao início da utilização da IoT e a falta de segurança no desenvolvimento dos sistemas das empresas para essa nova tecnologia.

3.3 Outro problema que poderá surgir

Outro problema que poderá aparecer com o surgimento da IoT é o aumento de baterias e equipamento a serem descartados, pois cada vez mais são utilizados aparelhamentos portáteis ou remotos que precisam de baterias para seu funcionamento, com o objetivo de armazenar e fornecer energia de maneira correta. Como as baterias estão ficando cada vez menores elas aparentam ser inofensivas, porém representam um grave problema ambiental, pois estão ficando cada vez mais potentes. “Esse pequeno dispositivo muito usado por todos, sem exceção, de mocinho pode virar um vilão se descartado incorretamente.” (AFONSO, 2003).

Com o rápido crescimento da IoT, será quase impossível conciliar um local adequado para realizar o descarte das baterias e equipamentos, pois baterias necessitam de ser descartadas em lugares apropriados como aterros sanitários específicos para substâncias perigosas, por ser considerado um lixo tóxico.

4 SOLUÇÕES PARA OS PROBLEMAS ENCONTRADOS

No presente capítulo são abordadas as possíveis soluções para as falhas apontadas neste trabalho, de modo a orientar aos usuários uma maneira de prevenir os riscos existentes na IoT.

4.1 Prevenção contra as Falhas de Segurança

Como apresentado anteriormente existem inúmeras falhas de segurança nos sistemas que utilizam a tecnologia da IoT. A seguir são descritas diferentes maneiras para se prevenir dessas falhas existentes, podendo assim o usuário conseguir usufruir apenas dos benefícios trazidos por essa tecnologia.

- **Autenticidade** – por meio da autenticidade integrada nos sistemas, como senhas digitais, desbloqueio por meio de biometrias, digitalização facial e de voz, e senhas de acesso, será possível garantir que apenas o usuário tenha acesso às informações, entradas e saídas de ambientes. Contudo, nenhum método é totalmente confiável, pois mesmo se prevenindo com autenticidades avançadas, ainda temos o risco da perda de aparelhos, como smartphones, que liberariam o acesso, através de alguma foto (digitalização facial) ou comando voz (acessando algum áudio salvo). Sendo assim, para se assegurar desse risco, é necessário deixar os smart's conectados a uma rede, como conta do Google, podendo realizar o bloqueio total do aparelho em casos de perdas, não permitindo nenhum acesso. É interessante deixar o backup dos dados automático para o usuário não perder nenhum dado contido no dispositivo.

- **Confidencialidade** – a confidencialidade de senhas e códigos é sempre um assunto muito óbvio. Porém, não deixa de ser essencial para a segurança do equipamento, principalmente na Domótica. Sendo assim, quando o sistema é confidencial consegue garantir a segurança, pois o acesso estando restrito é capaz de assegurar que o conteúdo transmitido do remetente ao destinatário não seja alterado.

- **Prevenção Contra Malware** – conhecido também por vírus, por conseguirem se propagar rapidamente no ambiente onde se encontram. Esses vírus estão mais presentes em computadores, e são atraídos por meio de download ou e-mail infectados. A maneira mais

trivial de se proteger dos malwares é tomando sempre o cuidado das mensagens e aplicativos baixados, certificar sempre se é um ambiente confiável antes de abrir a mensagem ou baixar o aplicativo, e manter na máquina conectado a um bom antivírus ou anti-spyware, que irá detectar e removê-lo. Além disso, conte sempre com um firewall, que é um dispositivo de rede capaz de detectar o vírus antes mesmo dele chegar no sistema.

- **Conexão em redes** – como mencionado em cima, redes abertas são sempre um perigo vinculado com sua conexão, por isso a conexão deve ser feita somente em redes seguras e certificadas, evitando assim sequestros de informações.

- **Atualizações de sistemas** – manter os sistemas atualizados é sempre bom, pois as atualizações são realizadas para melhoria dos dispositivos, evitando as brechas e falhas de segurança, deixando assim o sistema mais seguro.

4.2 Proteção Contra Ataques Cibernéticos

Como os ataques cibernéticos nos sistemas de IoT estão crescendo, as empresas estão desenvolvendo diferentes maneira de se proteger, implementando assim, segurança nos seus dispositivos.

O estudo realizado pela Irdeto (2019) apontou que 18% das empresas entrevistadas planejam adicionar proteção de software no próximo ano, entrando em vigor em 2020. Enquanto 29% das empresas planejam adicionar proteção para os aplicativos móveis, como smartphones, notebook, tablets, entre outro, já 30% pretendem tornar a segurança parte do desenvolvimento do projeto e 29% desejam realizar uma segurança contínua, mantendo sempre revisões do código. Deixando assim os sistemas mais robustos e impossibilitando as falhas existentes aos ataques cibernéticos.

Para a produção inteligente na Indústria 4.0, existirão dois requisitos para a segurança contra os ataques cibernéticos: arquitetura de segurança e Segurança by Design. Estes requisitos assegurarão que os sistemas detectem automaticamente a presença de malware e ataques, por meio de rastreamento, análise e identificação de ameaças de segurança digital existentes na internet.

Porém, para que a segurança contra os ataques tenha melhor desempenho, não bastam apenas às empresas se preparem e atualizarem seus sistemas, os usuários deverão se adaptar com requisitos de proteção, pois uma rede que transmiti informações deve apresentar um bom controle de acesso, evitando assim, que ocorram visualizações ou alterações por pessoas inadequadas que venham a interceptar os dados do sistema. Algumas mudanças que deverão acontecer são:

- **VPN** – o VPN (rede virtual privada) é usado para assegurar a conexão do seu dispositivo à Internet, prevenindo assim das diferentes falhas já apresentadas anteriormente, como Wi-Fi livre, hackers, roubo de informações entre outras ameaças existentes na internet. Sendo assim, se o usuário usa aparelhos remotos, é imprescindível ativar o VPN para que os dados fiquem protegidos e seguros. Dessa forma, mesmo que tentem atacar o sistema será muito difícil à pessoa obter os dados e informações. No caso apontado em Mississipi nos Estados Unidos, a mãe da criança não ativou a autenticação do dispositivo, deixando assim o dispositivo vulnerável à internet, em que, se os pais tivessem ativado aumentaria uma camada a mais de proteção contra a ação do hacker.

- **Orientações aos usuários** – é de suma importância criar uma cultura de segurança entre os usuários, para assim evitar exposições de dados. Cuidados básicos e simples são fundamentais para a segurança contra os ataques cibernéticos, como sempre verificar a confiabilidade dos sites, e-mails e links suspeitos, além de realizar instalações apenas de programas confiáveis. E nunca compartilhar informações sigilosas por e-mail ou para usuários externos, evitando assim possíveis aberturas para as falhas.

- **Senhas** – como é do conhecimento de todas as senhas fortes, que contenham letras, números e símbolos são indispensáveis, e sempre mantenha suas contas deslogadas dos computadores e celulares, pois é através das senhas que se dá o acesso ao sistema. Por isso, é necessário sempre manter padrões fortes para evitar invasões.

- **Armazenamento em nuvem** – para proteção de seus documentos, uma boa solução é o armazenamento em nuvem, onde os dados são gravados em conjuntos lógicos. Para o acesso a nuvem, basta ter uma boa conexão a internet em algum dispositivo móvel, podendo assim

acessar todos os arquivos salvos, assegurando seus dados e liberando espaço de memória do dispositivo.

- **Backups** – realizar backups em sistemas é uma maneira de manter em segurança os dados, pois se um ataque cibernético ocorrer ou um Ransomware, os dados permanecerão disponíveis para o usuário.

Usuários que passam por ataques cibernéticos podem ter muitos prejuízos pessoais e até mesmo empresariais. Então, é de suma importância os usuários manterem uma rotina de segurança, contando assim com requisitos de proteção. Se prevenindo de golpes e deixando a integridade dos dados e informações intactas.

4.3 Solução para Outro Problema encontrado

Outro problema que poderá aparecer com o surgimento da IoT será o excesso de equipamentos eletroquímicos (dispositivos que através da reação de oxidorredução produzem uma corrente elétrica, como por exemplo pilhas e baterias) para descarte. Para solucionar esse problema, poderão ser substituídas as baterias comuns por baterias recarregáveis, na Tabela 4 são apresentadas as baterias mais usadas para a alimentação dos equipamentos que utilizam a tecnologia da IoT segundo o portal Embarcados. Ou então, fazer uso de baterias de longa duração, no mercado atualmente existe baterias em que os dispositivos embarcados podem ter uma vida útil de 10 anos. Tais baterias podem ser encontradas nas empresas *The IOT Store* e *IoT in a Box – Turnkey IoT Solutions*.

Tabela 4 – Baterias recarregáveis para dispositivos usados na IoT

TIPO	CARACTERÍSTICA	TENSÃO NOMINAL (V)
Níquel Cádmio	Bateria de NiCd	1,2
Níquel-hidreto Metálico	Bateria de NiMh	1,2
Lithium-Ion Polímero	Bateria de Li-Ion	3,2 – 3,6 – 3,7

Fonte: EMBARCADOS, 2019.

Outra maneira de solucionar esse problema será a substituição dos dispositivos normais por dispositivos que contam com sensores autossustentáveis, que realizam sua carga com as

próprias vibrações do ambiente, como ondas de rádio ou eletromagnéticas, ou usar do princípio das placas fotovoltaicas, utilizando os raios solares para realizar seu carregamento. Evita-se assim o aumento de descartes de eletrônicos.

5 CONCLUSÕES

Neste trabalho realizou-se uma revisão teórica, buscando conhecer melhor a tecnologia IoT, principalmente nas aplicadas a um projeto de Domótica. No segundo capítulo foi feita uma revisão sobre automação residencial, apresentando suas principais características e protocolos utilizados. Foi realizada uma breve definição de Domótica e apresentado os principais tipos de sistemas que existem no mercado. Foram expostos também, as definições, protocolos e aplicações da nova tecnologia da IoT, apontando os benefícios trazidos com ela. No capítulo três, foram relatadas as falhas que existem nesses sistemas e os possíveis problemas que poderemos enfrentar com o crescimento dessa tecnologia agregada a automatização dos equipamentos. E no capítulo quatro foram apresentadas soluções para os problemas e falhas encontradas.

Diante do exposto, constata-se que a Internet das Coisas é uma tecnologia que consegue incorporar uma série de facilidades em equipamentos por meio de sensores, trazendo mais conforto e bem estar para o usuário. Essa tecnologia é muito relevante para o dia a dia, principalmente nos setores residencial e industrial. Porém, desenvolver um sistema de tecnologia que seja cem por cento seguro é quase impossível, pois sistemas computacionais sempre estão sujeitos a falhas. De qualquer modo, a busca por sistemas mais robustos é uma preocupação constante dos fabricantes e da sociedade de um modo geral. Com hardware e software mais aprimorados, e com um comportamento mais cuidadoso por parte dos usuários, a segurança desses sistemas é sobremaneira aumentada.

Para trabalhos futuros poderão ser realizados estudos de aprofundamento da aplicação da IoT no Brasil e como as empresas brasileiras estão se adaptando com essa mudança tecnológica, bem como desenvolver um protótipo de domótica de baixo custo, usando por exemplo microcontroladores, de forma a alcançar todas as classes sociais, trazendo assim comodidade e bem estar para todos.

REFERÊNCIAS

EVANS, Dave. **The Internet of Things How the Next Evolution of the Internet Is Changing Everything**. Cisco Internet Business Solutions Group (IBSG), 2011.

RAZA, U.; KULKARNI, P.; SOORIYABANDARA, M. **Low power wide area networks: An overview**. IEEE Communications Surveys Tutorials, v. 19, n. 2, p. 855–873, Secondquarter, 2017.

ROGRIGUES, Fabiano. Dispositivos IoT conectados à Internet em casa são um perigo. **SempreUPdate**, 2019. Disponível em: < sempreupdate.com.br/dispositivos-iot-conectados-a-internet-em-casa-sao-um-perigo >. Acesso em: 01 de set. de 2019.

ADAMI, Anna. Domótica. **Info Escola**, 2014. Disponível em: <infoescola.com/tecnologia/domotica >. Acesso em: 02 de set. de 2019.

DOMÓTICA. **Sentido Digital – Building Management Technologies**, 2019. Disponível em: < sentidodigital.pt/produtos/domotica >. Acesso em: 02 de dez. de 2019.

O QUE É A DOMÓTICA. **Sislite – Integração de Sistemas,** Portugal, 2019. Disponível em: <sislite.pt/domus.htm>. Acesso em: 25 de nov. de 2019.

BERRY, Jean. Industrial Internet of Things Trends to Dominate in 2020. **Movidev**, 2019. Disponível em: <mobidev.biz/blog/industrial-iot-internet-of-things-trends>. Acesso em: 26 de nov. de 2019.

Quais os protocolos mais utilizados para IoT. **Datamon - Monitoramento em Tempo Real**, 2019. Disponível em: <datamon.com.br/Noticia/quais-os-protocolos-mais-utilizados-para-iot>. Acesso em: 03 de set. de 2019.

MIZUSAKI, Lucas Eishi Pimentel. **Comparação de mecanismos de Comunicação para a Casa Inteligente**. Trabalho de Conclusão de Curso (Engenharia de Cumputação) Universidade Federal do Rio Grande do Sul, 2009.

GONÇALVES, João Pedro Araújo. **Protocolos de Automação Doméstica - Solução de Automação Residencial e Vigilância Baseada em Protocolo Z-Wave**. Dissertação (Mestrado em Engenharia Eletrotécnica) Instituto Superior de Engenharia do Porto. 2017.

ALVES, José Augusto; MOTA Jos. **Casas Inteligentes**. 1ª edição. Portugal. Centro Atlântico, Lda. 2003.

New 2019 Global Survey: IoT-Focused Cyberattacks are the New Normal. **Irdeto Building a Secure Future**. Holanda, 2019. Disponível em: <irdeto.com/news/new-2019-global-survey-iot-focused-cyberattacks-are-the-new-normal>. Acesso em: 02 de dez. de 2019.

NIC.br alerta: esgotamento de endereços IPv4 acontecerá nos próximos meses. **NIC.br**. Brasil, 2014. Disponível em: <nic.br/noticia/na-midia/nic-br-alerta-esgotamento-de-enderecos-ipv4-acontecera-nos-proximos-meses>. Acesso em: 30 de nov. de 2019.

Estoque de IPv4 na América Latina chega à fase final. **NIC.br**. Brasil, 2017. Disponível em: <nic.br/noticia/releases/estoque-de-ipv4-na-america-latina-chega-a-fase-final>. Acesso em: 30 de nov. de 2019.

Endereços IPv4 acabam em janeiro de 2020 na América Latina. **NIC.br**. Brasil, 2018. Disponível em: <nic.br/noticia/na-midia/enderecos-ipv4-acabam-em-janeiro-de-2020-na-america-latina>. Acesso em: 30 de nov. de 2019.

O que é um CLP e como ele funciona. **PLCWIFI. Net**, 2019. Disponível em: <plcwifi.net/>. Acesso em: 02 de nov. de 2019.

SOUZA, Marcelo Varela. **Domótica de baixo custo usando princípios de IoT**. Dissertação (Pós-Graduação em Engenharia de Software) Universidade Federal do Rio Grande do Sul, Natal, 2016.

BOLZANI, Caio Augustus Morais. **Residências inteligentes: domótica, redes domésticas e automação residencial**. 1a Ed. São Paulo. Cia dos livros. 2004.

ALVES, José Augusto e MOTA, José. **Casas Inteligentes**. 1a Ed. Portugal. Centro Atlântico, Lda. 2003.

WAHER, Peter. **Learning Internet of Things Paperback**. Birmingham Mumbai. Packt Publishing Ltd. 2015.

ELOLA, Joseba. Hiperconectados e ultravulneráveis ao 5G. **EL PAÍS**, 2019. Disponível em: <brasil.elpais.com/brasil/2019/08/30/eps/1567160455_999269.html>. Acesso em: 02 de out. de 2019.

BUTTLER, PETER. DECIPHERING DATA SECURITY FLAWS. **CSO magazine from International Data Group**, 2017. Disponível em: <csoonline.com/blog/deciphering-data-security-flaws>. Acesso em: 04 de out. de 2019.

IoT Failures Plague 64% of Users Worldwide, as Cloud Complexity Surges. **Dynatrace,** 2018. Disponível em: <dynatrace.com/news/page/4/?post_type=news-coverage&language=em>. Acesso em: 29 de nov. de 2019.

6 aplicações de Internet das Coisas em sua rotina. **TOTVS,** 2019. Disponível em: <totvs.com/blog/aplicacoes-da-internet-das-coisas/>. Acesso em: 15 de set. de 2019.

Lava & Seca QDrive. **Samsung**, 2019. Disponível em: <samsung.com/br/washing-machines/combo-qdrive-inox-10kg>. Acesso em: 29 de nov. de 2019.

Ar Condicionado Split Samsung Inverter Wind Free 12.000 Btu/h Frio. **Samsung**, 2019. Disponível em: <samsung.com/br/air-conditioners/wind-free-inverter>. Acesso em: 29 de nov. de 2019.

Geladeira French Door Family Hub 582L Black Edition com CoolSelect Zone™. **Samsung**, 2019. Disponível em: <samsung.com/br/refrigerators/french-door-rf265beaesgaz>. Acesso em: 13 de dez. de 2019.

Câmera Wi-Fi Full HD 180º. **D-Link,** 2019. Disponível em: <dlink.com.br/produto/omna-camera-wi-fi-full-hd-180-dsh-c310>. Acesso em: 29 de nov. de 2019.

Bridge. **Philips**, 2019. Disponível em: <2.meethue.com/pt-br/p/hue-bridge/8718696555019>. Acesso em: 29 de nov. de 2019.

E27 7W RGBW WIFI APP Control LED. **Banggood**, 2019. Disponível em: <https://pt.banggood.com/E27-7W-RGBW-WIFI-APP-Control-LED-Smart-Light-Bulb-Works-With-Alexa-AC85-265V-p-1257235.html?cur_warehouse=CN>. Acesso em: 29 de nov. de 2019.

FECHADURA INTELIGENTE. **TecNeo**, 2019. Disponível em: <tecneo.com.br/casa-inteligente/fechadura-inteligente--p>. Acesso em: 29 de nov. de 2019.

CÂMERA INTELIGENTE LINHA PREMIUM. **TecNeo**, 2019. Disponível em: <tecneo.com.br/casa-inteligente/camera-inteligente-linha-premium--p>. Acesso em: 29 de nov. de 2019.

NAPOL, Igor. Smart homes: você forneceria seus dados pessoais em troca de dinheiro. **TecMundo**, 2016. Disponível em: <tecmundo.com.br/comportamento/103304-smart-homes-voce-forneceria-dados-pessoais-troca-dinheiro.htm>. Acesso em: 29 de nov. de 2019.

Echo Dot (3ª Geração): Smart Speaker com Alexa - Cor Preta. **Amazon**, 2019. Disponível em: <amazon.com.br/Echo-Dot-3%C2%AA-Gera%C3%A7%C3%A3o-Cor-Preta/dp/B07PDHSJ1H/ref=sr_1_1?__mk_pt_BR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&keywords=alexa&qid=1576540816&sr=8-1&th=1>. Acesso em: 29 de nov. de 2019.

Aplicações e Soluções. **Occa**, 2019. Disponível em: <http://www.casaocca.com.br/occa-pt-saiba-mais/>. Acesso em: 13 de dez. de 2019.

Internet das Coisas: coloque-a para trabalhar a favor da sua organização. **ANALYTICS SOFTWARE & SOLUTIONS**, 2019 Disponível em: <sas.com/pt_br/webinars/integrando-iot-na-sua-organizacao.html>. Acesso em: 29 de set. de 2019.

MORROW, Susan; CRABTREE , Tony. THE FUTURE OF CYBERCRIME & SECURITY. **Juniper Research**, 2019. Disponível em: <juniperresearch.com/researchstore/innovation-disruption/cybercrime-security/subscription/the-future-of-cybercrime-security-threat-analys>. Acesso em: 27 de nov. de 2019.

Hacker invade câmera e conversa com menina de 8 anos nos EUA. **Portal FolhaPE**. 2019. Disponível em: < folhape.com.br/noticias/noticias/estados-unidos/2019/12/13/NWS,125130,70,586,NOTICIAS,2190-HACKER-INVADE-CAMERA-

CONVERSA-COM-MENINA-ANOS-NOS-EUA-VEJA-VIDEO.aspx> Acesso em: 13 de dez. de 2019.

AFONSO, Júlio Carlos et al. – **PROCESSAEMTNO DA PASTA ELETRONICA DE PILHAS USADAS** - Química Nova – Nota Técnica Vol. 26, N°. 4, 573-577, 2003 – Departamento de Química Analítica, Instituto de Química, Universidade Federal de rio de Janeiro, CP 68563, 21949-900 Rio de Janeiro – RJ

ALECRIM, Emerson. O que é IPv6. **Info Wester**, 2019. Disponível em: <infowester.com/ipv6.php>. Acesso em: 28 de nov. de 2019.

OLIVEIRA, Fábio Ricardo. Baterias Recarregáveis para Aplicações em Sensores IOT. **Embarcados,** 2019. Disponível em: <embarcados.com.br/baterias-recarregaveis-para-aplicacoes-em-sensores-iot>. Acesso em: 05 de dez. de 2019.

MACHADO, Marcel Jacques. **Segurança da Informação: uma Visão Geral sobre as Soluções Adotadas em Ambientes Organizacionais**. Trabalho de Conclusão de Curso (Ciência da Computação) Universidade Federal do Paraná, Curitiba, 2012.

TEZA, Vanderlei Rabelo. **Alguns Aspectos sobre a Automação Residencial – Domótica**. Dissertação (Pós-Graduação em Ciência da Computação) Universidade Federal de Santa Catarina. Florianópolis, 2002.

ALMEIDA, Fernando Mendonça de. **Internet das coisas aplicada à domótica**. Trabalho de Conclusão de Curso (Engenharia de Computação) Universidade Federal de Sergipe, São Cristóvão, 2013.

TÓFOLI, Ricardo José. **Casa Inteligente – Sistema de Automação Residencial**. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) Instituto Municipal de Ensino Superior de Assis, Assis, 2014.