INTERNET DAS COISAS: DO OTIMISMO DE MERCADO ÀS PREOCUPAÇÕES DE SEGURANÇA

Trabalho de Conclusão de Curso

Engenharia da Computação

Marcel Airlen Souza Ramos
Orientador: Prof. Edison De Queiroz Albuquerque

Universidade de Pernambuco
Escola Politécnica de Pernambuco
Graduação em Engenharia de Computação

MARCEL AIRLEN SOUZA RAMOS

INTERNET DAS COISAS: DO OTIMISMO DE MERCADO ÀS PREOCUPAÇÕES DE SEGURANÇA

Monografia apresentada como requisito parcial para obtenção do diploma de Bacharel em Engenharia de Computação pela Escola Politécnica de Pernambuco – Universidade de Pernambuco.

Recife, maio de 2022.

Ramos, Marcel Airlen Souza

Internet das coisas: do otimismo de mercado às preocupações de segurança / Marcel Airlen Souza Ramos. – Recife - PE, 2022.

xii, 44 f. : il. ; 29 cm.

Trabalho de Conclusão de Curso (Graduação em Engenharia de Computação) Universidade de Pernambuco, Escola Politécnica de Pernambuco Recife, 2022

Orientador: Prof. Dr. Edison de Queiroz Albuquerque.

Inclui referências.

1. Internet das coisas. 2. Segurança de redes. 3. Segurança de internet das coisas. I. Internet das Coisas: do otimismo de mercado às preocupações de segurança. II. Albuquerque, Edison de Queiroz. III. Universidade de Pernambuco.

MONOGRAFIA DE FINAL DE CURSO

Avaliação Final (para o presidente da banca)*

No dia 1/6/2022, às 14h00min, reuniu-se para deliberar sobre a defesa da monografia de conclusão de curso do(a) discente **MARCEL AIRLEN SOUZA RAMOS**, orientado(a) pelo(a) professor(a) **EDISON DE QUEIROZ ALBUQUERQUE**, sob título INTERNET DAS COISAS: DO OTIMISMO DE MERCADO ÀS PREOCUPAÇÕES DE SEGURANÇA, a banca composta pelos professores:

LUIS CARLOS DE SOUSA MENEZES (PRESIDENTE)
EDISON DE QUEIROZ ALBUQUERQUE (ORIENTADOR)

Após a apresentação da monografia e discussão entre os membros da Banca, a mesma foi considerada:

☒ Aprovada ☐ Aprovada com Restrições* ☐ Reprovada

e foi-lhe atribuída nota: 8,0 (oito)

*(Obrigatório o preenchimento do campo abaixo com comentários para o autor)

O(A) discente terá 5 dias para entrega da versão final da monografia a contar da data deste documento.

Luis Carlos de Sousa Menezes
AVALIADOR 1: Prof (a) **LUIS CARLOS DE SOUSA MENEZES**

Edison de Queiroz Albuquerque
AVALIADOR 2: Prof (a) **EDISON DE QUEIROZ ALBUQUERQUE**

AVALIADOR 3: Prof (a)

* Este documento deverá ser encadernado juntamente com a monografia em versão final.

Dedico este trabalho à minha família que me apoia incondicionalmente e me oferece suporte emocional para que eu possa alcançar meus objetivos.

Agradecimentos

Agradeço primeiramente a Deus, por me permitir a saúde e determinação para me dedicar por todos esses anos ao meu curso, e por estar sempre à frente dos meus objetivos e conquistas.

Aos meus pais e irmão, que me incentivaram nos momentos difíceis, e me promoveram a sabedoria necessária para enfrentar as dificuldades no decorrer da minha vida e dos meus anos na universidade.

À minha namorada, que compreendeu minha ausência, e me apoiou, enquanto me dedicava a este trabalho e ao meu curso.

Por fim agradeço aos professores, que direta, ou indiretamente, contribuíram para a elaboração deste trabalho promovendo toda a base acadêmica necessária para que obtivesse o máximo aproveitamento de seus ensinamentos, em especial ao professor Edison de Queiroz Albuquerque, por acompanhar a elaboração deste trabalho e oferecer o seu apoio durante esta jornada.

ESCOLA POLITÉCNICA
DE PERNAMBUCO

Autorização de publicação de PFC

Eu, **Marcel Airlen Souza Ramos** autor(a) do projeto de final de curso intitulado: **INTERNET DAS COISAS: DO OTIMISMO DE MERCADO ÀS PREOCUPAÇÕES DE SEGURANÇA;** autorizo a publicação de seu conteúdo na internet nos portais da Escola Politécnica de Pernambuco e Universidade de Pernambuco.

O conteúdo do projeto de final de curso é de responsabilidade do autor.

Marcel A. S. Ramos

Marcel Airlen Souza Ramos

Orientador(a): **Edison de Queiroz Albuquerque**

Coorientador(a):

Prof, de TCC: **Daniel Augusto Ribeiro Chaves**

Data: 1/6/2022

Resumo

O presente trabalho tem como objetivo apresentar uma análise sobre a segurança dos dispositivos da Internet das Coisas bem como relacionar os potenciais riscos e vulnerabilidades da tecnologia com o crescimento na adoção da tecnologia pelo mercado. Inicio com a contextualização dos temas Internet das Coisas e Segurança Cibernética. A partir das informações obtidas, foi realizada uma reflexão sobre o contexto de segurança cibernética de dispositivos da Internet das Coisas, evidenciando que apesar de um cenário otimista do mercado e com crescimento na adoção, diversas políticas de privacidade e melhorias na segurança dos protocolos e tecnologias embarcadas nos dispositivos devem ser desenvolvidas para podermos considerar a tecnologia segura.

Palavras-chave: Segurança cibernética. Internet das coisas. Internet. Segurança. Privacidade.

Abstract

The present work aims to present an analysis of the security of Internet of Things devices as well as to relate the potential risks and vulnerabilities of the technology with the growth in the adoption of technology by the market. I begin with the contextualization of the topics Internet of Things and Cyber Security. From the information obtained, a reflection was carried out on the cybersecurity context of the Internet of Things devices, showing that despite an optimistic market scenario and growth in adoption, several privacy policies and improvements in the security of protocols and technologies embedded in devices must be developed so that we can consider the technology safe.

Keywords: Cybersecurity. Internet of Things. Internet. Security. Privacy.

Lista de Figuras

Lista de Símbolos e/ou Siglas

API – *Application Program Interface*

ASP – *Active Server Pages*

IAB - Internet Architecture Board

CoAP - *Constrained Application Protocol*

DDoS – *Distributed Denial of Service*

DoS – *Denial of Service*

HTTP – *Hypertext Transfer Protocol*

IoT – *Internet of Things*

IP – *Internet Protocol*

IPv6 – *Internet Protocol version 6*

M2M – *Machine-to-Machine*

NFC - *Near Field Communication*

REST – *Representational State Transfer*

RFID – *Radio Frequency Identification*

SMS – *Short Message Service*

TCP – *Transmission Control Protocol*

UDP – *User Datagram Protocol*

US$ - Dólares Americanos

Sumário

Capítulo 1
Introdução

Ao longo da última década, o termo *Internet of Things* (IoT) tem ganhado cada vez mais tração e feito parte do conhecimento de grande parcela da população, seja pelas aplicações em dispositivos para *smart homes*, seja pelas diversas outras aplicabilidades e comodidades que ter um dispositivo conectado a rede nos traz (ROSE; ELDRIDGE; CHAPIN, 2015)

A Internet das Coisas (IoT – *Internet of Things*) é o conceito de uma rede de interconexão entre objetos físicos do dia a dia. Em outras palavras, é uma maneira de objetos como por exemplo, a sua geladeira, seu aparelho de ar-condicionado e sua televisão, estarem conectados a mesma rede de internet e se comunicando entre si, de forma a executar algum processo computacional (ATZORI; IERA; MORABITO, 2010)

Em 2020, estimava-se que o número de dispositivos IoT no mundo fosse de 8,74 bilhões, com previsão de triplicar para mais de 25,4 bilhões de dispositivos IoT em 2030 (VAILSHERY, 2020). Tendo este cenário em vista, “A Bain & Company espera que os mercados combinados para a Internet das Coisas, incluindo *hardware*, *software*, integração de sistemas e serviços de dados e telecomunicações, cresçam para US$ 520 bilhões até 2021 – mais que o dobro dos US$ 235 bilhões gastos em 2017 – a maioria dos quais serão capturados pelos segmentos empresarial e industrial” (BAIN & COMPANY, 2018).

Apesar do cenário extremamente otimista em torno do mercado e da tecnologia, existem questões, principalmente relacionadas a segurança, que incomodam os clientes. Muito é questionado sobre o quanto os dispositivos IoT interferem na violação da privacidade dos usuários e os potenciais riscos aos negócios, sejam eles financeiros ou industriais, que as brechas de segurança podem vir a causar.

Este trabalho busca promover uma análise sobre a segurança da Internet das Coisas, dado o cenário atual de segurança cibernética, apoiando-se em análise de artigos, relatórios, fundamentações estatísticas e revisões de literatura para alcançar o estado da arte.

O trabalho está disposto de forma que os próximos dois capítulos servirão para nos contextualizarmos sobre os temas: Internet das Coisas – Capítulo 2; e Segurança de IoT – Capítulo 3; de forma a compreendermos o contexto geral da análise proposta que está situada no capítulo 4. Por fim no capítulo 5 traremos conclusões sobre a análise que foi realizada e os resultados que foram obtidos com a pesquisa.

Capítulo 2

IoT: *Internet of Things*

A Internet das Coisas se tornou um tópico bastante popular na última década, dados os avanços tecnológicos inerentes aos dispositivos eletrônicos que estão a cada passo mais potentes e em tamanho reduzido, muito em conta também aos avanços industriais e de produção em escala de componentes como *chips* e microcontroladores, essenciais para tornar os objetos, ou "coisas", conectáveis.

Atualmente nos deparamos com diversas propagandas de produtos ou serviços com o termo "smart", sejam *smart homes*, *smart cities*, *smart security*, cada dia estamos mais familiarizados com a tecnologia que nos permite mais comodidade e interoperabilidade seja presencialmente ou de maneira remota. Soluções como geladeiras e aparelhos de televisão inteligentes já não são mais produtos *high end* destinados a poucos consumidores, e soluções ainda mais abrangentes como sistemas de assistência veicular integrada, desenvolvidos para oferecer mais segurança e relatórios mais precisos sobre o desempenho e estado de conservação dos componentes dos veículos já são amplamente utilizados.

A partir deste momento usaremos o termo IoT para descrever a Internet das Coisas, termo este que foi usado pela primeira vez em 1999 por Kevin Ashton, para descrever um sistema em que objetos poderiam se conectar com a internet por meio de sensores. O uso deste termo foi feito para ilustrar o poder do uso de tarjas de identificação por rádio frequência (RFID) na cadeia de suprimentos a fim de obter o rastreio de produtos e bens sem intervenção humana com o uso da Internet (ROSE; ELDRIDGE; CHAPIN, 2015). Atualmente o IoT se tornou um termo aplicável a todos os tipos de itens, dispositivos e sensores que usamos no dia a dia.

2.1 Conceitos e definições

O IoT além de ser um campo de estudos recente, também embarca questões multidisciplinares do campo das tecnologias e telecomunicações, por este motivo

também não há uma definição formal para o conceito de IoT. Alguns estudiosos afirmam que para ser um dispositivo IoT, ele deve se comunicar através da internet com o protocolo IP, entretanto outros afirmam que o conceito não se prende apenas à conexão com a internet, podendo haver essa comunicação de forma *Machine-to-Machine* (M2M), ou de forma a ter uma conexão física, que por fim se conecte com um gateway atrelado à rede.

Entre algumas das definições, podemos destacar a definição de IoT segundo o dicionário Cambridge, “objetos com dispositivos computacionais em que são capazes de conectar-se entre si e trocar dados usando a internet” (“the internet of things”, 2022).

Podemos também destacar a definição apresentada por Rose et al. em que cita o documento RFC7452 “Architectural Considerations in Smart Object Networking” da Internet Architecture Board (IAB) (TSCHOFENIG et al., 2015):

> O termo “Internet of Things” (IoT) denota uma tendencia onde muitos dispositivos embarcados empregam serviços de comunicação oferecidos pelos protocolos de internet. Muitos desses dispositivos, muitas vezes chamados de “objetos inteligentes”, não são operados diretamente por humanos, mas existem como componentes em edifícios ou veículos, ou estão espalhados no ambiente (ROSE; ELDRIDGE; CHAPIN, 2015, p. 15).

Portanto, diante destas observações, para o presente trabalho consideraremos a definição de Internet das Coisas como sendo uma rede, ou sistema, que interconecta diferentes dispositivos, sensores e objetos, que possuam capacidade de processamento, interagem com o ambiente e gerem dados que então serão compartilhados de alguma forma pela internet.

2.2 Arquitetura e Modelos de Comunicação

Um aspecto crítico para a essência da Internet das Coisas é a interconexão comunicação entre os dispositivos e sensores, entretanto isto é um dos grandes desafios da tecnologia, dado a falta de padrões de estrutura de dados e as

diferentes tecnologias que podem ser embarcadas na solução a livre critério do fabricante do dispositivo. Como exemplo temos dispositivos que utilizam de protocolos como Bluetooth, Z-Wave ou ZigBee, e esta interoperabilidade dentre diferentes protocolos de comunicação é um dos desafios chave da tecnologia. Abaixo apresentaremos os quatro modelos de comunicação mais comumente utilizados para a definição da comunicação entre os dispositivos IoT.

2.2.1 Modelo *Device-to-Device*

Este modelo representa a comunicação direta entre dois ou mais dispositivos diretamente, sem a necessidade de uma aplicação ou serviço intermediário. Os dispositivos neste modelo podem se comunicar de diversas formas, seja pela internet, ou mais comumente por protocolos como o Bluetooth, o Z-Wave e o ZigBee, como mostra a Figura 1 (PAWAR; TRIVEDI, 2019).

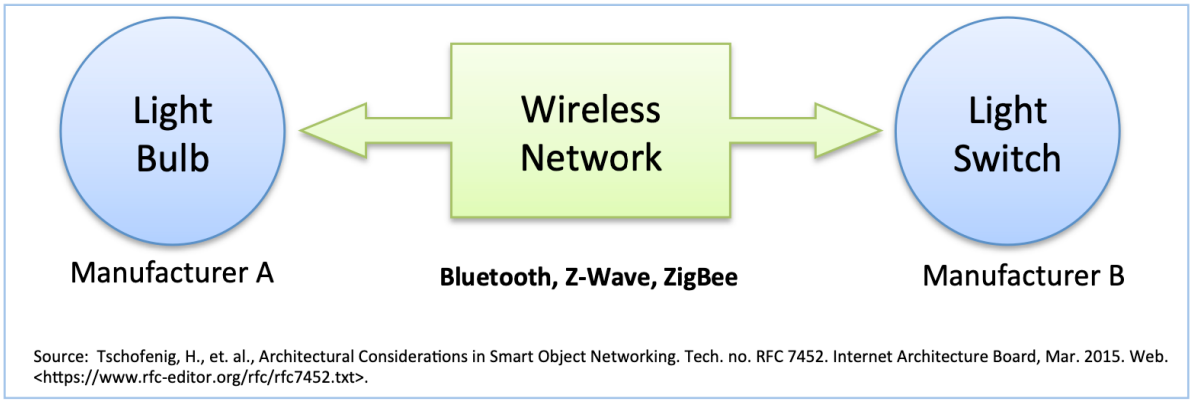

Figura 1. Exemplo de modelo de comunicação *device-to-device* (ROSE; ELDRIDGE; CHAPIN, 2015)

Usualmente este tipo de comunicação é feito por dispositivos que trocam pequenos pacotes de dados entre si, como dispositivos ligados à automação residencial. Entretanto, um ponto de atenção é referente à interoperabilidade dos diferentes fabricantes com outros dispositivos, por exemplo, uma lâmpada que opera com o protocolo ZigBee, não se comunica nativamente com um interruptor que faz uso do protocolo Z-Wave, e vice-versa (TSCHOFENIG et al., 2015). Dado este cenário, isto requer uma atenção dos usuários na obtenção destes dispositivos, dado que para o correto funcionamento eles devem conseguir se comunicar, levando muitas vezes à compra de produtos de uma mesma linha ou fabricante. Já

por parte dos fabricantes, exige um custo maior para adaptação dos produtos aos diferentes protocolos de comunicação existentes (ROSE; ELDRIDGE; CHAPIN, 2015).

2.2.2 Modelo *Device-to-Cloud*

Na comunicação *device-to-cloud*, o dispositivo IoT conecta-se diretamente a um serviço de internet em nuvem como uma aplicação de serviço que irá trocar dados com um servidor, geralmente um servidor proprietário do próprio fabricante do dispositivo, o qual posteriormente se conectará com a internet a fim de promover os serviços. Conforme podemos observar o exemplo na Figura 2 (TSCHOFENIG et al., 2015).

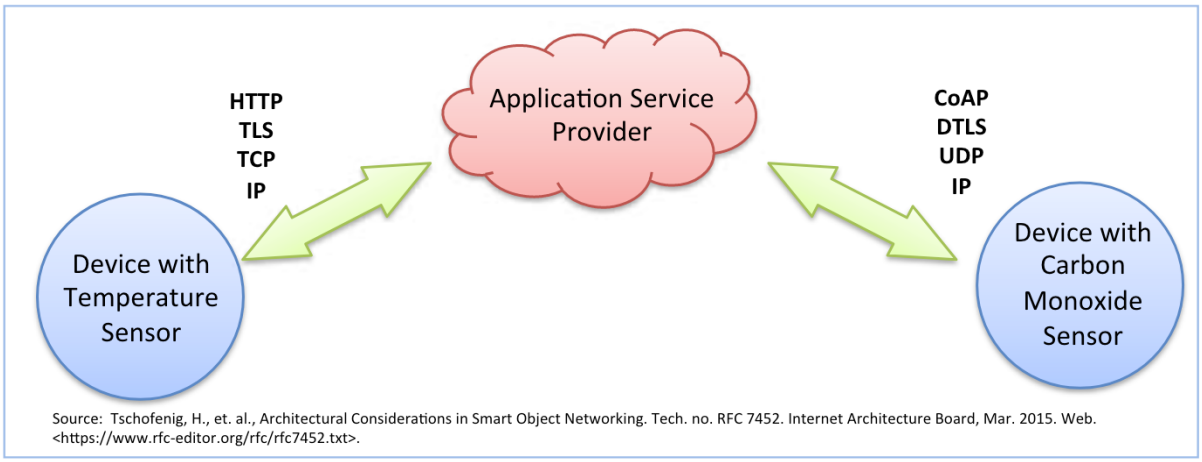

Figura 2. Exemplo de modelo de comunicação *device-to-cloud* (ROSE; ELDRIDGE; CHAPIN, 2015)

Este modelo de comunicação é interessante pois opera já baseado em conexões de redes IP, e possibilita o tratamento de informações dos dispositivos para estender suas capacidades de uso, como por exemplo no caso dos equipamentos de ar-condicionado, ou termostatos, que podem ter processamento dos dados a fim de relatar ao usuário final o seu consumo de energia elétrica (HASSAN; UR; MADANI, 2017).

Apesar desta maior facilidade de comunicação, a interoperabilidade entre dispositivos de diferentes fabricantes ainda se mostra um desafio, dado que as redes conectadas pelos dispositivos geralmente são de proprietários, o que impacta no

formato e estrutura de dados que não atendem a um único padrão dados os diferentes fabricantes dos dispositivos. Entretanto, os usuários podem ter maior segurança na aquisição de equipamentos da mesma fabricante, dado que a comunicação se mostra muito mais favorável e o padrão dos dados se mantém (ROSE; ELDRIDGE; CHAPIN, 2015).

2.2.3 Modelo *Device-to-Gateway*

A comunicação *device-to-gateway* consiste na comunicação dos dispositivos IoT com um gateway local, onde este *gateway* será responsável por interagir com os dispositivos que não tenham capacidade de se conectar diretamente à internet, e transferir os dados coletados por estes dispositivos para a nuvem. O modelo pode ser observado na Figura 3 (TSCHOFENIG et al., 2015).

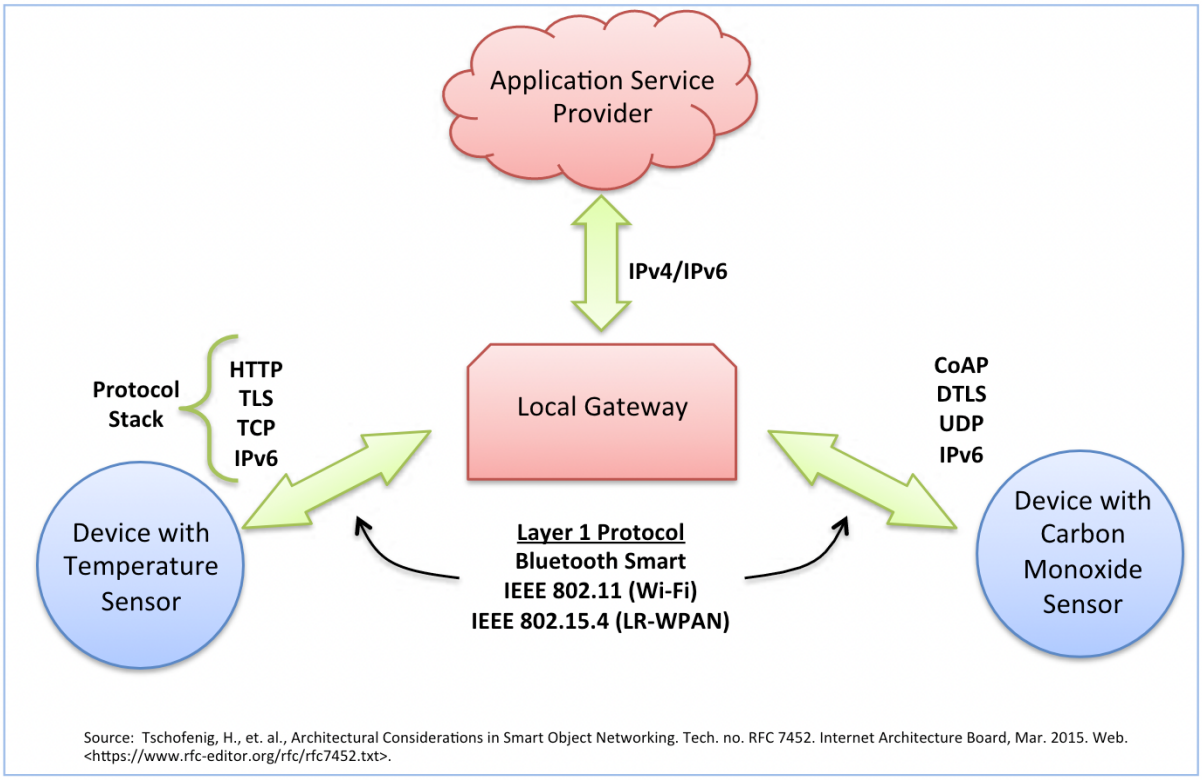

Figura 3. Exemplo de modelo de comunicação *device-to-gateway* (ROSE; ELDRIDGE; CHAPIN, 2015)

Este modelo de comunicação pode ser visto em dispositivos *wearables* como *smart watches* e *fitness trackers*, dada a impossibilidade de comunicação direta destes dispositivos eles utilizam-se de um *gateway*, usualmente um *smartphone*,

onde há um aplicativo proprietário que coleta estes dados dos dispositivos e se comunica com o serviço em nuvem do produto a fim de gerar relatórios das atividades físicas do usuário.

O uso de um *gateway* também pode ser atribuído pela facilidade de comunicação de diferentes dispositivos de variados fabricantes e a adição de camadas de segurança na comunicação dos dados e operação dos dispositivos, diminuindo a dificuldade do desafio da interoperabilidade, dado que smartphones modernos atendem a diversos protocolos de comunicação implantados nos dispositivos IoT atualmente, como Bluetooth, Wi-Fi, *Near Field Communication* (NFC) etc. (HASSAN; UR; MADANI, 2017).

Entretanto, a utilização deste modelo de comunicação implica um desafio técnico de implementação da camada de aplicação, o serviço que estará hospedado no *gateway*, de forma que isto implica em maior complexidade para o desenvolvimento e adaptação aos diferentes protocolos, além da maior complexidade no lançamento de atualizações de *software* e cobertura de novos dispositivos que venham a ser fabricados (ROSE; ELDRIDGE; CHAPIN, 2015).

2.2.4 Modelo *Back-End Data-Sharing*

Segundo Mouha (2021, p. 93), o modelo de *back-end data-sharing*, ou compartilhamento de dados de *back-end* – tradução livre:

> Refere-se à arquitetura de comunicação que permite ao usuário exportar e analisar dados de dispositivos inteligentes de um serviço em nuvem em conjunto com dados de outras fontes. O dado é enviado para dois *Active Server Pages* (ASPs).

Esta arquitetura permite por exemplo que responsáveis de indústrias ou escritórios possam coletar e analisar dados a partir de dispositivos IoT, e outros dispositivos conectados a rede, a fim de estimar o consumo de energia na planta (ROSE; ELDRIDGE; CHAPIN, 2015).

No modelo de comunicação de *device-to-cloud*, que vimos anteriormente, ocorre a geração de silos de dados por parte de cada um dos dispositivos, estes

silos são locais onde os dados são armazenados e ficam indisponíveis para consumo de outros serviços devido à esta arquitetura. No *back-end data-sharing*, se bem implementada esta arquitetura, permite o fácil acesso e análise dos dados produzidos por todo o espectro de dispositivos presentes no ambiente. Além de facilitar a migração destes dados quando ocorre a mudança entre os dispositivos IoT (HASSAN; UR; MADANI, 2017).

Neste modelo há a sugestão de implementação de uma abordagem que utilize serviços de nuvem ou *Application Program Interfaces* (APIs) conectadas a nuvem para promover a interoperabilidade entre os dados dos diferentes dispositivos que estão armazenados em nuvem, conforme demonstrado na Figura 4 (TSCHOFENIG et al., 2015).

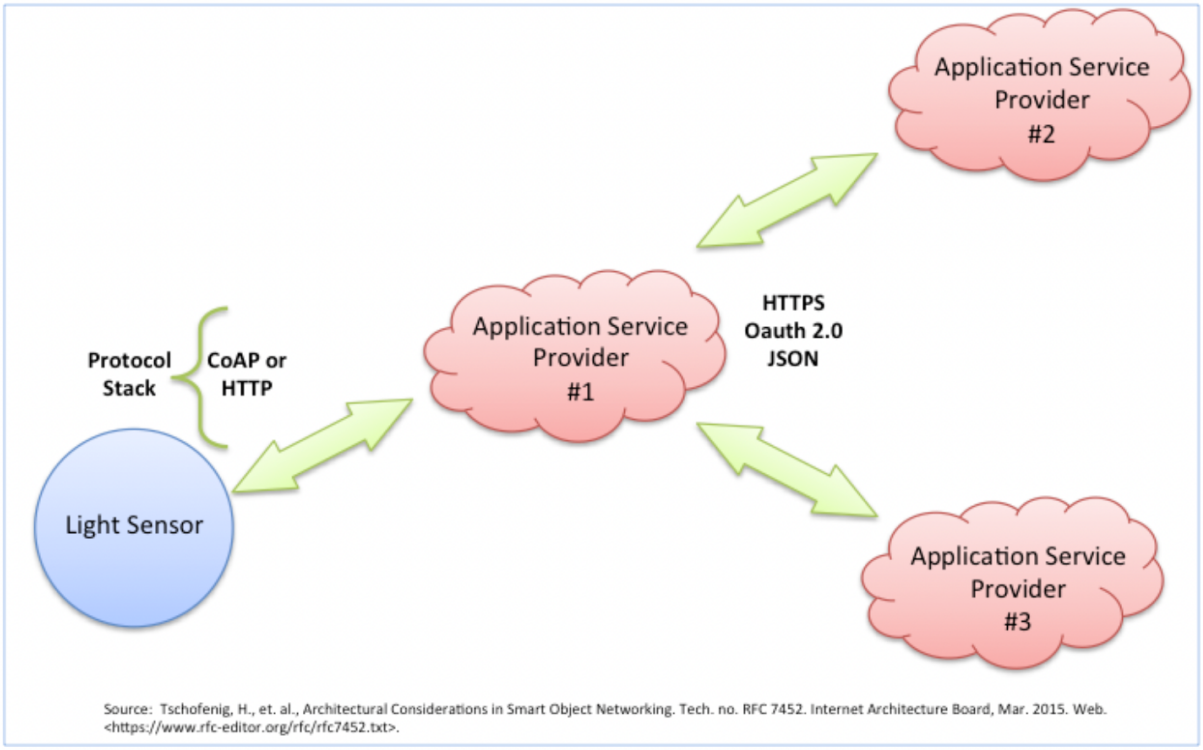

Figura 4. Exemplo de modelo de comunicação *back-end data-sharing* (ROSE; ELDRIDGE; CHAPIN, 2015)

2.3 Aplicações e Tendências

A Internet das Coisas vem crescendo de forma exponencial, apesar de termos cada vez mais familiaridade com os termos iniciados por "*smart*", como *smart homes*, *smart watches*, o IoT não se resume apenas a estas áreas de aplicação ou produtos. Atualmente o IoT vem sendo cada vez mais pesquisado e inserido em contextos de produção diversos, como por exemplo: monitoramento de doenças, gerenciamento de energia, controle de tráfego nas cidades, entre outros, gerando diferentes produtos em diferentes áreas de aplicação, mas todos com um mesmo propósito, facilitar a vida das pessoas e gerar um impacto positivo na humanidade e nos negócios.

O IoT se divide em nove áreas de aplicação, sendo elas: Seres Humanos, Residências, Ambientes Comerciais, Escritórios, Fábricas, Indústrias, Transportes, Cidades e Ar-livre (FAZION FILHO, 2016). A seguir, apresentaremos algumas das definições e soluções de cada área de aplicação:

2.3.1 Seres Humanos

Os dispositivos IoT categorizados como aplicações voltadas aos seres humanos são geralmente dispositivos vestíveis, ou dentro do copo humano, onde tem como objetivo promover a saúde, o bem-estar, mudanças de hábitos, controle e monitoramento de doenças, entre outros. Dentro desta área os dispositivos podem ser divididos entre duas categorias de objetivos: melhorar a saúde e aumentar a produtividade (JAMES MANYIKA et al., 2015).

Estes dispositivos se diferem dos demais, pois comumente as aplicações IoT geram uma ação como consequência da interação entre os sensores e o ambiente, como o desligamento de um equipamento por exemplo, entretanto neste caso as informações geradas pelos sensores servem para auxiliar a tomada de decisões do ser humano.

Estima-se que o impacto econômico da aplicação de IoT na saúde e bem-estar seja entre 170 bilhões de dólares e 1,6 trilhões de dólares em 2025, dada a crescente adoção das soluções por parte dos usuários e o potencial de

desenvolvimento de tecnologias como nano robótica e injetáveis, que possam favorecer ainda mais a área de aplicação, a diminuição dos custos com tratamento de doenças e o aumento da expectativa de vida da população (JAMES MANYIKA et al., 2015).

2.3.2 Residências

As aplicações residenciais abrangem principalmente o controle e gerenciamento de água e energia das residências, execução automatizada de tarefas domésticas, e segurança. Gerando assim ambientes conectados onde possa haver o desligamento automático de equipamentos, a execução de tarefas domésticas ao controle de um toque, e a detecção de invasores ou fogo de forma remota. Gerando assim redução de custos com energia, e controle total de equipamentos como fechaduras e janelas (HASSAN; UR; MADANI, 2017).

Estima-se que o impacto econômico das aplicações de IoT voltadas para uso doméstico sejam na casa dos 350 bilhões de dólares em 2025 (JAMES MANYIKA et al., 2015). A depender da implementação de soluções que convençam os usuários da sua praticidade e usabilidade, de forma a poder desempenhar principalmente tarefas domésticas como lavar, cozinhar, limpar, que demandam bastante tempo diariamente e consomem a nossa produtividade.

Outro ponto que pode ser de grande impacto é o gerenciamento de energia, automatizando horários com base em Inteligência Artificial, de forma a aprender os padrões de horários que os residentes se encontram dentro e fora de casa, auxiliaria no controle de temperatura de um termostato por exemplo, coordenando os aparelhos de ar-condicionado, entre outros a trabalhar de maneira inteligente e otimizada, tudo ao alcance do smartphone que acompanharia todos os status emitidos pelos dispositivos.

2.3.3 Ambientes Comerciais

Nesta categoria estão incluídas aplicações de IoT em espaços físicos onde há o comércio de bens e serviços, como por exemplo lojas, mercados e até mesmo

showrooms e exibições onde esteja acontecendo apenas a exposição de produtos, além de cinemas, teatros e arenas esportivas.

Os dispositivos IoT nestes espaços se beneficiam do crescimento das vendas online, que apoiam o consumo de bens e serviços, que podem incluir o tipo de venda "*cross-channel*" onde a experiência de compra e venda inicia online e finaliza de forma presencial com a retirada do produto, ou mesmo a experimentação do produto na loja física e a compra virtual (HASSIJA et al., 2019).

Algumas das aplicações incluem o *self-checkout*, onde o próprio cliente realiza o mapeamento do produto que quer adquirir e o pagamento sem a necessidade de um atendente de caixa. Outros exemplos de aplicações seriam dispositivos para controle de estoque automatizado, sensores antifurto, disposição de produtos em loja baseado em padrões de comportamento dos clientes que podem ser obtidos através de câmeras com processamento de imagem ou sensores de presença, entre outras.

Estima-se que o impacto econômico desta área esteja entre 410 bilhões de dólares e 1,2 trilhões de dólares por ano em 2025 (JAMES MANYIKA et al., 2015). Entretanto esta área sofre bastante resistência devido ao modelo de mercado atual, onde vemos muitos estabelecimentos comerciais familiares e de pequeno porte, que esbarram nos custos e volume de vendas que suportariam os investimentos nesse tipo de tecnologia.

2.3.4 Escritórios

No contexto de aplicações voltadas para escritórios ou prédios corporativos destacam-se principalmente aplicações voltadas à redução de custos com energia e cuidados ao meio ambiente, dado o volume de recursos que são gastos diariamente nestes espaços que alocam uma grande quantidade de pessoas, além da segurança que é outro fator chave e indispensável no contexto empresarial.

Como exemplos de aplicações podemos destacar sensores de presença que se comunicam com sistemas de gerenciamento de dispositivos e energia, a fim de reduzir o desperdício de energia em salas com aquecimento, aparelhos de ar-condicionado e luzes ligadas em que não há a presença de pessoas ou a

necessidade de gastos excessivos destes recursos. Câmeras de segurança que monitoram ativamente através de processamento de imagem, o acesso dos indivíduos a determinados setores críticos, também podendo mitigar riscos de acidentes e intrusão, e até mesmo mapear a produtividade dos trabalhadores que gostam de passar longos períodos nas copas conversando e tomando café.

Estima-se que em 2025, de 70 bilhões de dólares a 150 bilhões de dólares por ano sejam movimentados neste área de aplicação (JAMES MANYIKA et al., 2015). Entretanto, a adoção de soluções voltadas para essa área possui um alto custo, fator esse que se torna restritivo para a maioria das empresas e escritórios. O desenvolvimento de novas soluções e pesquisas na área favorecerá a diminuição do custo de desenvolvimento destes produtos e impulsionará a adoção destes dispositivos e serviços nos próximos anos.

2.3.5 Fábricas

A categoria de fábricas abrange os locais onde há a produção de itens, juntamente aos *data centers*, fazendas e hospitais. As soluções propostas atuam na otimização da produção e controle das operações, permitindo mais segurança para os colaboradores e controle total das etapas da cadeia de produção.

Estima-se que serão aplicados em torno de 3,7 bilhões de dólares por ano em 2025 no mercado em torno de soluções IoT para fábricas (JAMES MANYIKA et al., 2015), seja com o controle logístico de armazéns, monitoramento de atividade dos funcionários a fim de detectar possíveis interações perigosas com máquinas da fábrica pelos trabalhadores e promover um maior bem-estar para os colaboradores que atuam nestes locais.

Entretanto diversas melhorias em maquinário, operações e processos precisam ser implantados a fim de agregar todos os possíveis benefícios que a implantação de sistemas e dispositivos IoT, como a manutenção preditiva dos equipamentos, possam trazer para estes ambientes.

2.3.6 Indústrias

Nesta categoria estão inclusas operações de exploração e produção de petróleo e gás, mineração e construção. Estas operações são feitas ao ar-livre, com um alto nível de complexidade e imprevisibilidade, com a atuação de diversas equipes especializadas para obter o propósito final.

Os setores de petróleo e gás têm sido onde mais houve a implementação de soluções IoT, dado a utilização de maquinário pesado, rígidos padrões de segurança ambiental necessários e alto custo das operações. Neste cenário houve bastante espaço para implantação de caminhões autônomos, centros de controle especializado, que comandam bombas de sucção de petróleo mesmo do outro lado do mundo, e uma vasta quantidade de dados que são coletados, processados e analisados em tempo real para o perfeito funcionamento destas operações.

Estima-se que a economia em torno destas aplicações girará em torno de 160 bilhões de dólares por ano em 2025, dado um cenário pessimista, até 930 bilhões de dólares por ano nos cenários mais otimistas. Estes valores são baseados em expectativas de redução de custos, maior eficiência das operações e produtividade nestes ambientes (JAMES MANYIKA et al., 2015).

2.3.7 Transportes

O uso de aplicações de IoT tem hoje uma ótima visibilidade com o sucesso da montadora Tesla, que é referência no desenvolvimento de carros autônomos e sistemas de segurança informatizados. O uso de IoT nos transportes também está atrelado ao monitoramento da necessidade de manutenção nos veículos - sejam eles carros, caminhões, trens ou aviões –, a redução de custos e aumento da vida útil destes meios de transporte (HASSAN; UR; MADANI, 2017).

Projeta-se que o impacto econômico na cadeia dos transportes estará situada entre 210 bilhões de dólares a 740 bilhões de dólares por ano em 2025 (JAMES MANYIKA et al., 2015). Onde a maior parte deste valor estará concentrada em aumentar a segurança dos veículos e a manutenção condicionada ao monitoramento do estado das peças e sistemas do veículo.

2.3.8 Cidades

O termo “*smart cities*” – Cidades Inteligentes - está cada vez mais em pauta nos dias de hoje, dados os avanços em urbanização e a preocupação com as questões ambientais e o bem-estar da população, as cidades estão buscando cada vez mais maneiras de otimizar os seus gastos com recursos como água e energia, prover melhores sistemas de gerenciamento de lixo e esgoto, aliviar o congestionamento principalmente nos grandes centros, além de soluções para a área da saúde e educação.

Alguns exemplos de cidades que já adotam alguma solução de IoT voltada a *smart cities* são Londres no Reino Unido; Barcelona na Espanha e Amsterdam nos Países Baixos (HASSAN; UR; MADANI, 2017). No qual estima-se uma movimentação de até 1,7 bilhões de dólares por ano em 2025, impulsionados principalmente pela redução nos custos de recursos, melhoria e otimização de infraestrutura nas cidades e melhora na saúde e redução de doenças causadas pela poluição (JAMES MANYIKA et al., 2015).

2.3.9 Ar-livre

Nesta categoria estão incluídas aplicações ao ar-livre como envio de pacotes, transporte de contêineres, navegação de veículos, monitoramento de condições climáticas, entre outras (FAZION FILHO, 2016).

Esta é uma área que ainda está em desenvolvimento, principalmente no contexto da infraestrutura fora das cidades, baixo custo dos sensores e o alcance destes equipamentos para poderem ser monitorados em espaços fora das cidades. Estima-se que este mercado tem potencial de alcançar até 850 bilhões de dólares por ano em 2025 (JAMES MANYIKA et al., 2015).

2.4 Riscos inerentes à tecnologia

A Internet das Coisas já vem sendo pesquisada a alguns anos e vem cada vez mais sendo aplicada e adotada nas mais diversas áreas como foi visto na seção anterior. Porém, o grande volume de dados transacionados por estes dispositivos e

sensores geram algumas questões que intrigam os usuários e os mais resistentes à adoção da tecnologia.

Questões como, qual é o limite de dados que estes sensores geram estando em nossas casas, observando e coletando dados sobre os nossos hábitos e rotinas, obedecem? Trazem á tona o quanto as empresas e fabricantes destes produtos e serviços têm acesso à nossa privacidade, podendo expor e mapear questões íntimas que não dizem respeito a tal exposição ou mesmo o propósito daquele produto.

Outra questão bastante ressaltada é o quão seguros estes dados estão quando em posse das empresas que realizam a coleta e processamento, ou mesmo se criminosos não poderão obter acesso ao sistema de segurança residencial que instalamos nos nossos lares, permitindo observar o interior das nossas casas. Ou mesmo, os potenciais riscos quando aplicados em sistemas de infraestrutura, como sistemas de distribuição de água e energia, que caso infiltrados e colapsados podem gerar grande prejuízo e caos para empresas, governos e principalmente a população das cidades.

Ao longo do próximo capítulo, aprofundaremos no tema segurança da informação, com o propósito de entendermos melhor como estas informações e dados devem ser geridos, quais paradigmas são tratados antes mesmo da concepção do produto e os padrões de segurança que são aplicados no contexto das aplicações IoT.

Capítulo 3
Segurança de IoT

A segurança cibernética busca prover meios e técnicas de proteger as informações de pessoas e empresas que transitam na internet, de forma a preservar a confidencialidade, integridade e disponibilidade das informações (VON SOLMS; VON SOLMS, 2018) do ataque de agentes maliciosos, os temidos hackers, que buscam maneiras de explorar esses dados e obter de forma criminosa estas informações violando direitos básicos como a privacidade e causando danos nas vidas dos indivíduos.

De acordo com a CompTIA (2020), a segurança cibernética pode ser categorizada em cinco tipos distintos: Segurança de infraestrutura crítica; Segurança do aplicativo; Segurança de rede; Segurança de nuvem; e Segurança da Internet das Coisas (IoT). Este último será o tópico de discussão deste capítulo, abordando os paradigmas que regem esta categoria, além de discussões sobre a privacidade dos dados que são gerados por este tipo de aplicações e dispositivos, e quais os tipos mais comuns de ataques e ameaças que são exploradas nestes dispositivos.

3.1 Princípios que regem a segurança

A segurança cibernética e a segurança da informação muitas vezes são confundidas, dados os seus aspectos e paradigmas que são próximos e bastante relacionados.

A segurança da informação se apoia em três pilares chave, a conservação da confidencialidade, integridade e disponibilidade da informação (WANG; LU, 2013), onde não há uma definição específica do local onde esta informação se encontra, ou o meio por onde transita.

Já a segurança cibernética compartilha dos mesmos pilares, entretanto ela se restringe ao meio cibernético, no qual as informações estão armazenadas ou transitam por meio da internet (VON SOLMS; VON SOLMS, 2018).

Introduzidos estes conceitos, importante para definirmos corretamente que a segurança cibernética está contida dentro do espectro da segurança da informação. Segundo Goel (2019) e Mahmoud et al. (2015), há ainda um quarto pilar, sendo este atrelado à segurança de IoT, a autenticidade. A seguir, exploraremos melhor as definições de cada um destes objetivos de segurança:

- Confidencialidade: Baseia-se em duas premissas, a primeira é a de garantir a proteção e privacidade das informações proprietárias. E a segunda é a negação ao acesso de informações privadas por terceiros que não tenham autorização.

- Integridade: A integridade garante que os dispositivos IoT e as informações não possam ser modificadas ou utilizadas por alguém que não está autorizado.

- Disponibilidade: Significa que a informação e os recursos computacionais estarão sempre disponíveis quando requeridos. Ou seja, sempre que um dispositivo IoT detectar um parâmetro físico, o sistema deve armazenar e processar os dados para operar corretamente nos canais de comunicação.

- Autenticidade: Garante a genuinidade das transações e informações. Portanto, os sistemas devem validar-se entre si respeitando este princípio para poderem participar na transação.

3.2 Paradigmas de segurança de IoT e a segurança das comunicações

Por serem dispositivos com limitado poder computacional e com restrições de comunicação e energia, os protocolos convencionais de segurança atrelados ao protocolo IP não podem ser utilizados. Por isto, foram criados novos métodos e

mecanismos de comunicação específicos para o cenário do IoT (MENEGHELLO et al., 2019). Logo abaixo falaremos sobre algumas destas tecnologias de comunicação mais populares.

3.2.1 ZigBee

ZigBee é um padrão de comunicação criado pela ZigBee Alliance e que é amplamente utilizado como tecnologia para conectar dispositivos IoT devido o seu baixo custo e consumo de energia (MENEGHELLO et al., 2019; RAMYA; SHANMUGARAJ; PRABAKARAN, 2011).

O ZigBee devido a suas propriedades permite que dispositivos que necessitem de um longo tempo de bateria, mas que não precisam de uma alta taxa de transferência, como no caso do Bluetooth, a obterem vários meses ou até anos de autonomia de bateria (ERGEN, 2004).

A rede ZigBee é composta de três tipos de nós (KHANJI; IQBAL; HUNG, 2019) sendo o primeiro deles o Coordenador (*Coordinator*). Este é o nó raiz da rede, que administra as conexões de outros nós e permite outros nós filhos se juntarem a rede. Além disto, também provê serviços de roteamento e segurança. O segundo é o nó de Roteamento (*Router*), este não é obrigatório na rede, mas é comumente encontrado e responsável por entregar mensagens para os outros nós. Por fim, temos os nós de Dispositivo Fim (*End Device*), os quais apenas enviam e recebem mensagens.

Cada rede ZigBee é composta por um Centro de Confiança (*Trust Center*), um dispositivo confiado por todos os outros nós da rede, geralmente sendo este o nó Coordenador que possui como responsabilidades (MENEGHELLO et al., 2019):

- Autenticar os dispositivos que desejam se juntar a rede;
- Decidir pelo aceite ou não dos pedidos de entrada na rede;
- Manter e distribuir as chaves de rede;
- Possibilitar a segurança de ponta-a-ponta entre os dispositivos;

Alguns pontos de vulnerabilidade se dão devido a possibilidade de *sniffing* da rede ZigBee de forma a obter as chaves de comunicação da rede, e a partir disto interceptar as mensagens. Outra maneira é utilizando softwares especializados, como o KillerBee, que permite o *sniffing* e a injeção de tráfego na rede, além de decodificar e manipular ataques (WHITEHURST; ANDEL; MCDONALD, 2014).

3.2.2 Bluetooth Low Energy

O *Bluetooth Low Energy* (BLE) é uma tecnologia que foi projetada para complementar o Bluetooth clássico, bem como ser a tecnologia sem fio de menor potência possível que pode ser projetada e construída (HEYDON, 2012).

O BLE permite que redes de baixa distância sejam criadas utilizando características semelhantes ao Bluetooth convencional, de forma a aliar um baixo custo e um baixo poder computacional por parte dos dispositivos que utilizam essa comunicação, sendo empregada para sistemas que precisam de poucas conexões em momentos específicos, o que permite o seu baixo consumo de energia. Por estes motivos, o BLE se tornou a forma de comunicação mais amplamente utilizada nos dispositivos IoT (BARUA et al., 2022).

Os dispositivos inteligentes que utilizam o BLE são geralmente conectados aos smartphones dos usuários e trabalham como portais de informação. Por exemplo nos *smart watches* e *smart bands* temos a possibilidade de ler mensagens *Short Message Service* (SMS) ou notificações que são transportadas desde os nossos celulares para os nossos pulsos graças à essa tecnologia (WANG et al., 2020).

A rede BLE é composta por dois tipos de dispositivos: mestres (masters) e escravos (*slaves*). Onde o mestre geralmente é um dispositivo com maior poder computacional, geralmente os aparelhos celulares, e o escravo é o nosso *fitness tracker* por exemplo, que possui recursos de energia, memória e capacidade de processamento limitados. O mestre é responsável por administrar as conexões da rede e solicitar as informações aos nós escravos. E apenas um mestre pode ser associado a cada nó escravo (WILLINGHAM et al., 2018).

Por ser um protocolo de comunicação que prioriza o baixo consumo de energia e o baixo poder de processamento, o BLE não dispõe de camadas e serviços de segurança robustos. Por conta disto, ele se mostra vulnerável a diversos tipos de ataques, desde simples ataques de *sniffing*, onde o hacker apenas visualiza os dados que estão sendo transacionados, até ataques de negação de serviço – *Denial of Service* (DoS), no qual é explorada a propriedade de que os dispositivos BLE permanecem “acordados” apenas durante determinados momentos, para poupar energia. Desta forma o ataque visa manter acordado o dispositivo, o que aumenta o seu consumo de energia e indisponibiliza os canais de comunicação entre o dispositivo mestre e os escravos, prejudicando o tráfego de dados na rede e exaurindo mais rapidamente os recursos de energia disponíveis nos dispositivos (BARUA et al., 2022).

3.2.3 6LoWPAN

6LoWPAN é um protocolo do IETF que pode ser implementado em dispositivos IoT para facilitar sua interação com sistemas baseados em padrões IP (MENEGHELLO et al., 2019). O 6LoWPAN é a abreviação para *IPv6 Low Power Wireless Personal Area Networks*, o que significa que é uma versão adaptada do protocolo IPv6 para dispositivos com restrições de recurso ou conexão (MULLIGAN, 2007).

O 6LoWPAN faz uso de mecanismos de compressão e fragmentação das mensagens, simplificando os cabeçalhos do protocolo e retirando informações redundantes (SHELBY; BORMANN, 2011).

A arquitetura de uma rede 6LoWPAN pode ser observada na figura 4 e é composta por três componentes, que são: *host node*, *router node* e o *edge node*. O host node pode perceber as mudanças e os estímulos ao dispositivo. Os pacotes de dados dos dispositivos são encaminhados para o *edge router* ou para a rede privada 6LoWPAN pelos roteadores. Por fim o *edge router* vai se comunicar com outras redes IP para prover a interconexão e o gerenciamento de tráfego entre eles (KASAH et al., 2020).

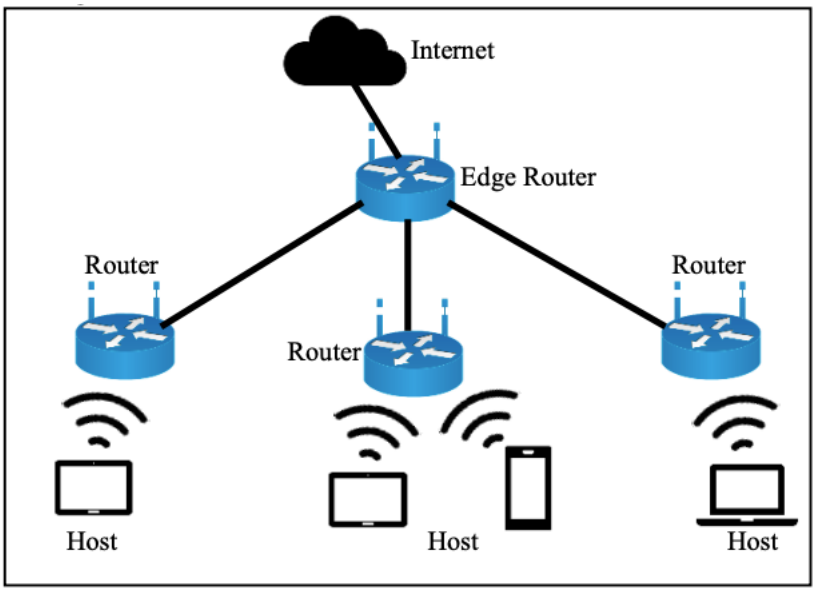

Figura 5. Arquitetura de uma rede 6LoWPAN (KASAH et al., 2020)

Pelas suas características de permitir uma implementação baixo custo de protocolo IPv6 para redes com restrições de conexão e energia, o 6LoWPAN não provê nenhum tipo de mecanismo de autenticação, ficando assim exposto a ataques de fragmentação (PONGLE; CHAVAN, 2015).

Nos ataques de fragmentação, o atacante insere seus próprios fragmentos da mensagem na cadeia de fragmentação já que não há nenhum mecanismo de autenticação no lado do receptor para checar se o fragmento recebido não foi alterado ou duplicado (PONGLE; CHAVAN, 2015).

3.2.4 CoAP

CoAP é a sigla para *Constrained Application Protocol*, que, assim como o HTTP, é um protocolo da camada da aplicação desenhado para redes com restrições de conexão (SHELBY; HARTKE; BORMANN, 2014). Ela facilita a comunicação entre a Internet e os dispositivos com restrições. O CoAP segue a arquitetura REST e suporta os métodos GET, POST, PUT e DELETE (BORMANN; CASTELLANI; SHELBY, 2012).

A arquitetura do CoAP se divide em duas camadas, *message layer* e *request/response layer*. A primeira é responsável por controlar a troca de

mensagens através do UDP entre dois pontos. Já a segunda camada carrega as requisições e as respostas que contém os métodos da requisição e os códigos de resposta para evitar problemas como a entrega de mensagens fora de ordem, a perda de mensagens ou a duplicação (RAHMAN; SHAH, 2016).

O CoAP é vulnerável a ataques de *spoofing*, ataques de cache onde um proxy tendo a capacidade de cache podem obter o controle. E também ataques referentes à transições entre a comunicação TCP e UDP que envolve a rede CoAP (ARVIND; NARAYANAN, 2019).

3.3 Privacidade

Como foi visto anteriormente, a confidencialidade é um dos princípios básicos que regem a segurança da informação, e consequentemente a segurança de IoT. Entretanto, com a série de restrições que são impostas a este tipo de dispositivos, desde restrições de consumo de energia, até a baixa oferta de recursos computacionais e qualidade de conexão, são geradas lacunas de segurança que se transformam em vulnerabilidades exploradas por agentes maliciosos.

A preocupação com a privacidade vem crescendo à medida que mais e mais dados são armazenados e transmitidos, muitos deles dados pessoais e sensíveis. Questões como vigilância por parte dos governos, exposição de informações sensíveis como dados financeiros, padrões de consumo e endereços, são só alguns dos exemplos que podemos citar.

Os dispositivos IoT estão no centro destas preocupações pois mesmo que as fabricantes aleguem que as informações coletadas respeitam a anonimização dos indivíduos, o cruzamento de diferentes informações dentro de um mesmo contexto pode potencialmente gerar um perfil do indivíduo em questão expondo informações e características que podem levar a discriminação e outros danos.

Como exemplo podemos citar o cenário das *smart homes*, uma escova de dentes inteligente coleta dados anonimizados sobre a frequência da higiene bucal do indivíduo, a geladeira coleta informações sobre o consumo dos alimentos e quais alimentos estão no dia a dia do indivíduo, e estes dados se cruzados e

correlacionados podem gerar uma impressão digital da saúde e hábitos desse indivíduo (ROSE; ELDRIDGE; CHAPIN, 2015)

Dispositivos como câmeras e sensores de presença que comumente eram utilizados para cenários de segurança e proteção em espaços abertos estão cada vez mais sendo introduzidos para o contexto pessoal e individual das nossas residências e locais de trabalho, gerando dados que aliados a dispositivos de rastreamento viabilizam a vigilância excessiva de governos ou pessoas mal-intencionadas, a quebra da privacidade dos nossos familiares e a intrusão nas nossas casas (WANG; LU, 2013).

Muito ainda precisa ser feito em regulação de dados, proteção de informações e regras para coleta e tratamento dos dados por parte dos fabricantes dos dispositivos e dos terceiros que possam obter estas informações de maneira legal. O cenário da privacidade está diretamente ligado à confiança na Internet e a adoção das tecnologias que estão embarcadas na Internet como o IoT, podendo essa quebra de confiança gerar diversos impactos econômicos e sociais ao redor do mundo (MCKINSEY GLOBAL INSTITUTE, 2015).

Capítulo 4
Crise de segurança e o cenário para o IoT

O processo de inovação tecnológica gera impactos positivos incontestáveis para a sociedade. A geração de empregos, disponibilidade facilitada de produtos e serviços, e aumento na qualidade de vida, são só alguns dos diversos benefícios atrelados. Apesar destes fatores, o processo de inovação tecnológica também está atrelado a riscos, muitos deles de segurança, e estes riscos se potencializam em um mundo cada vez mais interconectado e dependente da Internet.

Com a chegada da pandemia de Covid-19 em 2020 e as medidas de controle sanitário para a propagação do vírus levaram a um aumento na adoção de dispositivos IoT, principalmente para aplicações de *smart homes*, buscando otimizar o novo espaço de trabalho que agora eram as nossas casas e trazer mais conforto e comodidade para a nova rotina (ARIF, 2021). Neste período também houve um crescimento alarmante no número de ataques cibernéticos, cerca de 600% (A. B. C. NEWS, 2021). O crescimento do número de ataques cibernéticos só evidencia a crise de segurança que vivemos, de forma onde os avanços tecnológicos, nem sempre estão acompanhados dos avanços nas pesquisas e cuidados de segurança que são aplicados nos serviços e produtos que são desenvolvidos e consumidos a cada dia.

Em 2019 um estudo projetou que o impacto econômico na indústria do IoT estaria avaliado em 11 trilhões de dólares em 2025 (ARIF, 2021), outro estudo projetou que o número de dispositivos conectados alcançaria a marca de 75 bilhões em 2025 (STATISTA RESEARCH DEPARTMENT, 2016), um relatório da Ericsson (2016) projetou que em 2018 o número de dispositivos IoT superaria o número de *smartphones*, e chegaria à marca de 16 bilhões de dispositivos IoT.

Podemos observar que de um lado, o cenário para o IoT é otimista quanto à adoção da tecnologia, e por outro o cenário de segurança é cada vez mais incerto e com um crescente risco potencial para toda a economia mundial. Com isso, apesar do otimismo por parte dos analistas econômicos, há um impacto significativo na adoção da tecnologia pelas indústrias e pelo consumidor final. Segundo a Gartner (2018) em 20% das organizações foram constatados pelo menos um ataque cibernético envolvendo IoT, e a previsão para o gasto mundial em segurança de IoT chegaria a 1,5 bilhões de dólares em 2018, um crescimento de 28% em relação ao ano anterior.

Um grande exemplo da vulnerabilidade dos dispositivos IoT pôde ser visto em 2016, quando um ataque cibernético derrubou os sites de empresas como o Twitter, Netflix, The Guardian, CNN e tantos outros ao redor dos Estados Unidos e da Europa durante todo o dia do ataque. A vítima foi a empresa Dyn, responsável por controlar grande parte da infraestrutura DNS (WOOLF, 2016).

O ataque foi causado pelo Mirai Botnet (ANTONAKAKIS et al., 2017), e foi o maior ataque da história envolvendo *botnets*. O Mirai botnet age infectando computadores com um vírus especial que formam uma rede chamada *botnet*, esta rede então é orquestrada para bombardear o tráfego de um servidor, até causar o seu colapso. Este tipo de ataque é chamado de ataque de negação de serviço distribuído – *Distributed Denial of Service* (DDoS) (MIRKOVIC; REIHER, 2004).

Porém, diferente dos malwares comuns que infectam computadores, o foco do Mirai foi dispositivos IoT, como câmeras de circuito interno e outros aparelhos. Por conta do grande número de dispositivos IoT conectados a rede isso potencializou o ataque e o tornou maior do que qualquer outro ataque DDoS já registrado, onde foi estimado que 100.000 pontos de conexão foram infectados e uma força de ataque de surpreendentes 1,2 *terabytes* por segundo foi registrada (WOOLF, 2016).

Este foi apenas um episódio envolvendo dispositivos IoT e crimes cibernéticos, outros incidentes ocorreram como por exemplo o ataque ao SUV da Jeep, orquestrado pelo time de pesquisa da IBM (GREENBERG, 2015). Onde neste ataque eles exploraram o mecanismo de atualização de *firmware* e conseguiram

obter controle total do veículo, tanto de aceleração, frenagem e controle de direção, mostrando o risco potencial que essa falha acarreta.

Tendo em consideração o que foi exposto, o cenário para o IoT apesar de otimista se mostra bastante desafiador no contexto de segurança, a introdução de dispositivos IoT no nosso dia a dia, muitas vezes de maneira não tão perceptível, e o risco de segurança que está atrelado a eles são os principais causadores do atraso na adoção da tecnologia e evolução nas áreas de aplicações.

Na pesquisa da Bain & Company (2018) foi constatado que clientes corporativos estariam sujeitos a comprar na média 70% mais produtos IoT caso as suas preocupações com segurança fossem atendidas, e também que pagariam em média 22% a mais por dispositivos com melhor segurança. Desta forma, a visão clara do mercado para a indústria do IoT é apenas uma: O futuro do IoT e a sua adoção dependem principalmente da evolução nas tecnologias e mecanismos de segurança.

Capítulo 5
Conclusões

A internet das Coisas já deixou de ser uma tecnologia emergente e está presente no nosso dia a dia, seja em nossas roupas, carros, casas, locais de trabalho e ambientes que frequentamos ao redor da cidade. As preocupações existentes em relação à segurança são factíveis e fundadas, dado o quanto os dados que são coletados e transmitidos pela Internet cada vez mais expõem as nossas atividades cotidianas, hábitos e padrões.

Fato é que a indústria do IoT está cada vez mais aquecida, com mais aplicações sendo desenvolvidas e inovações sendo apresentadas para as mais diversas áreas a fim de otimizar processos, impactar financeiramente as cadeias produtivas e promover a qualidade de vida e segurança na sociedade. O aumento no número de crimes cibernéticos, atrelado ao crescimento no número de dispositivos IoT levanta preocupações quanto à quantidade massiva de dados pessoais que passaram a ser coletados por estes dispositivos e que não possuem regulação no que diz respeito a como as empresas utilizam essas informações, muitas vezes violando os direitos básicos do cidadão, como a privacidade, e também os padrões de segurança existentes e aplicados para proteger as informações dos usuários quando estes dados estão em posse das empresas.

Apesar da euforia da indústria do segmento, muito ainda precisa ser feito no contexto de privacidade e segurança destes dispositivos para sanar as dúvidas dos usuários e promover um ambiente digital mais seguro e responsável, onde não apenas as empresas e fabricantes se beneficiem, mas os consumidores não tenham medo. Novas políticas de proteção e anonimização dos dados devem ser implementadas, e as vigentes reforçadas. Os padrões de comunicação e arquitetura devem ser constantemente revisados e melhorias devem ser propostas a fim não só de melhorar a capacidade de processamento dos dispositivos, ou maneiras facilitadas de comunicação, mas de trazer maior estabilidade no contexto de

segurança para as aplicações e diminuir assim os impactos devastadores dos ataques cibernéticos.

Referências

A. B. C. NEWS. **The Latest: UN warns cybercrime on rise during pandemic**. Disponível em: <https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542>. Acesso em: 8 maio. 2022.

ALI, S.; BOSCHE, A.; FORD, F. **Cybersecurity Is the Key to Unlocking Demand in the Internet of Things**. Disponível em: <https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/>. Acesso em: 8 maio. 2022.

ANTONAKAKIS, M. et al. **Understanding the Mirai Botnet**. 26th USENIX Security Symposium (USENIX Security 17). **Anais**...Vancouver, BC: USENIX Association, ago. 2017. Disponível em: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>

ARIF, R. **With An Economic Potential Of $11 Trillion, Internet Of Things Is Here To Revolutionize Global Economy**. Disponível em: <https://www.forbes.com/sites/raufarif/2021/06/05/with-an-economic-potential-of-11-trillion-internet-of-things-is-here-to-revolutionize-global-economy/>. Acesso em: 8 maio. 2022.

ARVIND, S.; NARAYANAN, V. A. **An Overview of Security in CoAP: Attack and Analysis**. 2019 5th International Conference on Advanced Computing Communication Systems (ICACCS). **Anais**... Em: 2019 5TH INTERNATIONAL CONFERENCE ON ADVANCED COMPUTING COMMUNICATION SYSTEMS (ICACCS). mar. 2019.

ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A survey. **Computer Networks**, v. 54, n. 15, p. 2787–2805, 28 out. 2010.

BAIN & COMPANY. **Bain & Company predicts the Internet of Things market will more than double to $520 billion by 2021**. Disponível em: <https://www.bain.com/about/media-center/press-releases/2018/bain-predicts-the-iot-market-will-more-than-double-by-2021/>. Acesso em: 8 maio. 2022.

BARUA, A. et al. Security and Privacy Threats for Bluetooth Low Energy in IoT and Wearable Devices: A Comprehensive Survey. **IEEE Open Journal of the Communications Society**, v. 3, p. 251–281, 2022.

BORMANN, C.; CASTELLANI, A. P.; SHELBY, Z. CoAP: An Application Protocol for Billions of Tiny Internet Nodes. **IEEE Internet Computing**, v. 16, n. 2, p. 62–67, mar. 2012.

COMPTIA. **What Is Cybersecurity | Types and Threats Defined | Cybersecurity | CompTIA**. Disponível em: <https://www.comptia.org/content/articles/what-is-cybersecurity>. Acesso em: 19 abr. 2022.

ERGEN, S. C. ZigBee/IEEE 802.15.4 Summary. p. 37, 10 abr. 2004.

FAZION FILHO, M. **Internet das Coisas (Internet of Things)**. [s.l: s.n.].

GARTNER INC. **Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018**. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018>. Acesso em: 8 maio. 2022.

GOEL, A. K. et al. **Attacks, Countermeasures and Security Paradigms in IoT**. 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT). **Anais**... Em: 2019 2ND INTERNATIONAL CONFERENCE ON INTELLIGENT COMPUTING, INSTRUMENTATION AND CONTROL TECHNOLOGIES (ICICICT). Kannur, India: IEEE, jul. 2019. Disponível em: <https://ieeexplore.ieee.org/document/8993338/>. Acesso em: 3 maio. 2022

GREENBERG, A. Hackers Remotely Kill a Jeep on the Highway—With Me in It. **Wired**, 21 jul. 2015.

HASSAN, Q. F.; UR, R. K. A.; MADANI, S. A. **Internet of Things: Challenges, Advances, and Applications**. New York: Chapman and Hall/CRC, 2017.

HASSIJA, V. et al. A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. **IEEE Access**, v. 7, p. 82721–82743, 2019.

HEYDON, R. **Bluetooth low energy: the developer's handbook**. Upper Saddle River, NJ: Prentice Hall, 2012.

JAMES MANYIKA et al. **The Internet Of Things: Mapping The Value Beyond The Hype**. [s.l.] McKinsey Global Institute, jun. 2015. Disponível em: <https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20internet%20of%20things%20the%20value%20of%20digitizing%20the%20physical%20world/the-internet-of-things-mapping-the-value-beyond-the-hype.pdf>. Acesso em: 30 jun. 2022.

KASAH, N. BINTI H. et al. **Investigation on 6LoWPAN Data Security for Internet of Things**. 2020 2nd International Conference on Computer and Information Sciences (ICCIS). **Anais**... Em: 2020 2ND INTERNATIONAL CONFERENCE ON COMPUTER AND INFORMATION SCIENCES (ICCIS). out. 2020.

KHANJI, S.; IQBAL, F.; HUNG, P. **ZigBee Security Vulnerabilities: Exploration and Evaluating**. 2019 10th International Conference on Information and Communication Systems (ICICS). **Anais**... Em: 2019 10TH INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION SYSTEMS (ICICS). jun. 2019.

MAHMOUD, R. et al. **Internet of things (IoT) security: Current status, challenges and prospective measures**. 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). **Anais**... Em: 2015 10TH INTERNATIONAL CONFERENCE FOR INTERNET TECHNOLOGY AND SECURED TRANSACTIONS (ICITST). London, United Kingdom: IEEE, dez. 2015. Disponível em: <http://ieeexplore.ieee.org/document/7412116/>. Acesso em: 19 abr. 2022

MCKINSEY GLOBAL INSTITUTE. **Unlocking the potential of the Internet of Things | McKinsey**. Disponível em: <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>. Acesso em: 30 abr. 2022.

MENEGHELLO, F. et al. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. **IEEE Internet of Things Journal**, v. 6, n. 5, p. 8182–8201, out. 2019.

MIRKOVIC, J.; REIHER, P. A taxonomy of DDoS attack and DDoS defense mechanisms. **ACM SIGCOMM Computer Communication Review**, v. 34, n. 2, p. 39–53, 1 abr. 2004.

MÖLLER, R. et al. Ericsson Mobility Report June 2016. p. 32, jun. 2016.

MOUHA, R. A. Internet of Things (IoT). **Journal of Data Analysis and Information Processing**, v. 9, n. 2, p. 77–101, 18 mar. 2021.

MULLIGAN, G. **The 6LoWPAN architecture**. Proceedings of the 4th workshop on Embedded networked sensors. **Anais**...: EmNets '07.New York, NY, USA: Association for Computing Machinery, 25 jun. 2007. Disponível em: <https://doi.org/10.1145/1278972.1278992>. Acesso em: 3 maio. 2022

PAWAR, P.; TRIVEDI, A. Device-to-Device Communication Based IoT System: Benefits and Challenges. **IETE Technical Review**, v. 36, n. 4, p. 362–374, 4 jul. 2019.

PONGLE, P.; CHAVAN, G. **A survey: Attacks on RPL and 6LoWPAN in IoT**. 2015 International Conference on Pervasive Computing (ICPC). **Anais**... Em: 2015 INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING (ICPC). jan. 2015.

RAHMAN, R. A.; SHAH, B. **Security analysis of IoT protocols: A focus in CoAP**. 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC). **Anais**... Em: 2016 3RD MEC INTERNATIONAL CONFERENCE ON BIG DATA AND SMART CITY (ICBDSC). mar. 2016.

RAMYA, C. M.; SHANMUGARAJ, M.; PRABAKARAN, R. **Study on ZigBee technology**. 2011 3rd International Conference on Electronics Computer Technology. **Anais**... Em: 2011 3RD INTERNATIONAL CONFERENCE ON ELECTRONICS COMPUTER TECHNOLOGY (ICECT). Kanyakumari, India: IEEE, abr. 2011. Disponível em: <http://ieeexplore.ieee.org/document/5942102/>. Acesso em: 3 maio. 2022

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. The Internet of Things: An Overview. p. 54, 2015.

SHELBY, Z.; BORMANN, C. **6LoWPAN: The Wireless Embedded Internet**. [s.l.] John Wiley & Sons, 2011.

SHELBY, Z.; HARTKE, K.; BORMANN, C. **The Constrained Application Protocol (CoAP)**. [s.l.] RFC Editor, jun. 2014. Disponível em: <https://www.rfc-editor.org/info/rfc7252>. Acesso em: 3 maio. 2022.

STATISTA RESEARCH DEPARTMENT. **Number of IoT devices 2015-2025**. Disponível em: <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>. Acesso em: 8 maio. 2022.

the internet of things. Disponível em: <https://dictionary.cambridge.org/pt/dicionario/ingles/internet-of-things>. Acesso em: 21 abr. 2022.

TSCHOFENIG, H. et al. **Architectural Considerations in Smart Object Networking**. [s.l.] Internet Engineering Task Force, mar. 2015. Disponível em: <https://datatracker.ietf.org/doc/rfc7452>. Acesso em: 21 abr. 2022.

VAILSHERY, L. S. **IoT connected devices worldwide 2019-2030**. Disponível em: <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>. Acesso em: 8 maio. 2022.

VON SOLMS, B.; VON SOLMS, R. Cybersecurity and information security – what goes where? **Information & Computer Security**, v. 26, n. 1, p. 2–9, 12 mar. 2018.

WANG, J. et al. **BlueDoor: breaking the secure information flow via BLE vulnerability**. Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services. **Anais**...: MobiSys '20.New York, NY, USA: Association for Computing Machinery, 15 jun. 2020. Disponível em: <https://doi.org/10.1145/3386901.3389025>. Acesso em: 3 maio. 2022

WANG, W.; LU, Z. Cyber security in the Smart Grid: Survey and challenges. **Computer Networks**, v. 57, n. 5, p. 1344–1371, 7 abr. 2013.

WHITEHURST, L. N.; ANDEL, T. R.; MCDONALD, J. T. **Exploring security in ZigBee networks**. Proceedings of the 9th Annual Cyber and Information Security Research Conference. **Anais**...: CISR '14.New York, NY, USA: Association for Computing Machinery, 8 abr. 2014. Disponível em: <https://doi.org/10.1145/2602087.2602090>. Acesso em: 3 maio. 2022

WILLINGHAM, T. et al. **Testing vulnerabilities in bluetooth low energy**. Proceedings of the ACMSE 2018 Conference. **Anais**...: ACMSE '18.New York, NY, USA: Association for

Computing Machinery, 29 mar. 2018. Disponível em: <https://doi.org/10.1145/3190645.3190693>. Acesso em: 3 maio. 2022

WOOLF, N. DDoS attack that disrupted internet was largest of its kind in history, experts say. **The Guardian**, 26 out. 2016.