Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Segurança da Informação em Internet das Coisas voltado para Mobilidade Urbana

João Pedro Buso Leite
Luan Agnaldo Silva Guedes

Americana, SP.
2021

Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

João Pedro Buso Leite
Luan Agnaldo Silva Guedes

Segurança da Informação em Internet das coisas Voltado para Mobilidade Urbana

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. João Emmanuel D' Alkmin Neves

Área de concentração: Segurança da informação.

Americana, SP.
2021

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

L553s LEITE, João Pedro Buso

Segurança da informação em internet das coisas voltado para mobilidade urbana. / João Pedro Buso Leite, Luan Agnaldo Silva Guedes. – Americana, 2021.

41f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. João Emmanuel D'Alkmin Neves

1 Segurança em sistemas de informação 2. Internet das coisas I. GUEDES, Luan Agnaldo Silva II. NEVES, João Emmanuel D'Alkimin III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

João Pedro Buso Leite
Luan Agnaldo Silva Guedes

Segurança da Informação em Internet das coisas Voltado para Mobilidade Urbana

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 14 de junho de 2021.

Banca Examinadora:

_____
João Emmanuel D' Alkmin Neves (Presidente)
Mestre em Tecnologia
Fatec Americana

_____
Carlos Henrique Rodrigues Sarro (Membro)
Mestre
Fatec Americana

_____
Jonas Bodê (Membro)
Especialista
Fatec Americana

AGRADECIMENTOS

Agradecemos a todos os amigos e familiares que contribuíram e nos apoiaram no desenvolvimento desse trabalho, nosso orientador que nos auxiliou no desenvolvimento e agradecer a Deus pelo dom do conhecimento.

RESUMO

Hoje, com o aumento exponencial da Internet, tudo é procurado, acessado, vendido e até mesmo roubado, através do acesso de computadores, celulares, *tablets*, relógios e até mesmo pequenos dispositivos interconectados. No cotidiano é fácil encontrar instrumentos que se conectam na Internet, sejam eles *notebooks*, lâmpadas inteligentes, assistentes virtuais, eletrodomésticos que interagem com o usuário e até mesmo uma cadeia complexa de sensores que juntos conseguem identificar uma ambulância, carro de polícia e pedestres, tudo para facilitar a mobilidade urbana, visando conforto, agilidade, segurança e com um valor acessível dentro de uma Cidade Inteligente, conhecida como as *Smarts Cities*. Com tudo o que foi citado até o presente momento, pode-se chamar de a Internet das Coisas, isto é, N aparelhos conectados, processando dados e gerando informações, para distintas aplicações, sejam elas dentro de uma empresa controlando a logística, em um hospital coletando informações dos pacientes, em uma cidade inteligente onde a mobilidade urbana é controlada por sensores e outros dispositivos etc. Esse trabalho visa o estudo da segurança da informação voltado para mobilidade urbana, estudando os conceitos básicos e o desenvolvimento de um projeto básico simulando um radar inteligente.

Palavras Chaves: Internet das coisas; segurança da informação; mobilidade urbana.

ABSTRACT

Today, with the exponential increase of the Internet, everything is sought, accessed, sold and even stolen, through the access of computers, cell phones, tablets, watches and even small, interconnected devices. In everyday life it is easy to find instruments that connect to the Internet, like notebooks, smart lamps, virtual assistants, home appliances that interact with the user and even a complex chain of sensors that together can identify an ambulance, police car and pedestrians, everything to facilitate urban mobility, aiming at comfort, agility, security and with an accessible value within a Smart City, known as the Smarts Cities. With everything that has been mentioned so far, it can be called the Internet of Things, that is, N connected devices, processing data and generating information, for different applications, whether within a company controlling logistics, in a hospital collecting patient information, in a smart city where urban mobility is controlled by sensors and other devices etc. This work aims to study information security aimed at urban mobility, studying the basic concepts and the development of a basic project simulating an intelligent radar.

Keywords: *internet of things; security; and urban mobility.*

SUMÁRIO

ÍNDICE DE ILUSTRAÇÕES

1. INTRODUÇÃO

A Internet das Coisas (IoT) – *Internet of Things* – é um sistema que interliga os aparelhos eletrônicos conectados em uma determinada rede. Esses aparelhos coletam informações sem interação humana, podendo compartilhar essas informações entre si. Essa coleta de dados é realizada através de sensores, que por sua vez, fazem a análise desses dados utilizando diversos parâmetros pré-estabelecidos - esses parâmetros são desenvolvidos dependendo do objetivo do aparelho IoT em questão.

Aplicar a segurança desses dispositivos é um desafio pois, a cada dia, surge uma ideia nova para aplicações IoT e novos tipos de malwares que podem atingir os dispositivos de diversas maneiras. Não importa o quão protegido o dispositivo está, há sempre uma vulnerabilidade nele. Conforme Fakuda (2019) dentre os diversos desafios de segurança da IoT, segue alguns, como:

- Dispositivos IoT com menos recursos, poder de processamento, capacidade de armazenamento;
- Difícil de aplicar a segurança;
- Os atuais antivírus e softwares de segurança *endpoint* não podem ser instalados em dispositivos IoT.

Com o crescimento e fácil acesso desses dispositivos, a maneira que eles vêm sendo usados, seja em empresas, cidades e residências, acende uma luz amarela de preocupação devido o manuseio desses dispositivos, pois prontamente apresentam benefícios, porém com a negligência de certos aspectos de segurança simples, podem apresentar severos riscos a instituição ou pessoa que usufrui da IoT.

Justifica-se o estudo devido à alta demanda tecnológica, o número de aparelhos conectados aumenta a cada ano. Segundo Lueth (2019), a estimativa é que tenha 22 bilhões de aparelhos IoT conectados até 2025. Procedendo dessas informações, este trabalho focou um uso específico dos dispositivos da Internet das Coisas em cidades inteligentes voltado para mobilidade urbana.

Partindo deste aclaramento, este trabalho ascende a seguinte hipótese: Com o grande aumento de dispositivos IoT, o índice de ameaças e vulnerabilidades

também irão crescer? Por esta hipótese será crucial desenvolver métodos de segurança física (*hardware*) e segurança lógica (*software*).

O objetivo geral do trabalho é estudar e desenvolver mecanismos de segurança para IoT, obtendo um gerenciamento mais seguro deles e mapear as vulnerabilidades dos dispositivos IoT visando a sua aplicação em mobilidade urbana.

Como objetivos específicos elenca-se: estudo de *softwares*, conceitos da segurança da informação e mobilidade urbana, instalação e configuração dos *softwares* e *hardwares* para a realização de projeto prático.

Devido a essa enorme quantidade de aparelhos conectados, será necessário investir em cidades inteligentes para que a infraestrutura seja devidamente gerenciada, evitando riscos desnecessários, diminuindo os custos e tornando os aparelhos IoT conectados mais eficazes. Com esses aparelhos IoT conectados e devidamente gerenciados espalhados pela cidade, a qualidade de vida das pessoas irá melhorar, promovendo a cidadania, a sustentabilidade e a interação social.

A estrutura do trabalho é composta por 7 capítulos, onde o primeiro capítulo é a introdução que insere o leitor ao tema e proporciona uma visão geral do assunto.

Segundo capítulo aborda a segurança da informação, explicando o que é segurança da informação, seus princípios e explicação do que é dado, informação e ativo.

Terceiro capítulo é dividido em três subtópicos, sendo o primeiro uma apresentação da IoT, o texto explica sua arquitetura e suas camadas: aplicação, rede e percepção e alude a segurança em IoT como o uso de criptografia, tipos de ataques e OWASP. Já no segundo subtópico é mostrado os ramos da internet das coisas, como por exemplo: casas inteligentes, cidades inteligentes, indústria e agricultura inteligente. No último subtópico cita a mobilidade urbana, com o intuito de explicar o que é mobilidade urbana e seus conceitos.

Quarto capítulo traz os materiais e métodos que foram usados ao decorrer do desenvolvimento de todo o trabalho para sua parte prática.

Quinto capítulo é dedicado ao estudo de caso prático, onde é explicado e demostrado através de algumas imagens e explicações passo a passo de como foi realizado o mesmo.

Sexto capítulo elucida todos os resultados obtidos através desde trabalho.

Sétimo primeiro e último capítulo soma tudo o que foi discutido ao decorrer do trabalho e contém posições pessoais dos autores sobre alguns aspectos do tema e dos resultados do estudo de caso.

2. SEGURANÇA DA INFORMAÇÃO

Segundo o Hintzbergen *et al*. (2018), a segurança da informação proporciona a proteção contra diversos tipos de ameaça, com objetivo de garantir a continuidade dos negócios, minimizar os riscos e maximizar o retorno sobre os investimentos, tudo isso, garantindo a confidencialidade, a integridade e a disponibilidade das informações de uma corporação.

Para melhor gerenciamento da segurança da informação, normalmente se utiliza de um Sistema de gerenciamento de Segurança da Informação – SGSI (*Information Security Management System* – ISMS), do qual se incluem estruturas organizacionais, políticas de segurança, práticas, padrões, procedimentos, recursos, entre outras boas práticas que visam a segurança da informação.

- **Os Princípios Da Segurança Da Informação**

Existem diversas maneiras de fornecer segurança às informações de uma empresa, pode ser feito através de softwares, normas, treinamentos etc. Porém, os princípios mais importantes de segurança da informação são a disponibilidade, a confidencialidade e a integridade, os três juntos são conhecidos como o Triângulo CID (HINTZBERGEN *et al*. 2018).

- **Confidencialidade**

A confidencialidade, também chamada de exclusividade, é o princípio que garante o sigilo das informações, impedindo qualquer meio de divulgação e acesso não autorizado (HINTZBERGEN *et al*. 2018).

- **Integridade**

Consiste em garantir o estado o estado de uma informação, protegendo de qualquer modificação não autorizada. Garantir a integridade de uma informação significa garantir com que a informação esteja completa e intacta, seja ela uma informação correta ou incorreta (HINTZBERGEN *et al*, 2018).

- **Disponibilidade**

A disponibilidade é um princípio que garante que os as informações estejam sempre prontas para serem usadas. A disponibilidade possui três características, são elas:

Robustez: capacidade de uma equipe inteira consiga trabalhar no sistema;

Oportunidade: a informação estará disponível sempre que necessário;

Continuidade: a equipe poderá continuar trabalhando caso haja alguma falha no sistema (HINTZBERGEN *et al*. 2018).

- **Dado**

Setzer (2015) define dado como uma sequência de símbolos quantificados ou quantificáveis, ou seja, texto, foto, vídeo, números, figuras e entre outras coisas. O dado é algo simbólico, em um texto pode ser representado por palavras, em um vídeo por imagens, em imagens por pixels e em computadores por ponteiros.

- **Informação**

Setzer (2015) tem como definição da informação a organização dos dados em uma sequência lógica e racional. Um exemplo fácil é um texto composto por dados/palavras organizadas em uma sequência que dê sentido e coerência, exemplo: “Lucas mora na rua Varella, número 512”, isto torna os dados inteligíveis, diferente de: “número rua Lucas Varella, mora na 512”, isto é, os dados são os mesmos e estão íntegros, porém não de uma maneira compreensiva.

Também diz Setzer (2015) que a informação varia do modo que ela é transmitida e recebida, pois nem toda informação vem com dado. Um exemplo é um grito de dor, para o receptor não vem nenhum dado, mas pela semântica é feito a interpretação da informação. Já em um sistema de computadores é impossível existir a semântica, já que um computador interpreta apenas 0 ou 1, sim ou não e é extremamente matemático.

- **Ativo da Informação**

A classificação de ativo poder qualquer coisa que tenha valor para a empresa, ou seja, hardware, software, documentos impressos, pessoa, imagem da empresa e até mesmo a reputação Heintznergen *et al*. (2015).

3. IOT E MOBILIDADE URBANA

A IoT (*Internet* of Things) é uma rede de objetos que utilizam sensores e APIs para se conectar e realizar trocas de informações. A quantidade de aparelhos IoT conectados está em constante crescimento e, até 2025, a estimativa é que existam 22 bilhões de aparelhos IoT conectados, melhorando a qualidade de vida das pessoas. Porém, os aparelhos IoT devem ser devidamente gerenciados e protegidos contra-ataques (LUETH, 2019).

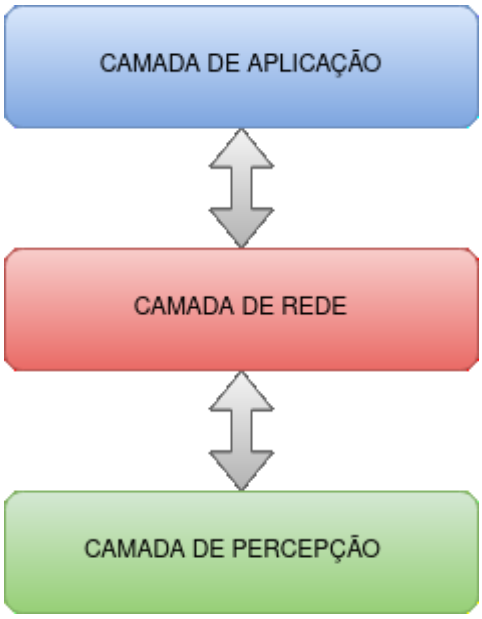
Por esse motivo, a segurança é um dos principais conceitos que resguardam a IoT, além de sua administração, tendo que prover boas práticas para garantir o máximo de segurança. Em sua maioria, recomenda-se uma série de cuidados, como instalação de antivírus, firewall e criptografia, além de proteções físicas como portas corta-fogo, nobreaks, refrigeração, câmeras, entre outros. Ou seja, a segurança da informação não só protege o maior patrimônio de uma corporação, mas também busca melhorias contínuas e sabedoria nas aplicações de recursos tecnológicos (LUETH, 2019).

De acordo com Valente (2011) IoT “é um paradigma que tem por objetivo criar uma ponte entre acontecimentos do mundo real e as suas representações no mundo digital, por meio da conexão de objetos”. Ao conectar tantos aparelhos IoT à internet, um leque de oportunidades de criação de aplicativos de diversas áreas de automação se abre, podendo melhorar a vida das pessoas.

- **Arquitetura da IoT**

A IoT suporta uma grande diversidade de aplicações e, consequentemente, diversas arquiteturas de aplicações. Dentre elas, a mais conhecida está dividida em camada de aplicação, camada de rede e camada de percepção. (Ameaças de Segurança, Defesas e Análise de Dados em IoT Baseada em SDN segundo Prates Jr. *et al*. (2018).

Figura 1 - Arquitetura IoT



Fonte: Autores (2021)

- **Camada de Aplicação**

Além de orientar como todos os dispositivos devem se comunicar para suprir os requisitos das aplicações suportadas pela IoT, essa camada também é responsável por englobar todos os protocolos para entregar ao usuário final uma interface entre a camada de aplicação e a camada de rede.

A camada de aplicação utiliza os dados coletados para se comunicar com o usuário, emitindo alertas, ligando, desligando, coordenando atividades entre dispositivos, entre outras coisas (PRATES JR *et al*. 2018).

Os principais protocolos utilizados pela camada de aplicação, são o CoAP (*Constrained Application Protocol)* e o MQTT (*Message Queuing Telemetry Transport).* O CoAP faz a comunicação entre dispositivos *endpoints* e inclui conceitos-chaves sobre a Web, como URIs e tipos de mídia de internet. Este protocolo é projetado para interagir com HTTP, interligando a Web enquanto atende os requisitos especializados. O protocolo MQTT é o protocolo padrão para a IoT, foi designado para ser um transporte de mensagens extremamente leve, ideal para conectar dispositivos remotos com uma banda larga de rede mínima (PRATES JR *et al*. 2018).

- **Camada de Rede**

A camada de rede agrega todas as funcionalidades e todos os serviços disponíveis na camada física, na camada de rede e na camada de transporte da arquitetura TCP/IP.

Ela é responsável por controlar a forma que as mensagens são transmitidas e, para cada tipo de comunicação, são utilizados determinados protocolos e padrões para realizar a transmissão dos dados. Os principais tipos de comunicação são:

- Comunicação direta entre dois dispositivos;
- Comunicação de um dispositivo IoT, sendo utilizado como um *gateway*, com outros dispositivo através da internet;
- Comunicação ponto-a-ponto entre dois dispositivos.

Na IoT, podem estar presentes mais de um tipo de comunicação, o que leva a certos dispositivos precisarem de suportes de diferentes protocolos de comunicação que estão fora do padrão TCP/IP. Devido a isso, foi implementado o padrão IPv6 sobre redes sem fio de área pessoal e baixo consumo de energia (6LoWPAN), que permite a comunicação entre dispositivos de baixa estrutura de rede e de curto alcance, além de permitir que dispositivos com tecnologia diferentes se conectem utilizando o 6LoWPAN (PRATES JR *et al*. 2018).

- **Camada de Percepção**

A camada de percepção é responsável por determinar como os dispositivos IoT interagem com o ambiente onde estão. Isso é feito através de sensores que captam os dados e os enviam para serem interpretados e que sejam realizados os procedimentos determinados (PRATES JR *et al*. 2018).

3.1 Segurança em IoT

Com o grande aumento de dispositivos conectados, a dificuldade de garantir a segurança dos dispositivos e suas informações cresce ainda mais. Aparelhos IoT que são utilizados dentro de residências (como lâmpadas, alarmes, sensores etc.) coletam informações sobre o comportamento dos usuários, informações das quais podem ser consideradas informações pessoais. Por isso, é necessário implementar

mecanismos para garantir tanto a segurança física quanto a segurança durante a fase de coleta, de transmissão e no armazenamento das informações contidas no aparelho conectado (FUKUDA, 2019).

- **Criptografia**

A criptografia pode ser definida como um conjunto de princípios e técnicas utilizadas para fazer com que um determinado texto se torne ilegível para aqueles que não possuam acesso a tal informação, conforme o dicionário Michaelis, criptografia é “arte ou processo de escrever em caracteres secretos ou em cifras” WEISZFLOG, (2015).

O tipo de criptografia mais utilizado hoje são as cifras de bloco. As cifras de bloco encriptam trechos inteiros de um *plaintext* (texto claro), que é feito normalmente em blocos de 64 ou 128 bits, dando entrada de tamanho N e uma saída do mesmo tamanho *n*, utilizando técnicas de permutação e substituição. Para que a decriptação seja possível, devemos levar em consideração que existem 2^n saídas possíveis, as duas entradas diferentes não devem produzir a mesma saída, fazendo com que a transformação não seja singular STALLINGS, (2015).

- **Tipos de ataques**

Os ataques cibernéticos podem ser feitos pelo hardware ou pelo software, sendo em sua maioria os ataques de software.

Os ataques de software consistem em identificar falhas em seus sistemas, explorando suas vulnerabilidades e conseguindo acesso não autorizado e controle sobre o sistema infectado. Uma maneira eficiente de evitar esses tipos de ataques é evitar fontes desconhecidas, dessa forma, há menos riscos da rede ser infectada.

Os ataques físicos geralmente consistem em acesso não autorizado e adulteração física, podendo levar ao vazamento de informações. Eles podem ser considerados como Passivos e Ativos.

Ataques passivos: são tipos de ataques não invasivo, ou seja, ataques lógicos e monitoramento de canais secundários;

Ataques ativos: são ataques invasivos, e semi-invasivos. Porém, existem alguns ataques ativos que não são invasivos, como falsa injeção, seja ela de temperatura, voltagem, entre outras, e *timing*, como análise de atraso (IEEE, 2019).

- **OWASP**

Conforme OWASP (2018), segue o Top 10 de falhas de segurança em IoT.

1. **Senhas fracas:** senhas existentes na web, credenciais imutáveis, uso de *bruteforce*;
2. **Serviços de rede inseguros:** serviços de redes desnecessários, principalmente aqueles que expõem o aparelho à internet e que comprometem a confidencialidade, integridade e disponibilidade dos dados.
3. **Interface de sistemas inseguros:** web vulnerável, API *backend*, nuvem ou interfaces mobiles são sistemas que podem comprometer o aparelho ou componentes relacionados.
4. **Falta de mecanismo de atualização seguro:** Atualização irregular, incluindo a falta de validação do firmware do aparelho.
5. **Uso de componentes inseguros ou desatualizado:** Uso de softwares vulneráveis que podem comprometer o aparelho. Incluindo configuração do sistema operacional defeituosa e uso de softwares ou hardwares de terceiros que tenham uma cadeia de suprimentos comprometida.
6. **Proteção de privacidade insuficiente:** informações pessoais do usuário armazenadas que são utilizadas indevidamente, sem permissão ou de maneira imprópria.
7. **Armazenamento e transferência de dados inseguro:** falta de criptografia ou controle de acesso de dados sensíveis dentro do sistema.
8. **Falta de gerenciamento de dispositivos:** falta de suporte em dispositivos utilizados durante a produção.
9. **Configurações de padrões inseguros:** Aparelhos ou software que possuam padrões inseguros podem comprometer o sistema.

10. **Falta endurecimento físico:** permitir que atacantes ganhem acesso a informações sensíveis que possam ajudá-los futuramente.

3.2 Ramos da Internet das Coisas

A IoT está presente em vários ramos da tecnologia. Hoje ela é encontrada em muitos dispositivos, desde pequenos utensílios, roupas e grandes estruturas das cidades. O uso de dispositivos IoT vem crescendo de maneira exponencial. Hoje a integração homem-máquina acontece de maneira quase que imperceptível, pois como o famoso WEISER (1991) "As tecnologias mais importantes são aquelas que desaparecem. Elas se integram à vida do dia a dia, ao nosso cotidiano e tornam-se indistinguíveis*".* E não está sendo diferente com a Internet das Coisas, hoje praticamente tudo o que tem botão de liga e desliga já pode fazer parte da IoT, ou seja, criou-se uma regra “tudo o que pode ser conectado, será conectado”.

- **Casas inteligentes**

No conceito de casas inteligentes envolve muitos equipamentos que são uteis dentro de uma residência. Os equipamentos podem ser uma lâmpada até uma geladeira que percebe a falta de um produto e solicita a compra no mercado. Normalmente essas casas são controladas por um ou uma assistente virtual, como *Google home*, Alexa e Siri que são os assistentes mais famosos. Eles permitem você controlar os aparelhos por comando de voz e fazer pesquisas na Internet (ZBOROWSKI e VILA LIMA 2017).

Imagine o seguinte cenário, você acordou com o despertador, ele envia um sinal para sua cafeteira que no mesmo instante começa a preparar o café, ainda deitado você solicita para o assistente virtual para abrir as janelas da casa e ler as notícias do dia. Essas tarefas que você levaria alguns minutos para realizar, foram concretizadas em menos de 1 minuto (ZBOROWSKI e VILA LIMA, 2017).

Quanto mais inteligente sua casa for, ou seja, quanto mais equipamentos forem conectados, mais fácil será realizar as atividades do cotidiano.

- **Cidades inteligentes**

No âmbito de cidades inteligentes é possível encontrar inúmeros sensores que podem prevenir enchentes, melhorar o sinal do trânsito, controle da iluminação pública, segurança pública e controle do lixo. Um exemplo é sensores nas ruas que informa aos usuários vagas disponíveis, sendo assim, evita que várias pessoas fiquem rodando com os seus veículos buscando uma vaga, gastando menos combustível, economiza tempo e dinheiro e reduz os impactos ambientais (KAMIENSKI *et al*. 2016).

- **Indústria 4.0**

Para a indústria, a internet das coisas está fazendo com que as empresas alterem e reinventem as práticas e modos de pensar, buscando implementar soluções tecnológicas e conectadas, de maneira que possam acompanhar o crescimento dessas tecnologias (DA SILVA, 2019). Em dos usos dessa tecnologia, é a instalação de sensores em construções de pontes, prédios ou grandes construções que informam dados como a qualidade do cimento durante a cura, informações do comportamento da estrutura depois de pronta e informar possíveis defeitos, evitando futuros problemas ou grandes desastres (DRUM, 2018).

- **Agricultura Inteligente**

Distante dos centros urbanos, os dispositivos inteligentes ajudam os produtores agrícolas em suas plantações. Esses dispositivos possuem sensores que detectam a temperatura do ar, a umidade do ar e até mesmo ativam o sistema de irrigação. Além de disso, pela internet conseguem ver as previsões meteorológicas, sendo assim, sabendo que vai chover, evita ligar o sistema de irrigação por um tempo prolongado ou em caso de situações extremas é enviado uma notificação ao produtor informando o incidente, um exemplo é em plantações de flores que costumam ser sensíveis, esses sensores enviam uma notificação informando ao produtor agrícola se será necessário proteger as flores do frio, colocar mais adubo e com o conjunto dos dispositivos é possível até mesmo ter a projeção de colheita DRUM, 2018).

3.3 Mobilidade Urbana

Mobilidade tem seu significado segundo o dicionário Scotini (2009) de característica do que é móvel ou do que é capaz de se movimentar, logo mobilidade urbana vem com o significado de como a população urbana se movimenta dentro dos espaços geográficos urbanos para realizar suas atividades do cotidiano.

A mobilidade urbana visa sempre atingir quatros pilares, o conforto, agilidade, segurança e preço acessível (JUNQUEIRA, 2016). Com o uso de dispositivos IoT, esses pilares são contemplados de maneiras mais eficientes e econômicas.

Antigamente os deslocamentos em meios urbanos eram difíceis, desde o uso de animais como asno e cavalos, uso de carroças, bicicletas, pequenos veículos motorizados e até chegar aos veículos que existem atualmente. O uso de semáforos e sistemas inteligentes não eram usados, dificultando a mobilidade nos grandes centros urbanos. Um exemplo fácil é dos semáforos que tinham seu tempo padrão determinado e não havia possibilidade de mudança rápida para aumentar ou diminuir o fluxo em determinada via.

A mobilidade urbana antes de sua explosão devido ao aumento de uso de automóveis, não necessitava de auxílio de tecnologia eletrônica. Segundo Rodrigues e*t al.* (2016):

> Na medida em que o processo de urbanização no Brasil, ao longo do século XX, foi se consolidando as maneiras e as condições de deslocamento nas cidades também foram se alterando. Em um contexto de profundas transformações econômicas, sociais e demográficas se formou um modelo específico de mobilidade urbana. A partir de 1950, se intensificou um processo de mudança nas grandes cidades e as redes de bondes foram gradativamente sendo substituídas pelos ônibus, ao mesmo tempo em que as redes metropolitanas de trens, que desempenharam importante papel na estruturação das cidades, foram sendo desmanteladas, até o triunfo do automóvel a partir da década de 1990.

Por meados de 2000 com o crescimento da internet e o triunfo dos automóveis, a necessidade de usar artefatos tecnológicos para a integração do usuário, controle e agilidade da mobilidade, se tornou algo primordial (CRUZ, 2019).

A Internet das Coisas pode ser definida como um conjunto de aparelhos conectados que podem coletar diversos tipos de informações em seus diversos ambientes, como em casas, na agricultura, na medicina ou no transporte urbano.

Novas tecnologias surgirão em conjunto a com a IoT trazendo melhorias no nosso dia a dia no transporte, fornecendo informações das melhores rotas para irmos até o nosso destino, ou até mesmo nos levar até algum lugar, como o Uber ou 99 Taxi por exemplo. Com a implementação da IoT na mobilidade urbana, através de radares inteligentes, sensores, entre outros dispositivos, a qualidade do tráfego irá melhorar (ARAUJO *et al.* 2019).

4. MATERIAIS E MÉTODOS

No presente capítulo será explicada a Metodologia desse estudo. Conforme Marconi e Lakatos (2003) “Os contatos diretos, pesquisa de campo ou de laboratório são realizados com pessoas que podem fornecer dados ou sugerir possíveis fontes de informações úteis. As duas tarefas, pesquisa bibliográfica e de campo, podem ser executadas concomitantemente.”. Com isso a pesquisa vai ter seu rumo levado à pesquisa de campo. A metodologia de desenvolvimento deste trabalho será dividida em algumas etapas:

Etapa 1: Pesquisa bibliográfica com técnica de coleta de dados indireta (pesquisa documental e bibliográfica) de artigos e websites, apresentada nos Capítulos1, 2 e 3 do presente trabalho.

Etapa 2: Após realizada pesquisa, serão realizados testes utilizando um Arduino UNO e um *Raspberry PI*, para simular um aparelho IoT e sua central.

Etapa 3: Por último será realizado um relatório técnico para controle interno e uma monografia contendo todas as informações e conclusões.

A pesquisa utilizou tais materiais: um Raspberry 3 – *Model* B 2018, uma placa Arduino modelo Uno 2010 e um sensor ultrassônico da marca OSEPP *Electronics* modelo hc rs04.

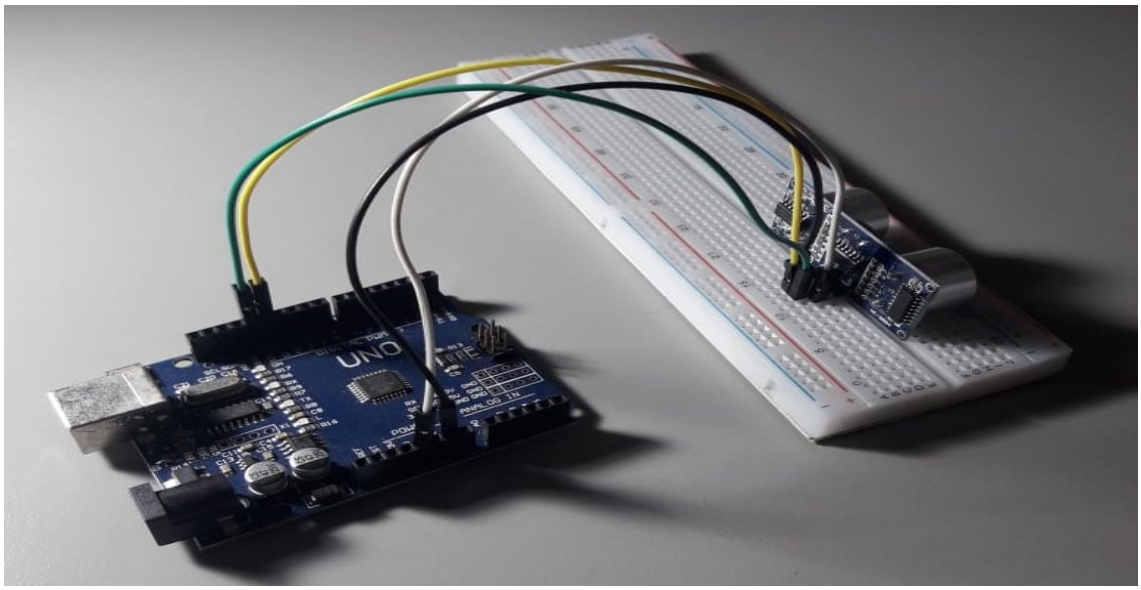
O Raspberry Pi (RASPBERRY, [s.d.]) é um microcomputador com placa única reduzida. Foi criado no Reino Unido pela fundação Raspberry Pi no ano de 2012.

Figura 2 - Raspberry PI

Fonte: Autores (2021)

O Arduino é um dispositivo composto por um microcontrolador Atmel, circuitos de entrada e de saída, podendo ser conectado à um computador e programado via IDE utilizando linguagem C/C++ (ARDUINO, 2018).

Figura 3 - Arduino Uno



Fonte: Autores (2021)

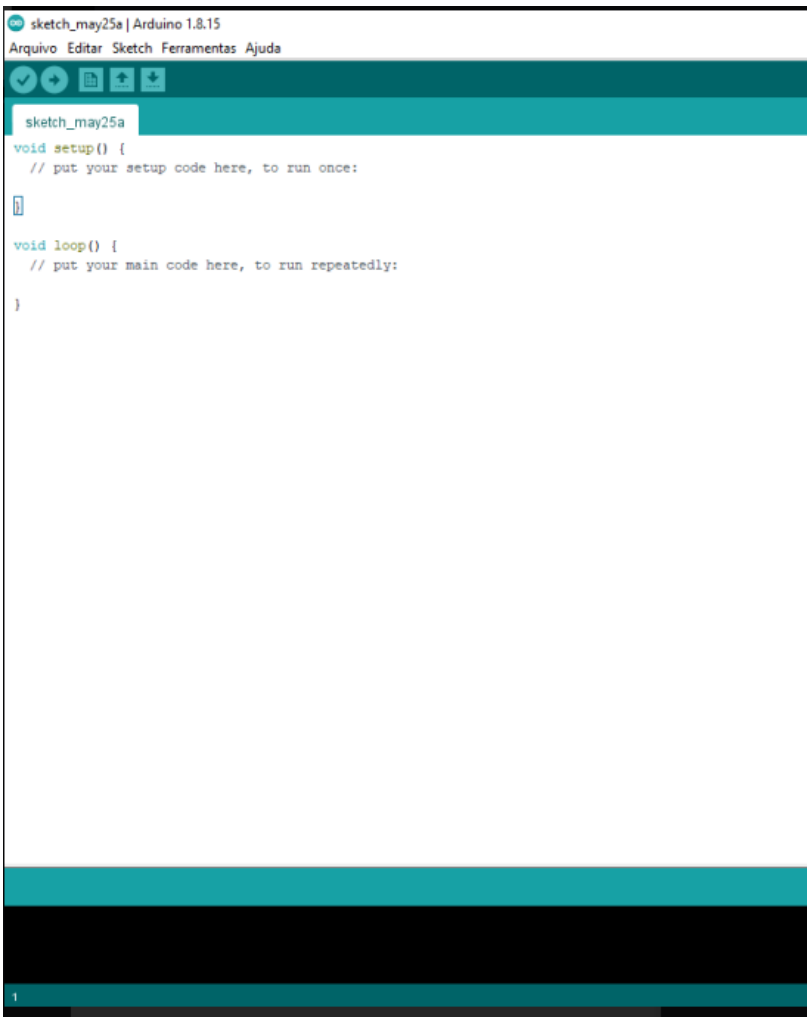
O sensor ultrassônico emite sinais ultrassônicos pelo sensor e realiza a leitura desses sinais quando retornam, a distância entre o objeto e o sensor é calculada com base no tempo entre o envio e o retorno do sinal (THOMSEN, 2011).

Figura 4 - Sensor Ultrassônico

Fonte: Autores (2021)

Arduino IDE (Integrated Development Environment) é um ambiente de desenvolvimento com as linguagens C e C++, é utilizado para fazer os uploads dos programas desenvolvidos nas placas Arduino

Figura 5 - Arduino IDE



Fonte: Autores (2021)

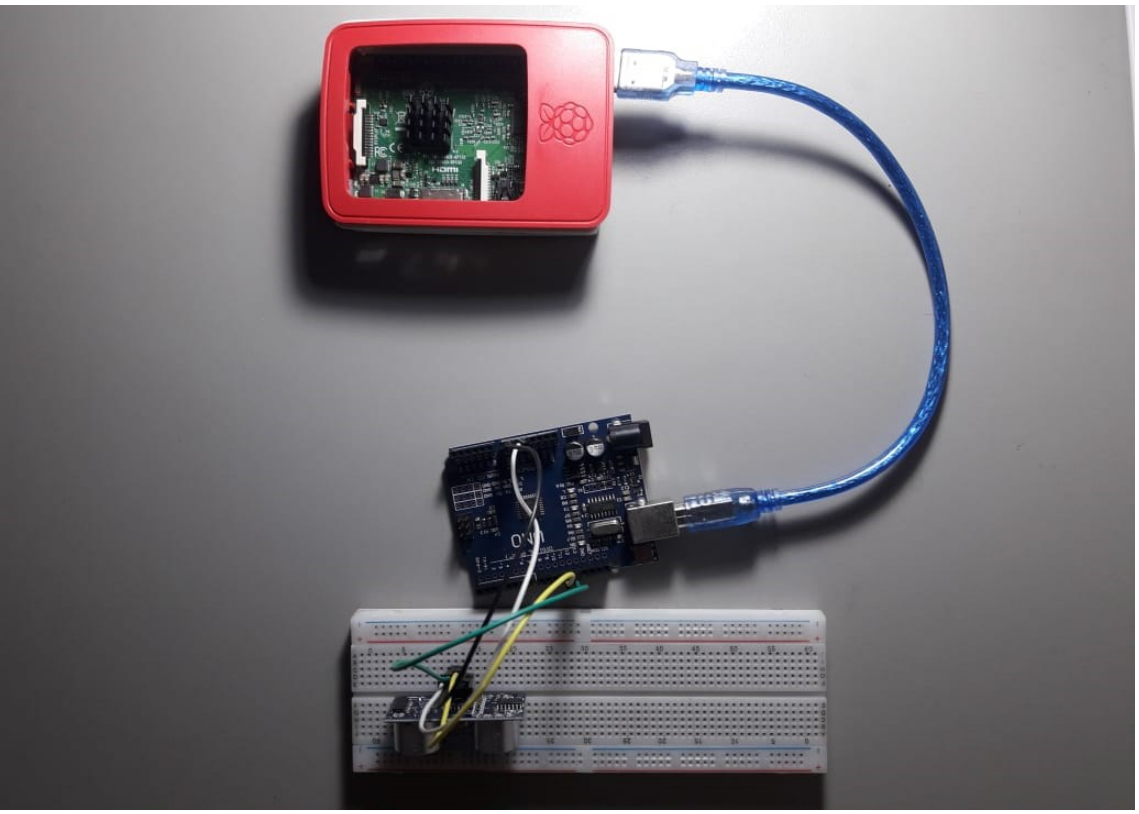
E a partir desses materiais e métodos a pesquise irá desenvolver uma aplicação que identifica e coleta informações através do uso do sensor ultrassônico, fazendo uma contagem e mandando os dados coletados para o Raspberry Pi. Os dados são coletados através do software Coolterm e armazenado no servidor Raspberry Pi.

5. ESTUDO DE CASO

Para o desenvolvimento do estudo de caso foi utilizado todos os dispositivos citados no capítulo anterior.

Primeiramente todos os *hardwares* foram conectados apresentado na figura 7.

Figura 6 - Conexão do Raspberry Pi e o Arduino Uno



Fonte: Autores (2021)

Após a conexão dos *hardwares* foi inserido o código fonte da aplicação no Arduino através do Raspberry. Apresentado na figura 8.

Figura 7 - Código do Arduino

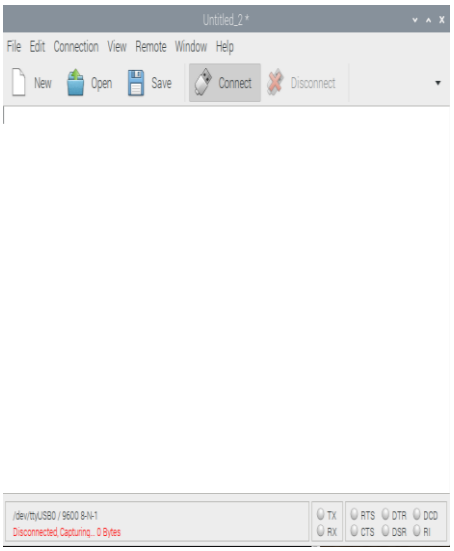
```
#define trigPin 13
#define echoPin 12
int counter = 0;
int current = 0;
int previous = 0;
void setup() {
 Serial.begin (9600);
 pinMode(trigPin, OUTPUT);
 pinMode(echoPin, INPUT);
}

void loop() {
 long duracao, dist;
 digitalWrite(trigPin, LOW);
 delayMicroseconds(2);
 digitalWrite(trigPin, HIGH);
 delayMicroseconds(10);
 digitalWrite(trigPin, LOW);
 duracao = pulseIn(echoPin, HIGH);
 dist = (duracao/2) / 29.1;
 if (dist <= 10){
 current = 1;
 }
 else {
 current = 0;
 }
 delay(100);
 if(current != previous){
if(current == 1){
counter = counter + 1;
Serial.println(counter);
    }
  }
}
```

Fonte: Autores (2021)

O código acima fará com que o sensor some ao contador toda vez que um objeto passar a uma determinada distância do próprio sensor, no caso 10 cm de distância.

Foi utilizado o software CoolTerm Raspberry Pi, que salvará em um arquivo chamado “log.txt” os dados que o sensor irá capturar. Apresentado na figura 9.

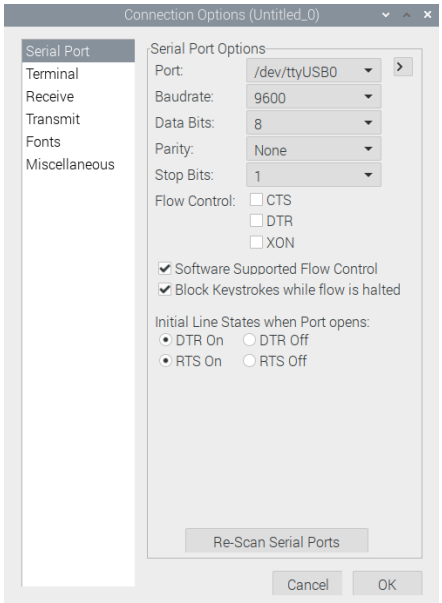
Figura 8 - CoolTerm Raspberry Pi



Fonte: Autores (2021)

Para iniciar a coleta dos dados, é necessário a configuração da porta USB corretamente no *software* CoolTerm. Apresentado na figura 10.

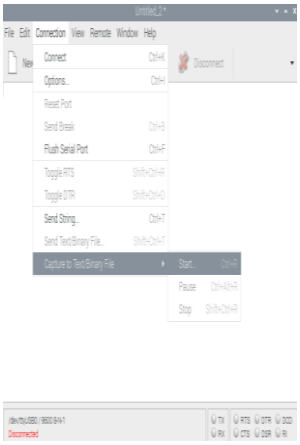
Figura 9 - Configurações CoolTerm



Fonte: Autores (2021)

Após conectar o CoolTerm com o Arduino, deve-se iniciar a captura dos dados com o *software.* Apresentado na figura 11.

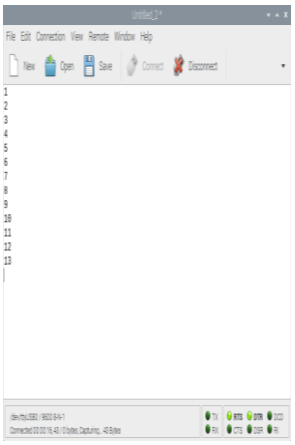
Figura 10 - Captura de dados



Fonte: Autores (2021).

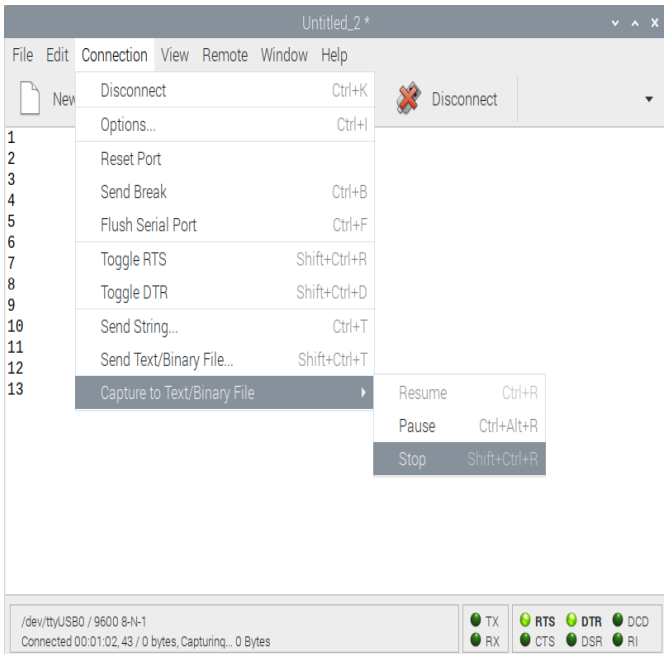
Após isso, o *software* irá capturar os dados e salvá-los em um arquivo determinado após encerrar a conexão e encerrar a captura de dados. Apresentado nas figuras 12 e 13.

Figura 11 - Dados do sensor



Fonte: Autores (2021)

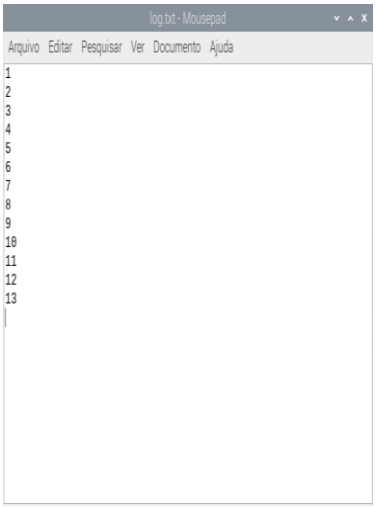
Figura 12 - Encerrando a captura dos dados



Fonte: Autores (2021)

Por último, ao encerrar a captura, os dados serão salvos em um arquivo txt conforme apresentado na figura 14.

Figura 13 - Arquivo de log



Fonte: Autores (2021)

6. RESULTADOS

A IoT é uma área muito ampla, existem muitas vertentes de estudo dentro dela, porém, ao passar dos anos, a IoT foi se desenvolvendo e aumentando o número de

aparelhos IoT existentes, pessoas estão utilizando aparelhos IoT em seu cotidiano, automatizando processos e melhorando a qualidade de vida.

Por esse motivo, a segurança é e sempre será um grande desafio, pois não basta proteger apenas contra fraudes e ataques cibernéticos, é necessário garantir um bom armazenamento dos dispositivos, para evitar situações como roubo, acidentes (sejam de causas naturais ou não), defeitos técnicos, sequestro de dados e apropriação de dados.

Como resultado do projeto, foi possível entender como funciona a IoT, desde seus conceitos básicos até como a IoT funciona na prática, com a simulação de um sensor inteligente utilizando o Arduino e o Raspberry Pi como um servidor de armazenamento local.

Após realizar o projeto, foi possível ver brevemente como funciona a IoT na prática, a forma como ela capta os dados e os transfere para algum servidor, tratando o dado para transformá-lo em informação.

Foi utilizado um sensor ultrassônico para realizar a captura dos dados de um determinado ambiente e, com o servidor Raspberry Pi, realizar o tratamento dos dados, podendo armazená-los e realizar outros processos que forem necessários.

Durante a criação do ambiente de testes, foi identificado em questão da segurança dos *hardwares*, os componentes apresentaram certas fragilidades ao ambiente. A placas, conexões e sensores tiveram que ser manuseadas cautelosamente, para não gerar danos irreparáveis.

No ambiente de testes em questão dos *softwares* não houve nenhum grande problema, pois todos possuíam boas documentações facilitando o seu manuseio e configuração.

Para simular a captação do sensor em uma via pública, utilizamos um código que limitava uma certa distância da captação dos objetos. Foi utilizado objetos aleatórios para a contabilização, podendo ser apenas uma mão passando em frente ao sensor, pedaço de papel ou plástico.

O armazenamento do dados ocorreu através do *software* Coolterm, onde ele armazenava todos os dados no servidor em um arquivo tipo txt. A cada vez que o programa era rodado, um novo arquivo com os novos dados era gerado e armazenado.

O servidor por padrão continha algumas configurações básicas e necessárias para permitir a segurança dos dados/informação e mitigar os riscos. Um *firewall*

configurado, um usuário específico com todas as permissões alteradas, com limitações de operações dentro do sistema para evitar escalabilidade. Criptografia do disco e *backup*.

7. CONSIDERAÇÕES FINAIS

Com a pesquisa, observou-se que a IoT é uma linha crescente, que cada vez mais faz parte do cotidiano e, com o tempo, ela será algo do cotidiano e, por isso, devemos conhecer os riscos e as vulnerabilidades que os aparelhos IoT apresentam para o desenvolvimento de mecanismos de defesa, tanto para o *hardware* quanto para o *software*.

Durante todos os testes realizados, foram identificados alguns problemas que podem ser resolvidos com alguns métodos simples e outros nem tanto.

Observou-se que cem porcento dos *hardwares* utilizados, não podem ficar expostos ao ambiente, devem ficar em um local seco e arejado. A sua caixa de proteção pode ficar exposta, mas seu conteúdo não. Pois como são componentes pequenos e, com ligações frágeis, ou seja, quaisquer interferências externas irão danificar o aparelho ou prejudicar o seu funcionamento.

O servidor utilizado continha seus usuários e senhas padrão. Foi necessário adicionar e alterar as senhas. O método usado para a senha foi o que a torna segura, utilizando senhas com caracteres maiúsculos, minúsculos, caráter especial, números e maior senha maior que 10 dígitos. Dessa maneira já impede a facilidade no acesso.

Foi criado uma conexão ao servidor via SSH, para poder ter acesso ao servidor remotamente. A autenticação ao servidor é feita com uma chave especifica, permitindo que apenas quem possui a chave possa se autenticar, evitando tentativas de invasão que utilizam de força bruta.

Com toda essa ressalva, foi concluído que com não importa a quantidade de mecanismos de defesas que é implantando ao sistema, ele sempre estará sujeito a ameaças e riscos. Por isso deve-se sempre realizar manutenções preventivas no sistema.

Utilizando esse sistema em mobilidade urbana, seja em ruas, avenidas, estradas e calçadas, é possível coletar dados de veículos, pessoas e objetos que passam em determinada via, obtendo informações da quantidade de tráfego no local. Com esse projeto foi possível ter uma introdução em como a IoT pode ajudar na mobilidade urbana, fazendo com que as cidades possam se tornar cidades inteligentes.

7.1 Sugestões para Trabalhos Futuros

Como sugestões para trabalhos futuros os pesquisadores sugerem dar continuidade no projeto executando em uma escala maior. Utilizando mais sensores interconectados e possibilitando a simulação de um trânsito em várias vias, utilizando para o controle delas, semáforos que identificaram o tempo que devem estar abertos com sinal verde ou fechados com sinal vermelho utilizando os dados que são coletados através dos sensores instalados nas vias. Visando aplicar a segurança da informação nesses dispositivos IoT e descobrir novas ferramentas, métodos e possíveis falhas.

REFERÊNCIAS

ARAUJO, J.; MOREIRA, E.; FREITAS, C.; CASTRO, F.; ARAUJO, A.; CARVALHO, T. ***Smart cities***: um estudo prospectivo sobre
internet das coisas (IoT) aplicada ao setor de mobilidade urbana. Disponível em: https://periodicos.ufba.br/index.php/nit/article/view/32691/20799. Acesso em 9 jan. 2021.

ARDUINO. **O que é arduino?** Disponível em: https://www.arduino.cc/en/Guide/Introduction. Acesso em 12 out 2021.

CRUZ, Carlos Daniel Santana. **Desenvolvimento de um sistema IoT voltado à acessibilidade na mobilidade urbana**. Disponível em: http://ri.ucsal.br:8080/jspui/handle/prefix/874. Aceso em 18 jan. 2021.

DA SILVA, Jonathan Galdino. **Dispositivo para conexão a redes IoT para indústria 4.0**. Disponível em: http://repositorio.utfpr.edu.br/jspui/bitstream/1/15626/1/SH_COCIC_2019_2_7.pdf. Acesso em 05 fev. 2021.

DRUM, Marluci. **O que é internet das coisas (IoT)?** Disponível em: https://www.oficinadanet.com.br/post/16655-internet-das-coisas. Acesso em: 06 fev. 2021.

FUKUDA, Leonardo Massami. **Segurança da informação em Iot**. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/13066/1/CT_GETIC_VIII_2019_05.pdf. Acesso em 05 nov. 2020.

HINTZBERGEN, J.; HINTZBERGEN, K.; SMULDERS, A.; BAARS, H. **Fundamentos de segurança da informação:** com base na ISO 27001 e na ISO 27002. Rio de Janeiro: Brasport, 2018.

IEEE, *Electronics Packaging Society*. ***Heteogeneus integration roadmap***, 2019 Ed, Capítulo 19: *Security*. Disponível em: https://eps.ieee.org/images/files/HIR_2019/HIR1_ch19_security.pdf. Acesso em 03 ago. 2020.

JUNQUEIRA, Hermes João. **Mobilidade urbana e cidades inteligentes**. Disponível em YouTube. https://www.youtube.com/watch?v=13w_Z6Sfaccw&list=LL&index=4. Acesso em 26 fev. 2021.

KAMIENSKI, C.; BIONDI, G.; BORELLI, F.; HEIDEKER, A.; RATUSZNEI, J.; KLINSCHMIDT, J. **Computação Urbana:** tecnologias e aplicações para cidades inteligentes. Disponível em: https://www.researchgate.net/profile/Carlos_Kamienski/publication/303810868_Computacao_Urbana_Tecnologias_e_Aplicacoes_para_Cidades_Inteligentes/links/575479a208ae6807fb04cf20/Computacao-Urbana-Tecnologias-e-Aplicacoes-para-Cidades-Inteligentes.pdf. Acesso em 10 nov 2020.

LUETH, Knud Lasse. **State of the IoT 2018:** number of IoT devices now at 7B – market accelerating. Disponível em:https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/. Acesso em 15 dez 2020.

LUETH, Knud Lasse. **State of the IoT 2020:** 12 billion iot connections, surpassing non-iot for the first time**.** Disponível em: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/. Aceso em 18 out. 2020.

MARCONI, Marina De Andrade, LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. Disponível em: http://docente.ifrn.edu.br/olivianeta/disciplinas/copy_of_historia-i/historia-ii/china-e-india/view. Acesso em 10 jul 2020.

OWASP. **OWASP top 10 IoT**. Disponível em: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project. Acesso em 10 nov. 2020.

PRATES JR.; NELSON, G. PELLOSO, M.; MACEDO, R.; NOGUEIRA, M. **Ameaças de segurança, defesas e análise de dados em IoT baseada em SDN**. Disponível em: https://www.inf.ufpr.br/aldri/disc/INFO7015-Minicurso_Redes_SDN_SBSeg2018.pdf. Acesso em 01 nov. 2020.

RASPBERRY. **O que é um raspberry pi?** Disponível em: https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/. Acesso em 17 ago. 2020.

RODRIGUES, J.; LOPES, B.; MIESENBERGER, C.; SANTOS, L.; VIANNA, M.; DE PAULA, M.; YAMADA, M.; LEMOS, A.; BARTELT, D.; LIMA, J.; FANINI, V. **Mobilidade urbana no Brasil**: desafios e alternativas. Disponível em: https://br.boell.org/sites/default/files/mobilidade_urbana_boll_brasil_web_.pdf. Acesso em 03 jan. 2021.

SCOTTINI, A. **Dicionário escolar da língua portuguesa**. Blumenau: Todolivro, 2009.

SETZER, Valdemar. **Dado, informação, conhecimento e competência**. Disponível em: https://www.ime.usp.br/~vwsetzer/dado-info.html. Acesso em 10 jul 2020.

STALLINGS, William. **Criptografia e segurança de redes**. 6ª ed. São Paulo: Pearson, 2015.

THOMSEN, Adilson. **Como conectar o sensor ultrassônico HC-SR04 ao arduino.** Disponível em: https://www.filipeflop.com/blog/sensor-ultrassonico-hc-sr04-ao-arduino/. Acesso em 28 set. 2020.

VALENTE, Bruno Alexandre Loureiro. **Um middleware para a internet das doisas.** Disponível em: https://repositorio.ul.pt/bitstream/10451/9211/1/ulfc104490_tm_Bruno_Valente.pdf. Acesso em 03 jan. 2021.

WEISER, Mark. ***The computer for the 21 century***. Disponível em: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf. Acesso em 09 ago. 2020.

WEISZFLOG, Walter. **Dicionário brasileiro da língua portuguesa**. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/criptografia/. Acesso em 25 ago. 2020.

ZBOROWSKI, Felipe Augusto.; VILA LIMA, Felipe Augusto. **SGCI – Sistema de gerenciamento de casas inteligentes**. Disponível em: http://repositorio.utfpr.edu.br/jspui/bitstream/1/9240/1/CT_COSIS_2017_1_2.pdf. Acesso em 10 jan. 2021.