CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA

REDES DE COMPUTADORES

DIOGENES LAURENTINO DE VASCONCELOS

MATHEUS FERREIRA DE LIMA

HUGO ESTEVÃO DE LIMA E SILVA

DISPOSITIVOS IOT EM ÁREA DOMÉSTICA

RECIFE/2023

DIOGENES LAURENTINO DE VASCONCELOS

MATHEUS FERREIRA DE LIMA

HUGO ESTEVÃO DE LIMA E SILVA

DISPOSITIVOS IOT EM ÁREA DOMÉSTICA

Trabalho de Conclusão de Curso apresentado ao Curso de Redes de Computadores, da UNIBRA, como requisito parcial para a obtenção do certificado.

Orientador(a): Prof Ameliara Freire

RECIFE/2023

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 2338/ O.

V331d Vasconcelos, Diogenes Laurentino de.
Dispositivos IOT em área doméstica/ Diogenes Laurentino de Vasconcelos; Matheus Ferreira de Lima; Hugo Estevão de Lima e Silva. - Recife: O Autor, 2023.
18 p.

Orientador(a): Me. Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2023.

Inclui Referências.

1. IOT. 2. Internet. 3. Smart. I. Lima, Matheus Ferreira de. II. Silva, Hugo Estevão de Lima e. III. Centro Universitário Brasileiro. - UNIBRA. IV. Título.

CDU: 004

AGRADECIMENTOS

Gostaríamos de agradecer os nossos professores por compartilhar o conhecimento neles incumbidos, aos nossos familiares e amigos pelo apoio dado durante toda trajetória acadêmica.

"Em algum lugar, algo incrível está esperando para ser descoberto."

(Carl Sagan,1977)

DISPOSITIVOS IOT EM ÁREA DOMÉSTICA

DIOGENES LAURENTINO DE VASCONCELOS

MATHEUS FERREIRA DE LIMA

HUGO ESTEVÃO DE LIMA E SILVA

Profª Ameliara Freire – Orientadora

RESUMO: A tecnologia está cada vez mais presente em nossas vidas nos mais diversos âmbitos nos ajudando com diversos tipos de atividades, gerando conforto e economia de tempo. Com a *smart home* não seria diferente. Ela possibilita que possamos controlar funções que antes eram manuais como acender a luz usando um simples comando de voz e ainda nos fornece umas informações do uso e de quanto de energia que aquela lâmpada está gastando.

Palavras-chave: *IOT*, Internet, *Smart.*

IOT DEVICES IN DOMESTIC AREA

DIOGENES LAURENTINO DE VASCONCELOS

MATHEUS FERREIRA DE LIMA

HUGO ESTEVÃO DE LIMA E SILVA

Profª Ameliara Freire – Orientadora

ABSTRACT: Technology is increasingly present in our lives in the most diverse areas, helping us with different types of activities, generating comfort and saving time. With a smart home it would be no different. It allows you to control functions that were previously manual, such as turning on the light using a simple voice command, and also provides us with information on usage and how much energy that lamp is using.

Keywords: IOT, Internet, Smart.

1 Introdução

É inegável o crescimento exponencial da nossa tecnologia e o anseio de pessoas para uso doméstico sobre um dispositivo que facilite sua vida ou que até “pense” por você. Isso pode se encaixar nos termos de produtos *smarts* e IOT’s (*Internet of things*) que ainda se misturam entre eles, como exemplos podem ser tomados os dispositivos Alexa (Amazon), Google home (Google), Siri (Apple) que são inteligências artificiais criadas para ajudar no dia a dia de pessoas, mudando a forma de fazer as coisas, como saber o clima, marcar um despertador ou um lembrete na agenda entre várias outras funções. (L. GONÇALVES, 2018)

Com o simples ato de falar para que seja realizada uma ação pela inteligência e às vezes nem esse ato precisa ser realizado, tendo a opção de programar ações que você faria manualmente para serem feitas automaticamente, liberando as pessoas de fazerem certas atividades facilitando até como o estilo a vida, como abrir as cortinas em um determinado horário, desligar ou ligar o ar condicionado, acender luzes, fazer café, e etc. Como um mordomo. (L. GONÇALVES, 2018)

Consequentemente o maior uso dos dispositivos *Smart Homes* abre janelas para *hackers,* que são pessoas que agem intencionalmente procurando brechas em sistemas conectados a uma rede, podendo ter uma boa intenção de acionar a empresa sobre um problema que pode acarretar em alguma recompensa para tal, mesmo assim existe o contraponto que são os *hackers* que usam a sua “habilidade” de má fé tirando proveito próprio. (L. GONÇALVES, 2018)

Abrindo uma gama de possibilidades para os hackers, pessoas mal-intencionadas, tentarem achar brechas na segurança de dispositivos que estão conectados na rede. Como os diversos dispositivos celulares, fechaduras, lâmpadas, câmeras, TVs, e até geladeiras inteligentes, tudo armazenando informações em um banco de dados ligado na rede e que você pode controlar pela voz ou pela palma da sua mão, é importante que você tenha segurança e privacidade dentro de sua casa sem abdicar da comodidade tecnológica que isso gera. (L. GONÇALVES, 2018)

2 Referencial teórico

Apresenta-se neste capítulo, uma revisão bibliográfica sobre *IoT* e *smart home*, suas vantagens, novidades, perigos e possíveis soluções.

2.1 Explicação da tecnologia

O termo *IoT* é bastante amplo e engloba diversas definições, tecnologias, componentes e finalidades diferentes. Uma definição comum seria a de “objetos físicos” que foram incorporados com *softwares*, sensores e outras tecnologias para coletar informações e/ou trocar informações com outros dispositivos e sistemas. Esses dispositivos variam de objetos residenciais comuns a ferramentas industriais. (L. GONÇALVES, 2018)

Um dos componentes da IoT seria a *Smart Home* ou Casas Inteligentes. Uma *smart home* é uma casa que possui tecnologia que permite que equipamentos domésticos possam ser controlados automaticamente. Podemos citar cortinas que abrem sozinhas, geladeiras que fazem relatório e até compras, câmeras que podem ser controladas à distância, lâmpadas que se acendem sozinhas e etc. (ORACLE, 2021)

Nos últimos anos, a IoT se tornou uma das tecnologias mais importantes do século XXI. Agora que podemos conectar objetos do cotidiano - eletrodomésticos, carros, termostatos, babás eletrônicas - à Internet por meio de dispositivos incorporados, é possível uma comunicação perfeita entre pessoas, processos e outras coisas. (ORACLE, 2021)

O termo *Smart Home IoT* surge a partir do momento em que os dispositivos *smarts* se conectam a internet, como bem sugestivo IoT (Internet das coisas), isso é bem complicado pois a autores que chamam *Smart Home IoT* apenas por *Smart Home*. Sendo assim uma possível definição mais “correta” seria,” residências equipadas com redes de comunicações de última geração, sensores, dispositivos domésticos, aplicações e funções que podem ser monitorizadas, acedidas e

controladas remotamente, e que disponibilizam serviços que respondem às necessidades dos seus habitantes” (A. GHAFFARIANHOSEINI, 2016).

A *Smart Home* não é uma ideia tão nova como aparenta, apesar dela está se popularizando atualmente pela maior acessibilidade a esse tipo de tecnologia. Mas em 1966 um engenheiro de Pittsburgh chamado Jim Sutherland configurou em sua própria casa a esse sistema no computador ECHO IV para que sua esposa e seus filho controlassem a TV, rádio e outros dispositivos. Construído bem antes dos primeiros computadores domésticos oficiais que entraram para o mercado como, 'trindade' do Apple II, o Commodore PET e o Radio Shack TRS-80, todos introduzidos em 1977.

A tecnologia contava com vários teclados espalhados pela casa que permitiam a interação da Sra. Sutherland e seus filhos. (DAG SPICER, 2016)

2.2. Algumas tecnologias de comunicação

Neste tópico será apresentado as tecnologias que possibilitam a comunicação entre os dispositivos de uma *Smart Home*.

2.2.1 NFC

O *Near-Field Communication (Comunicação de Campo Próximo)* é uma evolução da tecnologia RFID *(Radio FrequencyIdentifier)* ou identificador por radiofrequência, que permite leitura de informações por proximidade, a comunicação é realizada de um terminal ativo (que tem energia) para um passivo (que não tem energia) através de ondas de rádio, que geram um campo eletromagnético que energizam um pequeno conjunto de finos fios de cobre que fornece energia para alimentar um pequeno chip onde pode ser lido informações, nas versões mais sofisticadas da tecnologia também pode-se gravar informações, através da alteração da frequência pudesse também alterar a distância em que a informação é transmitida, a gama de frequências podem ir de 125KHz que permite comunicação a até 50 centímetros e vai até 2,5GHz a uma distância de 10 metros.(RFID…,[S.D.])

O NFC é bem parecido com sua tecnologia antecessora, mas com algumas diferenças, ela foi projetada para operar apenas em baixíssimas distâncias no

máximo até 10cm, mas geralmente operados entre 1 e 5cm de distância em uma frequência de 13,56 MHz com o envio de informações a uma velocidade de mais ou menos 424kbit/s.

As principais diferenças com o RFID é: A capacidade de emular outros dispositivos como por exemplo um celular emulando o chip de um cartão de crédito; O modo de Leitura/gravação bidirecional que permite que que seja lido e escrito em outros dispositivos; E o modo ponto a ponto, que permite que o dispositivo se comunique e troque dados com outro par.

Apesar do seu uso geralmente ser em celulares e cartões de crédito, ele pode ser usado em casa, como em fechaduras eletrônicas residenciais, que podem ser abertas por cartões e celulares que possuem NFC (NFC…, [S.D.])

2.2.2 Wi-Fi

A CISCO (2021) define a o *Wi-Fi* como uma rede tecnologia de rede sem fio capaz de ligar vários dispositivos como celulares, impressoras, e outros equipamentos ele permite que esses dispositivos troquem informações entre si e também com a internet, utilizando como como central um roteador sem fio

O *Wi-Fi* (*Wireless Fidelity*) é regido pelos padrões da IEEE (*Institute of Electrical and Eletronics Engineers*) que construiu um grupo aberto de estudos formados por engenheiros para tornar a tecnologia sem fio uma realidade.

O Padrão IEEE 802.11 que receberia o nome de *Wi-Fi* (*Wireless Fidelity*) nasceu em 1990, porém ficou inerte por sete anos devido a fatores que dificultavam o andamento do projeto, sendo um deles a baixa taxa de transferência que inicialmente a tecnologia oferecia. De acordo com a evolução da tecnologia e da taxa de transferência de dados que passou a atingir velocidades mais altas, a rede sem fio começou a ser vista como promissora, os padrões que se sucederam foram IEEE 802.11b; a; g; n; ac; ax sendo as mais modernas o ac(Wi-Fi 5) e ax (Wi-Fi 6) operando nas frequências de rádio de 2.4GHz e 5GHZ (GARCIA, [S.D.])

Os dispositivos atuais que podem se conecta ao Wi-Fi geralmente usam a frequência de 2.4GHz,pelo fato de ser uma frequência já consolidada e mais com

chips mais baratos, e sua maior facilidade em atravessar as barreiras como as paredes quando comparado com a frequência de 5GHz, já que a maioria dos dispositivos inteligentes de casa não precisam trafegar muitos dados e como o Wi-Fi já é uma tecnologia bem consolidada e que permite também o acesso a internet, essa tecnologia vem se tornando a mais popular entre os dispositivos para o lar, como ar-condicionado, máquina de lavar, câmeras, lâmpadas, TVs, caixas de som e etc.

Porém uma de suas características também é seu defeito, a conexão com a internet constante do roteador e consequentemente dos dispositivos conectados a ele viraram um prato cheio para invasores que podem entrar na rede e secretamente ver e ouvir o que ocorre na sua casa graças a redes mal configuradas ou dispositivos com segurança muito baixa, o que torna ataques a dispositivos cada vez mais comum, porém as empresas estão cada vez mais preocupadas com essa situação e estão lançando atualizações e novos produtos cada vez mais seguros.(ROHR, 2021)

2.2.3 Zigbee

O protocolo zigbee é mantido pela *Zigbee Alliance* - formada por diversas empresas que utilizam a tecnologia da Zigbee, como Amazon, Samsung e Ikea, que tem como objetivo desenvolver e publicar o padrão, em 2021, a *Zigbee Alliance* foi nomeada para *Connectivity Standards Alliance* (CSA). (TILLMAN, 2021)

O Zigbee é baseado no padrão para rede de área pessoal 802.15.4 do IEEE. (802.15.4 é um padrão técnico que define a operação de redes de área pessoal sem fio de baixa taxa e de baixo consumo de energia com a sigla em inglês LR-WPANs).(Ieee 802.15,2010)

Essa tecnologia é amplamente considerada como uma alternativa ao *bluetooth* e ao Wi-Fi principalmente para dispositivos que não precisam de altas velocidades de transferência, como lâmpadas e sensores, O Zigbee não se concentra na comunicação ponto a ponto, como Bluetooth, mas opera em uma rede *mesh*, onde basicamente cada dispositivo funciona como um ponto de amplificação do sinal formando assim uma rede com múltiplos pontos como se fosse vários

roteadores de Wi-Fi espalhados pela casa, aumentando assim a capacidade de transmissão e a estabilidade. (TILLMAN, 2021)

2.2.4 Bluetooth

O Bluetooth é um protocolo de comunicação, projetado originalmente para baixo consumo de energia e curto alcance, que permite dois dispositivos trocarem informações entre si sem fios.

O nome Bluetooth é uma alusão ao rei da Dinamarca Haroldo I, cujo “apelido” era o Dente-Azul, acredita-se, por causa de um dente podre; já o símbolo é a união das runas escandinavas  e  , as iniciais do nome do monarca em Dinamarquês. s(GOGONI, 2019)

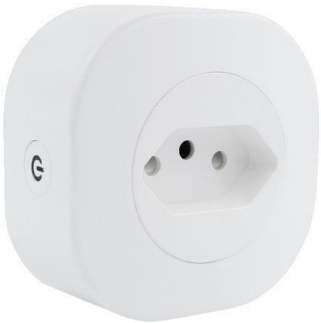
O sistema utiliza uma frequência de rádio de onda curta (2.4 GHz) para criar uma comunicação entre aparelhos, como em algumas versões da tecnologia o seu alcance é curto seu consumo de energia é baixo. (CÂMARA, 2012)

2.3 Alguns dispositivos comuns em *smart home* (*Gadgets*)

Quando falamos em dispositivos para uma *Smart Home* é normal pensarmos em eletrodomésticos mais populares como *smart* TVs, geladeiras *smart*, entre outros. Porém, existem outros dispositivos que passam despercebidos que podem ser indispensáveis em uma casa inteligente:

2.3.1 Adaptador de tomada Wi-Fi.

Permite a transformação de produtos comuns em produtos *Smarts* tornando possível a ativação do eletrodoméstico por voz ou por aplicativo no celular. O controle pode ser realizado por tomada ou por cômodo. Além da possibilidade de um maior controle da energia gasta. (ALVES, 2021)

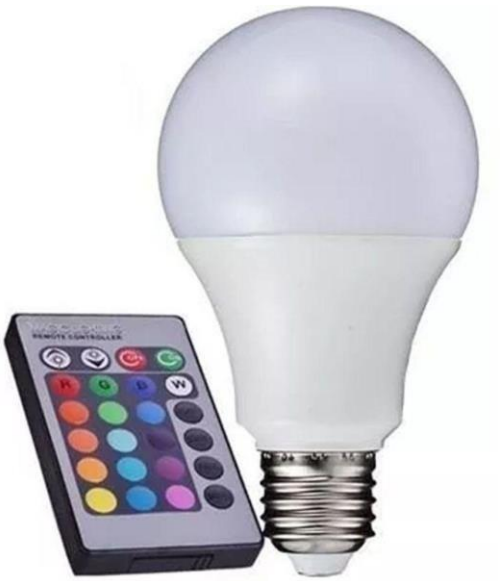


Exemplo de uma tomada que pode ser controlada pelo celular

A tomada pode ser controlada por dispositivos Android e IOS e alguns por comando de voz pela Alexa e Google Assistente e servem para otimizar mais o tempo que algo fica ligado, como a televisão do seu filho ou programar para a cafeteira ligar e já esteja quente ao acordar. Não só para comodidades, mas alguns modelos leem a corrente elétrica e podem cortar a passagem por questões de segurança.

2.3.2 Lâmpadas inteligentes

Permite muito mais do que o controle da iluminação por comando de voz. Com as lâmpadas inteligentes você pode escolher a intensidade da luz conforme a atividade que esteja executando, podendo escolher uma iluminação mais fria em determinados momentos e mais quentes em outros.

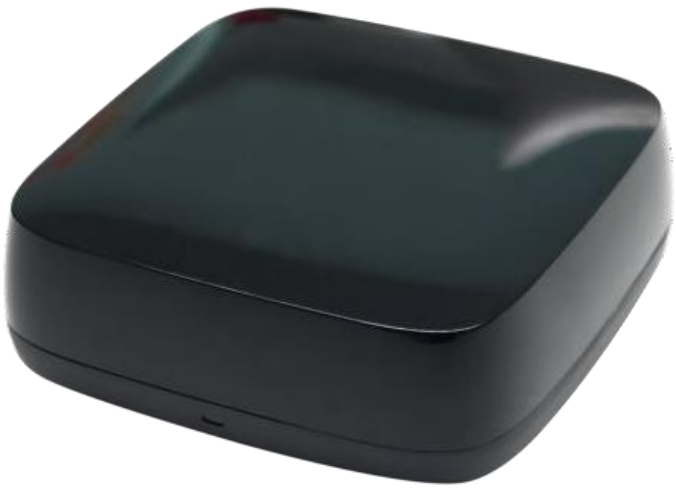


Exemplo de uma lâmpada com a possibilidade de troca da cor e intensidade da luz por controle remoto ou *Wi-Fi*

Também é possível configurar a intensidade da luz por cômodo e por horário. Podendo personalizar a intensidade da luz ao anoitecer e programar para que as luzes estejam apagadas ao sair de casa e que se acendam ao chegar. (ALVES, 2021)

2.3.3 Central de Controle Remoto Universal

Seu funcionamento é parecido com o de um *smart speaker*, após conectado à rede Wi-Fi irá conceder o controle inteligente aos dispositivos conectados na rede. Você irá conseguir controlar sua *smart* TV, ar-condicionado, caixas de som, *home theater* e outros.

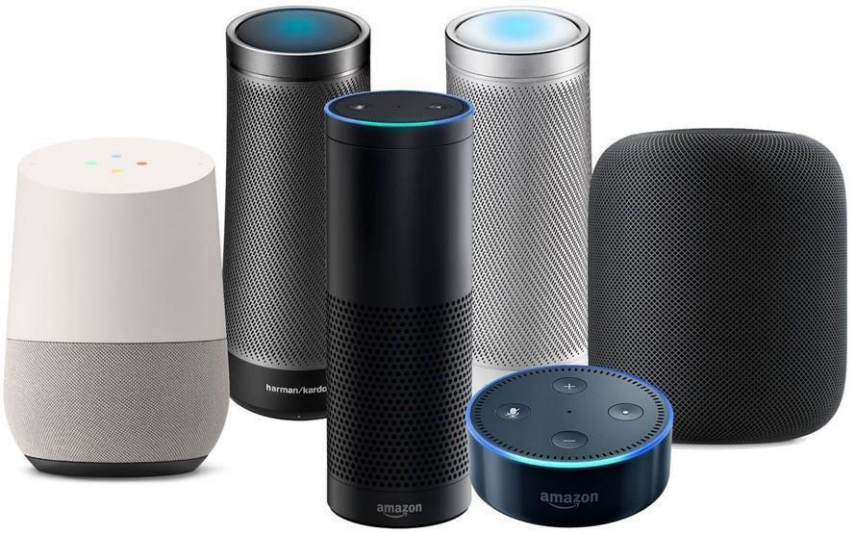


Exemplo de uma central de controle remoto universal

Existem modelos que permitem o controle inclusive de aparelhos utilizando a tecnologia de infravermelho substituindo todos os controles comuns e centralizando todas as funcionalidades na Central de Controle Remoto Universal. (LIMA, 2021)

2.3.4 Smart speakers

Os *Smart speakers* são caixas de som inteligentes que possuem assistentes virtuais e se conectam aos demais dispositivos inteligentes da casa através da rede Wi-Fi. Com ele é possível realizar pesquisas, ouvir música, controlar outros aparelhos inteligentes desde que sejam compatíveis e até mesmo fazer pedidos no Ifood.



Exemplo de *smarts speakers(caixas de som que responde a comandos de voz)*

Existem diversos tipos de *smart speakers* no mercado com diferentes assistentes virtuais. Os principais são *Echo dots* e *Nest* que possuem as assistentes Alexa e Google Assistente, respectivamente.

Além desses existem também a *Homepod* e a *Homepod mini* da Apple que usa a assistente de voz Siri, porém esses não estão disponíveis no Brasil sendo necessário importar e não estão disponíveis no idioma Português.

Existem também exemplos bem menos comuns, como a *Galaxy Home*, assistente da Samsung com a assistente Bixby, que recebeu a versão português a recentemente. (LEANDRO, 2021)

2.3.5 Fechadura digital com Biometria

A fechadura digital com Biometria permite que seja cadastrada diversas senhas, usuários e cadastrados diversos cartões para que possa abrir a porta sem precisar se preocupar em encontrar a chave ou correr o risco de ficar trancado do lado de fora por ter esquecido a chave no trabalho.

Exemplo de uma fechadura com biometria, bluetooth, chave e senha

Também conta com a função de “Não perturbe” que impede que a porta seja aberta por senha, cartão ou aplicativo pelo lado de fora. Além da comodidade de poder abrir a porta para uma visita mesmo se você não estiver em casa pois a fechadura permite que você abra a porta por aplicativo. (ALVES, 2021)

3 Desenvolvimento da Pesquisa

Apresenta-se neste capítulo, uma explicação sobre os problemas constatados durante a pesquisa e as precauções a serem tomadas para evitar problemas não esperados.

3.1 Problemas de segurança

Como pudemos ver até aqui, são vários os benefícios oferecidos pelas *smart homes* que vão de informações sobre o consumo até a comodidade de executar algumas ações de forma mais prática e confortável. Mas todas essas vantagens vêm acompanhadas de um problema de segurança que pode ocorrer por diversos motivos. Os principais seriam:

- Hoje os fabricantes colocam sensores *IoT* em carros, geladeiras, relógios, fechaduras e muitos outros aparelhos. Estes sensores permitem que esses aparelhos captem informações e posteriormente se conectem à internet, permitindo que se comuniquem com outros aparelhos e sistemas. Esses dispositivos oferecem uma grande gama de recursos, mas também nos trazem algumas vulnerabilidades. Cada dispositivo requer proteção conforme essas vulnerabilidades são detectadas.

- O segundo problema é similar ao primeiro, muitos dos dispositivos *IoT* não possuem recursos de segurança. Talvez por pressa para lançar os dispositivos ou por ser muito complicado desenvolver uma medida de segurança para dispositivos subjacentes. Embora sejam muito sofisticados e com bastante recursos, não há uma estrutura de segurança.

- E o terceiro motivo é que mesmo quando o dispositivo possui uma medida de segurança o usuário opta por configurá-lo em outro momento. Muitas das vezes esse momento nunca chega, deixando então uma brecha na segurança.

Agora que sabemos que existe um problema de segurança, precisamos entender que tipo de problema isso pode trazer para o usuário e esses variam bastante dependendo do dispositivo. (FISHER, 2019)

Entre os principais problemas temos:

3.1.1 Proteção de Dados

Os produtos *IoT's* nos últimos anos levaram a coleta de dados a níveis preocupantes, tornando a preocupação com a privacidade um dos problemas mais urgentes dos produtos. Por exemplo, algumas televisões foram flagradas gravando a conversa do usuário enquanto aguardava o comando. (FISHER, 2019)

3.1.2 Dispositivos sequestrados

O cibercriminosos consegue sequestrar o dispositivo conseguindo controlar câmeras, enviando mensagens de voz para o usuário com ameaças e até assumindo o controle do termostato e alterando a temperatura da residência.

Algumas dessas situações ocorreram devido ao baixo nível da senha dos usuários ou usaram a mesma senha que usaram em outro lugar e quando o cibe criminoso descobriu a senha conseguiu acesso aos dispositivos. E, diferente de aparelhos que nos informam quando um acesso é realizado, os dispositivos *IoT* nem sempre possuem esse mecanismo.

Outro problema dos dispositivos *IoT* é que eles estão sempre conectados através da mesma rede e quando um deles é acessado abre uma brecha que facilita o acesso aos demais dispositivos. (FISHER, 2019)

3.2 Solução para os problemas de segurança

Não pretendemos abrir mão da comodidade apesar dos problemas de segurança, então algumas recomendações de segurança podem evitar prejuízos e roubo de dados dos dispositivos. No âmbito de ajudar fabricantes, desenvolvedores e consumidores foi formado o *open web application security project* (*OWASP) com* o intuito de definir para empresas base de testes e de programação para novos produtor e atualizações para os que já foram lançados, e para consumidores dica de segurança importante podendo ser mencionadas algumas delas como: (FREDRIC PAUL, 2019)

- Senhas fracas ou previsíveis é geralmente a forma mais fácil de ter seu dispositivo invadido, evite colocar senhas como admin admin,12345 ou a data

do seu aniversário, apesar de tentadoramente fácil de lembrar você está praticamente deixando aberta as portar para qualquer invasor.

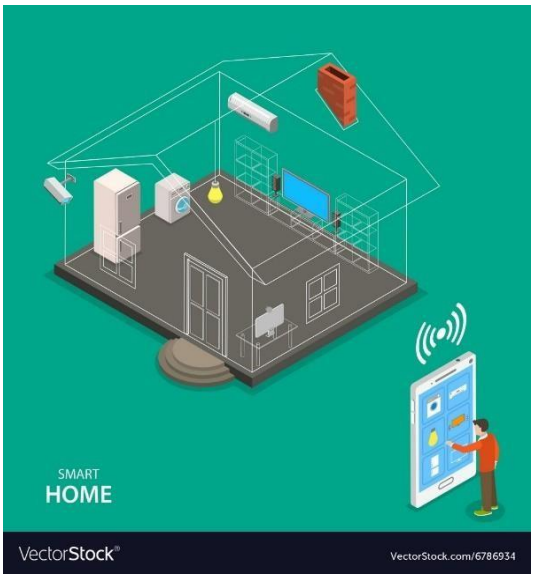
- Uso de componentes inseguros ou desatualizados como por exemplo equipamentos comprados sem marca ou com marcas desconhecidas, apesar de tentador pelo preço é necessário ter em vista que esse tipo de equipamento pode vir com brechas para invasão desde a fábrica. É importante também manter seus dispositivos sempre atualizado pois a cada nova falha descoberta geralmente é lançado também uma atualização para corrigi-la.

- Transferência e armazenamento de dados inseguros, falta de criptografia no armazenamento ou armazenar dados desnecessários dentro do dispositivo pode não ser uma boa ideia, deve-se prestar atenção também na criptografia durante a transferência de dados, questão importante que é geralmente esquecida pelos fabricantes. (OWASP, 2018)

4 Implementação

Uma implementação da tecnologia é transformar um ar-condicionado que não tenha nenhuma forma de conexão remota com controle remoto ou aplicativo, em um dispositivo que possa ser controlado remotamente com a instalação de um interruptor com conexão *wi-fi*.

Onde pode-se deixar o interruptor do ar condicionado em uma posição pré-determinada e quando liberar a passagem de energia com o auxílio do interruptor controlado pelo celular o ar-condicionado ligara sem precisar de nenhuma intervenção física no aparelho.



Outra implementação prática de uma *Smart Home* criamos uma casa com alguns dispositivos inteligentes que podem ser controlados e monitorados a distância.

A lâmpada pode ser controlada pelo celular, sem a necessidade de se levantar para ir até o interruptor, além de conseguir escolher cores diferentes e até a intensidade da luz para diferentes horários do dia.

Com um controle remoto universal, seria possível controlar a televisão e o ar condicionado sem a necessidade de diversos controles diferentes para cada dispositivo.

Com um *Smart Speaker* seria possível conversar com a assistente (inteligência artificial) para controlar os dispositivos *smarts* da residência. Se utilizar juntos ao *smart speaker* com o controle universal, você poderia controlar inclusive alguns dos dispositivos que não são *smarts* com comando de voz, como televisores e ar-condicionado que possuem tecnologia infravermelho para se conectar ao controle universal.

Além dessas vantagens, também seria possível ter um controle do consumo de energia de todos os equipamentos *smarts* pelo celular e receber informações de uso, entre outras informações e até programar funcionalidades desde que o software forneça essas funções.

5 Resultado

Nessa pesquisa pede-se ver o quanto a tecnologia *Smart Home* avançou desde os primeiros protótipos com ações simples em 1966 do engenheiro Jim Sutherland até os dispositivos mais tecnológicos com inteligências que reconhecem a quem devem se dirigir os seus comandos.

Durante a pesquisa foi apresentado os protocolos de comunicação que fazem com que toda a *Smart Home* aconteça, sendo desde os mais comuns como o *Wi-Fi* e Bluetooth, mas também uma alternativa do *Zigbee* que é uma tecnologia exatamente para dispositivos como as luzes, tomadas, sensores, fechaduras que necessitam de baixa taxa de transferência de dados.

Em contraponto se encontra a *OWASP (*Open Web Application Security Project) que basicamente se dedicam a artigos, metodologias, documentação, ferramentas e tecnologias pela segurança, podendo ser aplicadas pelas empresas.

Com o surgimento de várias tecnologias podemos concluir que uma das principais formas do usuário convencional se proteger de eventuais problemas de segurança é o uso de senhas fortes, sempre fazer atualizações de rotina dos dispositivos, evitar transferência de dados duvidosos e usar dispositivos com marcas desconhecidas geralmente com preços bem competitivos que não valem o perigo.

6 CONSIDERAÇÕES FINAIS

Esse trabalho foi desenvolvido através de pesquisas em diversos sites e trazido as partes mais importantes para ajudar a compreender melhor sobre os novos dispositivos que vieram para facilitar a vida das pessoas no ambiente doméstico, que vem crescendo bastante em quantidade e qualidade dentro das casas das pessoas mais comuns, trazendo comodidade e praticidade.

Explicando como funciona os dispositivos, e as tecnologias que já conhecemos como o *bluetooth*, Wi-Fi, entre outros meios de comunicação que tornam possível a integração humana-máquina.

Expondo também os problemas que essas comodidades trazem que antes era inexistente, já que não havia por exemplo o risco de você ser visto por outras pessoas dentro de sua casa, mas também trazendo recomendações de como se proteger e alertando sobre a cautela que deve se ter com esses equipamentos.

Sem dúvidas toda nova tecnologia enfrenta problemas, mas também traz diversas vantagens, afinal de contas tudo que é novo deve e tende a ser aprimorado, assim como acontece com outros produtos como os carros, as pessoas não vão abrir mão de quaisquer itens que lhes forneçam mais praticidade para suas vidas apesar de apresentar algumas desvantagens.

Sem dúvida em alguns anos não saberemos mais como vivermos sem dispositivos que facilitam nova vida ao ponto de não precisarmos realizar tarefas desagradáveis do dia a dia, no futuro a grande maioria terá robôs limpando suas casas, caixas de som que recebem comandos e preparam café e abrem cortinas deixando para nós o prazer de sentar e relaxar lendo um livro ou vendo TV e beber um café que você não precisou mexer um músculo para prepara-lo.

7 REFERÊNCIAS

Referência: GONÇALVES, L.. Vulnerabilidades em Dispositivos IoT em Ambiente Smart Home. 2018. Disponível em: https://repositorio.ipbeja.pt/bitstream/20.500.12207/4827/1/Dissertacao_Luis_Costa_PDFA.pdf. Acesso em: 16 set. 2021.

Referência: K. Bing, L. Fu, Y. Zhuo, e L. Yanlei, “Design of an Internet of Things-based *smart home* system,” in 2011 2nd International Conference on Intelligent Control and Information Processing. Harbin, China: IEEE, 7 2011, pp. 921–924. (citado nas págs. 10 e 12)

Referência: RAYMUNDO, Rafael Tourinho. Pesquisa Bibliográfica: significado e etapas de como fazer. 2020. Disponível em: https://viacarreira.com/pesquisa-bibliografica/. Acesso em: 5 set. 2021.

Referência: ORACLE. IoT. Disponível em: https://www.oracle.com/br/internet-of-things/what-is-iot/#link0. Acesso em: 18 set. 2021.

Referência: ALVES, Robinson Samulak. *Smart home*: 10 produtos para deixar sua casa inteligente. Disponível em: https://www.tecmundo.com.br/produto/217957-*smart-home*-10-produtos-deixar-casa-inteligente.htm. Acesso em: 15 set. 2021.

Referência: LIMA, Ramalho. Conheça as principais funções do *Smart* controle universal. 2021. Disponível em: https://www.tecmundo.com.br/produto/209484-conheca-principais-funcoes-*smart*-controle-universal.htm. Acesso em: 20 set. 2021.

Referência: LEANDRO, Lucimara. Quer um *smart speaker*? Saiba o que buscar em uma nova caixinha do tipo. Disponível em: https://www.techtudo.com.br/listas/2020/12/vai-comprar-um-*smart-speaker*-saiba-o-que-buscar-em-um-novo-modelo.ghtml. Acesso em: 20 set. 2021.

Referência: FISHER, Sharon. Riscos de segurança da Internet das Coisas. 2019. Disponível em: https://www.avast.com/pt-br/c-iot-security-risks. Acesso em: 25 set. 2021.

Referência: RFID: COMO FUNCIONA. Disponível em: https://www.gta.ufrj.br/grad/07_1/rfid/RFID_arquivos/como%20funciona.htm. Acesso em: 19 set. 2021.

Referência: NFC vs. RFID: Qual é a diferença entre eles?. Disponível em: https://www.asiarfid.com/pt/nfc-vs-rfid.html. Acesso em: 19 set. 2021.

Referência: RFID x NFC. Disponível em: https://www.tag-id.com.br/blog/rfid-vs-nfc/. Acesso em: 19 set. 2021.

Referência: WHAT Is Wi-Fi? Disponível em: https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html. Acesso em: 26 jun. 2027.

Referência: GARCIA, Luis Guilherme Uzeda. Redes locais sem fio que atendem ao ao padrão IEEE 802.11. Disponível em: https://www.gta.ufrj.br/grad/01_2/802-mac/. Acesso em: 26 set. 2021.

Referência: ROHR, Altieres. Microsoft encontra 25 falhas de segurança em sistemas criados para dispositivos da 'internet das coisas'. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/05/03/microsoft-encontra-25-falhas-de-seguranca-em-sistemas-criados-para-dispositivos-da-internet-das-coisas.ghtml. Acesso em: 26 set. 21.

Referência: SPICER, Dag. THE ECHO IV HOME COMPUTER: 50 YEARS LATER. 2016. Disponível em: https://computerhistory.org/blog/the-echo-iv-home-computer-50-years-later/?key=the-echo-iv-home-computer-50-years-later. Acesso em: 26 set. 2021.

Referência: Ieee (org.). IEEE 802.15 WPAN™ Task Group 4 (TG4). 2010. Disponível em: https://www.ieee802.org/15/pub/TG4.html. Acesso em: 30 out. 2021.

Referência: TILLMAN, Maggie. What is Zigbee and why is it important for your smart home? 2021. Disponível em: https://www.pocket-lint.com/smart-home/news/129857-what-is-zigbee-and-why-is-it-important-for-your-smart-home. Acesso em: 30 out. 2021.

Referência: GOGONI, Ronaldo. O que é Bluetooth? 2019. Disponível em: https://tecnoblog.net/278962/o-que-e-bluetooth/. Acesso em: 31 out. 21.

Referência: CÂMARA, Marlon. Bluetooth: O que é e como funciona: como funciona o bluetooth?. Como funciona o Bluetooth?. 2012. Disponível em: https://www.techtudo.com.br/noticias/2012/01/bluetooth-o-que-e-e-como-funciona.ghtml. Acesso em: 31 out. 21.

Referência: OWASP (org.). Seek & Understand. 2018. Disponível em: https://owasp.org/www-project-internet-of-things/#. Acesso em: 20 nov. 2021.

Referência: FREDRIC PAUL (Eua). Networkworld. 10 principais vulnerabilidades da Internet das Coisas. 2019. Disponível em: https://cio.com.br/gestao/10-principais-vulnerabilidades-da-internet-das-coisas/. Acesso em: 20 nov. 2021.