



UNIBRA
CENTRO UNIVERSITÁRIO BRASILEIRO

**CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
REDE DE COMPUTADORES**

LILIAN VITORIA MARTINS DA COSTA
LEANDRO HENRIQUE MONTE DE MELO
REGINALDO DA SILVA OLIVEIRA
ALINE FERREIRA BARBOSA – CO ORIENTADORA

**CASAS INTELIGENTES: UMA BREVE ABORDAGEM
SOBRE DISPOSITIVOS, SEGURANÇA E
GERENCIAMENTO**

RECIFE

2020

LILIAN VITORIA MARTINS DA COSTA
LEANDRO HENRIQUE MONTE DE MELO
REGINALDO DA SILVA OLIVEIRA
ALINE FERREIRA BARBOSA – CO ORIENTADORA

CASAS INTELIGENTES: UMA BREVE ABORDAGEM SOBRE DISPOSITIVOS, SEGURANÇA E GERENCIAMENTO

Artigo apresentado ao Centro Universitário Brasileiro – UNIBRA,
como requisito parcial para obtenção do título de tecnólogo em
Redes de Computadores.

Professora Orientadora: Prof.^a Ameliara Freire

RECIFE
2020

C837c

Costa, Lilian Vitoria Martins da
Casas Inteligentes: uma breve abordagem sobre dispositivos, segurança e gerenciamento. / Lilian Vitoria Martins da Costa; Leandro Henrique Monte de Melo; Reginaldo da Silva Oliveira. - Recife: O Autor, 2020.
24 p.

Orientador(a): Ameliara Freire Santos de Miranda;
Coorientadora: Aline Ferreira Barbosa

Trabalho de Conclusão de Curso (Graduação) – Centro
Universitário Brasileiro – UNIBRA. Graduação Tecnológica em Redes
de Computadores, 2020.

1. Casas inteligentes. 2. Internet of things. 3. Gerenciamento
de dispositivos. 4. Rede de computadores. I. Centro Universitário
Brasileiro. – UNIBRA. II. Título.

CDU: 004.7

LILIAN VITORIA MARTINS DA COSTA
LEANDRO HENRIQUE MONTE DE MELO
REGINALDO DA SILVA OLIVEIRA
ALINE FERREIRA BARBOSA – CO ORIENTADORA

CASAS INTELIGENTES: UMA BREVE ABORDAGEM SOBRE DISPOSITIVOS, SEGURANÇA E GERENCIAMENTO

Artigo aprovado como requisito parcial para obtenção do título de Tecnólogo em Redes de Computadores pelo Centro Universitário Brasileiro – UNIBRA, por uma comissão examinadora formada pelos seguintes professores:

Prof.^a Ameliara Freire Santos de Miranda
Professora Orientadora

Prof.^a Aline Ferreira da Silva
Professora Examinadora

Prof. Diego Ribeiro Gomes
Professor Examinador

Recife, ___/___/___

NOTA: _____

Dedicamos esse trabalho a nossa família, mestres e amigos.

Agradecimentos

Agradecemos primeiramente a Deus, pois ele que nos deu sabedoria e luz para a realização deste trabalho. Segundamente aos nossos familiares, que nos apoiaram e incentivaram durante esta caminhada para conclusão deste curso. E aos nossos mestres e amigos, que contribuíram no andamento desta pesquisa.

“A perfeição não é atingível. Mas se perseguir a perfeição, podemos alcançar a excelência.”

(Vince Lombardi)

Resumo

Nos últimos anos a tecnologia vem avançando cada vez mais e tornou-se algo essencial para a sociedade. Com esse avanço surge a praticidade de se interligar todos os dispositivos domésticos para maior comodidade das pessoas. Neste intuito, o presente artigo tem o objetivo de demonstrar como as casas inteligentes vem tomando espaço no cotidiano das pessoas e a necessidade de possuir um controle sobre essa tecnologia, pois já estamos vivendo o futuro. Foi realizado uma pesquisa de revisão da literatura para identificar a real necessidade, de gerenciar esses dispositivos, como isso pode influenciar na rede e que tecnologias temos no momento para auxiliar a ter este controle. Para isso, se fez necessário realizar uma análise em trabalhos relacionados com o assunto proposto, buscando focar em como possuir um ótimo desempenho na rede em casas inteligentes. Através da pesquisa realizada constata-se que os objetivos foram atendidos pois foi possível identificar métodos para um bom gerenciamento de dispositivos e ter uma rede estável.

Palavras-chave: Casas inteligentes. Internet of things. Gerenciamento de dispositivos. Rede de computadores.

Abstract

In recent years technology has been advancing more and more and has become something essential for society. With this advance comes the convenience of connecting all household devices for greater convenience of people. In this way, this article aims to show how smart homes have been taking space in people's daily lives and the need to have control over this technology, because we are already living the future. A literature review research was conducted to identify the real need to manage these devices, how this can influence the network and what technologies we currently have to help have this control. For this, it was necessary to perform an analysis in studies related to the proposed subject, seeking to focus on how to have a great performance in the network in smart homes. Through the research carried out it was verified that the objectives were met because it was possible to identify methods for a good management of devices and have a stable network.

Keywords: Smart houses. Internet of things. Device management. Computer network.

SUMÁRIO

1 INTRODUÇÃO	9
1.1 Motivação	10
1.2 Problemáticas	10
1.3 Objetivos gerais	10
1.3.1 Objetivos específicos	10
1.4 Organização do trabalho	11
2 REFERENCIAL TEÓRICO	12
2.1 IoT (Internet das coisas)	12
2.1.2 Segurança na informação em IoT	12
2.2 Rede	13
2.3 Domótica	13
2.4 Google assistant	14
2.4.1 Como google assistente influência em IoT	14
3 METODOLOGIA	15
4 RESULTADOS	16
4.1 Dispositivos	16
4.2 Segurança	18
4.3 Gerenciamento	19
5 CONCLUSÃO E TRABALHOS FUTUROS	21
REFERÊNCIAS	22

1 INTRODUÇÃO

Nos últimos anos estamos presenciando cada vez mais a evolução das TICs (Tecnologias de Informação e Comunicação) que nos proporcionam acesso a informações e recursos de forma integrada, facilitando até a realização de tarefas cotidianas, com isso, a utilização de tais tecnologias têm mudado de forma abrangente o modo em que as pessoas se organizam em suas atividades diárias (INFOESCOLA, 2020).

A IoT (Internet of Things) chega na sociedade como um suporte para esse tipo de transformação, de forma em que com o seu uso é possível controlar todos os dispositivos ao seu favor, em seu próprio tempo e modo destinado trazendo assim mais eficiência e conforto para o portador (TOMÁZ, Márcio Raonni de Santana, 2020a). A IoT é uma solução factível para diferentes aplicações da automação, seja industrial, comercial e até mesmo residencial.

Neste contexto, a tendência da automação residencial (comumente chamada de casa inteligente ou Domótica) apresenta-se como uma alternativa de ponta capaz de automatizar e controlar parte dos dispositivos de uma casa, fornecendo uma série de benefícios aos seus usuários. O seu funcionamento compõe um conjunto de aplicações, ferramentas, protocolos e dispositivos centralizados capazes de tornar a execução desses sistemas automatizados mais simples e rápido (TOMÁZ, Márcio Raonni de Santana, 2020b).

Junto com a disseminação da automatização do ambiente residencial veio o aumento da demanda de integração e conexão entre diferentes dispositivos nesse ambiente. Sendo um desafio garantir que a tecnologia utilizada seja eficaz e que garanta a transferência de dados de forma confiável (MAIER; SHARP; VAGAPOV, 2017). Para isso, este estudo se propõe a realizar uma análise sobre o tema, identificando e esclarecendo algumas especificações da rede, segurança e sistemas integrados inerentes aos ambientes residenciais inteligentes.

1.1 Motivação

A escolha do tema foi baseada no grande aumento de dispositivos interligados em uma casa e a adoção de sistemas interligados para o gerenciamento dos mesmos, transparecendo a relevância de gerenciar dispositivos em casas inteligentes e pondo em pauta os riscos em que podem ocorrer sem o uso do mesmo, e proporcionar uma melhor segurança dos dados e dispositivos juntamente com a utilização do mesmo.

Sendo de interesse geral mostrar alguns desses dispositivos e relatar algumas ameaças, que podem trazer riscos à segurança.

1.2 Problemáticas

De acordo com os autores o tema proposto, será demonstrado o desempenho com o uso do gerenciamento em casas inteligentes e suas vantagens em utilizar essa forma de serviço.

- A falta de monitoramento dos dispositivos pode acarretar em vários problemas em sua utilização, fazendo com que não funcionem de forma devida;
- Privacidade dos dados, pelo grande número de dispositivos os dados que trafegam pela rede ficam mais vulneráveis;
- Alto custo de energia com vários tipos de dispositivos, que por muitas vezes, podem-se encontrar ociosos, porém permanecem consumindo energia.

1.3 Objetivos gerais

Realizar uma análise em casas inteligentes, sua instalação e o uso do gerenciamento com o auxílio das ações em que essa função pode proporcionar ao usuário. Verificar a segurança dos dados, fazendo o uso do gerenciamento, na utilização de dispositivos integrados.

1.3.1 Objetivos específicos

Para alcançar nosso propósito foi definido os seguintes objetivos específicos:

- Analisar e fazer estudo de pesquisas relacionados ao tema mencionado;
- Apresentar os tipos de dispositivos integrados;
- Apresentar evidências sobre a segurança em casas inteligentes;
- Apresentar o uso do gerenciamento;

1.4 Organização do trabalho

A estrutura deste estudo está organizada em 5 capítulos, a seguir é resumido a proposta de cada capítulo:

- O primeiro capítulo foi composto pela introdução, no qual descreveu a problemática e a proposta do estudo por meio dos objetivos.
- O segundo capítulo aborda os principais conceitos, tais como: IoT, Casas Inteligentes, Segurança de redes.
- O terceiro capítulo descreve os procedimentos metodológicos utilizados neste trabalho.
- O quarto capítulo mostra os resultados, isto é, descrição detalhada dos trabalhos analisados.
- Por fim, no quinto capítulo apresenta as conclusões e trabalhos futuros.

2 REFERENCIAL TEÓRICO

Neste capítulo é apresentada a fundamentação teórica sobre casas inteligentes, protocolos utilizados para a interligação entre os dispositivos, os conceitos das tecnologias utilizadas em casas inteligentes.

2.1 IoT (Internet das coisas)

Para Bassi e Horn (2008), a Internet das Coisas são dispositivos que operam em espaços inteligentes e usam interfaces inteligentes onde eles se conectam e se comunicam dentro dos contextos sociais, ambientais e de usuários. De acordo com os autores, de forma geral Internet das Coisas significa uma rede mundial de objetos interligados, com base em protocolos de comunicação. (BASSI e Horn, 2008).

Internet das Coisas (IoT) de modo facilitado, é a parte em que conecta todos os dispositivos ao seu redor, e é onde pode feita a comunicação de pessoas com os dispositivos de maneira em que pode ser processado, gerenciado e ser feito coleta de dados de forma remota e automática. Com o crescimento do IoT no mundo não será apenas utilizado, dispositivos celulares e computacionais, mas ele envolverá todos os dispositivos como cafeteira, geladeira, microondas, fogão e entre outros eletrodomésticos. E com isso, todos os dispositivos poderão se comunicar um com o outro e fazer a interação com pessoas (Eduardo Magrani, 2018).

2.1.2 Segurança na informação em IoT

Em termos de computação, para que tenha a garantia da segurança da informação é necessário seguir os três pilares da segurança: a disponibilidade onde a informação deve estar sempre disponível para o usuário quando solicitado, a integridade que é a informação em sua essência, sem alguma modificação e a confidencialidade onde só pode ser acessado com o agente autorizado, e todos esses pilares devem trabalhar todos devidamente juntos para que a segurança seja feita de forma devida (DANTAS, 2011; CHERDANTSEVA; HILTON 2013; MATTORD, 2015).

Assim como qualquer outra tecnologia, também vale ressaltar a segurança de IoT nas casas inteligentes, pois essa tecnologia também pode sofrer algumas vulnerabilidades porque ela também é mais vulnerável do que as outras tecnologias. E com o aumento de dispositivos conectados podem ter conseqüentemente o crescimento de vulnerabilidades como por exemplo, no armazenamento de informações, privacidade do usuário, o controle do acesso e o gerenciamento dos

dispositivos, também se aplica em uso de políticas de segurança para IoT. (DANTAS, 2011)

2.2 Rede

A rede em uma casa inteligente se encarrega de interligação dos meios físicos (dispositivos e derivados). Caracterizando-se por um determinado meio de comunicação e protocolos (A.M. Rodríguez, M. Fernández. 2017)

Segundo Ana e Miguel (2007), há diferentes tipos de redes que podem ser utilizadas na ligação dos dispositivos. A escolha de uma delas, vai de acordo com o dispositivo a ser conectado. Podemos destacar:

- Rede de controle - Conecta o gateway diretamente dos sistemas de controle aos dispositivos. Normalmente com uma baixa largura de banda e usa tecnologias como, por exemplo, X-10.
- Rede de dados – Faz a conexão de diferentes dispositivos e seus periféricos através de compartilhamento de recursos. Normalmente com uma largura de banda alta usando tecnologias como USB, bluetooth e wi-fi.
- Redes de entretenimento – É usada para a transmissão de conteúdo interativo (Áudio e vídeo) com alta fidelidade para toda a casa. Com uma largura de banda muito alta, exige que a conexão seja feita via rede de banda larga ou wi-fi 5ghz.

2.3 Domótica

De acordo com Andrade Mariotoni (2007), a domótica é definida como uma utilização de um conjunto com a eletricidade com a eletrônica e com as tecnologias da informação tudo implementado nas casas inteligentes, permitindo que aconteça o gerenciamento tanto local quanto remota e ainda assim oferecer várias aplicações de diversas áreas como, por exemplo, áreas de segurança, conforto, comunicação e gestão da energia.

A domótica surgiu nos anos 80, na França com a necessidade do homem em querer realizar o mínimo esforço em suas tarefas cotidianas. Ela vem do latim “Domus”, que significa casa, junto com a palavra “Robótica”, que está ligada ao ato de automatizar, ou seja, associar automação a uma residência, tornando-a uma casa inteligente. A domótica procura ser um recurso central em uma casa inteligente, é ela que faz a ligação de todos os dispositivos da casa em um único sistema central,

utilizando e associando todas as vantagens dos meios eletrônicos e computacionais. (HUIDOBRO, 2010).

2.4 Google assistant

De acordo com a Google (2020), Google Assistente é uma assistente pessoal desenvolvido pela própria Google que pode realizar tarefas simples do dia-a-dia como mandar mensagens, pesquisar no Google, e ainda conversar com o usuário. Ou pode fazer tarefas complexas, tais como controlar a temperatura de sua casa, ligar e desligar luzes, travar e destravar portas dentre outras funções. As funções mais complexas requerem a aquisição de outros dispositivos inteligentes que tenha suporte ao Google Assistente.

2.4.1 Como google assistente influência em IoT

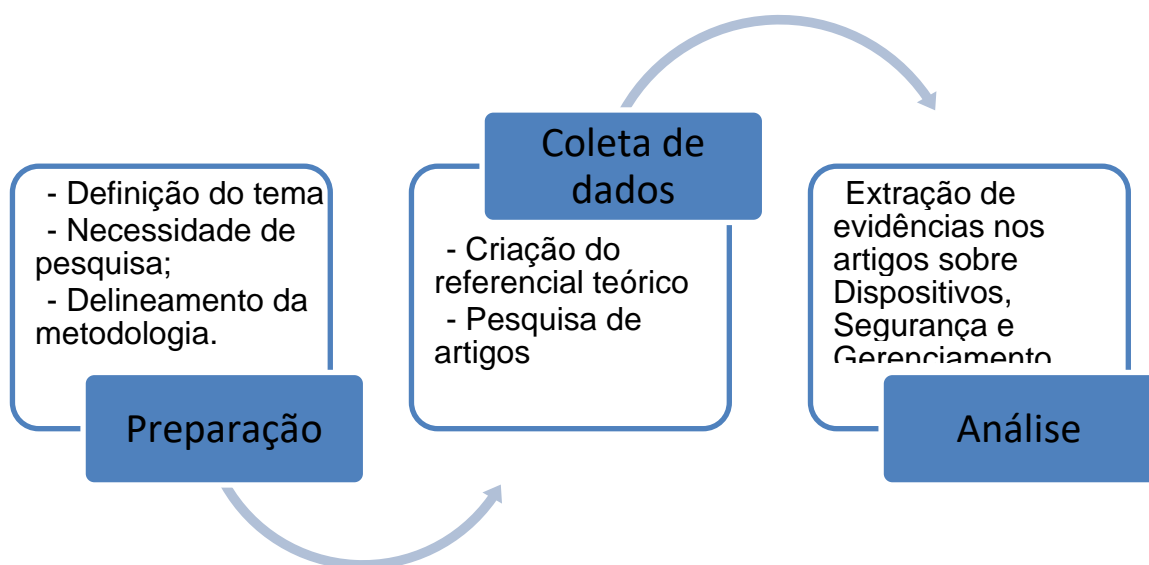
Segundo Google Cloud (2020), a Google Assistente é uma plataforma de serviços inteligentes em IoT, e juntamente com o Google Cloud que é uma suíte que traz a otimização onde é realizado todo o processamento, armazenamento e análise de dados no perímetro e na nuvem. Com o uso do Google Assistente a Google diz trazer mais agilidades, melhora a eficiência operacional fazendo com que funciona com variedades de sistemas operacionais facilitando ainda mais o uso dessa tecnologia, ele também melhora a solução de IoT com inteligência da localização independentemente de estarem perto ou longe do ambiente.

3 METODOLOGIA

Considerando o objetivo principal desta pesquisa, o trabalho definiu como procedimentos metodológicos um conjunto de etapas: iniciando com a preparação, onde buscou a definição do tema e sua relevância para a área pesquisada; seguindo da coleta de dados, etapa crucial para embasamento dos temas que fazem parte do contexto da pesquisa; por fim, a análise foi realizada para extração de evidências das fontes selecionadas (artigos e livro). A Figura 1 detalha a etapa e suas respectivas atividades.

Vale destacar, que foi utilizado strings de buscas no “Google acadêmico” com as palavras “Casas Inteligentes”, “Domótica”, “IoT”, “Segurança em IoT”, procurando por artigos e menções entre os anos 2008 á 2020 em português e espanhol ligadas a casas inteligentes e interligação de dispositivos domésticos, os resultados dos selecionados foram expostos no capítulo

Figura 1: Etapas do trabalho



Fonte: autores

4 RESULTADOS

No processo de busca e construção deste trabalho, encontramos algumas referências (artigos, livros) que abrangesse sobre a temática de casas inteligentes e suas especificações. Em específico, 3 trabalhos foram analisados com objetivo de capturar evidências sobre os dispositivos, segurança e gerenciamento. A Tabela 1 apresenta o resumo dos trabalhos analisados.

Tabela 1. Trabalhos analisados

Citação	Título
Silva et. al. (2016)	Domótica e tecnologias utilizadas na automação residencial
Rodríguez et. al. (2017)	La casa inteligente
Mota et. al. (2015)	Aspectos de segurança em ambientes residenciais inteligentes

Fonte: autores

4.1 Dispositivos

O trabalho de Silva et. al. (2016) foca em uma empresa chamada iHouse que oferecem dispositivos com tecnologias de automação residencial com uma grande variedade de produtos. Dentre os diferentes produtos apresentados pelos autores, o *touchdoor* (Figura 1) é um exemplo relevante quando se trata de fechadura inteligente. Este produto em específico busca agregar segurança a automação, liberando a porta através de leitura da impressão digital interligando a um sistema integrado que possibilita a criação de um log de eventos, onde pode ser armazenado as informações do acesso.



Figura 1 – Touchdoor

Já o trabalho de Rodríguez et. al. (2017) apresenta o *pasarela residencial*, ele controla todos os dispositivos da residência, onde é possível ter todo um amplo controle da rede, possibilitando-o gerenciar as interações com os dispositivos.

Em relação a dispositivos o trabalho de Mota et. al. (2015) menciona o Sentry@Home, ele tem como intuito de preservar os dados quando ocorrer acessos externos, seu papel é de controlar e aumentar a privacidade seguindo um padrão de políticas bem definidas.

Na tabela 2 é detalhado o conjunto de dispositivos citados pelos trabalhos analisados.

Tabela 2. Lista de dispositivos

Dispositivo	Descrição	Citado no trabalho
Touchdoor	Fechadura inteligente que utiliza um leitor biométrico para a liberação do acesso.	Silva (2016)
Geladeira inteligente	Dentro de suas funcionalidades, permite ao usuário ter controle sobre a qualidade dos alimentos guardados, mostrando a hora de reposição.	Rodríguez (2017)
Smartshower	Um chuveiro dotado de um painel lcd que prepara o banho de acordo com o perfil do usuário, controlando o fluxo de água e a temperatura	Silva (2016)

Cafeteira inteligente	É uma máquina de fazer café interligada ao seu smartphone ou ao sistema de automação de sua casa, que possibilita o agendamento para preparação do café.	Rodríguez (2017)
Smarthydro	Uma banheira que possui um sistema de hidromassagem e uma função de auto-clean.	Silva (2016)
Smartwatch	Um relógio inteligente que permite controlar a intensidade da luz, escolher a temperatura do ar condicionado, baixar as persianas ou acesso multimídia.	Silva (2016)

Fonte: autores

4.2 Segurança

O trabalho de Silva (2016) indica a segurança como um dos benefícios mais pensados, tanto segurança física quanto segurança de dados, onde é possível determinar que sejam instalados vários sensores pela residência afim de detectar algum tipo de invasão. A segurança de dados é imprescindível quando se fala em casas inteligentes, pois há uma preocupação em casos de vazamentos de dados, neste caso, a instalação de *firewalls* é de suma importância. No mercado atual, já existem diversos sistemas que possibilitam ao usuário escolher a melhor configuração para implementação de sistemas e equipamentos de segurança que podem ser controlados por uma interface interligada ao sistema de voz, controles remotos ou soluções inteligentes que reconhecem o usuário. Com esse reconhecimento, o sistema pode ser pré-programado para a desativação dos alarmes e acionamento das luzes internas.

No trabalho de Rodríguez et. al. (2017) a segurança foi exposta de forma sucinta, mencionando que intuito da casa inteligente é que a facilidade e a segurança andem juntos, porque ideias novas, tendem não possuir uma boa aceitação, até que provem que possam ser seguras.

Já no trabalho de Mota et. al. (2015) foi identificado possíveis Ameaças nas redes de sensores sem fios, aplicadas aos ambientes nas casas inteligentes. O objetivo geral da segurança em uma rede interna de casas inteligentes são: confidencialidade, integridade, disponibilidade e autenticidade. Levando em conta que os ataques mais comuns são:

- Bisbilhotagem – Quando um indivíduo visualiza a comunicação da rede e rouba os dados. O autor aponta como forma de prevenção a criptografia.
- Negação de serviços – Quando é enviados sinais de rádios com o objetivo de interferir nos sensores sem fio, causando uma colisão de mensagens fazendo com que os sensores retransmitam até causar uma pane geral. O autor sugeriu que haja limitação de tráfego por MAC para limitar os tamanhos dos quadros.
- Comprometimento do nó – É um ataque interno que captura um nó de dados da rede. Pode ser feito um teste de códigos como verificação de memória para impedir a realização deste ataque.
- Ataque físico – É quando o nó é acessado fisicamente, havendo a destruição dos dados. A prevenção seria a limitação de acessos não autorizados aos dados.

4.3 Gerenciamento

O trabalho de Silva et. al. (2016) relata que no desenvolvimento dos sistemas de automação, a uso limpo da energia foi um dos fatores mais impactantes, tendo um custo alto em relação aos gastos pessoais. Portanto, os autores indicam a implementação de sistemas de gerenciamento que utiliza sensores que geram dados de consumo e ativa uma otimização via software para que haja a regulação do consumo de energia. Os sensores podem ser utilizados para determinar se há algum usuário no ambiente, determinado a eficiência da climatização e iluminação, reduzindo também o consumo de energia. O uso da automação residencial pode ser uma grande vantagem à pessoas com deficiências físicas. Onde pode se utilizar um sistema integrado aplicado a sua rotina, possibilitando controlar a iluminação, abertura e fechamento de portas, cortinas, monitoramento das câmeras de segurança em qualquer ponto de sua residência através de um simples controle remoto.

No trabalho de Rodríguez et. al. (2017), os autores mencionam que o gerenciamento da residência, é controlado por uma central, e possui um relatório detalhado de todas informações específicas da residência. Também é possível acompanhar e realizar esse gerenciamento de dispositivos de forma externa. Um exemplo seria tele vigilância, no qual o usuário pode ver as imagens da sua residência

em tempo real, e além do mais pode ligar o ar-condicionado na temperatura que desejar, a luz da varanda ou o que o mesmo desejar.

Por fim, no trabalho de Mota et. al. (2015) foi mencionado sobre a redução de dissipação de energia, onde foi implementado um modo de gerenciamento de energia que realizado para quando os módulos do processador estivessem desligados não houvesse esse desperdício de energia.

5 CONCLUSÃO E TRABALHOS FUTUROS

O desenvolvimento deste trabalho consiste em evidenciar a necessidade de gerenciamento dos dispositivos que compõem uma casa inteligente, focando em aspectos essenciais como segurança e dispositivos. Sabendo que as demandas por serviços automatizados cresceram nos últimos anos, as empresas procuram se adequar a esta nova realidade, para oferecer o melhor serviço e comodidade para os usuários, levando em consideração a proposta de uma casa inteligente que seria facilidade e conforto no lar.

Para trabalhos futuros, planejamos buscar trabalhos em outras bases (exemplo: IEEE, Science direct, Springer dentre outros) e idiomas a fim de complementar nossas pesquisas sobre estes ecossistemas de casas inteligentes e IoT. Junto a este, alimentaremos o site: <http://tcccasainteligente.wordpress.com/>, evidenciando e explicando aos usuários como se comporta uma casa inteligente, suas ligações e dispositivos utilizados para automação residencial.

REFERÊNCIAS

INFOESCOLA. – **Tecnologia da Informação e Comunicação**, 2020, Brasil. Disponível em <https://www.infoescola.com/informatica/tecnologia-da-informacao-e-comunicacao/>. Acesso em 13/05/2020.

TOMÁZ, Márcio Raonni de Santana. - **Internet of Things (IoT) e as profundas modificações nos processos industriais**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 05, Ed. 04, Vol. 06, pp. 134-150. Abril de 2020. ISSN: 2448-0959, Disponível em: <https://www.nucleodoconhecimento.com.br/tecnologia/internet-of-things>

CHERDANTSEVA, Y.; HILTON, J. A Reference Model of Information Assurance & Security* In: IEEE. Availability, reliability and security (ares), 2013 eighth international conference on 2013. P. 546 – 555. Disponível em: <http://users.cs.cf.ac.uk/Y.V.-Cherdantseva/RMIAS.pdf>

A.M. Rodríguez, M. Fernández. La casa inteligente - Universidad Carlos III de Madrid, 2017 – Disponível em: <http://www.it.uc3m.es/~jvillena/irc/practicas/08-09/24.pdf>

BASSI, A.; HORN, G. Internet of Things in 2020: **A Roadmap for the Future**. **European Commission: Information Society and Media**, v. 22, p. 97-114, 2008.

MAURICIO CESAR SILVA; VIVIAN TOLEDO S. GAMBARATO. DOMÓTICA E TECNOLOGIAS UTILIZADAS NA AUTOMAÇÃO RESIDENCIAL, Tekhne e Logos, Botucatu, SP, v.7, n.2, Abril, 2016. Disponível em: <http://revista.fatecbt.edu.br/index.php/tl/article/view/389>

EDUARDO MAGRANI. A internet das coisas. Editora FGV, 15 de jun. de 2018 187 p. Disponível em: <https://books.google.com.br/books?id=qYtIDwAAQBAJ&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>

WHITMAN, M. E; MATTORD, H. J. Principles of Information Security. 5. ed. [S.L]: Cengage Learn, 2015. 656 p. Disponível em: https://www.researchgate.net/publication/311574857_Principles_of_Information_Security_5th_Edition

MARIOTONI; ANDRADE. AUTOMAÇÃO RESIDENCIAL UTILIZANDO UMA PLATAFORMA DE BAIXO CUSTO. 2018 Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/8691/1/PG_COAUT_2016_1_04.pdf

HUIDOBRO. Manual de Domótica. Creaciones Copyright SL, 2010 - 204 p. Disponível em: < https://books.google.com.br/books?id=V6lzqqDcfF8C&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>

DANTAS, M.L. Segurança da informação: uma abordagem focada em gestão de riscos. [S.L]: Livro Rápido-Elógica, 2011. 150 p.

Google assistente. – Disponível em https://assistant.google.com/intl/pt_br/

Google Cloud. – Disponível em <https://cloud.google.com/solutions/iot>