SEGURANÇA E PRIVACIDADE NA INTERNET DAS COISAS

SECURITY AND PRIVACY IN THE INTERNET OF THINGS

Jheniffer C. Pereira[1], Gabriel P. Seno[2], Rogério L. S. Oliveira[3]

[1]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, jheniffer.pereira@fatec.sp.gov.br
[2]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, gabriel.seno@fatec.sp.gov.br
[3]Faculdade de Tecnologia Prof. José Camargo – Fatec Jales, rogerio.leao@fatec.sp.gov.br

Informação e Comunicação
Subárea: Tecnologia da Informação

RESUMO

A cada ano que passa, a Internet das Coisas vem ganhando mais espaço no mundo moderno, mostrando-se eficiente e privilegiando diversas áreas onde é aplicada. Contudo, problemas relacionados à segurança são recorrentes, graças às limitações físicas, o pouco investimento da indústria na implementação de novos sistemas de segurança e o descaso dos usuários quanto ao assunto, os dispositivos de IoT possuem vulnerabilidades que estão sendo cada vez mais exploradas pelos cibercriminosos. Frente ao exposto, o presente trabalho tem como objetivo abordar sobre os principais desafios da segurança e privacidade dos dados na Internet das Coisas e entender os aspectos que devem ser atendidos quanto ao desenvolvimento de dispositivos de IoT. Além do referencial teórico, que apresenta informações baseadas em sites, livros e artigos, foi realizada uma pesquisa quantitativa com o objetivo de identificar se as pessoas reconheciam a importância das medidas de segurança, e se possuíam o conhecimento necessário para realizá-las, onde os resultados obtidos revelam dados preocupantes em relação ao descuidado que a grande maioria têm sobre o assunto.
Palavras-chave: segurança; coleta de dados; internet das coisas; LGPD.

ABSTRACT

With each passing year, the Internet of Things has been gaining more space in the modern world, proving to be efficient and privileging various areas where it is applied. However, security-related problems are recurrent, thanks to physical limitations, and the industry's little investments in the implementation of new security systems and the neglect of users on the subject, IoT devices have vulnerabilities that are being increasingly exploited by cybercriminals. In view of the above, the present work aims to address the main challenges of data security and privacy in the Internet of Things and understand the aspects that must be met regarding the development of IoT devices. In addition to the theoretical framework, which presents information based on websites, books and articles, a quantitative survey was carried out with the objective of identifying whether people recognized the importance of security measures, and if they had the necessary knowledge to carry them out, where the results obtained reveal worrying data in relation to the carelessness that the vast majority have on the subject.
Keywords: security; data collect; internet of things; LGPD.

1 INTRODUÇÃO

A *Internet* das Coisas (IoT - *Internet Of Things*), caracterizada como uma rede de dispositivos inteligentes capazes de coletar dados do mundo real e transmiti-los a outros dispositivos, inclusive a grandes servidores (LEE, 2019), vem ganhando cada vez mais espaço na vida das pessoas. Nesse contexto, dispositivos como assistentes virtuais, relógios (*smartwatches*), TVs (*smart tvs*), lâmpadas, chaves de automóveis, casas inteligentes, dentre

outros, estão cada vez mais populares. De acordo com Newman (2020), estima-se que 41 bilhões de objetos estarão conectados à *Internet* até 2027.

O uso da IoT no agronegócio, governo, saúde, entre outros setores, tem se tornado uma realidade em muitos países do mundo. De acordo com Ellen (2016), um estudo do McKinsey estima que o impacto de IoT na economia global será de até 11% do PIB do planeta em 2025 (algo entre 3,9 e 11,1 trilhões de dólares). Considerando todo esse potencial da IoT, muitos artigos, livros, palestras e tipos de conteúdo costumam enaltecer seus potenciais, esquecendo-se de aspectos importantes como a privacidade e a segurança dos seus usuários.

Segundo Fisher (2019), o grande aumento no número de dispositivos que se encaixam na categoria de IoT, traz diversos problemas relacionados à segurança. Embora a coleta de dados destes dispositivos chegue a níveis assustadores, muitos fornecedores não incluem recursos de segurança, o que acaba gerando vulnerabilidades que poderão ser usadas por cibercriminosos. Outra preocupação importante é sobre quem terá acesso aos dados coletados, considerando que, segundo revelado por Ren et al. (2019) em um estudo, de 81 dispositivos analisados, 72 estavam enviando dados a terceiros.

Diante desse cenário, como parte dos esforços relacionados aos problemas de segurança da informação e privacidade, em agosto de 2018 foi sancionada a Lei Geral de Proteção de Dados (LGPD). A referida lei tem como propósito proteger os dados pessoais dos usuários e estabelecer princípios e regras que devem ser cumpridas por organizações públicas ou privadas (BRASIL, [2019]).

Convém destacar que entre as áreas mais impactadas por essa nova tecnologia está a indústria. Assim, a IoT está se tornando um dos pilares da quarta revolução industrial, também chamada de Indústria 4.0. Essa revolução está inserindo de forma acelerada tecnologias que melhoram as linhas de produção e auxiliam no monitoramento de setores onde há riscos para seus funcionários, tornando-as mais inteligentes e eficientes. Segundo pesquisa da Eclipse Foundation (2020), entre as empresas entrevistadas, 40% já utilizam IoT em seus meios de produção e 22% planejam implantar em até 2 anos.

Essa explosão de conectividade que tem o potencial de impulsionar negócios e melhorar a vida das pessoas, também eleva a outro patamar a insegurança cibernética. Uma casa ou empresa podem ser facilmente alvos de ataques, se houver alguma falha em um dos dispositivos conectados à rede, ela poderá ser usada para invadir todo o sistema e colher informações. Invasões de câmeras ou dispositivos de áudio expondo a privacidade dos usuários vem se tornando cada vez mais comum.

Em um episódio recente, um executivo de uma empresa de serviços financeiros foi alvo de cibercriminosos que localizaram e controlaram um alto-falante inteligente conectado à rede doméstica via *bluetooth* e conseguiram espionar conversas particulares expondo informações privadas do diretor executivo (ACOHIDO, 2021).

Atualmente, já existem *botnets* direcionados ativamente para dispositivos IoT utilizando-os para iniciar vários tipos de ataques distribuídos de negação de serviço conhecidos como ataque DDoS (CISO ADVISOR, 2020). Dispositivos *hackeados* também podem fazer parte de um *botnet* que envia *spam* ou mineram criptomoedas. Ademais, caso a rede da casa inteligente não seja isolada de outras redes, criminosos poderão ter acesso aos *e-mails*, contas bancárias, enviar vírus ou roubar dados pessoais. Grande parte desses ataques ocorre pois os usuários acabam negligenciando alguns cuidados necessários, como por exemplo a modificação da senha padrão.

Considerando o exposto, o objetivo deste trabalho é abordar os principais desafios da segurança e privacidade na Internet das Coisas, discutir e entender os fundamentos mais importantes desta tecnologia e os principais aspectos de segurança que devem ser atendidos quanto ao desenvolvimento de dispositivos de IoT.

Desta forma, o trabalho aqui apresentado está organizado da seguinte forma. Na Seção 2 são apresentados os conceitos e tecnologias utilizadas na IoT contendo informações referente à segurança da informação, vulnerabilidades e privacidade, proporcionando o entendimento dos principais riscos e termos utilizados. Na Seção 3 são apresentados os principais mecanismos utilizados na formação deste trabalho. Na seção 4 são apresentadas as principais análises e discussões dos resultados da pesquisa, e por fim na Seção 5 é apresentado a conclusão e discussão de resultados deste trabalho.

2 REFERENCIAL TEÓRICO

Nesta seção serão apresentados os principais conceitos relacionados a Internet das Coisas, segurança da informação, aspectos importantes da Lei Geral de Proteção de Dados (LGPD), privacidade dos dados coletados por dispositivos e sensores, implementação e crescimento da IoT.

2.1 INTERNET DAS COISAS

Nos últimos anos, a IoT tornou-se uma das tecnologias mais importantes do século XXI. Caracterizada por uma rede de objetos que comunicam-se entre si, dispositivos e outras tecnologias (ORACLE, 2021). Acredita-se que o termo *"Internet of Things"*, tenha sido usado pela primeira vez por Kevin Ashton em uma apresentação feita na *Procter & Gamble* em 1999, de acordo com ele as pessoas precisam se conectar com a *internet* de diversas formas devido à falta de tempo ocasionada pela rotina (ASTHON, 2009).

A ideia de conectar tudo faz-se cada vez mais concreta à medida que esta tecnologia vem evoluindo e se consolidando. Devido a este crescimento os dispositivos IoT vem gerando um número massivo de dados coletados em tempo real, estima-se que até 2025 chegaremos à quantia de 73,1 bilhões de zettabytes (IDC, 2020).

Isso nos leva a um dos termos mais utilizados atualmente, a *big data* que torna-se essencial para IoT devido ao grande número de dados coletados, segundo Gomes (2019), a *big data* é uma análise de um grande volume de dados armazenados e extraí valor de grandes quantidades de informações, tornando possível a tomada de decisões automatizadas aumentando a eficiência do tratamento de dados em diversos setores.

A internet das coisas é composta por um conjunto de fatores que determina como o conceito de IoT é constituído. O modelo de arquitetura básica da IoT apresenta três camadas. A primeira camada é a camada de Percepção, esta camada representa componentes físicos, dispositivos eletrônicos, sensores que estão dispostos nos ambientes para realizar coletas de dados ou responder de acordo com a proposta. A segunda é a camada de rede, nesta camada as abstrações das tecnologias de comunicação, serviços de gerenciamento, roteamento e identificação devem ser realizadas. A terceira camada é chamada de camada de aplicação, a qual é responsável por prover serviços para os clientes (SANTOS et al., 2016).

Em sua grande maioria os dispositivos IoT possuem limitações físicas de *hardware*. Sendo essa uma das grandes barreiras na questão de recursos computacionais, como processador, armazenamento, energia e transmissão de dados (TACHIBANA, 2017), desta forma tecnologias de comunicação devem levar em consideração essas limitações.

Entre as tecnologias de comunicação que levam estes fatores em conta está o *Wi-Fi*, RFID, *ZigBee, Bluetooth Low Energy* (BLE) que é uma versão do *Bluetooth*.

O *Wi-Fi* é baseado no protocolo IEEE 802.11, tratando-se de uma tecnologia de alto desempenho, mas de curto alcance sendo do tipo LAN (Rede de Acesso Local - *Local Area Network*), tendo transmissão de um raio de até 100 metros (EL-SHWEKY et al., 2018).

Entre as tecnologias mais recentes, vem se destacando o 5G, considerada uma das mais importante para a expansão da IoT pois permite um aumento significativo de dispositivos conectados à medida que aumenta a largura da banda de rede (SHATILIN, 2015).

Também está entre os fatores essenciais para IoT, a evolução do protocolo IP, que na versão 4 (IPv4) traz grandes preocupações, embora ainda muito utilizado, o IPv4 traz alguns problemas com o crescimento das redes, por exemplo: possíveis esgotamentos dos endereços IP, o aumento da tabela de roteamento, problemas relacionados à segurança dos dados transmitidos e a prioridade na entrega de determinados tipos de pacotes (IPV6.BR, 2012a). Após identificar esses problemas, foram iniciadas pesquisas que resultou na versão 6 do protocolo IP (IPv6), entre as principais características está o maior espaço de endereçamento, pois com o IPv6 é possível fornecer 79 octilhões de vezes a quantidade de endereços IPv4, o tornando ideal para os dispositivos IoT (IPV6.BR, 2012b).

O protocolo IP é o principal protocolo de comunicação da *Internet*, por consequência, o principal meio de comunicação entre dispositivos de soluções M2M (*machine-to-machine*) que segundo Höller et al. (2014), "refere-se àquelas soluções que permitem comunicação entre dispositivos, seja comunicação com fio ou sem fio", o que possibilita a troca de mensagens entre os elementos da solução permitindo seu controle remoto. Sendo essa comunicação bastante utilizada por monitoramento remoto de pacientes, vigilância residencial e automação industrial (WU et al., 2010).

Como já citado anteriormente existem diversas áreas onde os dispositivos IoT podem ser utilizados, entretanto uma das áreas que tem sido tópico de discussão e desenvolvimento nos últimos anos são as casas inteligentes (*Smart Homes*). As *Smart Homes* são sistemas domésticos integrados que incorporam dispositivos controlando seus recursos internos (MOCRII; CHENB; MUSILEK, 2018).

Uma casa inteligente é composta por sensores, aparelhos ou atuadores que devem gerar dados e agregar valor ao ambiente doméstico. Um ambiente pode ser considerado inteligente somente quando todos os dados são armazenados e analisados coletivamente, padrões extraídos e decisões tomadas sem a intervenção do usuário (MOCRII; CHENB; MUSILEK, 2018).

Atualmente já é possível, por exemplo, criar ambientes automatizados controlados por *smartphones* e *tablets*. Porém, com os avanços tecnológicos não será necessário o uso destes dispositivos, pois os ambientes poderão se controlar sozinhos reagindo à presença do usuário. Entretanto, para que isso seja possível será necessário um grande número de sensores espalhados no ambiente o que poderá acarretar riscos à segurança de informações consideradas privadas (FIGUEIRA, 2016).

2.2 SEGURANÇA DA INFORMAÇÃO

Com essa nova realidade gerada pela IoT, a segurança da informação vem sendo gradativamente diminuída, pois cada dispositivo IoT pode ser um ponto de vulnerabilidade. Esses dispositivos podem ser facilmente corrompidos por meio de códigos mal-intencionados que podem ser inseridos afetando toda a segurança dos sistemas (FIGUEIRA, 2016).

Segundo Maymi e Harris (2010), há três pilares da segurança da informação mais populares, que formam a chamada "*tríade CIA*" que são a confidencialidade, integridade e disponibilidade (do inglês *Confidentiality, Integrity and Availability*) e recentemente para reforçar os pilares da segurança da informação foram inseridos autenticação e não repúdio:

- Confidencialidade: É o primeiro pilar da segurança da informação, pois ela é a garantia que os dados estejam protegidos contra pessoas não autorizadas. É necessário tomar algumas medidas para garantir que a confidencialidade seja garantida para a proteção, como criptografia, uso de senhas fortes entre outras estratégias (MAYMI; HARRIS, 2010);

- Integridade: Dentro do contexto de segurança da informação, integridade diz respeito à preservação, precisão, consistência e confiabilidade dos dados durante todo o seu ciclo de vida. A integridade dos dados é frequentemente afetada por erros humanos, políticas de segurança inadequadas, processos falhos e ciberataques (MAYMI; HARRIS, 2010);
- Disponibilidade: É o que garante o acesso em tempo integral pelos usuários sendo mais um dos pilares da segurança da informação. Esse pilar pode ser prejudicado pois os sistemas são vulneráveis a desastres naturais, ataques de negação de serviço, blecautes, incêndios e diversas outras ameaças que prejudicam sua disponibilidade (MAYMI; HARRIS, 2010);
- Autenticação, Autorização e Auditoria: Busca verificar a identidade de quem realiza uma determinada função em um sistema, verificar que direitos esse usuário possui e armazenar informações de uso deste usuário (CHICARINO et al., 2017);
- Não Repúdio: O não repúdio foi criado para garantir que a pessoa não negue ter feito determinada ação no sistema. Ele garante provas suficientes sobre a identidade de todas as ações que o usuário realizou, como transferir dinheiro, autorizar uma compra ou enviar uma mensagem (CHICARINO et al., 2017).

Levando esses pontos em consideração no que diz respeito à segurança da informação, os sensores e dispositivos que estão conectados são o ponto de maior fragilidade e quebra de segurança. Pois diversos *softwares* e processos de segurança já foram criados para garantir os níveis de segurança adequados para os servidores. Portanto, a prioridade fundamental atualmente é encontrar soluções que garantam a segurança que os produtos e serviços IoT necessitam (FIGUEIRA, 2016).

Segundo publicado por Kalita e Kar (2009) existem pelo menos 37 possíveis ataques que podem ser direcionados a redes sem fio e que são transponíveis a IoT entre esse estão:

- Ataques de Negação de Serviço (DoS): impedimento ou restrição do uso normal da rede ou administração de dispositivos de rede ou rede sem fio;
- Análise de Tráfego: monitoramento das transmissões via redes sem fio para identificar padrões de comunicação e participantes;
- Wormhole: encaminhamento de mensagens recebidas em um link de baixa latência e as reproduz em outra parte diferente da rede com o propósito de interromper o roteamento;
- Ataques Sybil: dispositivos maliciosos ilegitimamente que tomam inúmeras identidades;
- Espionagem: um atacante mal-intencionado monitora de forma passiva redes sem fio para coletar dados, incluindo credenciais de autenticação.

A IoT ainda está muito longe de estar segura o suficiente contra os problemas de segurança e ataques da *internet*, muito em parte, devido a particularidades desta tecnologia, tais como as comunicações serem realizadas através de redes sem fio onde qualquer indivíduo mal-intencionado pode ter acesso a essas transmissões e se comunicar. Existe também o desafio dos dispositivos contarem com recursos limitados que impossibilitam medidas de segurança mais robustas.

2.3 COMPUTAÇÃO EM NUVEM PARA IOT

A computação em nuvem é um dos componentes fundamentais da Internet das Coisas, sendo criada a partir de diversas fazendas de servidores conectadas a redes de alta velocidade. Com o acesso aos recursos computacionais como redes, servidores, armazenamento e serviços, proporcionam o uso de aplicações a partir de qualquer lugar do mundo, sem os custos e a

complexidade que acompanham a obtenção e a administração de componentes de *hardware* e *softwares* (HUREL; LOBATO, 2018).

As informações e os dados produzidos pelas aplicações de IoT, necessitam de grande poder computacional. Por conta de seu grande volume e para o fornecimento ininterrupto de seus serviços de processamento e armazenamento, as fazendas de servidores devem estar amplamente distribuídas pelo mundo (HUREL; LOBATO, 2018).

Os problemas de segurança associados à computação na nuvem são divididos em duas amplas categorias. Sendo a primeira enfrentada pelos provedores de serviços, nos quais necessitam de uma boa e altamente segura infraestrutura para o armazenamento dos dados. A segunda refere-se aos problemas enfrentados pelos consumidores que armazenam aplicações ou seus dados na nuvem, fazendo-se necessário a utilização de senhas e soluções de autenticação robustas (HUREL; LOBATO, 2018).

Para assegurar que os dados estejam protegidos do acesso indevido de terceiros, algumas das principais medidas de segurança adotadas pelos provedores de serviços que utiliza a computação na nuvem são: o estabelecimento de padrões de criptografia de dados, segurança local e proteção dos *hardwares* onde os dados são armazenados, *firewalls*, aplicação e manipulação de cópias de segurança dos dados (HUREL; LOBATO, 2018).

2.4 PRIVACIDADE

Segundo Arruda (2019), os Princípios de Privacidade Geralmente Aceitos (GAAP), definem a privacidade como: "Os direitos e obrigações de indivíduos e organizações em relação à coleta, uso, retenção, divulgação e descarte de informações pessoais". O termo "informação pessoal" refere-se a qualquer tipo de informação que possa ser vinculada a alguém ou identificar um indivíduo, diretamente ou indiretamente. Alguns exemplos desses atributos são: nome, sobrenome, endereço, características físicas, entre outros.

Contudo, algumas informações são caracterizadas como confidenciais, exigindo uma proteção mais refinada, como por exemplo: antes da coleta de informações acontecer, deve-se pedir explicitamente a permissão e o consentimento das pessoas para o uso e a coleta desse tipo de dados. Alguns exemplos de informações pessoais confidenciais são: condições médicas, localização, orientação sexual, religião entre outras (ARRUDA, 2019).

Em casos de informações pessoais que necessitam ser anunciadas ao público, todos os dados secundários que podem ser utilizados para identificar o indivíduo devem ser anonimizados, de modo que a identidade do indivíduo não poderá ser determinada a partir dessas informações divulgadas (ARRUDA, 2019).

Segundo Balaguer (2015), com a vasta possibilidade de haver conexão com a *internet* em qualquer ambiente existente, é esperado um aumento significativo nas possibilidade de comunicação, interação ou serviços disponibilizados pela *web*, contudo assim como o número dessa conectividade cresce exponencialmente, o mesmo acontece com as vulnerabilidades e falhas de segurança, deixando as condições visivelmente mais propensas a ataques *hackers* nos ambientes de IoT.

2.5 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Segundo Sena (2021), as discussões sobre políticas de privacidade, segurança e o uso e processamento de dados pessoais não é de hoje, embora este tema já esteja sendo abordado no Marco Civil da *Internet*, torna-se necessário a adaptação e o aprofundamento das normas para um cenário mais amplo.

Pensando nisso, em 2018 foi criada a Lei Geral de Proteção de Dados Pessoais (LGPD), que foi inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR), considerada

referência quando se trata sobre o assunto. Depois de diversas prorrogações para o início de sua vigência, a LGPD entrou em vigor e passou a valer a partir de setembro de 2020. A partir desse momento, ela trouxe a obrigatoriedade de organizações adaptarem suas práticas sob o risco de altíssimas multas, chegando até 50 milhões de reais, mostrando assim a importância que suas diretrizes impõem sobre as empresas.

A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade das pessoas. Com a padronização de regulamentos e práticas para promover a proteção de dados pessoais de todos os cidadãos que estejam no Brasil, consequentemente é criado um cenário de segurança jurídica, de acordo com os parâmetros internacionais existentes (BRASIL, [2019]).

A lei também define o que são dados pessoais e explica que algumas informações necessitam de cuidados mais específicos, como dados pessoais sensíveis ou sobre crianças e adolescentes. Além disso, todos os dados que são processados, por meio físico ou digital estão sujeitos a regulação, ela também estabelece que não importa se a sede de uma organização ou seus *data centers* estão localizados no Brasil ou no exterior: se ocorrer o processamento de informações sobre pessoas, brasileiras ou não, dentro do país, a LGPD deve ser aplicada (BRASIL, 2022).

2.6 RISCOS INERENTES AOS ROTEADORES COMO PONTO DE CONEXÃO DE DISPOSITIVOS IOT NAS CASAS

Os roteadores são um dos pontos mais importantes quando falamos sobre proteção frente a ataques cibernéticos, já que ele é o responsável por receber os dados da maioria dos dispositivos que fazem parte da rede (GONÇALVES, 2020).

Ao conseguir invadir um roteador, a pessoa pode ter acesso aos dispositivos que estão conectados à rede, incluindo os dispositivos IoT. Por ser usado como centro de conectividade, qualquer tipo de falha pode permitir invasões aos dispositivos que estiverem conectados a ele (GONÇALVES, 2020).

Ao assumir o controle do roteador, cibercriminosos podem tomar uma série de ações, entre elas está a de conseguir o controle dos dispositivos conectados à rede e enviar comandos a eles, pode-se também usar para ataques DDoS. Ou seja, os dados que os dispositivos coletam como por exemplo imagem de câmeras de segurança podem acabar sendo acessados por terceiros (GONÇALVES, 2020).

Em 2018 ocorreu um ataque utilizando as vulnerabilidades dos roteadores, *hackers* conseguiram infectar 500 mil roteadores em todo o mundo e foram capazes coletaram informações, realizaram ataques a sites e inutilizaram aparelhos conectados através de utilização de *malwares* (GONÇALVES, 2020).

3 METODOLOGIA

Para alcançar os objetivos retratados na *Seção 1*, foram realizados estudos em artigos, sites e livros, visando a compreensão dos principais aspectos relacionados à segurança e privacidade na internet das coisas. Os resultados desses estudos foram exibidos na *Seção 2*.

Em seguida, utilizando a ferramenta Google Forms, foi elaborada uma pesquisa de campo quantitativa, onde o objetivo era identificar se as pessoas reconheciam a importância das medidas de segurança, e se possuíam o conhecimento necessário para realizá-las.

O formulário para a coleta dos dados foi divulgado por meios digitais através de um link, teve sua data de início no dia 3 de maio de 2022 e foi encerrado no dia 13 de maio, totalizando 10 (dez) dias de pesquisa de campo, retornando 232 (duzentas e trinta e duas) respostas.

A pesquisa não possui público alvo específico definido, é composta por diversos perfis diferentes, entretanto, foi respondida principalmente por alunos da Faculdade de Tecnologia Prof. José Camargo (Fatec Jales), habitantes das cidades de Jales, Santa Rita D'Oeste e região.

Após a aplicação do formulário, os dados foram apurados e organizados em uma planilha, gerando gráficos que possibilitam o fácil entendimento e uma análise crítica, conforme apresentado na *Seção 4*.

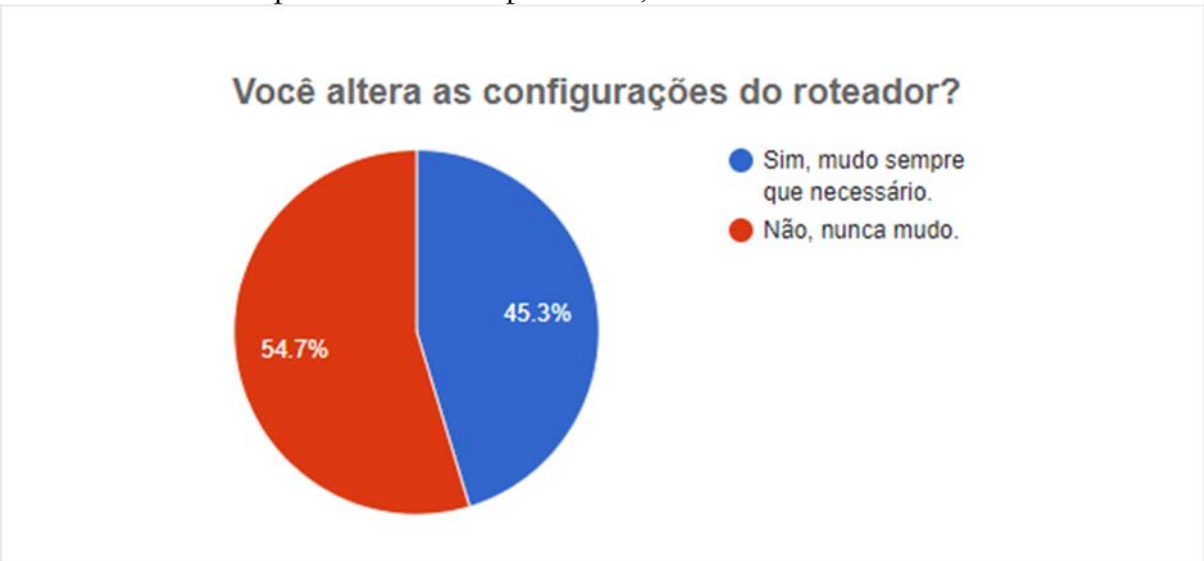
4 ANÁLISE E DISCUSSÃO DOS RESULTADOS

Nesta seção serão analisados os dados que foram coletados na pesquisa quantitativa citada na seção 3, onde foi possível colher informações sobre o comportamento das pessoas em relação às medidas de segurança que são tomadas e se elas julgam necessárias para manter os seus dispositivos protegidos.

Na pesquisa realizada, foram definidos níveis de conhecimento, onde os participantes seriam capazes de definir em qual nível os mesmos se encontram. Os níveis de conhecimento variam entre as pessoas que não sabem nada sobre tecnologia, até as que se declaram especialistas no assunto.

No Gráfico 1, é possível observar que 54,7% das pessoas que se declararam especialistas ou que sabem bastante e trabalham na área e nunca alteram as configurações de segurança do roteador, deixando assim, seus dispositivos vulneráveis.

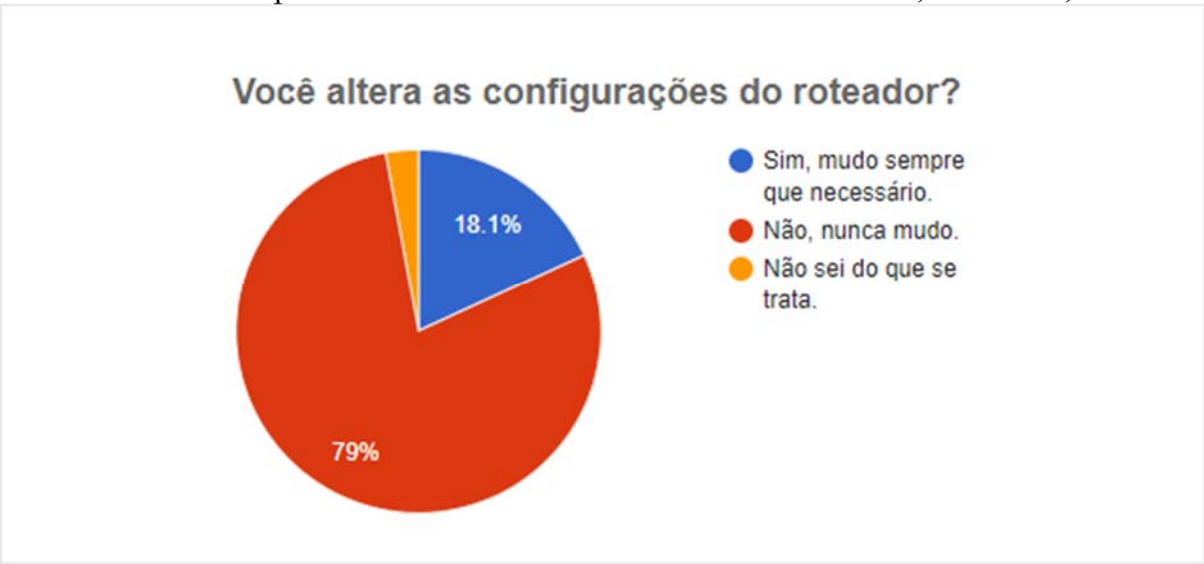
Gráfico 1 – Pessoas que se declaram especialistas, sabem bastante e trabalham na área



Fonte: Elaborado pelos autores.

No Gráfico 2, nota-se que o número de pessoas que nunca alteram as configurações do roteador é ainda maior, chegando a 79% das pessoas que sabem razoavelmente e utilizam bem os dispositivos.

Gráfico 2 – Pessoas que sabem razoavelmente e utilizam bem celulares, notebooks, etc.

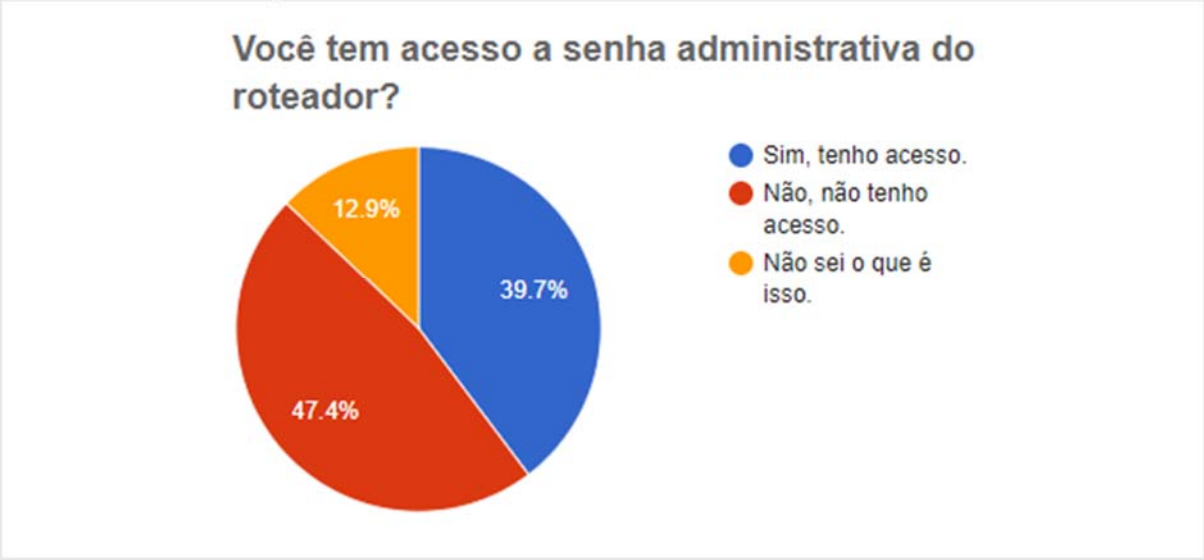


Fonte: Elaborado pelos autores.

Uma das causas que podem justificar a falta de cuidado das pessoas que não modificam as configurações, está no fato de que grande parte da população não tem acesso a senha administrativa do roteador. Ao fazer a instalação e configuração dos dispositivos, muitos provedores de *internet* não fornecem a senha de acesso para administrar o roteador.

No Gráfico 3, podemos observar que 47,4% das pessoas que participaram da pesquisa não possuem acesso a esta senha.

Gráfico 3 – Pessoas que têm acesso a senha administrativa do roteador

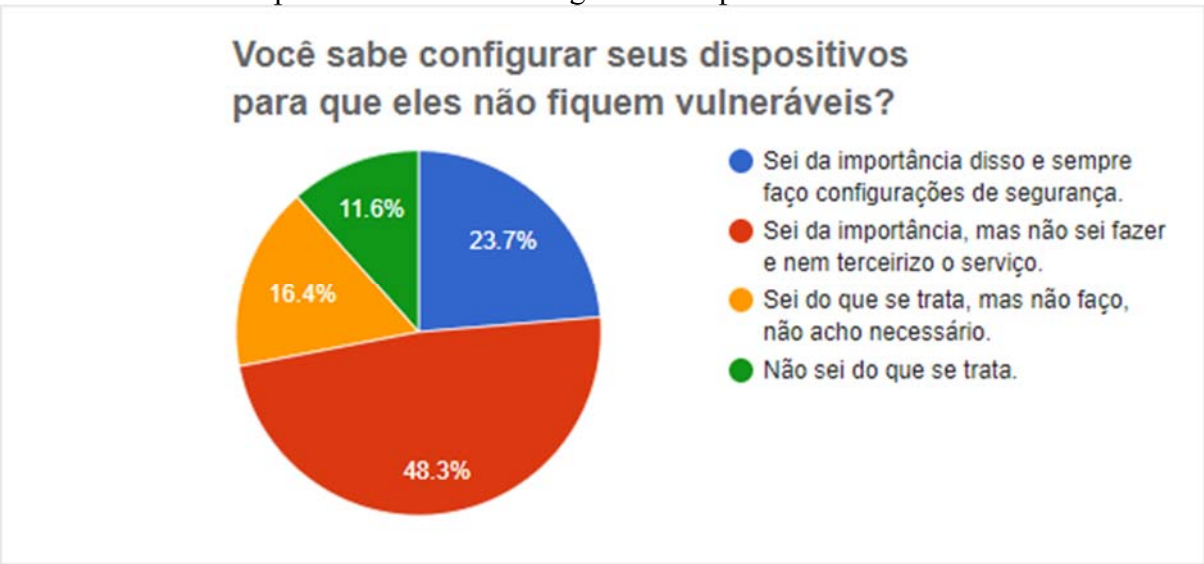


Fonte: Elaborado pelos autores.

Exposto os dados citados acima, leva-se a outro problema de segurança, onde as pessoas acabam ficando vulneráveis pelo fato de que somente os funcionários da empresa provedora de *internet* possuem o acesso à senha para administrar o roteador. Também há os consumidores que compram o roteador por conta própria e não tem ao menos o cuidado de alterar a senha padrão que o dispositivo traz de fábrica, o que permite muitas vezes a utilização dessa informação por pessoas e funcionários mal-intencionados, podendo agir de forma criminosa ou fornecendo dados a terceiros.

Existe também, as pessoas que não alteram as configurações porque não sabem como fazer isso. No Gráfico 4, percebe-se que 48,3% das pessoas que participaram da pesquisa sabem da importância, mas não sabem como realizar as configurações necessárias. Também é possível notar que 11,6% não fazem ideia do que se trata o assunto. Espanta-se que 16,4% das pessoas não fazem as configurações de segurança porque não acham necessário.

Gráfico 4 – Pessoas que sabem ou não configurar os dispositivos



Fonte: Elaborado pelos autores.

Tendo em vista os dados apresentados acima, podemos concluir que atualmente há uma grande falta de conscientização das pessoas sobre os perigos existentes. Deve-se discutir mais sobre a importância da segurança digital e em como manter-se prevenido, evitando vulnerabilidades e possíveis ataques.

No Gráfico 5, podemos analisar que 80,6% das pessoas que participaram da pesquisa não sabem para onde são enviados os dados coletados pelos dispositivos. Repara-se que 15,5% nem sabiam que seus dados eram coletados e 7,3% não sabiam do que se tratava. Demonstrando a grande falta de informação das pessoas sobre a privacidade dos dados.

Gráfico 5 – Pessoas que sabem para onde os dados coletados são enviados

Fonte: Elaborado pelos autores.

Atualmente, já existem estudos que demonstram os perigos desta coleta massiva de dados através dos dispositivos de IoT, já que geralmente não são divulgadas as informações sobre como os dados são utilizados. Segundo Ren et al. (2019), as informações geradas e compartilhadas com seu destino de tráfego IP podem ser observadas por quem monitora passivamente o tráfego de rede.

5 CONSIDERAÇÕES FINAIS

Os grandes problemas que circundam a *internet* todos os dias não são de hoje. A partir do momento que surge uma nova tecnologia para ajudar e facilitar a vida das pessoas, novos problemas acabam surgindo juntamente a ela, permitindo assim, que novas oportunidades sejam criadas para as pessoas mal intencionadas.

Não é diferente quando se trata da Internet das Coisas ou IoT. Essa tecnologia vem trazendo inúmeras vantagens às vidas das pessoas, tornando o que antes eram dispositivos normais e com uma simples função de uso, em dispositivos "inteligentes" capazes de monitorar e realizar ações para quem os usa. Dados pesquisados mostram que o crescimento de dispositivos inteligentes vem crescendo em proporções impressionantes, mostrando sua força e ganhando cada vez mais espaço na vida das pessoas.

Uma preocupação recorrente do assunto é quem possui o acesso às informações coletadas de seus usuários, já que de acordo com estudos realizados, grande parte desses dados coletados são enviados a terceiros. Pensando nisso, com o propósito de proteger os dados pessoais, o Brasil criou a Lei Geral de Proteção de Dados, estabelecendo algumas regras e diretrizes que devem ser estritamente seguidas pelas empresas.

Sem dúvidas a IoT tem grande potencial e atualmente já faz parte da vida das pessoas, porém as empresas que a desenvolvem em seus dispositivos não vêm acompanhando um dos aspectos mais importantes em relação a ela, que é a segurança e a privacidade dos dados. É certo que, com crescimento e popularização da IoT, grandes desafios foram propostos para as empresas e seus desenvolvedores. Existem diversas barreiras nos recursos computacionais para os *hardwares* de IoT, uma delas é a grande limitação física dos dispositivos, que muitas vezes são projetados para serem compactos e com pouco espaço para a implementação de sistemas de segurança.

Casas com recursos de IoT e dispositivos inteligentes podem ser facilmente invadidas a partir dos dados que são coletados. Câmeras de segurança, DVR's e alarmes podem ser desativados através da rede Wi-Fi. Considerando os roteadores como porta de entrada, nota-se a sua extrema importância, visto que, através deles ocorrem-se os ataques, roubos, exposição da privacidade, invasões, cibercrimes e dependendo a situação, até atentados contra a vida.

Dado os fatos demonstrados, no contexto atual, as pessoas acabam não dando o valor apropriado às medidas de segurança necessárias para que seus dispositivos conectados à *internet* estejam minimamente protegidos dentro de suas redes. Segundo a pesquisa exposta, mais da metade das pessoas que trabalham na área de tecnologia, ou se declaram especialistas no assunto responderam que nunca mudam as configurações do roteador.

Em vista dos argumentos apresentados, pode-se concluir que há uma falta de conscientização das pessoas para com a segurança digital, visto que mesmo sabendo da importância e dos grandes perigos existentes, não realizam os procedimentos adequados, deixando assim, todos os dispositivos vulneráveis a ciberataques e a invasões de privacidade, consequentemente expondo a segurança de todas as pessoas que convivem neste ambiente.

Além disso, os fornecedores desses dispositivos não desenvolvem mecanismos para tornar esses dispositivos seguros, sendo isso um dos maiores problemas atualmente da IoT fazendo com que o crescimento dessa tecnologia possa causar grandes riscos quanto à privacidade e segurança digital.

REFERÊNCIAS

ACOHIDO, B. **Ataques a dispositivos inteligentes IoT registram alta com a Covid-19**. 2021. Disponível em: https://blog.avast.com/pt-br/iot-attacks-intensified-by-covid-19-avast. Acesso em: 7 nov. 2021.

ARRUDA, M. **Um modelo ontológico e um serviço de gerenciamento de dados de apoio à privacidade na Internet das Coisas**. 2019. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Goiás, Goiânia, 2019. Disponível em: https://repositorio.bc.ufg.br/tede/bitstream/tede/9323/5/Disserta%C3%A7%C3%A3o%20-%20Mayke%20Ferreira%20Arruda%20-%202019.pdf. Acesso em: 29 mar. 2022.

ASTHON, K. **That 'Internet of Things' thing**. 2009. Disponível em: https://www.rfidjournal.com/articles/view?4986. Acesso em: 7 dez. 2021.

BALAGUER, A. **Segurança da informação no mundo da internet das coisas**. 2015. Disponível em: https://computerworld.com.br/2015/02/25/seguranca-da-informacao-no-mundo-dainternet-das-coisas. Acesso em: 29 mar. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei geral de Proteção de Dados Pessoais LGPD. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 out. 2019.

BRASIL. Ministério Público Federal – MPF. **Lei geral de proteção de dados**: o que é a LGPD?. Disponível em: http://www.mpf.mp.br/servicos/lgpd/o-que-e-a-lgpd. Acesso em: 23 mar. 2022.

CHICARINO, V. R. L. *et al*. Uso de Blockchain para privacidade e segurança em internet das coisas. *In*: SOCIEDADE BRASILEIRA DE COMPUTAÇÃO – SBC. **Minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – SBSeg**. Porto Alegre: SBC, 2017. Disponível em: https://www.researchgate.net/publication/321966650_Uso_de_Blockchain_para_Privacidade_e_Seguranca_em_Internet_das_Coisas. Acesso em: 23 fev. 2022.

CISO ADVISOR. **Nova botnet usa dispositivos de IoT para ataques DDoS**. 2020. Disponível em: https://www.cisoadvisor.com.br/nova-botnet-usa-dispositivos-de-iot-para-ataques-ddos/. Aceso em: 7 nov. 2021.

ECLIPSE FOUNDATION. **IoT commercial adoption survey 2019 results**. 2020. Disponível em: https://outreach.eclipse.foundation/iot-adoption-2019. Acesso em: 11 out. 2021.

ELLEN, P. **Internet das coisas já é realidade, porém falta regulamentá-la**. 2016. Disponível em: https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/internet-das-coisas-ja-e-realidade-porem-falta-regulamenta-la. Acesso em: 14 dez. 2021.

EL-SHWEKY, B. E. *et al*. Internet of Things: a comparative study. *In*: ANNUAL COMPUTING AND COMMUNICATION WORKSHOP AND CONFERENCE – CCWC, 8., 2018, Las Vegas. **Proceddings** [...]. Las Vegas, 2018. p. 622-631. Disponível em: https://ieeexplore.ieee.org/abstract/document/ 8301678. Acesso em: 25 fev. 2022.

FIGUEIRA, V. P. **Internet das Coisas**: um estudo sobre questões de segurança, privacidade e infraestrutura. 2016. Trabalho de Conclusão de Curso (Tecnólogo em Sistemas de Computação) – Universidade Federal Fluminense, Niterói, 2016. Disponível em: https://app.uff.br/riuff/bitstream/handle/1/5150/TCC_VITOR_PINHEIRO_FIGUEIRA_FINAL%20%281%29.pdf?sequence=1&isAllowed=y. Acesso em: 20 nov. 2021.

FISHER, S. **Riscos de segurança da Internet das Coisas**. 2019. Disponível em: https://www.avast.com/pt-br/c-iot-security-risks. Acesso em: 20 out. 2021.

GOMES, R. D. P. **Big data**: desafios à tutela da pessoa humana na sociedade da informação. 2. ed. Rio de Janeiro: lumen Juuris, 2019.

GONÇALVES, A. L. D. **Ataques a roteadores domésticos**: saiba como se proteger. 2020. Disponível em: https://blog.avast.com/pt-br/ataques-a-roteadores-domesticos-saiba-como-se-proteger. Acesso em: 15 mar. 2022.

HÖLLER, J. *et al*. Introduction and book structure. *In*: HÖLLER, J. *et al*. (org.). **From Machine-To-Machine to the Internet of Things**. Oxford: Elsevier, 2014. p. 3-8. Disponível em: https://www.sciencedirect.com/science/article/pii/B9780124076846000012?via%3Dihub. Acesso em: 8 dez. 2021.

HUREL, L. M.; LOBATO, L. C. Segurança e privacidade para a Internet das Coisas. **Nota estratégica**, Rio de Janeiro, n. 31, 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/11/Seguranc%CC%A7a-e-Privacidade-para-a-Internet-das-Coisas.pdf. Acesso em: 11 maio 2022.

IDC. **IoT growth demands rethink of long-term storage strategies, says IDC**. 2020. Disponível em: https://www.idc.com/getdoc.jsp?containerId=prAP46737220. Acesso em: 7 dez. 2021.

IPV6.BR. **Endereçamento**. 2012a. Disponível em: https://ipv6.br/post/enderecamento/. Acesso em: 6 dez. 2021.

IPV6.BR. **Introdução**. 2012b. Disponível em: https://ipv6.br/post/introducao/. Acesso em: 6 dez. 2021.

KALITA, H. K.; KAR, A. Wireless sensor network security analysis‖. **International Journal of Next-Generation Networks**, v. 1, n. 1, p. 87-115, 2009. Disponível em: https://airccse.org/journal/jcsit/1.pdf. Acesso em: 28 jan. 2022.

LEE, K. **Inteligência artificial**: como os robôs estão mudando o mundo, a forma como amamos, nos relacionamentos, trabalhamos e vivemos. Rio de Janeiro: Globo, 2019.

MAYMI, F.; HARRIS, S. **Cissp all-in-one exam guide**. 9. ed. Nova York: McGraw Hill, 2021.

MOCRII, D.; CHENB, Y.; MUSILEK, P. **IoT-based smart homes**: a review of system architecture, software, communications, privacy and security. 2018. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2542660518300477. Acesso em: 30 jan. 2022.

NEWMAN, P. **The internet of things 2020**: here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue. 2020. Disponivel em: https://www.businessinsider.com/internet-of-things-report?IR=T. Acesso em: 28 set. 2021.

ORACLE. **O que é Internet of Things IoT?** 2021. Disponível em: https://www.oracle.com/br/ internet-of-things/what-is-iot/. Acesso em: 5 dez. 2021.

REN, J. *et al*. Information exposure from consumer IoT devices: a multidimensional, network-informed measurement approach. *In*: INTERNET MEASUREMENT CONFERENCE, 19., 2019, Amsterdan. **Proceedings** [...]. New York: ACM, 2019. p. 267-279. Disponível em: https://moniotrlab.ccis.neu.edu/wp-content/uploads/2019/09/ren-imc19.pdf. Acesso em: 20 jan. 2022.

SANTOS, B. P. *et al*. **Internet das coisas**: da teoria à prática. 2016. Disponível em: https://homepages.dcc.ufmg.br/~mmvieira/cc/papers/internet-das-coisas.pdf. Acesso em: 8 dez. 2021.

SENA, M. **LGPD e TI**: o guia completo para implementar as regras da nova lei. 2021. Disponível em: https://blog.impulso.network/lgpd-e-ti-o-guia-completo-para-implementar-as-regras-da-nova-lei/#o-que-e-a-lgpd. Acesso em: 23 mar. 2022.

SHATILIN, I. **Rede 5G**: por que precisamos dela? 2015. Disponível em: https://www.kaspersky.com.br/blog/rede-5g-por-que-precisamos-dela/5322/. Acesso em: 11 fev. 2022.

TACHIBANA, F. M. O. **Implementação em hardware e sistemas embarcados de algoritmos de criptografia leve para aplicação em IoT**. 2017. Disponível em: https://aberto.univem.edu.br/handle/11077/1649. Acesso em: 8 dez. 2021.

WU, M. *et al*. Research on the architecture of Internet of Things. *In*: INTERNATIONAL CONFERENCE ON ADVANCED COMPUTER THEORY AND ENGINEERING – ICACTE, 3., 2010, Chengdu. **Proceedings** […]. Chengdu, 2010. p. V5-484-V5-487. Disponível em: https://ieeexplore.ieee.org/document/5579493. Acesso em: 23 dez. 2021.