INTERFACE TECNOLÓGICA

SEGURANÇA E PRIVACIDADE NO CONTEXTO DA INTERNET DAS COISAS

SECURITY AND PRIVACY IN THE CONTEXT OF THE INTERNET OF THINGS

Leandro Augusto Oliveira – lehzera.oli@outlook.com
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

André Castro Rizo – andre.rizo@fatectq.edu.br
Faculdade de Tecnologia de Taquaritinga (Fatec) – Taquaritinga – SP – Brasil

DOI: 10.31510/infa.v19i2.1507
Data de submissão: 01/09/2022
Data do aceite: 28/11/2022
Data da publicação: 20/12/2022

RESUMO

A Internet das Coisas ou *Internet of Things* (loT) é uma ferramenta que utiliza a tecnologia para conectar dispositivos eletrônicos a internet, e assim, possibilitar o alcance de várias funcionalidades nos mais diversos setores da indústria, do varejo, do agronegócio, etc. Entre os principais benefícios da loT estão o aumento de eficiência e produtividade, proporcionadas pela automoção de operações e tarefas. No entanto, Internet das coisas ainda pode apresentar alguns desafios, por exemplo, a segurança e privacidade dos dados e outras informações que são gerados de forma demasiada pelos dispositivos loT. Nesta perspectiva o objetivo do trabalho é demonstrar através de um levantamento bibliográfico a importância e os riscos relacionados à segurança e privacidade na loT. Foram apresentadas algumas alternativas, como a criptografia utilizada pelos *blockchains* e alguns modelos de autenticação e autorização de usuário ou dispositivo que se conectam a internet. É possível concluir que mesmo que existam ferramentas de proteção e segurança de dados, os estudos a cerca desse tema devem avançar, tendo em vista que novas vulnerabilidades podem surgir a todo instante.

Palavras-chave: Segurança da Informação. Privacidade de Dados. Internet das Coisas.

ABSTRACT

The Internet of Things (loT) is a tool that uses technology to connect electronic devices to the internet, and thus, enable the reach of various functionality in the most diverse sectors of industry, retail, agribusiness, etc. Among the main benefits of loT are the increase in efficiency and productivity, provided by the automation of operations and tasks. However, Internet of Things can still present some challenges, for example the security and privacy of data and other information that is generated way too much by loT devices. In this perspective, the objective of the work is to demonstrate through a bibliographic survey the importance and risks related to security and privacy in the loT. Some alternatives were presented, such as the encryption used by blockchains and some models of authentication and authorization of users or devices that connect to the internet. It is possible to conclude that even if there are data protection and security tools, studies on this topic must advance, given that new vulnerabilities can arise at any time.

INTERFACE TECNOLÓGICA

Keywords: Information Security. Data Privacy. Internet of Things.

1 INTRODUÇÃO

A Internet das Coisas ou *Internet of Things* (loT) é descrita como uma ferramenta que possibilita uma maior capacidade computacional e de comunicação aos objetos do cotidiano, quando estes realizam conexão com a internet (SANTOS, 2016). Para Vermesan (2014), não se trata apenas de uma nova tecnologia, e sim de um novo limiar para a internet, que é reflexo dos avanços tecnológicos alcançados no decorrer dos anos. Corroborando com essa ideia, Faccioni Filho (2016a), aponta que a IoT está fora do contexto das tecnologias, pois não provém delas, apenas faz uso dessas tecnologias para alcançar as suas funcionalidades.

A IoT abre inúmeras possibilidades em diferentes setores, como na indústria, no varejo e no agronegócio, entre os benefícios estão o aumento de eficiência e produtividade, tendo em vista que dispositivos e *softwares* baseados em loT reduzem erros na execução de operações e tarefas, melhorando a qualidade em um menor tempo, reduzindo assim os custos, pois o uso do sistema de automação elimina a necessidade de pessoal para realizar tarefas no local (ALBERTIN *et al*, 2017).

Segundo o levantamento de Pessoa *et al.* (2016), a loT também pode apresentar alguns desafios a serem superados, como armazenamento de dados, segurança das informações, entre outros. Conforme Santos (2016), assim como qualquer tecnologia, as novas habilidades da loT geram um grande número de oportunidades, no entanto, também apresentam riscos e acarretam desafios técnicos e sociais, especialmente na segurança dos sistemas de loT em relação ao destino e administração da massiva quantidade de dados coletados pelos dispositivos.

Tendo em vista a problemática, o objetivo do presente trabalho é demonstrar através de uma revisão bibliográfica as implicações a cerca da segurança e privacidade no contexto da internet das coisas, assim como as suas características e riscos, e como superá-los.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Definindo a Internet das Coisas

O termo Internet das Coisas, de acordo com Zambarda (2014), refere-se à revolução tecnológica que conecta dispositivos à internet, como por exemplo, eletrodomésticos, veículos, roupas, entre outros. Corroborando, Cavalli (2016), discute que a loT é um conjunto de tecnologias e protocolos, que associados possibilitam que objetos (ou "coisas") se conectem a rede. Enquanto para Faccioni Filho (2016a), a loT é um conceito que vai além do âmbito técnico, pois não é derivado de tecnologias, mas sim, as utiliza para alcançar uma gama de funções.

Para Minerva *et al.* (2015, p. 74) se trata de uma rede complexa, adaptável e autoconfigurável que interliga objetos físicos ou virtuais à internet através de protocolos de comunicação padronizados. Como resultado, os objetos tendem a controlar uma série de ações cotidianas, com ou sem intervenção humana, e podem ser realizadas com segurança a qualquer hora, em qualquer lugar (SANTAELLA *et al.*, 2018).

Segundo Magrani (2018) a loT ainda não possui uma definição unânime estabelecida, de forma geral, se trata de um ecossistema de comunicação que processa informações e dados com a finalidade de facilitar de alguma maneira o cotidiano da população.

2.2 Contexto histórico da Internet das coisas

Muito tem se falado sobre a loT nos dias atuais, no entanto essa expressão foi utilizada pela primeira vez em 1999 pelo pesquisador Kevin Ashton, naquele período ele discutia sobre o fato de que existem “coisas” que computadores são capazes de efetuar com maiores aptidões do que os humanos (ASHTON, 2009). Segundo Minerva *et al.* (2015), a loT teve seu fundamento antes mesmo da internet, logo que surgiu a tecnologia RFID - *Radio Frequency Identification*, durante a Segunda Guerra Mundial, com a finalidade de averiguar os aviões captados pelos radares, ou seja, o sinal captado deveria refletir características de um sistema passivo (amigo), ou emitir um novo sinal, considerado um sistema ativo (inimigo).

Os avanços da tecnologia RFID continuaram após o período de guerra e seguiram para o rumo comercial, a RFID passou a ser usada em etiquetas de roupas para evitar roubos em lojas, de forma que a etiqueta responde a um sinal de determinada frequência, sendo possível a

sua identificação pelo caixa, se isso não ocorrer o cliente ao sair com passar pela porta com a vestimenta, o alarme antirroubo é acionado (MINERVA *et al.*, 2015).

Em 2003 os professores David Brock e Sanjay Sarma usaram o mesmo sistema de etiquetas de RFID, porém com microchips de baixo custo, denominados de "*tags*" sua finalidade era identificar e movimentar as cargas de produtos em tempo real e online. Essa inovação incentivou grandes empresas e departamentos governamentais americanos custarem as pesquisas acerca do RFID e conexões com a internet, posteriormente essa movimentação viriam a ser denominadas "internet das coisas" (FACCIONI FILHO, 2016a).

O cenário da IoT se consolidou em 2008, após a primeira Conferência Internacional sobre o tema em Zurich na Suíça (FACCIONI FILHO, 2016b). Já em 2010, o número de objetos conectados à internet por meio de smartphones e tablets avançou exponencialmente, os cálculos do Cisco IBSG apontavam para 12,5 bilhões de dispositivos conectados, sendo que a população não passava de 6,8 bilhões de pessoas (EVANS, 2011, p. 3).

Nesse contexto, Carvalho (2020) aponta que atualmente a IoT traz grandes facilidades para todos, uma vez que essas ferramentas tecnológicas estão contribuindo para a transformação digital do cotidiano das pessoas e nos campos profissionais. As casas já contam com Smart TV, termostatos, geladeiras e fechaduras inteligentes. Na área da saúde, a IoT traz benefícios ao integrar o prontuário do paciente, mostrando o seu estado clínico. Enquanto na agricultura, ramo que não para de crescer, já se usam sensores para o monitoramento de aspectos como temperatura, umidade do solo e do ar (CARVALHO, 2020).

Os setores industriais também estão passando por uma transformação digital com a chegada da Quarta Revolução Industrial ou Indústria 4.0, caracterizada pela integração entre meios físicos e digitais, fazendo o uso da inteligência artificial, robôs de automação, sensores e loT (OZTEMEL e GURSEV, 2020). Com a interação entre maquina, por exemplo, é possível identificar e solucionar problemas sem a ação humana (COLOMBO e LUCCA FILHO, 2018).

2.4 Segurança e privacidade de dados

Segurança e privacidade são conceitos-chave de fundamental relevância para a loT, os termos são frequentemente usados como sinônimos, mas possuem significados diferentes. Segundo Whitman e Mattord (2015) a segurança se preocupa em manter três pilares relacionados às propriedades da informação: Confidencialidade, Integridade e Disponibilidade, e explicaram: (a) Disponibilidade - as informações pessoais devem estar à disposição apenas

quando necessário, podendo ser desabilitadas por meio de chaves de acesso (por exemplo, contas de e-mail, banco de dados, áreas específicas da empresa, etc.); (b) Integridade - todas as informações devem ser mantidas intactas sem qualquer alteração; (c) Confidencialidade - Somente os órgãos responsáveis podem ter acesso às informações.

Por outro lado, a privacidade está mais relacionada à particularidade de cada indivíduo e depende da realização de aspectos técnicos e princípios de segurança de cada sistema (SAKAMOTO, 2020). De acordo com PANEK (2019), a privacidade garante que: (a) Os dados só possam ser controlados pelo respectivo usuário; (b) Nenhum outro usuário pode acessar ou processar os dados; (c) Os usuários só podem exercer controle com base nos dados que recebem; não podendo inferir outras informações.

Segundo Alves *et al*. (2021) os dados podem ser coletados muitas vezes sem consentimento dos usuários, tomando como exemplo a Smart TV, assim que o usuário aceita os termos de política e privacidade do fabricante ele fica suscetível ao riscos. Por exemplo: (a) Informações como CEP – fornece a localização geográfica; (b) Coleta de *likes* e conteúdos procurados – possibilita que outros fornecedores façam ligações para venda ou mandem e-mail falsos; (c) Coleta de endereço IP, informações armazenadas em *cookies*, informações que identificam *hardware* ou *software* do navegador e das páginas acessadas – aumenta a suscetibilidade a ataques por interceptação; (d) Informações para autenticar o dispositivo - identifica o nome de usuário que pode ser usado para outras finalidades.

2.5 Normas de proteção privacidade e dados pessoais

Para garantir a privacidade, o Brasil apresenta algumas regulamentações. A própria Constituição Federal (CF) de 1988 estabelece em seu art. 5°, inciso X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando-se à reparação do dano material ou moral causado por violação” (BRASIL, 1988).

O Código Civil Brasileiro no Capítulo II no art. 20°, discute "A pedido do indivíduo, pode ser proibida a divulgação de palavras, publicação ou uso de imagens pessoais" e no art. 21 "A vida privada da pessoa física é inviolável e, a pedido do interessado, tomará medidas para evitar o contrário" (BRASIL, 2002).

No Marco Civil da Internet, a privacidade é abordada no art. 7° “Inviolabilidade das intimidades requer compensação por danos materiais ou morais"; “A coleta, armazenamento e processamento de dados, só podem ser utilizados para fins justificáveis”; “os dados pessoais

dever ser apagados ao final da relação entre as partes, salvo se a manutenção de registros for obrigada por lei". No art. 10° "A disponibilização dos dados pessoais e do conteúdo das comunicações privadas deve atender à proteção da intimidade" e no art. 11º "Em qualquer operação de coleta e armazenamento de dados deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade" (BRASIL, 2016).

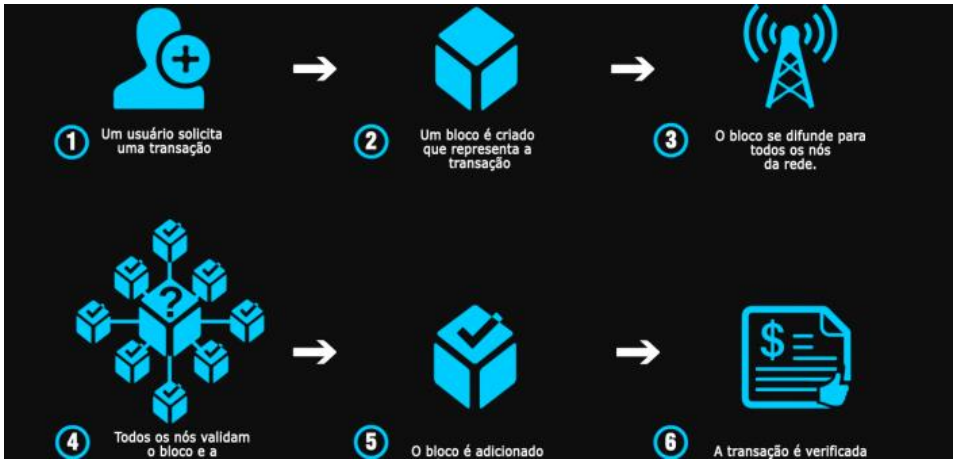
Outras disposições legais também estão relacionadas à privacidade, incluindo A Lei Geral de Proteção de Dados Pessoais que surgiu para proteger a liberdade e a privacidade (BRASIL, 2018). O Habeas Data (lei nº 9.507/1997) registra em seu art. 2º o direito de acesso a informações de registros ou bancos de dados governamentais ou público (BRASIL, 1997a), e pela Lei Geral de Telecomunicações (lei nº 9.472/1997), que são discutidas em seu art. 3º a inviolabilidade e confidencialidade das comunicações (BRASIL, 1997b), e o Código de Defesa do Consumidor (lei nº 8.078/1990), quanto ao seu art. 43º sobre as informações e dados pessoais em bancos de dados e cadastros de consumidores (BRASIL, 1990).

2.6 Uso de Blockchain em Internet das Coisas

Blockchain ou cadeia de bloco é a estrutura de banco de dados ou livro razão (Figura 1), essa tecnologia está por trás da criptomoeda Bitcoin (NAKAMOTO, 2017). Segundo Carvalho *et al*. (2021) a criptomoeda é uma forma de pagamento que usa blockchain para proteger os dados transmitidos e armazenados. Além da criptomoeda, blockchain pode ser usada em diferentes campos, fornecendo suporte confiável e seguro para realizar transações entre participantes descentralizados em uma rede peer-to-peer – P2P[1]) (NAKAMOTO, 2017). A palavra "bloco" significa informação digital, e podem ser divididas em três partes: (a) Blocos que armazenam informações da transação de dados; (b) Blocos que armazenam informações sobre os usuários que participaram das transações e (c) Blocos que armazenam informações que os diferenciam dos demais blocos (CAMARA, 2021, p. 93-112).

[1] Peer-to-peer, traduzido para o português, significa ponto a ponto. Na computação, o termo se refere a uma arquitetura de rede de computadores onde cada participante (peer) também é um servidor que auxilia no funcionamento do sistema.

Figura 1. Funcionamento da *Blockchain*



Fonte: https://101blockchains.com/pt/tecnologia-blockchain-guia/

Quando um bloco é finalizado e adicionado à cadeia de *blockchain*, é praticamente impossível alterar ou excluir as informações aplicadas (FROGERI, 2022). Segundo Chicarino (2017), o *blockchain* se mostra como uma tecnologia de natureza descentralizada, descartando a necessidade de confiança em terceiros, além de não apresentar um ponto único de falha.

3 PROCEDIMENTOS METODOLÓGICOS

O presente trabalho é uma revisão bibliográfica e documental descritiva de abordagem qualitativa. Para a pesquisa foram considerados livros, artigos científicos, teses e dissertações que abordassem o que é Internet das Coisas e o que ela representa para a população, assim como as adversidades que a loT apresenta no quesito segurança e privacidade que é o foco deste estudo.

4 RESULTADOS E DISCUSSÃO

A Internet das Coisas como já descrito, compartilham algumas informações por meio de dispositivos, gerando preocupações e discussões sobre segurança e privacidade. Lucro (2016) aponta que quanto mais dados coletados ou adquiridos, melhor a IoT funcionará. Por outro lado, de acordo com Corcoran (2016) isso implica em menor privacidade dos usuários, então a melhor opção seria limitar a quantidade de dados e informações pessoais compartilhadas. Nesse contexto, alternativas devem ser consideradas para que a loT continue

ativa, sem desconsiderar a segurança e privacidade, dessa forma Sakomoto (2020) propõe os *blockchain*s, onde a criptografia é utilizada para vincular blocos, formando uma rede P2P cuja operação é baseada na imutabilidade e descentralização. Complementando, que a identidade de um usuário de *blockchain* é definida por um par de chaves criptográficas, uma chave privada usada para assinar transações de rede e uma chave pública representando o usuário, que neste caso permite o anonimato, trazendo privacidade para a rede.

Chicarino *et al*. (2017) também aponta para a viabilidade da *blockchain*, no entanto, também discute os desafios que esse recurso pode apresentar, como consumo excessivo de energia e latência[2] para dispositivos loT com recursos limitados. Apesar das adversidades apontadas, se considerarmos a vulnerabilidade que alguns dispositivos loT apresentam, assim como os danos que o vazamento de dados pode causar os usuários, o *blockchain* em combinação com a loT se mostra como uma alternativa confiável para impedir tais atribulações, além de permitir que outras ações sejam realizadas com segurança, como transferir dinheiro e alocar recursos entre dispositivos.

Raj e Raman (2017) apontaram um padrão de regras de segurança da informação desenvolvido para garantir a privacidade dos dados, denominado Autenticação e Autorização. Sendo a autenticação é um mecanismo projetado para autenticar as credenciais de acesso *login* e senha, e a autorização tem a ver com que pode ser acessado por um usuário ou dispositivo autenticado.

Corroborando com a ideia de autorização e autenticação diversos autores defendem essa estrutura. Os modelos de autenticação mais populares são: (a) Uso de *tokens* de acesso[3], que são obtidos após o usuário se autenticar no servidor com um identificador e senha (KONIDALA *et al*, 2005); (b) Criptografia de chave pública (ROTONDI et al, 2011); (c) Uso do *OpenID* (*OpenID Authentication*), um sistema que possibilita acesso a diferentes sites com uma única credencial (AKRAM e HOFFMANN, 2008); (d) Autenticação mútua dentro do mesmo domínio, por meio de um par de chaves assimétricas e parâmetros de domínio a partir de chaves confiável (KDC) (MAHALLE *et al*, 2012); (e) *Datagram Transport Layer Security* (DTLS), um protocolo que realiza a autenticação automática e criptografia de dados (KOTHMAYR et

[2] Latência no contexto da internet significa a quantidade de atraso (tempo) que uma solicitação leva para ir de um ponto a outro.
[3] *Token* de acesso é um mecanismo que possibilita o acesso dos usuários a diferentes recursos mediante a autorização de um servidor.

al, 2012); (f) uso de técnicas de criptografia e autenticação, por meio de um *gateway*[4] (BONETTO *et al*, 2012).

Enquanto aos modelos de autorização: (a) Modelo baseado em papéis (*Role Based Access Control*-RBAC): Gerencia permissões de acordo com o papel desempenhado pelo usuário (LIU *et al*, 2012); (b) Modelo baseado em habilidades (*Capability Based Access Control* - CapBAC): usa um *token* de autorização sem confrontar a identidade do usuário (ROTONDI et al, 2011); (c) Modelo baseado em atributos (*Attribute Based Access Control* – ABAC): as autorizações são permitidas com base nos atributos do usuário e das ações solicitadas (HU *et al*, 2013).

5 CONSIDERAÇÕES FINAIS

A Internet das Coisas é capaz de processar e trocar grandes quantidades de dados que s podem conter informações consideradas críticas em relação à segurança e privacidade de indivíduos ou empresas. No decorrer do trabalho apontamos algumas das alternativas que tem se mostrado eficientes em superar tais adversidades, entre elas está à utilização do *blockchain*, uma tecnologia relativamente recente para a loT, vale lembrar que o *blockchain* já vem sendo usado há algum tempo nas criptomoedas Bitcoin, essa ferramenta através da criptografia evita que informações sejam passadas para frente através de dispositivos ligados a loT.

Outro método levantado pela revisão bibliográfica foi à autenticação e autorização, sendo a autenticação um processo de identificação do dispositivo, enquanto a autorização fornece permissões. Com isso, apenas dispositivos autorizados podem interagir com outros dispositivos, aplicativos, contas de nuvem e *gateways.* A loT tem alcançado cada vez mais as empresas de diferentes ramos, assim como a casa dos cidadãos através dos dispositivos eletrônicos, por tanto, os estudos sobre estratégias para a segurança e privacidade não podem cessar, uma vez que o mundo está cada vez mais conectado novas vulnerabilidades na segurança e privacidade podem surgir.

REFERÊNCIAS

ALBERTIN, Alberto Luiz; DE MOURA ALBERTIN, Rosa Maria. A internet das coisas irá muito além às coisas. GV EXECUTIVO, v. 16, n. 2, p. 12-17, 2017.

[4] *Gateway* na tradução para o português significa “porta de entrada”, na informática refere-se a uma ferramenta que atua como intermediária na troca de informações entre dispositivos conectados em rede.

ALVES, David; PEIXOTO, Mario; ROSA, Thiago. Internet Das Coisas (IoT): Segurança e Privacidade dos Dados Pessoais. Alta Books, 2021.

ASHTON, Kevin. That 'Internet of Things' thing. Publicando no RFID Journal, 2009. Disponível em: https://www.rfidjournal.com/rfid-video/retail-rfid-the-view-from-outer-space, Acesso em 08 de maio de 2022.

AKRAM, Hasan; HOFFMANN, Mario. Laws of identity in ambient environments: The hydra approach. In: **2008 the Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies**. IEEE, 2008. p. 367-373.

BONETTO, Riccardo et al. Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. In: **2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)**. IEEE, 2012. p. 1-7.

BRASIL. Constituição da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 31 de maio de 2022.

BRASIL. Lei n. 10.406/2002, de 10 de janeiro de 2002. Institui o Código Civil. 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 22 de maio de 2022.

BRASIL. Lei n. 9.472, de 16 de julho de 1997. Dispõem sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995. 1997a. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9472.htm. Acesso em: 31 de maio de 2022.

BRASIL. Lei n. 9.507/1997, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. 1997b. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm. Acesso em: 31 de maio de 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 22 de maio de 2022.

BRASIL. Lei n. 13.709/2018, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 31 de maio de 20221.

CAMARA, Maria Amália Arruda et al. Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. **Cadernos Ibero-Americanos de Direito Sanitário**, v. 10, n. 1, p. 93-112, 2021.

CARVALHO, Cristiana. Internet das coisa: entenda o que é e como funciona. Tecmundo. 2020. Disponível em: https://www.tecmundo.com.br/internet/230884-internet-coisas-entenda-funciona.htm. Acesso em 27 de maio de 2022.

CARVALHO, Carlos Eduardo et al. Cryptocurrencies: technology, initiatives of banks and central banks, and regulatory challenges. **Economia e Sociedade**, v. 30, p. 467-496, 2021.

CAVALLI, Olga. Internet das coisas e inovação na América Latina. Sl: sn, 2016.

COLOMBO, Jamires Fátima; DE LUCCA FILHO, João. INTERNET DAS COISAS (IoT) E INDÚSTRIA 4.0: revolucionando o mundo dos negócios. **Revista Interface Tecnológica**, v. 15, n. 2, p. 72-85, 2018.

CORCORAN, Peter M. A privacy framework for the Internet of Things. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE, 2016. p. 13-18.

CHICARINO, Vanessa RL et al. Uso de blockchain para privacidade e segurança em internet das coisas. Sociedade Brasileira de Computação, 2017.

EVANS, D. The Internet of Things: how the next evolutivon of the intenet is changing everything. White Paper, CISCO IBSG, 2011. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf. Acesso em 25 de maio de 2022.

FACCIONI FILHO, Mauro. Designing "things" for the Internet of Things. In: I CONGRESSO INTERNACIONAL, I; WORKSHOP DESIGN & MATERIAIS, VII, 2016, São Paulo: Universidade Anhembi Morumbi, 2016a.

FACCIONI FILHO, Mauro. Internet das coisas. Unisul Virtual, 2016b. Disponível em: https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf. Acesso em: 26 de maio de 2022.

FROGERI, Rodrigo Franklin et al. BLOCKCHAIN E INTERNET DAS COISAS. **Textos para Discussão-ISSN 2447-8210**, v. 1, n. 1, p. 813-835, 2022.

HU, Vincent C. et al. Guide to attribute based access control (abac) definition and considerations (draft). **NIST special publication**, v. 800, n. 162, p. 1-54, 2013.

KONIDALA, Divyan M. et al. A capability-based privacy-preserving scheme for pervasive computing environments. In: **Third IEEE International Conference on Pervasive Computing and Communications Workshops**. IEEE, 2005. p. 136-140.

KOTHMAYR, Thomas et al. A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. In: **37th Annual IEEE Conference on Local Computer Networks-Workshops**. IEEE, 2012. p. 956-963.

LIU, Jing; XIAO, Yang; CHEN, CL Philip. Authentication and access control in the internet of things. In: **2012 32nd international conference on distributed computing systems workshops**. IEEE, 2012. p. 588-592.

LUCERO, Sam et al. IoT platforms: enabling the Internet of Things. White paper, 2016. Disponível em: https://cdn.ihs.com/www/pdf/enabling-IOT.pdf. Acesso em: 30 de maio de 2022.

MAGRANI, Eduardo. A internet das coisas. Editora FGV, 2018.

MAHALLE, Parikshit N. et al. Identity authentication and capability based access control (iacac) for the internet of things. **Journal of Cyber Security and Mobility**, v. 1, n. 4, p. 309-348, 2013.

MINERVA, Roberto; BIRU, Abyi; ROTONDI, Domenico. Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, v. 1, n. 1, p. 1-86, 2015.

NAKAMOTO, SATOSHI. Bitcoin: A Peer-to-Peer Electronic Cash System. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 25 de setembro de 2022.

PANEK, Lin Cristina Tung. Lei geral de proteção de dados nº 13.709/2018: uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019.

PESSOA, Cláudio Roberto Magalhães et al. A Internet Das Coisas: Conceitos aplicações, desafios e tendências. In: 13th International Conference on Information Systems and Technology Management–Contecsi. 2016

RAJ, Pethuru; RAMAN, Anupama C. The Internet of Things: Enabling technologies, platforms, and use cases. Auerbach Publications, 2017.

ROTONDI, Domenico; SECCIA, Cristoforo; PICCIONE, Salvatore. Access control & iot: Capability based authorization access control system. In: **1st IoT International Forum, Berlin**. 2011.

SANTAELLA, Lucia et al. Desvelando a Internet das coisas. Revista GEMInIS, v. 4, n. 2, p. 19-32, 2013.

SANTOS, Bruno P. et al. Internet das coisas: da teoria à prática. 2016.

SAKAMOTO, Sarah Gomes. Security, Privacy and Blockchain in Internet of Everything Context. Monografia de Especialização em Internet das Coisas, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2020.

OLIVEIRA, Sergio Silva et al. Inovação na educação: internet das coisas e tecnologias inteligentes com novos modelos e estilo de aprendizagem. 2019.

OZTEMEL, Ercan; GURSEV, Samet. Literature review of Industry 4.0 and related technologies. **Journal of Intelligent Manufacturing**, v. 31, n. 1, p. 127-182, 2020. Disponível em: https://link.springer.com/article/10.1007/s10845-018-1433-8. Acesso em: 25 de maio de 2022.

VERMESAN, Ovidiu; FRIESS. Peter (Eds.). Internet of Things - From Research and Innovation to Market Deployment. Aalborg: River Publishers, 2014. Disponível em: http://www.internet-of-things-research.eu/pdf/IoT-From%20Research%20and%20Innovation%20to%20Market%20Deployment_IERC_Cluster_eBook_978-87-93102-95-8_P.pdf. Acesso em: 23 de abril de 2022.

ZAMBARDA, Pedro. 'Internet das Coisas': entenda o conceito e o que muda com a tecnologia. Disponível em: https://www.techtudo.com.br/noticias/noticia/2014/08/Internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html. Acesso em: 27 de maio de 2022.

WANGHAM, Michelle S.; DOMENECH, Marlon Cordeiro; DE MELLO, Emerson Ribeiro. Infraestruturas de Autenticação e de Autorização para Internet das Coisas. Sociedade Brasileira de Computação, 2013.

WHITMAN, Michael E., MATTORD, Herbert J. Principles of Information Security. 5 ed. Cengage Learn, 2015.