NETLOG 2021
International Conference on Network Enterprises & Logistics Management

SEGURANÇA DA INFORMAÇÃO APLICADA NA INTERNET DAS COISAS INDUSTRIAL: UMA REVISÃO SISTEMÁTICA

Souza, R. B., Santos, M.F.S., *Glória Júnior, I.

Faculdade de Tecnologia de Santana de Parnaiba - FATEC

*ijunior@ndsgn.com.br

Resumo

Os dispositivos do *Industrial Internet of Things* tem gradativamente sido incluídos nas indústrias, o que pode tornar as empresas alvo de invasões. Neste contexto a segurança da informação deve auxiliar na proteção dos dados. O presente artigo pretende identificar o que está sendo pesquisado na literatura em relação a esses dois termos e apresentar os focos de pesquisa encontrados. A pesquisa possui natureza qualitativa, com uso da metodologia de revisão sistemática baseada em Kitchenham. O resultado foi a identificação dos focos das pesquisas disponíveis na academia, dentre os principais a comunicação em redes industriais e a gestão de identidade em IIoT. A contribuição para a academia é a de indicar que existe carência em estudar este tipo de combinação e de apresentar o que está sendo pesquisado. A contribuição para a prática é de que os gestores de indústrias e de projetos poderão conhecer os principais desafios do emprego do IIoT nas empresas.

Palavras-chave. Internet das Coisas Industrial, Segurança da Informação, Revisão Sistemática

Abstract

Industrial Internet of Things devices have been gradually included in industries, which can make companies somehow invasive. In this context, information security should help protect data. This article aims to identify what is being researched in the literature in relation to these two terms and present the research focuses found. The research has a qualitative nature, using the methodology of systematic review based on Kitchenham. The result was the identification of the research focuses available at the academy, among which the main ones are communication in industrial networks and identity management in IIoT. The contribution to the academy is to indicate that there is a need to study this type of combination and to present what is being researched. The contribution to the practice is that industry and project managers will be able to know the main challenges of using IIoT in the companies.

Keywords. Industrial Internet of Things, Information Security, Systematic Review

1 Introdução

No final da década de 90, o cientista britânico Kevin Ashton cunhou o termo *Internet of Things* (IoT), que seria conhecido no Brasil por Internet das Coisas, como uma tecnologia com capacidade de identificação de produtos pelo meio eletrônico, melhorando a eficiência de troca de informações (Madakam, Ramaswamy & Tripathi, 2015).

A troca de informações entre diferentes tecnologias tem potencial para criar um ambiente inteligente que realiza análises para tomar decisões autônomas, quando aplicadas nas indústrias, é definida como *Industrial Internet of Things*, ou Internet das Coisas Industrial (Conway, 2016).

O *Industrial Internet of Things* (IIoT) gera uma grande quantidade de informações e que podem ser úteis para as análises e direcionamento de decisões, tornando-se um ativo da empresa e, sendo intrínseco o valor que representa para a corporação, assim impondo às empresas a criarem meios para proteger a segurança de seus dados (BSI, 2017).

Diante desse contexto, este trabalho pretende responder a seguinte questão de pesquisa: "O que está sendo pesquisado sobre Segurança da Informação em *Industrial Internet of Things*?". Os objetivos específicos são: (1) Identificar os artigos disponíveis sobre Segurança da Informação em *Industrial Internet of Things*; e (2) Apresentar o direcionamento de estudo dos artigos selecionados.

O trabalho é composto por seções, na seção 2 apresenta o referencial teórico a respeito da *Industrial Internet of Things* e segurança da informação, na seção 3 descreve sobre a metodologia e procedimentos utilizados para realizar a pesquisa, e na seção 4 traz os resultados e discussões da pesquisa. Por fim, a seção 5 deixa explícito as conclusões obtidas na realização do trabalho.

2 Referencial Teórico

2.1 *Industrial Internet of Things*

A Internet das Coisas (IoT) é vista como um grande avanço da Internet, verificado o enorme potencial para criação de novas aplicações e utilidades, transformando a rede em algo sensorial ao trafegar dados sobre temperaturas, pressões, vibrações, iluminação e umidade (Evans, 2011).

Uma nova evolução é apresentada da IoT em 2016, a chamada *Industrial Internet of Things* (IIoT), que pretende estabelecer a comunicação entre dispositivos mecânicos (Batista, 2018) e melhorar a eficiência da indústria aplicando soluções que podem incrementar a velocidade de produção e, possivelmente, tornar a produção autônoma (Himanshu, 2020).

É possível encontrar na literatura exemplos da utilização do IIoT, como no modelo implementado no simulador NS-3 que auxilia na automação industrial dos equipamentos, capaz de analisar as máquinas e aferir se estão em condições para atuar em determinada função por meio dos dados coletados pelos IIoT, desta forma permitiu melhorar o aproveitamento de recursos e aumentando a qualidade das informações geradas na produção (Pedroso *et al.*, 2020).

Outro exemplo é na produção de motores para aviões que a inspeção é feita baseada nas informações provenientes dos IIoT, detectando possíveis erros de fabricação, assim diminuindo o número de peças retornavam com defeitos e gerando maior lucros para a empresa (Sayar & Er, 2018).

A interação dos ambientes cibernético e físico precisou ser criada, culminando no *Cyber-Physical System* (CPS), que realiza a interação de protocolos de comunicação padronizados, permitindo construir uma rede autônoma capaz de tomar decisões sozinha junto com o uso da inteligência artificial (Conway, 2016), como um organismo humano, em que há um cérebro e órgãos sensitivos que sentem e atuam dependendo das informações processadas e reenviadas pelo cérebro, portanto, potencialmente um sistema tecnológico autônomo (Petroni, Glória Junior & Gonçalves, 2018).

É possível encontrar na literatura exemplos da integração do CPS com o IIoT, como uma universidade que automatizou um reator, que mede as concentrações das moléculas e toma ações mediante os valores obtidos (Sousa, Taira & Park, 2019) e uma outra universidade que integrou IIoT com controladores lógicos programáveis e processos físicos que atuavam e influenciavam no comportamento da produção de um produto (Siemon & Costa, 2018).

2.2 Segurança da Informação

A Segurança da Informação (SegInfo) visa proteger toda e qualquer informação que passa pela rede e pertence a empresa e deve seguir algumas diretrizes para mitigar qualquer ataque ou vazamento de informações (ISO, 2005): (1) **Confiabilidade**, é disponibilizar as informações somente para pessoas autorizadas e que necessitem do acesso; (2) **Legalidade**, ato de manter os dados dentro das regras da organização; (3) **Auditabilidade**, controlar o acesso, por meio da identificação do usuário; (4) **Integridade**, as informações precisam estar verídicas e protegidas contra modificações não permitidas; e (5) **Disponibilidade**, deve-se assegurar que a informação seja acessada quando for requisitada.

Em SegInfo existem diversos tipos de ataques, como o DoS, DDoS, *SQL Injection* e *Sybil*. O ataque de *Denial of Service* (DoS) têm o propósito de impedir o uso de serviços ligados a internet, tornando-os indisponíveis. De forma semelhante existe o *Distributed Denial of Service* (DDoS) que é similar ao DoS, mas com utilização de vários computadores robôs, os *BotNet* (Haider, Et al., 2020).

Outro ataque que pode comprometer a confiabilidades dos dados é o de *SQL Injection* que gera imprecisão dos dados coletados, comprometendo a integridade das informações, sendo que os dispositivos mais visados são aqueles que realizam a autenticação na rede, recolhem e distribuem dados, como os IIoT (Alves & Montel, 2020).

O ataque *Sybil* explora as vulnerabilidades nos serviços de controle de acesso em que estes estão adaptados às redes convencionais e não comportam as necessidades de uma rede IoT/IIoT, que realizado a falsificação de identidades, como esforço para ser autenticado como um usuário da empresa e quando bem-sucedido, o invasor passa a ter acesso aos dados do usuário (Kim & Jum 2020).

Desta forma, é possível presumir que a gestão de segurança de informação poderá auxiliar na proteção dos dados trafegados e manipulados pela IIoT, sendo essa a inquietação que gerou essa pesquisa.

3 Metodologia

Esta pesquisa possui natureza qualitativa (Gil, 2008), com uso da metodologia de revisão sistemática (Kitchenham, 2004) com o intuito identificar as pesquisas disponíveis a respeito de Segurança da Informação em *Industrial Internet of Things* (Figura 1).

3.1 Procedimentos metodológicos

Os procedimentos metodológicos para essa pesquisa, de acordo com a figura 1, foram:

• **Passo 1: Definir os Critérios para a Seleção**. Foram definidos os critérios para a seleção dos artigos de forma a determinar quais os mais relevantes;

• **Passo 2: Definir os Termos de Busca**. A partir das definições encontradas na literatura, foram estabelecidos os termos a serem pesquisados e a criação da *String* de busca para o *Engine* do Google Scholar (www.scholar.google.com.br);

• **Passo 3: Selecionar Artigos**. O resultado da busca retornou os artigos candidatos que possivelmente serão utilizados, mas apenas se contemplarem os critérios de seleção e serão considerados na análise;

• **Passo 4: Análise dos Resultados**. Serão identificados os assuntos mais tratados;

• **Passo 5: Apresentar os Resultados**. Será apresentado o resultado quanto à evolução do número de artigos de Segurança da Informação em IIoT a cada ano, e seus direcionamentos das pesquisas.

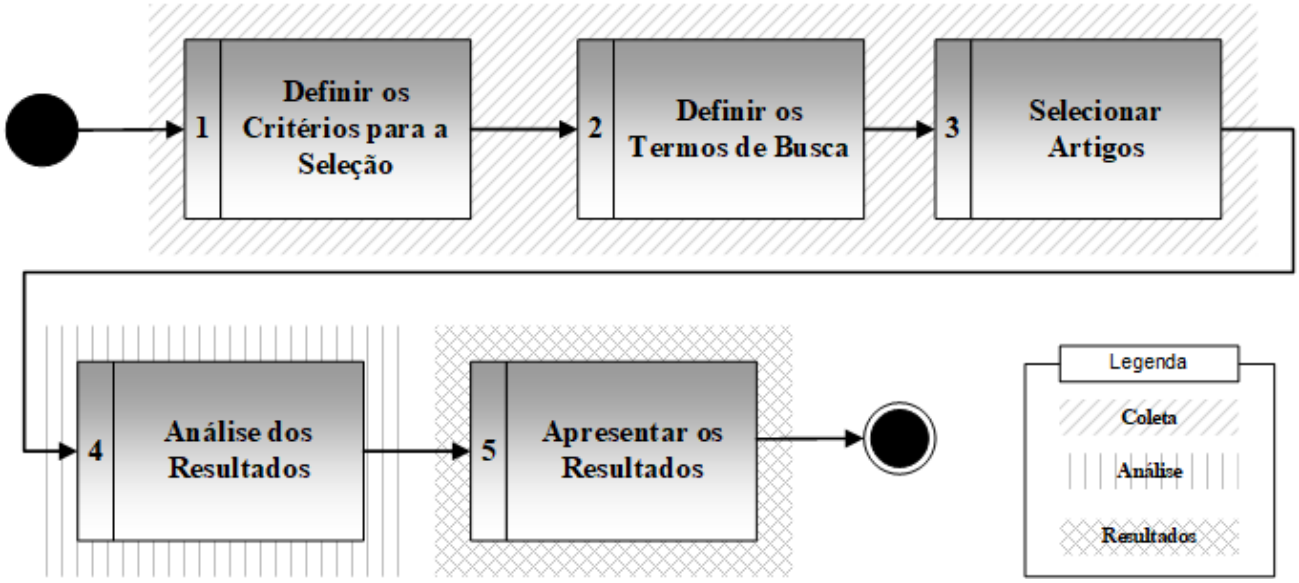

Figura 1 – Procedimentos Metodológicos

3.2 Critérios de Seleção

A revisão literária incluiu os seguintes critérios:

(1) O período de 2016 (ano de criação do termo) até 2020;

(2) Fará uso somente de artigos científicos publicados, excluindo monografias, dissertações, teses, livros e quaisquer outros materiais;

(3) Documento no formato pdf;

(4) Apresente em sua composição concepções sobre IIoT e Segurança da Informação;

(5) Tiverem em seu abstract e resumo palavras-chave pertinentes à questão de pesquisa.

3.3 Termos de Busca

Em relação ao termo de busca foi utilizado IIoT e Segurança com alusão à segurança da informação. conforme a Tabela 1.

Tabela 1 - Termo de busca

Base	***String***
Scholar Google www.scholar.google.com	IIoT+segurança filetype:pdf

3.4 Artigos Selecionados

A busca teve como resultado 15 artigos candidatos, no qual 6 foram selecionados (Tabela 2).

Tabela 2 - Artigos candidatos e selecionados

Item	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
Candidatas	3	1	2	4	5	15
Selecionadas	1	0	0	2	3	6

3.5 Artigos Selecionados e o Foco

Os artigos selecionados foram analisados tendo como objetivo obter qual o direcionamento que suas pesquisas representavam e como resultado foi criada uma lista dos artigos com seu respectivo foco identificado (Tabela 3).

Tabela 3 - Artigos Selecionados e seus Respectivos Focos

Ano	**Título**	**Foco**
2016	Simulação de aplicações utilizando o protocolo de comunicação MQTT com aplicações em ambientes industriais	Comunicação em IIoT
2019	Implementação e Análise de complexidade do sistema de criptografia de chave pública RSA	Criptografia
2019	Mitigação de ataques IDF no Serviço de Agrupamento de Disseminação de Dados em Redes IoT densas	Mitigação de Vulnerabilidade
2020	Análise de requisitos de identificação e autorização para dispositivos e gateways de bordas em IIoT	Gestão de identidade em IIoT
2020	Autenticação e autorização de dispositivos IoT e IIoT em infraestrutura de redes de identidade Federadas	Comunicação em IIoT
2020	Segurança e Interoperabilidade na indústria 4.0	Gestão de identidade em IIoT

4 Resultados e Discussão

4.1 Artigos Selecionados de IIoT e Segurança da Informação

A pesquisa apresentou, conforme Figura 2, em 2016 apenas 1 artigo sobre os temas, com ausência de pesquisas em 2017 e 2018. Em 2019 foram encontrados 2 artigos contendo os assuntos-chaves e em 2020 o número passou a ser 3. Desta forma, é possível aferir que existe crescimento do estudo da segurança da informação nas redes IIoT.

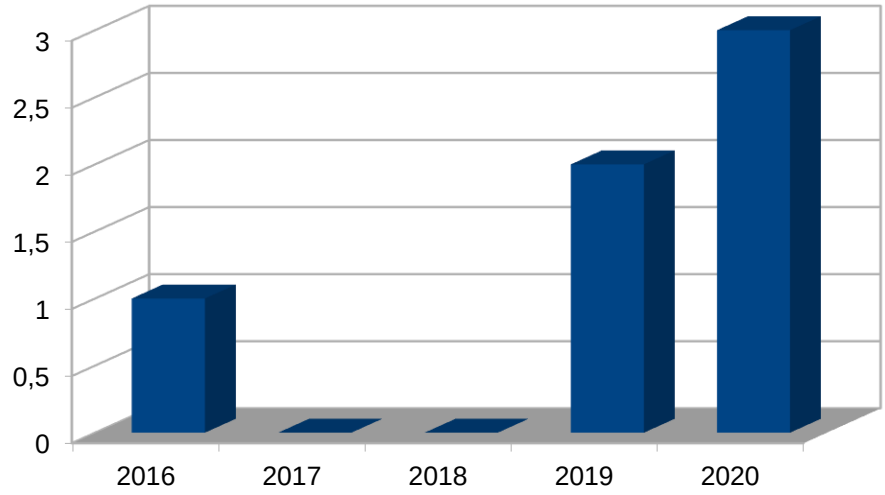

Figura 2 – Artigos Identificados

4.2 Direcionamento dos Artigos Selecionados

A seleção dos 6 artigos permitiu que fossem identificados os pontos focais nas pesquisas realizadas que estavam disponíveis na base de dados do Google Acadêmico, culminando na Tabela 4 e apresentada graficamente na Figura 3.

Foi possível observar que o foco em 2 artigos relacionado a **comunicação em redes industriais** (**F01**), sendo o primeiro que considerou a implementação do modelo de comunicação *Message Queue Telemetry Transport* (MQTT) para dispositivos IIoT que não realiza a comunicação direta entre os dispositivos que compartilham as informações, fazendo uso de um servidor como intermediário (Correa, Cunha, Almeida & Moraes, 2016). O outro artigo citou a necessidade de evidenciar a importância da comunicação para evitar precauções com a intrusão de invasores na defesa dos ativos (Abreu, 2020)

Em relação **gestão de identidade em IIoT (F02)** os artigos apresentados buscaram determinar medidas eficientes para identificação dos IIoT, tendo em vista a complexidade da gestão e da segurança desses dispositivos (Silva & Miers, 2020), além de medidas para promover a substituição de acesso de funcionários com perfis pelo uso de chaves ou credenciais (Meincheim & Miers, 2020)

A **criptografia (F03)** foi o tema de pesquisa como forma de defesa utilizando um algoritmo que pode ser implantado para garantir maior segurança nas conexões entre dispositivos IIoT e nas redes abertas (Welter & Batista, 2019).

Tabela 4 – Foco dos Artigos Analisados

#	Foco	Autores
F01	Comunicação em IIoT	Correa, Cunha, Almeida & Moraes (2016) Abreu (2020)
F02	Gestão de identidade em IIoT	Silva & Miers (2020) Meincheim & Miers (2020)
F03	Criptografia	Silva & Miers (2019) Welter & Batista (2019)
F04	Mitigação de Vulnerabilidade	Pedroso, Gielow, Santos & Nogueira (2019)

Outro ponto focal nos artigos foi a **mitigação de vulnerabilidades (F04)** destacado os riscos que as novas tecnologias de IIoT sofrem com relação a integridade das informações coletadas, em que o uso de ataques como a injeção de dados falsos (IDF) visam comprometer as informações (Pedroso *et al.*, 2019).

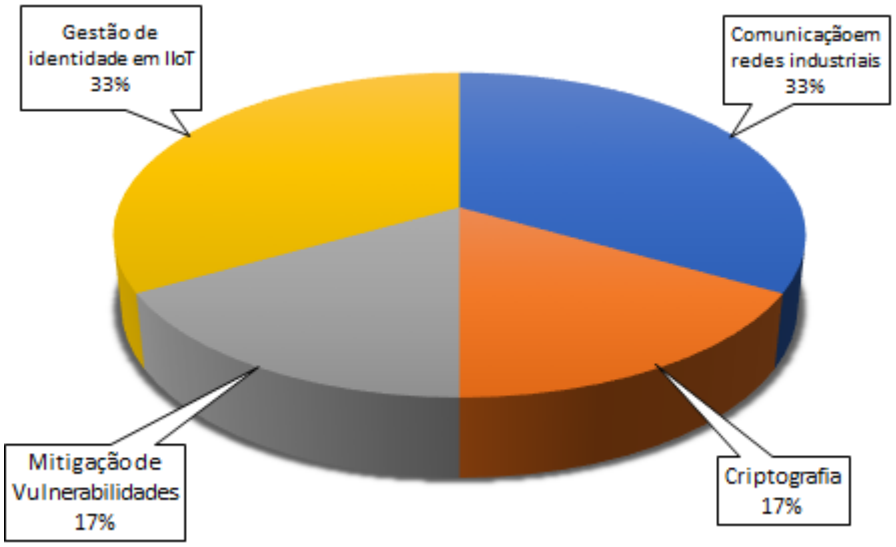

Figura 3 – Proporção dos Temas

4.3 Discussão

É possível observar que as maiores concentrações de pesquisa estão relacionadas a gestão de identidade e na comunicação em redes industriais que representam a base da interoperabilidade dos dispositivos, que é a responsável por qualquer projeto baseado nessa tecnologia.

Outro ponto a ser destacado é pelo crescente aumento do número de artigos relacionados ao tema, mesmo com 2 anos sem publicação, a retomada vigorosa com o triplo de pesquisas no ano de 2020 após 2 anos sem interesse aparente nos anos de 2017 e 2018.

Desta forma, é possível aferir que é uma tecnologia nova, criada em 2016, que está em processo de solidificação da sua estrutura base e que poderá fomentar o transbordamento tipos de temas tecnológicos e processuais na academia.

A escassez de artigos sobre a relação entre IIoT e segurança da informação pode ser um indicador de que é possível pesquisar mais a respeito de como são relacionados, complementados e de novas técnicas de defesa de dados.

5 Conclusão

A pesquisa apresentou que *Internet of Things* é uma grande evolução para a Internet e seus conceitos que foram implementados nas indústrias. A IIoT está sujeita aos mais diversos ataques, como o *Denial of Service*, *Distributed Denial of Service*, *SQL Injection* e o *Sybil*.

O resultado foi a identificação dos focos das pesquisas disponíveis na academia como a comunicação em redes industriais (33%), a gestão de identidade em IIoT (33%), a criptografia (17%) e a mitigação de vulnerabilidades (17%).

A limitação desta pesquisa foi a busca em uma única base de dados. A contribuição para a academia é de que existe espaço para pesquisar mais a respeito da IIoT e Segurança da Informação, bem como apresenta um panorama do que está sendo estudado. A contribuição deste trabalho possibilitará os gestores das indústrias e de projetos a visualizarem os principais desafios do emprego do IIoT nas empresas. Em futuros trabalhos serão ampliadas as bases de conhecimento e serão traçados paralelos com o desenvolvimento da Indústria 4.0.

Referências

Abreu, M. (2020). Segurança e Interoperabilidade na indústria 4.0. II Simpósio Internacional de Inovação E Tecnologia (SIINTEC), p. 1-12.

Alves, H. N. & Montel, B.M.M. (2020) Segurança Cibernética em *Smart Grids*: Uma *support Vector machine*. Sociedade Brasileira de Automática, p. 1-7. DOI https://doi.org/10.48011/asba.v2i1.1629

Batista, L. (2018) Utilização de Redes Neurais Nebulosas para criação de um Sistema Especialista em Invasões Cibernéticas. *The Tenth International Conference on FORENSIC COMPUTER SCIENCE and CYBER LAW*, p. 12-22.

BSI (2020) Análise da ISO/IEC 207001 Gestão de Segurança da Informação. Disponível em: https://www.bsigroup.com/pt-BR/ISO-IEC-27001-Seguranca-da-Informacao/#:~:text=A%20ISO%2FIEC%2027001%20%C3%A9,e%20certificado%20de%20forma%20independente

Conway, John. (2016) *The industrial internet of things: An Evolution to a Smart Manufacturing Enterprise.* Schneider Eletric, p. 1-15.

Correa, R. P. S., Cunha, M.J., Almeida, M.B. & Moraes, J.S. (2016) Simulação de Aplicações utilizando o protocolo de comunicação MQTT com Aplicações em Ambientes Industriais. Disponível em: https://www.peteletricaufu.com/static/ceel/doc/artigos/artigos2016/ceel2016_artigo108_r01.pdf, p. 1-6.

Dufty, C. (2017) *The Industrial IoT: A Timeline of Revolutionary Technology*. *Kepware,*. Disponível em: https://www.kepware.com/en-us/blog/2017/the-industrial-iot-a-timeline-of-revolutionary-te/ .

Evans, D. A (2011) Internet das Coisas: Como a próxima evolução da Internet está mudando tudo. Cisco. Disponível em: https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/ internet_of_things_iot_ ibsg_0411final.pdf, p. 1-13.

Gil, A.C. (2008). Métodos e técnicas de pesquisa social. 6a ed. São Paulo: Editora Atlas.

Haider, S. & Akhunzada, A. (2020) *A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks*. IEEE Access, p. 1-12. Disponível em: https://ieeexplore.ieee.org/ stamp/stamp.jsp?tp=&arnumber=9016053 .

Himanshu, N. (2020) *Evolution of IoT to IIoT: Applications & Challenges. International Conference on Innovative Computing and Communication* (ICICC), p. 1-17.

ISO (2005) NBR ISO/IEC 17799, ABNT, 2005. p. 1-132.

Kim, M. & Yum, J. (2020) *SybilEye: Observer-Assisted Privacy-Preserving Sybil Attack Detection on Mobile Crowdsensing. Hankyong National University*, p. 1-14.

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, v. 33, pp. 1-26.

Madakam, S., Ramaswamy, R. & Tripathi, S. (2015) *Internet of Things (IoT): A Literature Review. Jornal of Computer and Communications*, Vol. 3, 164-173. Disponível em: https://www.scirp.org/pdf/ JCC_2015052516013923.pdf

Meincheim, F. & Miers C.C. (2020). Autenticação e autorização de dispositivos IoT e IIoT em infraestrutura de redes de Identidades Federadas. Disponível em: www.sbc.org.br/2020/papers/ST_PG1_2_IIoT_Federada, p. 1-6.

Pedroso, C. (2020) A Atribuições Cooperativas de Tarefas de Sensoriamento Baseada em Consenso Relacional para Redes IIoT. Sociedade Brasileira da Computação. Disponível em: https://sol.sbc.org.br/ index.php/wgrs/article/view/12461/12326, p. 1-14.

Pedroso. C., *et al*. (2019). Mitigação de Ataques IDFs no Serviço de Agrupamento de Disseminação de Dados em Redes IoT Densas. Disponível em: https://sol.sbc.org.br/index.php/sbseg/article/view/13973/13822 p. 1-14.

Petroni, B. C., Glória Júnior, I. & Gonçalves, R.F. (2018) Indústria 4.0: conceitos e fundamentos. São Paulo: Editora Blücher, p. 47-55.

Sayar, D. & Er, Ö. (2018) *The antecedents of Successful IoT Service and System Design: Cases from the Manufacturing Industry. Izmir University of Economics & Instanbul Technical University*, Disponível em http://index.ijdesign.org/index.php/IJDesign/article/viewFile/3006/796, p. 1-12.

Siemon, F.B. & Costa, C. (2018) Plataforma integrada para Indústria 4.0 . III Seminário da Indústria 4.0, p. 1-3.

Silva S.H. & Miers, C. C. (2020). Análise de requisitos de identificação e autorização para dispositivos e gateways de borda em IIoT. Disponível em: http://www.sbc.org.br, p. 1–6.

Sousa, R. S., Taira, G.R. & Park, S.W. (2019) Integração do sistema ciber-físico para sistema de programação, intertravamento e controle de um reator batelada. Universidade Federal de Viçosa (UFV), 2019. Disponível em: https://periodicos.ufv.br/jcec/article/view/9381/5209 , p. 1-9.

Welter, F.N. & Batista, V. E. (2019) Implementação e Análise de Complexidade do Sistema de Criptografia de Chave Pública RSA. Disponível em: http://www.periodicos.net/profile/Criptografia, p. 1-8.