Conjecturas

DOI: 10.53660/CONJ-1086-Q01

Cyber Infrastructure: um estudo compreensivo

Cyber Infrastructure: a comprehensive study

Fábio Luis Fernandes Azarias[1]*, Lia Toledo Moreira Mota[2], Renata Kally Mendes Valente[1], Ademar Takeo Akabane[1]

RESUMO

O artigo contextua a infraestrutura cibernética a partir de periódicos de relevância internacional. Dessa forma buscou-se extrair os sistemas correlatos a essa infraestrutura como conectividade da Indústria 4.0. Destacou-se também o que há de comum e de singular entre os tópicos principais discutidos na coleção científica analisada. Os tópicos encontrados apontam o vínculo da infraestrutura com tecnologias de transmissão de dados. Essa infraestrutura cibernética encontra-se em desenvolvimento em cidades em paralelo com a aplicação de novos conhecimentos que tangenciam a inovação para aumento da qualidade de vida humana. Tendo-se a compreensão do campo de atuação, ramificação e interligação dessa infraestrutura, a tomada de decisões para ações de gestão pública e privada será facilitada e otimizada para desenvolvimento de cidades inteligentes e sustentáveis.

Palavras-chave: Quarta revolução industrial; Sistema ciber físico; Infraestrutura urbana.

ABSTRACT

The presented article contextualizes the cyber infrastructure from internationally relevant journal. Thus, it was sought to extract the systems correlated to this connectivity from Industry 4.0. It was also highlighted what is common and unique among the topics of the analyzed scientific collection. These topics point to the link between infrastructure and data transmission technologies. This cyber infrastructure is under development in cities in parallel with the application of new knowledge that touches innovation to increase the quality of human life. With the perception of the field of action, ramification and interconnection of this infrastructure, decision-making for public and private management actions will be facilitated and optimized for the development of smart and sustainable cities.

Keywords: Fourth industrial revolution; Cyber physical system; Urban infrastructure.

[1] Pontifícia Universidade Católica de Campinas
*E-mail: fabio.lfa@puccampinas.edu.br

INTRODUÇÃO

A humanidade caminha a uma evolução tecnológica e a infraestrutura cibernética abraça sistemas correlatos integrando-os em uma malha de comunicação. Esse entrelaço compartilha de sistemas de Rede Elétrica, *Internet of Things* (IoT), Criptografia de dados, Monitoramento SCADA, análise de dados, sensores e comunicação para automação industrial e residencial. Como também a tecnologia digital transformou o poder econômico de troca de valor e surgiu a moeda virtual (criptomoeda) e o blockchain (DONG et al.; 2018), interagindo com essa rede de comunicação de vanguarda.

O sistema de rede de geração, transmissão e distribuição de energia elétrica alimenta componentes da eletrônica fundamentais para a produção técnica humana. Para a Rede Elétrica o sistema cibernético atua no comportamento (NAEINI et al.; 2016. ZHANG; 2018. VENKATARAMANAN et al. 2020) e na dinâmica da performance (KRISHNAN et al.; 2019. JIA et al.; 2020. KHALEDIAN et al.; 2021) identificando erros e medições de sistemas de controle automatizados (ZHANG et al.; 2018. RAMANAN et al.; 2019) além da integração entre redes de produção de concessionárias e redes locais por Smart Grid (DAVIS et al.; 2015. LIU et al.; 2015. MARASHI et al.; 2018. CARDENAS et al.; 2020. LOU et al.; 2013). A telecomunicação também caminhou para uma malha de comunicação global (KASSEM et al.; 2020.NATIVI et al.; 2013) permitindo interoperabilidade, estudo e análise do Planeta Terra.

A eletricidade (KATEB et al.; 2019) bem como a produção de gás e óleo, telecomunicação, saneamento básico, agroindústria, mobilidade urbana e sistema de saúde estão no conjunto de infraestruturas críticas (MARASHI et al.; 2018) e a troca dos dados (PIETERSE et al.; 2019) necessita de *Data Security* para tratamento e defesa contra *cyber attacks* (PRADHAN et al.; 2017. LIN et al.; 2019. KUSHAL et al. 2019. EICHENHOFER et al.; 2020. AMIN et al.; 2021). Serviços *online* também requerem atenção contra possíveis eventos maliciosos de acesso (WANG et al.; 2019. XU et al, 2020. DING et al.; 2021).

Na área da automação, sensoriamento e IoT encontram aplicações de Automated Guided Vehicles (AGV) (DU et al.; 2018) que permitem, através de acesso a dados, que o passageiro seja guiado e transportado computacionalmente em carros. Também dentro da interação da malha de dados de IoT, os sensores sem fio (AN et al.; 2011) conduzem

as informações a um armazenamento em servidor em nuvem, ou seja, permitem o gerenciamento dos dados com disponibilidade de acesso remoto (LENKA et al.; 2018. DEHGHANI et al.; 2020). Concomitante, por meio de um supervisório de sistema SCADA (*Supervisory Control and Data Acquisition*) a infraestrutura de dados consegue centralizar visualmente a operação da aplicação e executar comandos remotamente (PRADHAN et al.; 2017. SRIDHAR et al., 2012).

No campo de saúde médica, os sistemas ciber físicos necessitam de vínculo ao banco de dados, sistema de transporte, gestão de veículo (WASIM et al.; 2021) e de aparelhos dinâmicos para controle vital. Com a ascensão de aplicações e aumento do tráfego de dado de baixa latência, engenheiros preparam meios para médicos realizarem procedimentos cirúrgicos remotamente por realidade virtual (LUP et al.; 2007). Computadores com alto grau de processamento passaram a ajudar no estudo do próprio ser humano (FORTES et al.; 2005), como exemplo disso destaca-se a análise computacional de dados neurais (CHEIN et al.; 2015).

Assim, serão um denso investimentos em rede de telecomunicação que sustentará toda a base da transformação de cidades brasileiras em cidades inteligentes (JORDÃO; 2016) e sustentáveis. Neste contexto, esse trabalho tem como objetivo compreender a importância da infraestrutura cibernética atual assim como destacar o avanço das pesquisas relacionadas e algumas das formas de aplicação de tecnologias interligadas.

METODOLOGIA

Estudo quali-quantitativo a partir de critérios definidos levando-se em consideração artigos em base de dado digital pelo acesso ao portal *Xplore* do *Institute of Electrical and Eletronic Engineers* (IEEE) publicados até o momento da elaboração deste manuscrito (maio de 2021) devido a atualidade do tema e credibilidade do periódico.

A busca pela palavra-chave *"Cyber infrastructure"* localizou a quantidade de referências descrita na Tabela 1. Encontrou-se o total geral de 239 artigos utilizando 13,40% (39 artigos) após o crivo selecionado filtrando as referências por *Jornals*.

Tabela 1. Filtros aplicados.

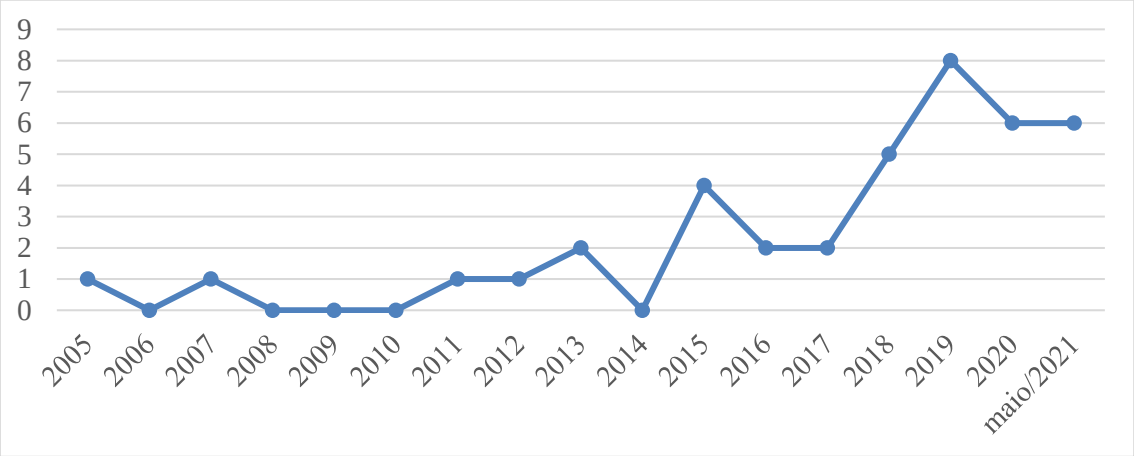
Filtro	Dado	Quantidade
Keyword	*"Cyber infrastructure"*	291
Documento	*Jornals*	39

Fonte: do autor.

EVOLUÇÃO DAS PESQUISAS NA ÁREA

Apesar da evolução anual (Figura 1) das publicações com o tema em estudo apresentar vários pontos de ascendência e outros descendentes, de maneira geral, ao longo do tempo, pode- se afirmar que houve um aumento da quantidade de artigos envolvendo Cyber infrastructure com um pico no ano de 2019.

Figura 1. Artigos publicados ao longo dos anos com a palavra-chave *Cyber infrastructure*.



Fonte: dos autores com base no IEEE Xplore.

Essa coleção de apenas 39 artigos foi citada individualmente em um total de 1184 vezes. Somente Cyber-Physical System Security for the Electric Power Grid (SRIDHAR at al; 2012) conta com 583 citações em artigos e mais 4 citações em patentes. A Tabela 2

apresenta a quantidade de citações que cada um destes 39 trabalhos apresentam até maio de 2021.

Tabela 2. Número de citações dos artigos relacionados a *Cyber infrastructure* obtidos até maio de 2021.

Ano de publicação	Título de documento	Autores	Citações
2005	*Virtual Computing Infrastructures for Nanoelectronics Simulation*	A. B. Fortes; J. Figueiredo; M. S. Lundstrom	20
2007	*Distributed Augmented Reality With 3-D Lung Dynamics - A Planning Tool Concept*	F. G. Hamza-Lup; A. P. Santhanam; C. Imielinska; S. L. Meeks; J. P. Rolland	15
2011	*Nonidentical Linear Pulse-Coupled Oscillators Model With Application to Time Synchronization in Wireless Sensor Networks*	Z. An; H. Zhu; X. Li; C. Xu; Y. Xu; X. Li	31
2012	*Cyber-Physical System Security for the Electric Power Grid*	S. Sridhar; A. Hahn; M. Govindarasu	583
2013	*Earth Science Infrastructures Interoperability: The Brokering Approach*	S. Nativi; M. Craglia; J. Pearlman	55
2013	*Profit-Optimal and Stability-Aware Load Curtailment in Smart Grids*	X. Lou; D. K. Y. Yau; H. H. Nguyen; B. Chen	27
2015	*Fast and Scalable Multi-Way Analysis of Massive Neural Data*	D. Chen; X. Li; L. Wang; S. U. Khan; J. Wang; K. Zeng; C. Cai.	63
2015	*Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid*	R. Liu; C. Vellaithurai; S. S. Biswas; T. T. Gamage; A. K. Srivastava	94
2015	*CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures*	C. Vellaithurai; A. Srivastava; S. Zonouz; R. Berthier	71
2015	*A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures*	K. R. Davis; C. M. Davis; S. A. Zonouz; R. B. Bobba; R. Berthier; L. Garcia; P. W. Sauer	69
2016	*Comparative Analysis of a Selected DCT-Based Compression Scheme for Haptic Data Transmission*	E. A. Baran; A. Kuzu; S. Bogosyan; M. Gokasan; A. Sabanovic	9
2016	*Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach*	M. Rahnamay-Naeini; M. M. Hayat	55

2017	*Experience With a Multidisciplinary, Team-Taught Smart Grid Cyber Infrastructure Course*	A. K. Srivastava; A. L. Hahn; O. O. Adesope; C. H. Hauser; D. E. Bakken	7
2017	*Stealthy Attacks in Dynamical Systems: Tradeoffs Between Utility and Detectability With Application in Anonymous Systems*	P. Pradhan; P. Venkitasubramaniam	8
2018	*A Distributed Message Delivery Infrastructure for Connected Vehicle Technology Applications*	Y. Du; M. Chowdhury; M Rahman; K. Dey; A. Apon; A. Luckow; L. B. Ngo	4
2018	*On the Impact of Measurement Errors on Power System Automatic Generation Control*	J. Zhang; A. D. Domínguez-García	2
2018	*Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems*	Z. Dong; F. Luo; G. Liang	9
2018	*Consideration of Cyber-Physical Interdependencies in Reliability Modeling of Smart Grids*	K. Marashi; S. S. Sarvestani; A. R. Hurson	14
2018	*Building Scalable Cyber-Physical-Social Networking Infrastructure Using IoT and Low Power Sensors*	R. K. Lenka; A. K. Rath; Z. Tan; S. Sharma; D. Puthal; N. V. R. Simha; M. Prasad; R. Raja; S. S. Tripathi	13
2019	*Evaluation Framework for Detecting Manipulated Smartphone Data*	H. Pieterse; M. Olivier; R. van Heerden	1
2019	*Enhancing WAMS Communication Network Against Delay Attacks*	R. Kateb; P. Akaber; M. H. K. Tushar; A. Albarakati; M. Debbabi; C. Assi	9
2019	*An Asynchronous, Decentralized Solution Framework for the Large Scale Unit Commitment Problem*	P. Ramanan; M. Yildirim; E. Chow; N. Gebraeel	2
	Contract-Based Methodology for Developing Resilient Cyber-Infrastructure in the Industry 4.0 Era	S. Andalam; D. J. X. Ng; A. Easwaran; K. Thangamariappan	1
2019	*Risk-Based Mitigation of Load Curtailment Cyber Attack Using Intelligent Agents in a Shipboard Power System*	T. R. B. Kushal; K. Lai; M. S. Illindala	6
2019	*RAINCOAT: Randomization of Network Communication in Power Grid Cyber Infrastructure to Mislead Attackers*	H. Lin; Z. T. Kalbarczyk; R. K. Iyer	3
2019	*Resilient Cyber Infrastructure for the Minimum Wind Curtailment Remedial Control Scheme*	V. V. G. Krishnan; S. Gopal; R. Liu; A. Askerman; A. Srivastava; D. Bakken; P. Panciatici	0

2019	*Source-Load Coordinated Reserve Allocation Strategy Considering Cyber-Attack Risks*	Q. Wang; M. Li; Y. Tang; M. Ni	1
2020	*Real-Time Federated Cyber-Transmission-Distribution Testbed Architecture for the Resiliency Analysis*	V. Venkataramanan; P. S. Sarker; K. S. Sajan; A. Srivastava; A. Hahn	0
2020	*Data-Driven Edge Intelligence for Robust Network Anomaly Detection*	S. Xu; Y. Qian; R. Q. Hu	7
2020	*Operating Reliability Evaluation of Power Systems With Demand-Side Resources Considering Cyber Malfunctions*	H. Jia; C. Shao; D. Liu; C. Singh; Y. Ding; Y. Li	0
2020	*An In-Depth Security Assessment of Maritime Container Terminal Software Systems*	J. O. Eichenhofer; E. Heymann; B. P. Miller; A. Kang	0
2020	*Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations*	D. J. S. Cardenas; A. Hahn; C. -C. Liu	1
2020	*The EPI Framework: A Dynamic Data Sharing Framework for Healthcare Use Cases*	J. A. Kassem; C. De Laat; A. Taal; P. Grosso	0
2021	*Resilient Control Systems-Basis, Benchmarking and Benefit*	C. Rieger; K. Schultz; T. Carroll; T. McJunkin	0
2021	*Hidden Markov Model and Cyber Deception for the Prevention of Adversarial Lateral Movement*	M. A. R. A. Amin; S. Shetty; L. Njilla; D. K. Tosh; C. Kamhoua	0
2021	*Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack*	M. Dehghani; M. Ghiasi; T. Niknam; A. Kavousi-Fard; E. Tajik; S. Padmanaban; H. Aliev	2
2021	*Secure State Estimation and Control of Cyber-Physical Systems: A Survey*	D. Ding; Q. -L. Han; X. Ge; J. Wang	2
2021	*Real-Time Synchrophasor Data Anomaly Detection and Classification Using Isolation Forest, KMeans, and LoOP*	E. Khaledian; S. Pandey; P. Kundu; A. K. Srivastava	0
2021	*A Novel Deep Learning Based Automated Academic Activities Recognition in Cyber-Physical Systems*	M. Wasim; I. Ahmed; J. Ahmad; M. M. Hassan	0

Fonte: dos autores com base no IEEE *Xplore*.

Entre todas as palavras-chave presumíveis dos artigos, como *Cyber* (36 vezes) e *Systems* (19 vezes), a palavra Markov (4 vezes), considerada fora da temática de tecnologia digital, o que apresenta indício de utilização considerável de processo

determinístico como método de estudo. A Figura 2 evidencia em nuvem os destaques gerais.

Figura 2. Nuvem de palavras-chave destacadas nos artigos em estudo.

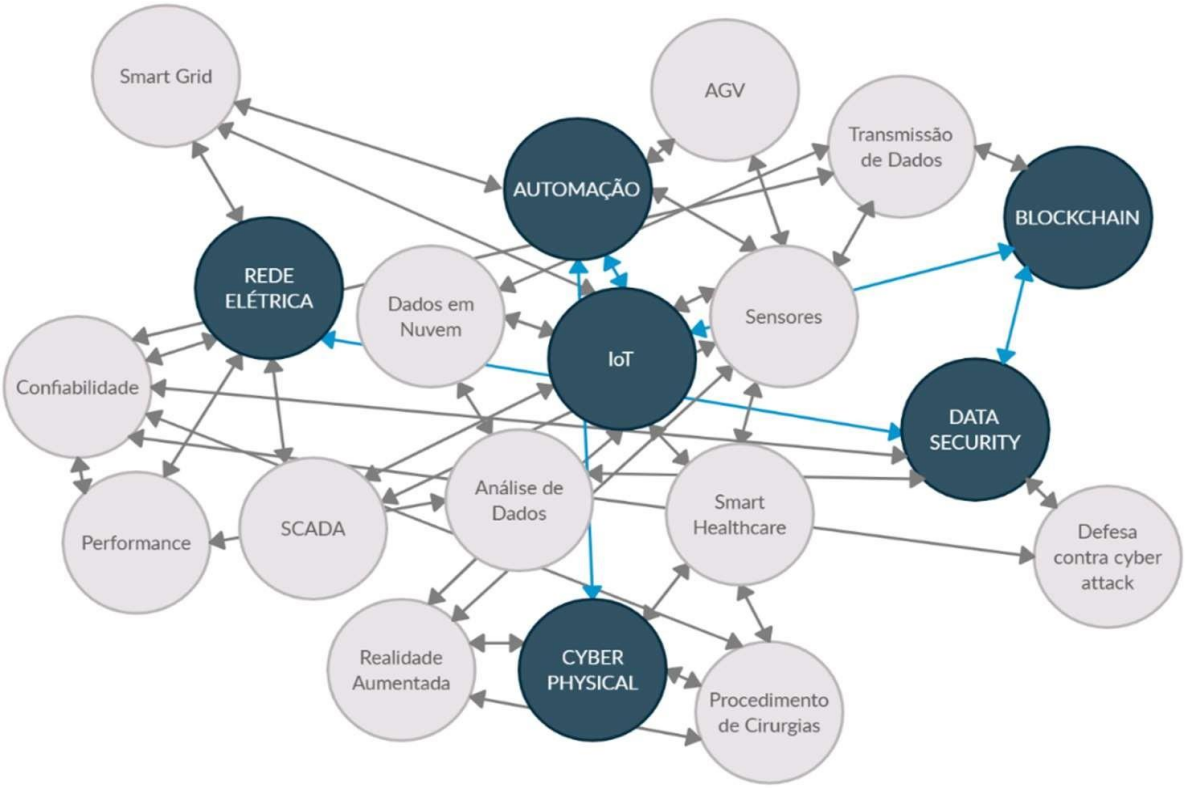
Fonte: dos autores

RAMIFICAÇÃO DO CONCEITO DE CYBER INFRASTRUCTURE

O emprego da infraestrutura cibernética pode ser manifestado em diversas áreas de aplicação interligadas umas com as outras. Essa infraestrutura forma uma malha conectando tecnologias e suas funcionalidades. Como pode ser observado na Figura 3, encontrou-se temas centrais destacados em bloco circular azul na como: (1) Rede Elétrica, (2) Automação, (3) IoT

(4) Cyber Physical, (5) Data Security e (6) Blockchain. A partir desses temas e motes principais ramificam-se subtemas como parte integrante da interligação dessa malha.

Figura 3. Suposição de mapa de ramificação e interligação da infraestrutura Cibernética.



Fonte: dos autores.

CONCLUSÕES

O emprego da Cyber infrastrucure não necessariamente encontra-se explícita à Quarta Revolução Industrial. Contudo faz parte integrante da Indústria 4.0 ao passo que engloba comunicação de dados, big data, machine learning, sensoriamento, análise de dados, integração e monitoramento entre sistemas. Essa infraestrutura propulsiona sistemas Cyber Physicals que contém o viés de complementar o raciocínio mental para alavancar a qualidade e expectativa de vida humana.

Nenhum artigo frisou diretamente o conceito global dessa infraestrutura, porém todos orbitaram pontos de Tecnologia de Informação e Comunicação (TIC) em comum. A maioria focou em descrever tratamento de cyber attack devido a frequente vinculação da palavra no campo de transmissão de dados. Na atualidade, os meios de interação de conhecimento e diálogo se tornam parte do sistema básico de cidade e comunidade inteligentes.

TRABALHOS FUTUROS

Entre possibilidade de trabalhos futuros encontram-se:

● Infraestrutura cibernética aplicada no E-Gov e na demogracia de Estado;

● Futuro da telecomunicação e utilização de dados móveis;

● Classificação de cidades de acordo com a infraestrutura cibernética.

REFERÊNCIAS

A. B. Fortes, J. Figueiredo and M. S. Lundstrom, "Virtual Computing Infrastructures for Nanoelectronics Simulation," in Proceedings of the IEEE, vol. 93, no. 10, pp. 1839-1847, Oct. 2005, doi: 10.1109/JPROC.2005.853545.

A. K. Srivastava, A. L. Hahn, O. O. Adesope, C. H. Hauser and D. E. Bakken, "Experience with a Multidisciplinary, Team-Taught Smart Grid Cyber Infrastructure Course," in IEEE Transactions on Power Systems, vol. 32, no. 3, pp. 2267-2275, May 2017, doi: 10.1109/TPWRS.2016.2611588.

C. Rieger, K. Schultz, T. Carroll and T. McJunkin, "Resilient Control Systems—Basis, Benchmarking and Benefit," in IEEE Access, vol. 9, pp. 57565-57577, 2021, doi: 10.1109/ACCESS.2021.3071874.

C. Vellaithurai, A. Srivastava, S. Zonouz and R. Berthier, "CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures," in IEEE Transactions on Smart Grid, vol. 6, no. 2, pp. 566-575, March 2015, doi: 10.1109/TSG.2014.2372315.

D. Chen et al., "Fast and Scalable Multi-Way Analysis of Massive Neural Data," in IEEE Transactions on Computers, vol. 64, no. 3, pp. 707-719, March 2015, doi: 10.1109/TC.2013.2295806.

D. Ding, Q. -L. Han, X. Ge and J. Wang, "Secure State Estimation and Control of Cyber- Physical Systems: A Survey," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 51, no. 1, pp. 176-190, Jan. 2021, doi: 10.1109/TSMC.2020.3041121.

D. J. S. Cardenas, A. Hahn and C. -C. Liu, "Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations," in IEEE Access, vol. 8, pp. 61161-61173, 2020, doi: 10.1109/ACCESS.2020.2983313.

E. A. Baran, A. Kuzu, S. Bogosyan, M. Gokasan and A. Sabanovic, "Comparative Analysis of a Selected DCT-Based Compression Scheme for Haptic Data Transmission," in IEEE Transactions on Industrial Informatics, vol. 12, no. 3, pp. 1146-1155, June 2016, doi: 10.1109/TII.2016.2555982.

E. Khaledian, S. Pandey, P. Kundu and A. K. Srivastava, "Real-Time Synchrophasor Data Anomaly Detection and Classification Using Isolation Forest, KMeans, and LoOP," in IEEE Transactions on Smart Grid, vol. 12, no. 3, pp. 2378-2388, May 2021, doi: 10.1109/TSG.2020.3046602.

F. G. Hamza-Lup, A. P. Santhanam, C. Imielinska, S. L. Meeks and J. P. Rolland, "Distributed Augmented Reality With 3-D Lung Dynamics—A Planning Tool Concept," in IEEE Transactions on Information Technology in Biomedicine, vol. 11, no. 1, pp. 40-46, Jan. 2007, doi: 10.1109/TITB.2006.880552.

K. C. P. Jordão. Cidades Inteligentes: uma proposta viabilizadora para a transformação das cidades brasileiras. Dissertação (Mestrado) – Pontifícia Universidade Católica de Campinas. São Paulo, 2016.

H. Jia, C. Shao, D. Liu, C. Singh, Y. Ding and Y. Li, "Operating Reliability Evaluation of Power Systems with Demand-Side Resources Considering Cyber Malfunctions," in IEEE Access, vol. 8, pp. 87354-87366, 2020, doi: 10.1109/ACCESS.2020.2992636.

H. Lin, Z. T. Kalbarczyk and R. K. Iyer, "RAINCOAT: Randomization of Network Communication in Power Grid Cyber Infrastructure to Mislead Attackers," in IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 4893-4906, Sept. 2019, doi: 10.1109/TSG.2018.2870362.

H. Pieterse, M. Olivier and R. van Heerden, "Evaluation Framework for Detecting Manipulated Smartphone Data," in SAIEE Africa Research Journal, vol. 110, no. 2, pp. 67-76, June 2019, doi: 10.23919/SAIEE.2019.8732797.

IEEE Xplore. Disponível em: <https://ieeexplore.ieee.org>. Acesso em 15 maio 2021.

J. A. Kassem, C. De Laat, A. Taal and P. Grosso, "The EPI Framework: A Dynamic Data Sharing Framework for Healthcare Use Cases," in IEEE Access, vol. 8, pp. 179909-179920, 2020, doi: 10.1109/ACCESS.2020.3028051.

J. O. Eichenhofer, E. Heymann, B. P. Miller and A. Kang, "An In-Depth Security Assessment of Maritime Container Terminal Software Systems," in IEEE Access, vol. 8, pp. 128050- 128067, 2020, doi: 10.1109/ACCESS.2020.3008395.

J. Zhang and A. D. Domínguez-García, "On the Impact of Measurement Errors on Power System Automatic Generation Control," in IEEE Transactions on Smart Grid, vol. 9, no. 3, pp. 1859-1868, May 2018, doi: 10.1109/TSG.2016.2601149.

K. Marashi, S. S. Sarvestani and A. R. Hurson, "Consideration of Cyber-Physical Interdependencies in Reliability Modeling of Smart Grids," in IEEE Transactions on Sustainable Computing, vol. 3, no. 2, pp. 73-83, 1 April-June 2018, doi: 10.1109/TSUSC.2017.2757911.

K. R. Davis et al., "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," in IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2464-2475, Sept. 2015, doi: 10.1109/TSG.2015.2424155.

M. A. R. A. Amin, S. Shetty, L. Njilla, D. K. Tosh and C. Kamhoua, "Hidden Markov Model and Cyber Deception for the Prevention of Adversarial Lateral Movement," in IEEE Access, vol. 9, pp. 49662-49682, 2021, doi: 10.1109/ACCESS.2021.3069105.

M. Dehghani et al., "Cyber Attack Detection Based on Wavelet Singular Entropy in AC Smart Islands: False Data Injection Attack," in IEEE Access, vol. 9, pp. 16488-16507, 2021, doi: 10.1109/ACCESS.2021.3051300.

M. Rahnamay-Naeini and M. M. Hayat, "Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach," in IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 1997-2006, July 2016, doi: 10.1109/TSG.2016.2539823.

M. Wasim, I. Ahmed, J. Ahmad and M. M. Hassan, "A Novel Deep Learning Based Automated Academic Activities Recognition in Cyber-Physical Systems," in IEEE Access, vol. 9, pp. 63718-63728, 2021, doi: 10.1109/ACCESS.2021.3073890.

P. Pradhan and P. Venkitasubramaniam, "Stealthy Attacks in Dynamical Systems: Tradeoffs Between Utility and Detectability with Application in Anonymous Systems," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 779-792, April 2017, doi: 10.1109/TIFS.2016.2607695.

P. Ramanan, M. Yildirim, E. Chow and N. Gebraeel, "An Asynchronous, Decentralized Solution Framework for the Large Scale Unit Commitment Problem," in IEEE Transactions on Power Systems, vol. 34, no. 5, pp. 3677-3686, Sept. 2019, doi: 10.1109/TPWRS.2019.2909664.

Q. Wang, M. Li, Y. Tang and M. Ni, "Source-Load Coordinated Reserve Allocation Strategy Considering Cyber-Attack Risks," in IEEE Access, vol. 7, pp. 111332-111340, 2019, doi: 10.1109/ACCESS.2019.2934646.

R. K. Lenka et al., "Building Scalable Cyber-Physical-Social Networking Infrastructure Using IoT and Low Power Sensors," in IEEE Access, vol. 6, pp. 30162-30173, 2018, doi: 10.1109/ACCESS.2018.2842760.

R. Kateb, P. Akaber, M. H. K. Tushar, A. Albarakati, M. Debbabi and C. Assi, "Enhancing WAMS Communication Network Against Delay Attacks," in IEEE

Transactions on Smart Grid, vol. 10, no. 3, pp. 2738-2751, May 2019, doi: 10.1109/TSG.2018.2809958.

R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, "Analyzing the Cyber- Physical Impact of Cyber Events on the Power Grid," in IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2444-2453, Sept. 2015, doi: 10.1109/TSG.2015.2432013.

S. Andalam, D. J. X. Ng, A. Easwaran and K. Thangamariappan, "Contract-Based Methodology for Developing Resilient Cyber-Infrastructure in the Industry 4.0 Era," in IEEE Embedded Systems Letters, vol. 11, no. 1, pp. 5-8, March 2019, doi: 10.1109/LES.2018.2801360.

S. Nativi, M. Craglia and J. Pearlman, "Earth Science Infrastructures Interoperability: The Brokering Approach," in IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 6, no. 3, pp. 1118-1129, June 2013, doi: 10.1109/JSTARS.2013.2243113.

S. Sridhar, A. Hahn and M. Govindarasu, "Cyber–Physical System Security for the Electric Power Grid," in Proceedings of the IEEE, vol. 100, no. 1, pp. 210-224, Jan. 2012, doi: 10.1109/JPROC.2011.2165269.

S. Xu, Y. Qian and R. Q. Hu, "Data-Driven Edge Intelligence for Robust Network Anomaly Detection," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 3, pp. 1481- 1492, 1 July-Sept. 2020, doi: 10.1109/TNSE.2019.2936466.

T. R. B. Kushal, K. Lai and M. S. Illindala, "Risk-Based Mitigation of Load Curtailment Cyber Attack Using Intelligent Agents in a Shipboard Power System," in IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 4741-4750, Sept. 2019, doi: 10.1109/TSG.2018.2867809.

V. V. G. Krishnan et al., "Resilient Cyber Infrastructure for the Minimum Wind Curtailment Remedial Control Scheme," in IEEE Transactions on Industry Applications, vol. 55, no. 1, pp. 943-953, Jan.-Feb. 2019, doi: 10.1109/TIA.2018.2868257.

V. Venkataramanan, P. S. Sarker, K. S. Sajan, A. Srivastava and A. Hahn, "Real-Time Federated Cyber-Transmission-Distribution Testbed Architecture for the Resiliency Analysis," in IEEE Transactions on Industry Applications, vol. 56, no. 6, pp. 7121-7131, Nov.-Dec. 2020, doi: 10.1109/TIA.2020.3023669.

X. Lou, D. K. Y. Yau, H. H. Nguyen and B. Chen, "Profit-Optimal and Stability-Aware Load Curtailment in Smart Grids," in IEEE Transactions on Smart Grid, vol. 4, no. 3, pp. 1411-1420, Sept. 2013, doi: 10.1109/TSG.2013.2249672.

Y. Du et al., "A Distributed Message Delivery Infrastructure for Connected Vehicle Technology Applications," in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 3, pp. 787-801, March 2018, doi: 10.1109/TITS.2017.2701799.

Z. An, H. Zhu, X. Li, C. Xu, Y. Xu and X. Li, "Nonidentical Linear Pulse-Coupled Oscillators Model With Application to Time Synchronization in Wireless Sensor Networks," in IEEE Transactions on Industrial Electronics, vol. 58, no. 6, pp. 2205-2215, June 2011, doi: 10.1109/TIE.2009.2038407.

Z. Dong, F. Luo and G. Liang, "Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems," in Journal of Modern Power Systems and Clean Energy, vol. 6, no. 5, pp. 958-967, September 2018, doi: 10.1007/s40565-018-0418-0.

Recebido em: 03/05/2022

Aprovado em: 05/06/2022

Publicado em: 08/06/2022