Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 00 (2024) 000–000

Procedia
Computer Science

www.elsevier.com/locate/procedia

The 14th International Conference on Sustainable Energy Information Technology
August 5-7, 2024, Marshall University, Huntington, WV, USA

Survey of Cybersecurity in Smart Grids Protocols and Datasets

Mamdouh Muhammad*, Abdullah S. Alshra‘a, Reinhard German

Computer Science 7
Friedrich-Alexander-Universitat, Martensstrasse 3, Erlangen, 91058, Germany
{*mamdouh.muhammad, abdullah.alshraa, reinhard.german*}@*fau.de*

Abstract

Smart grids are two-way communications grids that converge Information Technology (IT) and Operational Technology (OT) to transfer energy-related information between different industry components within the grid. Smart grids have changed the energy sector by increasing sustainability, efficiency and integrating renewable energy sources. However, smart grids are vulnerable to IT-related attacks because they rely on Information and Communication Technology (ICT). By surveying relevant papers and evaluating accessible statistics, this study explores cybersecurity in smart grids by examining current communication protocols and standards. We carefully compile various datasets with general information about four of the most smart grid-related datasets. Our study and conclusions address the key components of a smart grid and offer information that can help create cybersecurity plans specifically for smart grids. This research contributes to the discourse on smart grid security, which is important for preserving the stability of contemporary energy systems.

Keywords: Cyber-Physical Systems; cybersecurity; Information Technology; IT/OT convergence; smart grids.

1. Introduction

Despite the spread of conventional/traditional power grids worldwide, they suffer from many disadvantages; they are only one-way communication power grids typically consisting of four phases (Generation, Transmission, Distribution, and Consumption.) In the generation phase, conventional power resources exist, like thermal and nuclear power plants (NPP). Transmission aims to transport the generated power through high-voltage (HV) transmission lines with different voltage values. Stepping up the voltage in the transmission phase is needed to reduce the power loss due to the typical long length of the transmission lines. In distribution, stepping-down transformers decrease the

[*] Corresponding author. Tel.: +49 9131 85-27026 ; fax: +49 9131 85-27409.
E-mail address: mamdouh.muhammad@fau.de

voltage and distribute the received power to the customers. In consumption, the customers receive power with suitable voltage values. The consumption rates are shown at customers' homes using conventional meters, which provide no control or smart monitoring. Smart grids are two-way communication power grids that integrate both conventional and renewable energy resources, which leads to better power delivery and higher customer satisfaction. The following are the drawbacks of the conventional power grids compared to the smart grids:

1. Exposure to blackouts due to industrial faults or natural disasters, like in 2020 in Bavaria, Germany when more than 50,000 homes were left without electricity due to the Sabine storm [1].
2. Limited visibility due to the one-way power delivery hinders data acquisition and systems automation. In addition, it also leads to slow fault responses due to the absence of a comprehensive overview of the grid.
3. High environmental pollutants emissions of carbon monoxide (CO), sulfur dioxide (SO_2), and particulate matter (PM2.5) contribute to global warming and have a detrimental impact on the environment. [2].
4. Last but not least, customers consume power, resulting in higher bills than prosumers in smart grids, who consume, produce, and share leftover energy with the grid and other users [3].

This paper seeks to answer the following research questions:

1. Which smart grid protocols should we prioritize based on their usability and popularity?
2. How comprehensive are the datasets available for supporting smart grid cybersecurity?

The rest of this paper is organized as follows: Section 2 refers to some of the related previous works, and Section 3 introduces an overview of the smart grid communication protocols and standards. In section 4, an overview of the popular datasets with analysis of their content and more. The paper's discussion, future directions, and conclusion are in sections 5, 6, and 7, respectively.

2. Related work

This section discusses works in the literature that survey smart grid protocols and datasets. For instance, in [4], the authors compared the smart grid protocols and the existing smart grid datasets. The paper highlighted the differences between four main smart grid protocols and five datasets. However, this paper lacks many modern datasets covering network security in general and smart grid cybersecurity in particular. Chren et al. [5] explored the structure of smart grids in software reliability engineering, sorting datasets into categories like loss of loading probability, power distribution, and hardware. However, the paper has limited generalizability of its findings because evaluating datasets for reliability quantification in smart grids can differ depending on the grid's specific configuration and the technologies used. Wang et al. [6] presents the challenges and applications of analyzing data from smart meters to improve grid operations. Iqbal et al. [7] critically assessed Non-Intrusive Load Monitoring (NILM) datasets, detailing their characteristics without exploring their practical uses. Pereira and Nunes [8] reviewed performance evaluation in NILM, concentrating on datasets, metrics, and tools. Kazmi et al. [9] investigated data-driven approaches to energy communities, stressing the importance of using data to create sustainable energy solutions. Meinecke et al. [10] concentrate on the public datasets imported from distribution and transmission grids.

3. Smart grid communication protocols and standards

Most ICS communication protocols were designed traditionally to be air-gapped from the Internet and used in isolated or closed environments, i.e., offline-designed. The needed future integration/convergence between the ICS/OT systems and the Internet was not considered then, and the strict security border between ICS/OT and IT networks is no longer possible. This implies that the ICS networks are susceptible to cybersecurity attacks and need security countermeasures to detect and mitigate such attacks.
This section explores the seven most widely used and practical protocols in smart grid networks [11] [12] [13].
Table 1 summarizes them and more protocols and standards, considering that the scope parameter means the main usage scope of this protocol or standard [14].

Table 1. Summarization of Smart Grid Protocols (P) / Standards (S)

Protocol/Standard	**Scope**	**Description**	**Between**
IEC 60870-104 (P)	ICS	Telecontrol protocol for SCADA systems and RTUs.	Substations, SCADA systems
IEC 61850 (S)	ICS	Standard for power utility automation networks.	IEDs, SCADAs
Modbus (P)	ICS	Industrial communication protocol for PLCs.	PLCs, industrial sensors
S7Comm (P)	ICS	Siemens proprietary communication protocol for PLCs.	PLCs, industrial controllers
IEEE 1815 (DNP3) (P)	ICS	Communications protocol for process automation systems.	SCADA master stations, RTUs
IEC 62351 (S)	IT	Standards for securing communication protocols in power systems.	Substations, control centers
IEC 62443 (S)	IT	Standard for cybersecurity of industrial automation and control systems.	Industrial networks, control systems
IEEE C37.118 (S)	ICS	Standard for synchrophasor data transfer in power systems.	PMUs, data concentrators
IEEE 2030.5 (SEP2) (S)	IT	Standard for communication between utility companies and end-user devices.	Utility companies, end-user devices
OpenADR (S)	IT	Standard for automated demand response in electricity grids.	Utility companies, end-user devices
IEC 62056-21 (P)	ICS	Communication protocol for meter reading in smart grids.	Smart meters, data concentrators
IEC 61400-25 (P)	ICS	Communication protocol for wind power plants and control systems.	Wind power plants, control systems
IEEE 802.15.4 (S)	IT	Standard for low-rate wireless personal area networks.	Smart meters, home area networks
Zigbee (P)	IT	Communication protocol for low-power, low-data-rate wireless networks.	Smart meters, home area networks
Wi-SUN (S)	IT	Communication standard for outdoor, large-scale wireless networks.	Smart meters, distribution automation devices
CoAP (P)	IT	Lightweight protocol for IoT devices in smart grids.	Smart grid devices, control systems
MQTT (P)	IT	Messaging protocol for machine-to-machine communication in smart grids.	Smart grid devices, data management systems

1. **IEC 60870–5-104 (IEC104):** IEC104 is part of the IEC 60870 suite of standards, mainly focusing on telecontrol communication protocols in electrical substations. IEC 104 extends the capabilities of the IEC 60870-5-101 (IEC 101) protocol by using data packets. This extension facilitates communication between the SCADA system or controlling/master station and the substation or controlled/slave station over a standard TCP/IP network, typically using port 2404 [15]. IEC104 's most crucial feature is allowing simultaneous multi-transmission connections between the stations. It is worth mentioning that although it is considered an extension of the IEC101 protocol, it limits many parameters and fields, such as discarding the unbalanced and balanced transmission modes [12]. Although there are benefits to using IEC104, it lacks many paramount features, such as the encryption of data transmission, as it happens in clear text. This clear text transmission makes the network susceptible to attacks like Man-in-the-Middle (MITM) or False Data Injection (FDI)[16].
2. **IEC 61850:** is an international standard defining substation automation communication protocols. The primary objective behind this standard is to define unified protocols for an entire substation to ensure optimal

compatibility and seamless integration with vendor-neutral systems and devices. Besides being used in SCADA systems, IEC 61850 utilizes various mapped secure communication protocols between SCADA systems and IEDs/RTUs like circuit breakers or smart meters. IEC 61850 is mapped to protocols like:

- Generic Object-Oriented Substation Events (GOOSEs), which are primarily widely used for exchanging data between Intelligent Electronic Devices (IEDs), tailored to suit time-critical applications and operate in the publish-subscribe model,
- Manufacturing Message Specifications (MMSs) also aim to exchange data between IEDs but is generally used for less time-sensitive applications and operate in a client-server model, and
- Sampled Values (SV) facilitate the transfer of analog measurements, such as voltage and current, as digital data streams.

One of the main goals behind designing IEC 61850 is to ensure interoperability between different vendors, but this was done without considering the security risks or taking the appropriate procedures to ensure safe data transmission [12], [17], [18]. In addition, Cyberattacks like web attacks have been recorded due to the mapping of IEC 61850 over DWPS web service [19].

3. **Modbus:** is a broadly used client/server request/reply serial communication protocol within industrial communication systems that facilitates data exchange among industrial devices, such as PLCs, motors, and actuators. Modbus operates at the L7 of the OSI model and is available in many variants, such as Modbus RTU, Modbus ASCII, and Modbus TCP/IP. Modbus TCP/IP is not more than Modbus RTU, which has a TCP interface that uses Ethernet to transfer Modbus messages. Modbus TCP/IP Application Data Unit (ADU) is a 7-byte header that typically uses port 502. Although Modbus is considered the de facto protocol in ICS systems, it has many essential security gaps, such as the absence of encryption and authentication [20].
4. **S7 Communication Protocol (S7Comm):** is a proprietary communication protocol developed by Siemens to exchange S7 messages between Siemens step7 family Programmable Logic Controllers (PLCs) as servers and other ICS devices like Human Machine Interfaces (HMIs) and Supervisory Control And Data Acquisition (SCADA) systems as clients. Siemens models that use such protocols are S7-200 and S7-300. S7comm lacks encryption and is prone to session hijacking, replay attacks, session stealing, and other attacks [21], [22]. Due to the security gaps on s7comm and other aspects, a newer encrypted protocol called S7CommPlus has been developed to defend against replay attacks.
5. **IEEE 1815 (DNP3):** Developed by Westronics in Canada, Distributed Network Protocol version 3 (DNP3) is a prominent, highly reliable industrial communication protocol. It was designed to be used between the enterprise-level control stations (like SCADA/HMI as masters) and control-level outstations (like PLC/RTU as slaves). Many vital contributors to its reliability are using cyclical redundancy checks (CRC), the support of time-stamped data, and quality flags. Although DNP3 is competently suited and highly reliable for real-time data transfer, it suffers from many security concerns, like the default absence of authentication and encryption. DoS and MITM attacks represent two prevailing threats targeting DNP3 networks, intending to compromise the availability security aspect (in the case of the former) and the CIA security aspects (In the case of the latter) of either the control station or the outstation [23] and [24].
   It is worth mentioning that many versions have been released to enhance the security measures of DNP3, like DNP3 Secure Authentication (DNP3-SA), which fills the aforementioned security gaps [25] and [26].
6. **IEC 62351:** is a suite of standards to address key requirements of industrial automation and control systems (IACS) cybersecurity. It's particularly relevant for the smart grid, which heavily relies on information technology (IT) for efficient operation [27]. IEC 62351 is divided into various parts like IEC 62351-3, which defines the security for TCP/IP-based communications; IEC 62351-4, which covers MMS protocol authentication; and IEC 62351-5, which defines security specifications for IEC 60870-5.
7. **IEC 62443:** While IEC 62351 focuses on the communication security of protocols within energy and power systems, IEC 62443 is a broader framework focusing on the whole IACS cybersecurity. IEC 62443 handles the lifecycle for secure development, develops defense-in-depth strategies, manages vulnerabilities, and guides manufacturers in designing and maintaining secure industrial automation devices [28].
   The standard is organized into four major categories:

(a) **General Requirements:** outlines basic concepts and terminology and providing foundational guidance.
(b) **Policies and Procedures:** addresses the governance aspects of industrial systems cybersecurity, including roles and responsibilities, security management, risk assessment, and organizational practices.
(c) **System Integration:** focuses on the secure design, integration, and operation of ICS and includes guidance on secure architecture design, network segmentation, and defense-in-depth techniques.
(d) **Component Requirements:** provides requirements for individual components used within IACS, such as programmable logic controllers (PLCs), HMIs, and other industrial network devices.

4. Smart grids datasets

Here, we briefly overview them to learn more about their content and relevancy with smart grids. The order of the datasets is descending from the newest to the oldest, considering just four datasets.

1. **CIC Modbus Dataset:** was published in 2023 and includes both benign and attack traffic of the Modbus protocol. The dataset has network captures in PCAP format and Logs in CSV format. It was created using a simulated testbed, and traffic was captured using Wireshark. The dataset represents the captured Modbus protocol communication between SCADA HMIs and IEDs.
2. **DNP3 Intrusion Detection Dataset:** was published in 2022 and included both benign and attack traffic of the Modbus protocol. The dataset has both network captures in PCAP and CSV format. It was created using a simulated testbed, and traffic was captured using Wireshark. The dataset represents the captured DNP3 protocol communication between MTUs and outstations/slaves. It contains the traffic that covers 9 DNP3 cyberattacks with a focus on DoS and unauthorized command attacks.
   The hardware setup consists of one HMI, eight industrial entities, and three attackers, lasting 4 hours for each attack. Nmap and Scapy penetration testing tools have been used to launch the attacks. The TCP/IP and DNP3 network flow statistics were produced using CICFlowMeter and DNP3 Python Parser, respectively. The attacks included in this dataset are Disable Unsolicited Messages Attacks, Cold Restart Attacks, Warm Restart Attacks, Enumerate Attacks, Info Attacks, Initialize Data Attacks, MITM DoS, Replay Attacks, and Stop Application Attacks.
3. **ICS Dataset For Smart Grid Anomaly Detection:** as published in 2022 and includes both benign and attack traffic of the IEC104 and MMS protocols. The dataset has both network captures in PCAP and CSV format. It was created partly by real ICS devices and partly by a simulated testbed, and traffic was captured using Wireshark. The attacks included in this dataset are, for example, scanning and switching attacks.
4. **Electra Dataset:** was published in 2019 and includes benign and attack traffic. It has both network captures in CSV format. It was created using a real-time scenario, and traffic was captured using Wireshark. The dataset represents the captured Modbus and S7Comm industrial protocol between SCADA and PLCs. It contains traffic that covers reconnaissance, False data injection, and replay attacks.

The previous datasets and more are summarized in Table 2 highlighting informative information like the release date, the protocols, and the number of features.

5. Discussion

The survey findings indicate that to advance the field of smart grid cybersecurity, a more explicit and comprehensive understanding of smart grid topologies, methodologies, and related protocols or standards is required. Specifically, there needs to be clarity on how these seven protocols interact within the broader context of smart grid security. A significant observation from this survey is that existing datasets related to smart grids are outdated or irrelevant, often lacking real-time traffic data that accurately reflects the actual modern smart grid environments.

Additionally, the current number of surveys addressing smart grid cybersecurity is insufficient to meet the growing demand in this research domain. Only the Electra dataset is considered a real-time generated dataset from all four mentioned datasets. Further comparisons between it and other datasets are needed to ensure that this real-time advantage benefits the research area.

Table 2. Summarization of Smart Grids Datasets

Dataset	Release	Size	Data Format	Protocols	Features
CIC Modbus [29]	2023	3.6 GB	PCAP & CSV	Modbus	-
DNP3 Intrusion Detection [30]	2022	0.185 GB	PCAP & CSV	DNP3	84 (CIC) & 101 (Parser)
ICS for Smart Grid Anomaly Detection [31]	2022	0.115 GB	PCAP & CSV	IEC 61850 (MMS) & IEC 104	13-15
Electra [32]	2019	1.756 GB	PCAP & CSV	Modbus & S7comm	11
CIC-DDoS2019 [33]	2019	24.417 GB	PCAP & CSV	TCP/UDP-based protocols	88
Modbus for ICS Anomaly Detection [34]	2022	0.595 GB	PCAP & CSV	Modbus/TCP	N/A
IEC 60870-5-104 ID dataset [35]	2023	1.01 GB	PCAP & CSV	IEC 60870-5-104	84
CIC-IDS-2017 [36]	2017	51.1 GB	PCAP & CSV	HTTP, SSH, FTP (. . .)	80
UNSW-NB15 [37]	2015	102 GB	Argus, BRO, PCAP & CSV	TCP, UDP, ICMP, and others	49
ISCX NSL-KDD [38]	2009	-	ARFF & CSV	TCP/UDP/ICMP-based protocols	42
KDD Cup [38]	1999	743 MB	ARFF & CSV	TCP/UDP/ICMP-based protocols	42
Mississippi State University's SCADA Lab [39]	2015	-	ARFF & CSV	-	20
TON_IoT (4 different datasets) [40]	2019	67.7 GB	LOG, TXT, PCAP & CSV	-	Multivalued
BoT-IoT [41]	2018	≈ 137 GB	Argus, PCAP, & CSV	TCP/UDP-based protocols	45
CIC IoT [42]	2023	≈ 400 GB	PCAP & CSV	-	47
SWAT (A1&A2) [43]	2016	4.5 GB	CSV	Physical processes information	18
ICS-Flow [44]	2022	2 GB	PCAP & CSV	Modbus	54
BCCC-VulSCs-2023 [45]	2023	-	PCAP & CSV	TCP-based protocols	300

6. Future directions

In future research, researchers should focus on connecting smart grid protocols, datasets, and known attacks. This approach would help ensure that when investigating a particular smart grid attack, corresponding datasets exist that contain relevant attack information that targets specific smart grid protocols or standards.

As most of the available smart grid cybersecurity datasets are based on simulated testbeds, there is an urgent need to create modern, balanced, real-time datasets that mirror the actual smart grid operational environments. This would enable more accurate research and testing of cybersecurity measures.

Further research can be done to compare the current smart grid cybersecurity simulation testbed and highlight the advantages and disadvantages of each one with insights on how to improve them to match the real scenarios as much as possible.

Finally, it is worth exploring the suitability of using the current cybersecurity smart grid datasets in advanced technologies like Digital Twins, blockchain, and large language models (LLMs) to take advantage of the convergence of these advanced technologies. Digital Twins offer real-time, data-driven insights into physical systems, blockchain guarantees secure and transparent transactions, and LLMs enable advanced data analysis and automation.

7. Conclusion

This paper examined widely used Industrial Control System (ICS) protocols and standards, emphasizing the seven most relevant to smart grids cybersecurity. Specifically, we discussed how these protocols and standards manage communication and control functions within the smart grid, ensuring energy systems' secure and reliable operation. Our review included the identification of core protocols and standards, such as DNP3, IEC 61850, and Modbus, highlighting their value in the ICS systems.

Additionally, we reviewed existing cybersecurity datasets, focusing on four current ones related to smart grids. These datasets are crucial for developing and testing new cybersecurity measures, providing researchers with a baseline for simulating attacks and developing defense mechanisms. Our analysis examined these datasets' relevance and scope, identifying which of the abovementioned are more promising for smart grid research and where improvements are needed.

References

[1] Crisis24, "Germany: Storm sabine leaves one dead, thousands without power as of february 10 /update 2," May 2024. [Online]. Available: https://crisis24.garda.com/alerts/2020/02/germany-storm-sabine-leaves-one-dead-thousands-without-power-as-of-february-10-update-2

[2] "Particulate matter-attributable mortality and relationships with carbon dioxide in 250 urban areas worldwide — ncbi.nlm.nih.gov," https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6689059/, [Accessed 15-04-2024].

[3] A. D. Rathnayaka, V. M. Potdar, and S. J. Kuruppu, "An innovative approach to manage prosumers in smart grid," in *2011 World Congress on Sustainable Technologies (WCST)*. IEEE, 2011, pp. 141–146.

[4] M. M. ALANI and T. BAKER, "A survey of smart grid intrusion detection datasets," *19th International Conference on Intelligent Environments (IE2023)*, 2023.

[5] S. Chren, B. Rossi, B. Bühnova, and T. Pitner, "Reliability data for smart grids: Where the real data can be found," in *2018 Smart City Symposium Prague (SCSP)*, 2018, pp. 1–6.

[6] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3125–3148, 2019.

[7] H. K. Iqbal, F. H. Malik, A. Muhammad, M. A. Qureshi, M. N. Abbasi, and A. R. Chishti, "A critical review of state-of-the-art non-intrusive load monitoring datasets," *Electric Power Systems Research*, vol. 192, p. 106921, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779620307197

[8] L. Pereira and N. Nunes, "Performance evaluation in non-intrusive load monitoring: Datasets, metrics, and tools—a review," *WIREs Data Mining and Knowledge Discovery*, vol. 8, no. 6, p. e1265, 2018. [Online]. Available: https://wires.onlinelibrary.wiley.com/doi/abs/10.1002/widm.1265

[9] H. Kazmi, I. Munné, F. Mehmood, T. Abbas, and J. Driesen, "Towards data-driven energy communities: A review of open-source datasets, models and tools," *Renewable and Sustainable Energy Reviews*, vol. 148, 06 2021.

[10] S. Meinecke, L. Thurner, and M. Braun, "Review of steady-state electric power distribution system datasets," *Energies*, vol. 13, no. 18, 2020. [Online]. Available: https://www.mdpi.com/1996-1073/13/18/4826

[11] J.-M. Flaus, *Cybersecurity of Industrial Systems*. ISTE Ltd, 2019.

[12] E. Kabalci and Y. Kabalci, Eds., *Smart Grids and Their Communication Systems*. Springer, 2019.

[13] E. D. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing security controls into the modern power infrastructure*. Elsevier, Syngress, 2013.

[14] G. R. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and Related Systems*. Elsevier, 2008.

[15] P. Matoušek, "Iec 104 protocol," Technical Report, 2017. [Online]. Available: https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf

[16] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for iec 60870-5-104 based scada networks," in *2013 IEEE Power Energy Society General Meeting*, 2013, pp. 1–5.

[17] M. S. Thomas and J. D. McDonald, Eds., *Power System SCADA and Smart Grids*. CRC Press, 2015.

[18] R. Mackiewicz, "Overview of iec 61850 and benefits," in *2006 IEEE PES Power Systems Conference and Exposition*, 2006, pp. 623–630.

[19] A. Elgargouri, R. Virrankoski, and M. Elmusrati, "Iec 61850 based smart grid security," in *2015 IEEE International Conference on Industrial Technology (ICIT)*, 2015, pp. 2461–2465.

[20] R. Nardone, R. J. Rodríguez, and S. Marrone, "Formal security assessment of modbus protocol," in *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2016, pp. 142–147.

[21] P. K. Oliver Eigner and P. Tavolato., "Identifying s7comm protocol data injection attacks in cyber-physical systems." pp. 51–56, 2018.

[22] W. Alsabbagh and P. Langendörfer, "A stealth program injection attack against s7-300 plcs," in *2021 22nd IEEE International Conference on Industrial Technology (ICIT)*, vol. 1, 2021, pp. 986–993.

[23] C. Irvene, T. Shekari, D. Formby, and R. Beyah, "If i knew then what i know now: On reevaluating dnp3 security using power substation traffic," ser. ICSS. Association for Computing Machinery, 2019, p. 48–59. [Online]. Available: https://doi.org/10.1145/3372318.3372324

[24] "IEEE Standards Association — standards.ieee.org," https://standards.ieee.org/ieee/1815/5414/, [Accessed 06-04-2024].

[25] I. Power and E. Society. (2012) Ieee standard for electric power systems communications—distributed network protocol (dnp3). [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6675752

[26] E. D. Knapp and R. Samani, *Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Syngress, 2015.

[27] "IEC 62351 - Cyber Security Series for the Smart Grid - SyC Smart Energy — syc-se.iec.ch," https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62351/, [Accessed 10-04-2024].

[28] D. Dolezilek, D. Gammel, and W. Fernandes, "Cybersecurity based on iec 62351 and iec 62443 for iec 61850 systems," in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, 2020.

[29] K. Boakye-Boateng, A. A. Ghorbani, and A. Lashkari, "Securing substations with trust, risk posture, and multi-agent systems: A comprehensive approach," in *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*. Los Alamitos, CA, USA: IEEE Computer Society, aug 2023, pp. 1–12. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/PST58708.2023.10320154

[30] P. Radoglou-Grammatikis, V. Kelli, T. Lagkas, V. Argyriou, and P. Sarigiannidis, "Dnp3 intrusion detection dataset," 2022. [Online]. Available: https://dx.doi.org/10.21227/s7h0-b081

[31] P. Matoušek, O. Ryšavý, and P. Grofčík, "Ics dataset for smart grid anomaly detection," 2022. [Online]. Available: https://dx.doi.org/10.21227/1trw-n685

[32] L. Perales Gómez, L. Fernández Maimó, A. Huertas Celdrán, F. J. García Clemente, C. Cadenas Sarmiento, C. J. Del Canto Masa, and R. Méndez Nistal, "On the generation of anomaly detection datasets in industrial control systems," *IEEE Access*, vol. 7, pp. 177 460–177 473, 2019.

[33] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in *2019 International Carnahan Conference on Security Technology (ICCST)*, 2019, pp. 1–8.

[34] O. Rysavy and P. Matousek, "Modbus dataset for ics anomaly detection," 2021. [Online]. Available: https://dx.doi.org/10.21227/e1bc-3w91

[35] P. Radoglou-Grammatikis, K. Rompolos, T. Lagkas, V. Argyriou, and P. Sarigiannidis, "Iec 60870-5-104 intrusion detection dataset," 2022. [Online]. Available: https://dx.doi.org/10.21227/fj7s-f281

[36] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *International Conference on Information Systems Security and Privacy*, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:4707749

[37] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6.

[38] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 2009, pp. 1–6.

[39] I. P. Turnipseed, *A new scada dataset for intrusion detection research*. Mississippi State University, 2015.

[40] N. Moustafa, "A new distributed architecture for evaluating ai-based security systems at the edge: Network ton_iot datasets," *Sustainable Cities and Society*, vol. 72, p. 102994, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210670721002808

[41] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset," *Future Generation Computer Systems*, vol. 100, pp. 779–796, 2019.

[42] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, 2023. [Online]. Available: https://www.mdpi.com/1424-8220/23/13/5941

[43] "itrust labs dataset info itrust itrust.sutd.edu.sg," https://itrust.sutd.edu.sg/itrust-labs_datasets/dataset_info/, [Accessed 20-04-2024].

[44] "Ics-flow — kaggle.com," https://www.kaggle.com/datasets/alirezadehlaghi/icssim, [Accessed 21-04-2024].

[45] M. Shafi, A. H. Lashkari, V. Rodriguez, and R. Nevo, "Toward generating a new cloud-based distributed denial of service (ddos) dataset and cloud intrusion traffic characterization," *Information*, vol. 15, no. 4, 2024. [Online]. Available: https://www.mdpi.com/2078-2489/15/4/195