Industrial Control Systems

Subjects: Engineering, Electrical & Electronic

Contributor: Hasan Alkahtani, Theyazn H. H. Aldhyani

Industrial control systems (ICSs) for critical infrastructure are extensively utilized to provide the fundamental functions of society and are frequently employed in critical infrastructure. Therefore, security of these systems from cyberattacks is essential.

Keywords: industrial control systems ; intrusion detection system

1. Introduction

In critical infrastructures that supply crucial services such as water, electricity, or communications, industrial control systems (ICSs) are at the heart of the operation. ICSs provide the foundational services for monitoring and controlling industrial operations. The monitoring section uses sensors to collect data, keep track of the processes, and ensure that they run properly [1]. On the one hand, the monitoring section oversees operations and ensures that they run correctly. On the other hand, the controlling portion manages the processes and makes decisions that cause actions to be carried out by actuators. If this workflow is disrupted as a result of technological difficulties or cyberattacks, many citizens may be adversely affected, for example, as a result of interruptions in electrical power or communications [2].

Information technology stacks (ITS) and remote connections are commonly used to link ICS components. An increase in the likelihood of deliberate assaults on physical plants might result from reliance on communication networks to transmit measurements. Authentication, data encryption, and message integrity procedures are just a few methods for keeping network traffic safe. Despite this, these solutions cannot defend all layers of an ICS network from all types of invasions of privacy [3].

Operational technology (OT) processes, which are critical components of infrastructure, are routinely targeted by criminal organizations. In the past, OT and information technology (IT) networks were kept separate or “air-gapped” from one another [4]. However, due to increased efficiency gained via digitalization, new business requirements are emerging, increasing the time and money spent on digitalization. However, due to digitalization’s increased efficiency, new business requirements are emerging, increasing the number of organizations using the technology [5]. Over the Internet of Things (IoT), sensor and actuator data, and multimedia data such as images and videos, are transmitted. It is vital to put security measures in place to protect against malicious behavior and cyber risks. On the one hand, cybersecurity approaches, which are critical to the long-term health of supply chains, are required to ensure the safety of workers and commodities and to protect information passing via their networks, among other things. On the other hand, a cyberattack on an ICS might result in a malfunction, which could cause physical harm to other physical components or even humans [6]. A cyberattack may result in the theft of confidential information about a company’s business activities; it may also have the unintended consequence of decreasing the degree of competitiveness of the industry in the long term. The percentage of malware threats to ICSs over the last four years is presented in **Figure 1**.

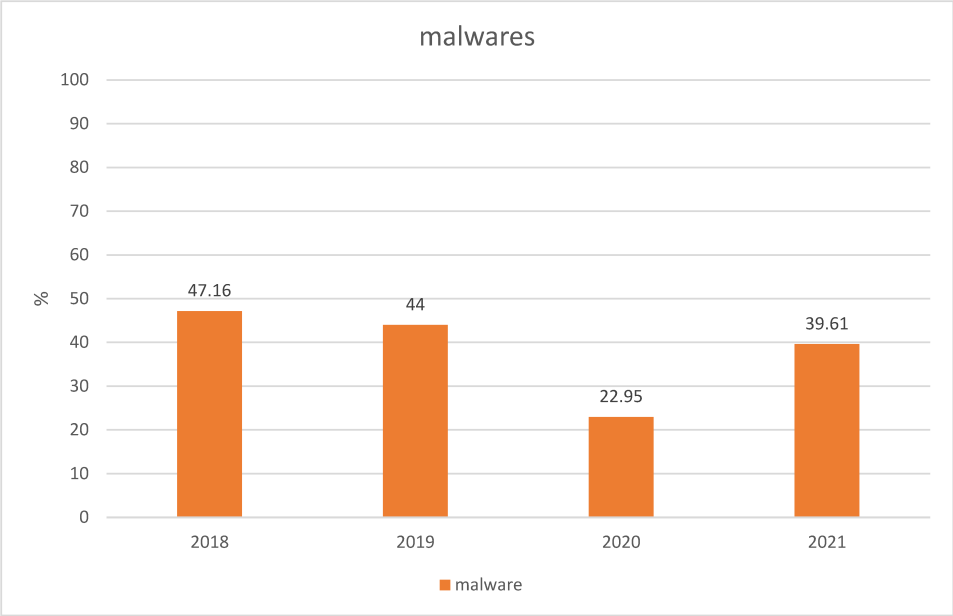

Figure 1. Malware threats to ICSs over the last four years.

An intrusion detection system (IDS) is one method of dealing with this problem. The detection methodologies used by signature-based and anomaly-based IDSs are distinct [7]. The signature-based technique instructs the system to seek specific anomalies. In contrast, the anomaly-based strategy instructs the system to look for any deviation from a previously defined standard of behavior. Most of the time, an IDS examines the network traffic of an ICS to detect irregularities in the incoming data packets. It is possible to safeguard a network from unwanted infiltration attempts by implementing a network intrusion detection system (NIDS), also known as packet filtering. The NIDS model utilized in various studies [8][9][10][11][12] was developed using machine learning approaches to detect network traffic intrusions. Because of its capacity to identify and quantify attacks in the network flow, even if its performance against encrypted data packets, fake IP packets, and regular false-positive alerts are not guaranteed, it is becoming increasingly popular.

Anomaly detection in industrial control systems (MADICSs) is a comprehensive technique for identifying abnormalities in ICSS and is presented as a solution. To detect cyber risks in ICSS, MADICSs seeks to provide a consistent and unified approach for comparing data, which any researcher can utilize to compare data from different sources. Although these processes are based on a standard machine learning/deep learning methodology [13][14], they have been tailored for industrial settings. They can deal with the unique challenges of these types of scenarios. The statistically significant relationship between the characteristics of an ICS and the repetitiveness of its actions is one of the peculiarities that distinguishes it from other scenarios, such as 5G networks [15] or clinical information systems [16].

2. Industrial Control Systems

Previous research has focused on detecting cyberattacks on ICSs, which has resulted in several publications. An IDS based on rules and deterministic finite automata (DFA) are two examples of this system. The majority of current research has focused on developing new approaches that have taken advantage of cutting-edge technologies, such as big data and machine learning/deep learning. A growing number of machine learning (ML) and deep learning (DL) approaches are being used to detect cyberattacks in the industrial sector. The most significant publications on ML and DL anomaly detection in industrial contexts are evaluated here [16].

Many academic ICSs use publicly available datasets to investigate ML algorithms, which is becoming increasingly common. The following are some of the drawbacks of the public database system in use today. The architecture proposed is limited to materials based on the Modbus/TCP protocol suite [17]. There was very little data acquired during online testing activities by [18], and only multi-ML algorithms were developed due to those activities. A similar issue existed in [19], where the database used was outdated and did not represent current threats. In contrast, the dataset in [20] was small (around 1000 occurrences) and was restricted to a single cyberattack. According to another report, the database was out of date and the assaults were linked to the field of IT [21]. The Singapore University of Technology developed a water treatment testbed that included supervisory control and data acquisition (SCADA) network traffic and assault scenarios for use in water treatment [22]. To train and test ML systems, real-time datasets, including common cyberattacks and 35 different types of cyberattacks, have recently been generated for training and testing ML systems. The only strategies that have been used to compare the performances of different algorithms are supervised ML techniques. The results have

shown that algorithms have a considerable probability of false detection, which is supported by the literature. The performance of ML algorithms on a public dataset may result in a decent output depending on the dataset [23]. However, the payload/data frame is controlled using dataset labels, and the assaults are manually randomized and parameterized to imitate the operational/attack situation [24].

Many DL and ML approaches have been reported in the literature, in addition to convolution neural network and long short-term memory (CNN-LSTM) networks. According to [25], unsupervised ML may be used to identify irregularities in cyber-physical systems (CPS). Among 23 methods, they tested deep neural networks (DNNs) and support vector machine (SVM) techniques, which were both designed specifically to work with time-series data. They used the test dataset's mean and standard deviation to scale the dataset to a new size. Autoencoders (AE) and 1D convolutional neural networks (CNN) were proposed in [26] as a DL approach for identifying ICS anomalies. Additionally, the authors recommended filtering features to choose those most suited for anomaly detection from among the DL models they presented. They developed a feature extraction method that used the discrete Fourier transform (DFT) to compute features in the frequency domain. When utilizing DFT to extract features, important information from the remaining signal was lost instead of using only the highest energy bands. In addition, they used a threshold for anomaly detection based on the test dataset's mean and standard deviation. Unsupervised anomaly detection was presented by the authors of [27] that focused on large-scale and real-time data processing. The three pillars of this strategy were update triggers, tree growth, and mass weighting methods. Thanks to this combination, random trees could be generated and updated in real time. They described the use of clustering analysis to reveal the dataset's underlying patterns for another unsupervised anomaly detection. Next, the researchers used cluster intra-distances and inter-distances to extract features from the clusters [28]. Finally, an inference method was used to determine whether an irregularity was sparked. The authors in [29] devised an unsupervised learning technique based on stacked denoising autoencoders. Because the original network stream was used in their solution, it did not require any special skills.

Furthermore, several surveys on IDSs have been conducted on IoT networks and their lightweight devices. Nevertheless, the majority of these surveys did not address the deployment of ML or DL approaches as detection mechanisms in IoT networks and their networks in any depth. In several recent studies, it was observed that the emphasis was on studying IoT security difficulties in general and categorizing them into multiple layers related to applications, network security, encryption, authentication, and access controls [30][31][32][33][34][35].

References

1. Oliver, E.; Philipp, K.; Tavolato, P. Identifying S7comm Protocol Data Injection Attacks in Cyber-Physical Systems. In Proceedings of the 2018 Proceedings of the 5th International Symposium for ICSS & SCADA Cyber Security Research, Hamburg, Germany, 29–30 August 2018.
2. Kargl, F.; van der Heijden, R.W.; König, H.; Valdes, A.; Dacier, M.C. Insights on the Security and Dependability of Industrial Control Systems. IEEE Secur. Priv. 2014, 12, 75–78.
3. Threats against Industrial Control Systems on the Rise in H2 2020, Growing by Nearly 8 Percentage Points in the Engineering Sector. Available online: https://www.kaspersky.com/about/press-releases/2021_threats-against-industrial-control-systems-on-the-rise-in-h2-2020 (accessed on 19 April 2022).
4. George, G.; Thampi, S.M. A Graph-Based Security Framework for Securing Industrial IoT Networks from Vulnerability Exploitations. IEEE Access 2018, 6, 43586–43601.
5. Fan, X.; Fan, K.; Wang, Y.; Zhou, R. Overview of cyber-security of industrial control system. In Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), Shanghai, China, 5–7 August 2015; pp. 1–7.
6. Jiang, B.; Yang, J.; Ding, G.; Wang, H. Cyber-physical security design in multimedia data cache resource allocation for industrial networks. IEEE Trans. Ind. Inform. 2019, 15, 6472–6480.
7. Wang, Y.; Meng, W.; Li, W.; Li, J.; Liu, W.X.; Xiang, Y. A fog-based privacy-preserving approach for distributed signature-based intrusion detection. J. Parallel Distrib. Comput. 2018, 122, 26–35.
8. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. 2019, 90, 101842.
9. Vinayakumar, R.; Alazab, M.; Soman, K.; Poornachandran, P.; Al-Nemrat, A.; Venkatraman, S. Deep learning approach for intelligent intrusion detection system. IEEE Access 2019, 7, 41525–41550.

10. Manzoor, I.; Kumar, N. A feature reduced intrusion detection system using ANN classifier. Expert Syst. Appl. 2017, 88, 249–257.
11. Miller, B.; Rowe, D. A survey SCADA of and critical infrastructure incidents. In Proceedings of the 1st Annual Conference on Research in Information Technology, Calgary, AB, Canada, 11–13 October 2012; pp. 51–56.
12. Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. SCADA security in the light of Cyber-Warfare. Comput. Secur. 2012, 31, 418–436.
13. Fernández Maimó, L.; Perales Gómez, A.L.; García Clemente, F.J.; Gil Pérez, M.; Martínez Pérez, G. A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. IEEE Access 2018, 6, 7700–7712.
14. Fernández Maimó, L.; Huertas Celdrán, A.; Gil Pérez, M.; García Clemente, F.J.; Martínez Pérez, G. Dynamic management of a deep learning-based anomaly detection system for 5G networks. J. Ambient Intell. Humaniz. Comput. 2019, 10, 3083–3097.
15. Fernández Maimó, L.; Huertas Celdrán, A.; Perales Gómez, A.L.; García Clemente, F.J.; Weimer, J.; Lee, I. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical environments. Sensors 2019, 19, 1114.
16. Goh, J.; Adepu, S.; Junejo, K.N.; Mathur, A. A Dataset to Support Research in the Design of Secure Water Treatment Systems. In Critical Information Infrastructures Security; Havarneanu, G., Setola, R., Nassopoulos, H., Wolthusen, S., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 88–99.
17. Almalawi, A.; Yu, X.; Tari, Z.; Fahad, A.; Khalil, I. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Comput. Secur. 2014, 46, 94–110.
18. Tomin, N.V.; Kurbatsky, V.; Sidorov, D.N.; Zhukov, A.V. Machine learning techniques for power system security assessment. In Proceedings of the IFAC Workshop on Control of Transmission and Distribution Smart Grids, Prague, Czech Republic, 11–13 October 2016; pp. 445–450.
19. Zaman, M.; Lung, C. Evaluation of machine learning techniques for network intrusion detection. In Proceedings of the IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; pp. 1–5.
20. Teixeira, M.A.; Salman, T.; Zolanvari, M.; Jain, R.; Meskin, N. SCADA system testbed for cybersecurity research using machine learning approach. Future Int. 2018, 10, 76.
21. Almseidin, M.; Alzubi, M.; Kovacs, S.; Alkasassbeh, M. Evaluation of machine learning algorithms for intrusion detection system. In Proceedings of the IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 14–16 September 2017; pp. 277–282.
22. Mathur, A.; Tippenhauer, N. SWaT: A water treatment testbed for research and training on ICSS security. In Proceedings of the International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater), Vienna, Austria, 11 April 2016; pp. 31–36.
23. Perez, R.L.; Adamsky, F.; Soua, R.; Engel, T. Machine learning for reliable network attack detection in SCADA systems. In Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy in Computing And Communications, New York, NY, USA, 1–3 August 2018; pp. 633–638.
24. Jicha, A.; Patton, M.; Chen, H. SCADA honeypots: An in-depth analysis of Conpot. In Proceedings of the IEEE Conference on Intelligence and Security Informatics (ISI), Tucson, AZ, USA, 28–30 September 2016; pp. 196–198.
25. Almomani, O. A hybrid model using bio-inspired metaheuristic algorithms for network intrusion detection system. Comput. Mater. Contin. 2021, 68, 409–429.
26. Kravchik, M.; Shabtai, A. Efficient cyber attacks detection in industrial control systems using lightweight neural networks. arXiv 2019, arXiv:1907.01216.
27. Liu, L.; Hu, M.; Kang, C.; Li, X. Unsupervised Anomaly Detection for Network Data Streams in Industrial Control Systems. Information 2020, 11, 105.
28. Tomlin, L.; Farnam, M.R.; Pan, S. A clustering approach to industrial network intrusion detection. In Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16), Huntsville, AL, USA, 30 September 2016.
29. Schneider, P.; Böttinger, K. High-performance unsupervised anomaly detection for cyber-physical system networks. In Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and Privacy, Toronto, ON, Canada, 19 October 2018; pp. 1–12.
30. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. Digit. Commun. Netw. 2018, 4, 118–137.
31. Keshk, M.; Moustafa, N.; Sitnikova, E.; Creech, G. Privacy preservation intrusion detection technique for SCADA systems. In Proceedings of the 2017 Military Communications and Information Systems Conference (MilCIS),

Canberra, Australia, 14–16 November 2017; pp. 1–6.

32. Zhao, K.; Ge, L. A survey on the internet of things security. In Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, China, 14–15 December 2013; pp. 663–667.
33. Kumar, J.S.; Patel, D.R. A survey on internet of things: Security and privacy issues. Int. J. Comput. Appl. 2014, 90.
34. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 3, pp. 648–651.
35. Kouicem, D.E.; Bouabdallah, A.; Lakhlef, H. Internet of things security: A top-down survey. Comput. Netw. 2018, 141, 199–221.