ADAPTIVE HIERARCHICAL CYBER ATTACK DETECTION AND LOCALIZATION IN ACTIVE DISTRIBUTION SYSTEMS

SAHIK IMRAN[1], HARSHITHA[2], CHANDANA[3], DIVIJA[4]

1ASSISTANT PROFESSOR, DEPARTMENT OF CSE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD.

2,3&4UG SCHOLAR, DEPARTMENT OF CSE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD

ABSTRACT

Recently, Cyber Physical System (CPS) is one of the core technologies for realizing Internet of Things (IoT). The CPS is a new paradigm that seeks to converge the physical and cyber worlds in which we live. However, the CPS suffers from certain CPS issues that could directly threaten our lives, while the CPS environment, including its various layers, is related to on-the-spot threats, making it necessary to study CPS security. Therefore, a survey-based in-depth understanding of the vulnerabilities, threats, and attacks is required of CPS security and privacy for IoT. In this paper, we analyze security issues, threats, and solutions for IoT-CPS, and evaluate the existing researches. The CPS raises a number challenges through current security markets and security issues. The study also addresses the CPS vulnerabilities and attacks and derives challenges. Finally, we recommend solutions for each system of CPS security threats, and discuss ways of resolving potential future issues.

INTRODUCTION The Cyber Physical System (CPS) is a new paradigm that pursues the convergence of physical and cyber spaces in which we live. It is a system that is tightly integrated in terms of scale and level with different cyber and physical systems. In the CPS, the cyber environment is a digital environment that is computed, communicated and managed by a world created by computer programs. The physical environment runs various sensors and the Internet of Things (IoT) in the course of time. As such, the CPS includes software, hardware, sensors, actuators, and embedded systems, and is connected to human-machine interfaces and multiple systems. A number of sensors, actuators, and control devices are connected by a network to form a complex system for acquiring, processing, calculating, and analyzing physical environment information and applying the results to the physical environment. The

CPS is a technology closely related to the IoT, and a next-generation network-based distributed control system that combines a physical system with sensors and actuators and a computing element that controls it. Therefore, it emphasizes that there are many interactions between the cyber and physical worlds as a result of the development of information and communication technology (ICT). Dependence on the CPS is gradually increasing in a variety of applications in the energy, transportation, medical and manufacturing sectors. The development of CPS technology is the key to improving the quality of life more efficiently than ever before, but the risks are becoming more and more acute in terms of security. In addition, the CPS has difficulty assessing threats and vulnerabilities caused by interactions, and new security issues are emerging. This complexity coupled with the heterogeneity of the CPS's components makes it difficult to guarantee the security and privacy of the CPS, and it is also difficult to identify, track, and examine the multiple components of the CPS and targeted attacks on them. Cyber-terrorists can attack real control systems as well as information security in virtual spaces such as computers or Internet servers. In other words, all IoT devices and sensors are connected and controlled on the network, which can result in the spread of security damage from virtual space, i.e., by computer hacking, to real physical systems. This is a serious issue that could shake the foundations of the CPS by directly threatening our lives in the real world. Therefore, we need to gain an in-depth understanding of all these vulnerabilities, threats, and attacks through research on CPS security and privacy controls. This survey presents the differences between IT systems and the CPS with reference to the basic concepts of the CPS.

Fig: The fundamental concept of CPS.

As shown in Fig. 1, the CPS is divided into three layers: the perceptual layer, the data transmission layer, and the application layer [1]. The first layer, or perception layer,

includes the recognition and the sensor, and consists of the global positioning system (GPS), RFID, sensor, actuator, camera, and IoT. The collected data can be composed of sound, light, mechanical, chemical, thermal, electrical, biology and location data, and the sensor can generate real-time data through node collaboration in wide-area and local network domains [2]. Thus, the perception layer recognizes and collects data, sends it to the communication layer, and collaborates between the IoT nodes in the network [3,4]. The communication layer is responsible for exchanging and processing data between the sensor and the application in communication. This layer communicates using various technologies such as wire (e.g., LAN, WAN), network devices (e.g., Switch, Router), and wireless (e.g., Bluetooth, ZigBee, WiFi, 4G, and 5G). This is one of the key elements of the CPS, which typically has a wide range from local to global [5]. Most communications are highly available and cost-effective because they can initially process and manage vast amounts of data over the Internet. The communication layer is also responsible for reliability and supports real-time transmission [6]. The application layer can be applied and interacted with various fields, and is sometimes referred to by a different name depending on the application one is using. For example, a typical CPS is the Supervisory Control and Data Acquisition (SCADA) system used in critical infrastructures such as the Smart Grid and the industrial control system (ICS) [7]. This layer processes the information received from the data transport layer and includes the commands to be executed by the physical sensors and actuators, and it controls the commands to be used in each field. In addition, data aggregation of different resources, intelligent processing of large amounts of data, object control and management are performed [5,8]. The range of the CPS includes the smartphones, computers, and automotive devices that we use in everyday life from power plants, water and sewage systems, airports, and industrial infrastructure to railroads. Wang et al. [9] presented the status and development of cyber physical systems and future research directions when applied to manufacturing. This allows future plants to demonstrate their production sites with enhanced security, while the CPS's unique capabilities in networking, communications, and integrated device control support manufacturing intelligence. Griffor et al.

[10] investigated the concept of the CPS, and tis domains, aspects, and facets in detail and studied the CPS framework, and presented analysis and output of the CPS framework and use cases using the CPS framework. Wang et al. [11] investigated the security issues and challenges facing the CPS, abstracted the general workflow of the cyber physics system, and identified the vulnerabilities, attack issues, enemy characteristics, and a set of challenges to be solved. They also proposed a context aware security framework for general CPS systems and studied potential research areas and issues. Shi et al. [12] provided a better understanding of the new multi-disciplinary methodology. They provided basic applications to illustrate the capabilities of the CPS, summarized the research process from various perspectives, and demonstrated the involvement of the CPS audience. Maheshwari [13] emphasized the importance of security issues in CPSs that are used extensively in a variety of areas such as critical infrastructure control, vehicle systems, and transportation, social networking, and medical and healthcare systems. Taking into account the existing security issues and security challenges, we have studied the security requirements of the CPS based on attacks on the CPS. Ashibani and Mahmoud [1] analyzed security issues at the various layers of the CPS architecture, studied risk assessment and CPS security technologies, and discussed the challenges, future research areas, and possible solutions. Considering this paper's limitations of the existing survey on CPS security, as shown in Table 1, we also present the contribution of our study in relation to the previous survey in terms of CPS overview and CPS security, issues, and challenges.

EXISTING SYSTEM

- In [11], ML algorithms, such as K-Nearest Neighbor (KNN), Random Forest (RF), DT, Logistic Regression (LR), ANN, Na¨ıve Bayes (NB), and SVM were compared in terms of their effectiveness in detecting backdoor, command, and SQL injection attacks in water storage systems. The comparative summary suggested that the RF algorithm has the best attack detection, with a recall of 0.9744; the ANN is the fifth-best algorithm, with a recall of 0.8718; and the LR is the worstperforming algorithm, with a recall of 0.4744. The authors also

reported that the ANN could not detect 12.82% of the attacks and considered 0.03% of the normal samples to be attacks. In addition, LR, SVM, and KNN considered many attack samples as normal samples, and these ML algorithms are sensitive to imbalanced data. In other words, they are not suitable for attack detection in ICS. In [12], the authors presented a KNN algorithm to detect cyber-attacks on gas pipelines. To minimize the effect of using an imbalanced dataset in the algorithm, they performed oversampling on the dataset to achieve balance.

- Using the KNN on the balanced dataset, they reported an accuracy of 97%, a precision of 0.98, a recall of 0.92, and an f-measure of 0.95. In [13], the authors presented a Logical Analysis of Data (LAD) method to extract patterns/rules from the sensor data and use these patterns/rules to design a two-step anomaly detection system. In the first step, a system is classified as stable or unstable, and in the second one, the presence of an attack is determined. They compared the performance of the proposed LAD method with the DNN, SVM, and CNN methods. Based on these experiments, the DNN outperformed the LAD method in the precision metric; however, the LAD performed better in recall and f-measure.
- In [14], the authors used the DNN algorithm to detect false data injection attacks in power systems. Findings of their evaluation using two datasets suggested 91.80% accuracy. In [15], the authors proposed an autoencoder-based method to detect false data injection attacks and clean them using denoising autoencoders. Their experiments showed that these methods outperformed the SVM-based method. To handle the effect of imbalanced data on the algorithm, they ignored attack data in training the autoencoder. In [16], the authors presented a technique based on Extreme Learning Machine (ELM) for attack detection in CPS. To address the imbalanced challenge of neural networks, training was conducted using only normal data. Based on these experiments, the

proposed ELM-based method outperformed the SVM attack detection method.

DISADVANTAGES

1) The system is implemented by Conventional Machine Learning.

2) The system doesn't implement for analyzing large data sets.

LITERATURE REVIEW In recent years, cyber-attacks have become more sophisticated in the field of security, making cyber threats increasingly unpredictable. According to a 2017 data breach study by the Ponemon Institute, a security consulting firm specializing in data breaches, the average cost of damages suffered by data breaches worldwide in 2017 was $36.2 million, though less than in the previous year, but the damage increased by 1.8% [14]. It also took an average of 191 days to identify data breach events. In a 2016 survey, a security expert monitored 200,000 security events everyday in order to respond quickly to cyber-attacks [14]. It is analyzed that 60,000 security blogs each month need to acquire information and track false alarms related to cyber threats, requiring around 20,000 hours (about 833 days, 2.3 years) of effort every year. It is also estimated that there will be a shortage of around 1.5 billion security professionals worldwide by 2020. Even now, the issue of cybersecurity shows that the damage is not decreasing even though companies are investing many resources in security. According to Gartner's latest forecast in 2017, worldwide spending on information security solutions and services was $86.4 billion, up 7 percent from 2016, while expenditure on forecasting amounted to $ 93 billion in 2018 [15]. Data on damage to the global market and security solution expenditure are shown in Fig. 2. Therefore, in the CPS, security is becoming more important in terms of behaviorial, analysis, multi-layer, visibility, and governance factors. It is necessary to pay closer attention to CPS security as the importance of cyber-security grows. In general, the security of the CPS is divided into three areas: physical security, communication security, and control and operational security. Physical security involves protecting information in the network environment, data aggregation in loosely coupled networks, processing, and large-scale sharing; communication security is focused on protecting data and the role of the control system against cyberattacks [4], and control and operational security is

focused on protecting the cyber environment with the aim of mitigating attacks of the control system on the system estimation and control algorithms [16]. Prior to CPS security, the CPS has a variety of goals, design principles, and security requirements. Therefore, we investigated the issues and security objectives pertaining to the CPS and described the requirements and design principles as follows [17]. □ Test and analysis complexity: CPS development includes software engineering, mechanical engineering, electrical engineering, systems engineering, and network engineering. In these diverse fields it is difficult to collect, test, and analyze the functional and non-functional software requirements. Overall testing has also become more difficult as there are no effective testing approaches or tools, as well as CPS-related issues. Therefore, development and testing should be capable of recognizing various contexts, working with various types of clients, and communicating smoothly in various fields.

- Design and implementation complexity: Due to the aforementioned issues and constraints, the software design for the target CPS can be very complex. In addition, the CPS must meet many of the requirements imposed by various factors, including the components, application logic, other development environments, programming languages and interface mechanisms, and external constraints.
- Safety: Safety is generally considered an important asset in industrial applications equipped with control systems that are responsible for the technical processes. Computer systems should be designed so that the operation of computer software or hardware does not threaten the environment in such a way that equipment failure will result in death, bodily injury, and large financial losses. Security: In the CPS, security can be largely classified into encryption, data information security, and control system security against cyber-attacks. These considerations can be defined as the three main components of security [18]. In cyber physical systems, confidentiality must be considered to protect the user's personal information. The integrity of the

CPS should take into account the prevention, detection or blocking of network attacks on the information exchanged between sensors and actuators or controllers. The wide availability of the CPS aims to provide services at all times while avoiding compromises of computing, control, and communications due to hardware failures, system upgrades, or DoS/DDoS attacks

PROPOSED SYSTEM

The proposed attack detection consists of two phases, namely representation learning and detection phase. Using a conventional unsupervised DNN on an imbalanced dataset yielded a DNN model that mainly learned majority class patterns and missed minority class characteristics. Most researchers have tried to address this challenge by generating new samples or removing certain samples to make the dataset balanced and then passing the data to a DNN. However, in ICS/IIoT security applications, generating or removing samples are not reasonable solutions. Due to the ICS/IIoT systems' sensitivity, generated samples should be validated in a real network, which is impossible since the generated attack samples may be harmful to the network and cause severe impacts on the environment or human life. In addition, validation of the generated samples is time-consuming. Moreover, removing the normal data from a dataset is not the right solution since the number of attack samples in ICS/IIoT datasets is usually less than 10% of the dataset, and most of the dataset knowledge is discarded by removing 80% of the dataset. To avoid the above mentioned problems in handling imbalanced datasets, this study proposed a new deep representation learning method to make the DNN able to handle imbalanced datasets without changing, generating, or removing samples. This model consisted of two unsupervised stacked auto encoders, each responsible for finding patterns from one class. Since each model tries to extract abstract patterns of one class without considering another, the output of that model represented its inputs well. The stacked auto encoders had three decoders and encoders with input and final representation layers. The encoder layers mapped the input representation to a higher, 800-dimensional space, a 400-dimensional space, and the final 16-dimensional space.

The system shows the encoder function of an auto encoder. The decoder layers did the opposite and tried to reconstruct the input representation by starting from the 16-dimensional new representation and mapping it to the 400-dimensional, 800-dimensional, and input representations. Equations 2 shows the decoder function of an auto encoder. These hyper parameters were selected using trial and- error to have the best performance in f-measure with the lowest architectural complexity.

ADVANTAGES

1) The proposed two-phase attack detection component has been implemented.

2) Unsupervised models that incorporate process/physical data can complement a system's monitoring since they do not rely on detailed knowledge of the cyber-threats.

CONCLUSION

Limited work has been done in the CPS security field because it is a new area that differs from the current network environment. The CPS is transmission medium can include various sensors, diverse types of data, real-time generated data, process analysis and various application interactions. This paper categorizes the various threats, solutions, and CPS security projects related to the issues and threats facing the CPS, and presents a solution to each threat. The CPS concept and security caused issues and challenges and showed the current security market and CPS related surveys. The CPS security assessed the threats and solutions for each tier and discussed future directions for analysis. We discussed the relationship between the threats and solutions of CPS security and studied open issues. In the future IT will expand the scope of CPS security by combining the IoT and various sensors. Therefore, we should interact with other systems in various environments to ensure that the system is secure. Since the CPS environment comprises various layers and is associated with field threats, it is concluded that the findings of this paper could improve the security of the entire system. CPS security should be a matter of constant concern because the CPS has been widely applied to various smart environments such as the smart home, smart city, smart industry, smart healthcare, and smart grid. As such, the progressive evolution of CPS security is expected to become increasingly important as the smart environment proliferates.

REFERENCES

[1] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions," Computers & Security, vol. 68, pp. 81-97, 2017.

[2] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, pp. 20-26, 2014.

[3] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: current status, challenges and prospective measures," in Proceedings of 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015, pp. 336-341.

[4] T. Lu, J. Lin, L. Zhao, Y. Li, and Y. Peng, "A security architecture in cyber-physical systems: security theories, analysis, simulation and application fields," International Journal of Security and Its Applications, vol. 9, no. 7, pp. 1-16, 2015.

[5] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in Proceedings of 2012 10th International Conference on Frontiers of Information Technology (FIT), Islamabad, India, 2012, pp. 257-260.

[6] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: the next computing revolution," in Proceedings of 2010 47th ACM/IEEE Design Automation Conference (DAC), Anaheim, CA, 2010, pp. 731- 736.

[7] Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie, "Cyber-physical system risk assessment," in Proceedings of 2013 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Beijing, China, 2013, pp. 442-447.

[8] B. Zhang, X. X. Ma, and Z. G. Qin, "Security architecture on the trusting internet of things," Journal of Electronic Science and Technology, vol. 9, no. 4, pp. 364-367, 2011.

[9] L. Wang, M. Torngren, and M. Onori, "Current status and advancement of cyber-physical systems in manufacturing," Journal of Manufacturing Systems, vol. 37, pp. 517-527, 2015.

[10] E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, "Framework for cyber-

physical systems: Volume 1, overview," National Institute of Standards and Technology, Gaithersburg, MD, Report No. 1500-201, 2017.

[11] E. K. Wang, Y. Ye, X. Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Security issues and challenges for cyber physical system," in Proceedings of 2010 IEEE/ACM International Conference on Green Computing (GreenCom) and Communications & International Conference on Cyber, Physical and Social Computing (CPSCom), Hangzhou, China, 2010, pp. 733-738.

[12] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in Proceedings of 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 2011, pp. 1-6.

.

[13] P. Maheshwari, "Security issues of cyber physical system: a review," International Journal of Computer Applications, pp. 7-11, 2016.

[14] Ponemon Institute, "2017 cost of data breach study: global overview," 2017 [Online]. Available:https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2017_Global_CODB_Report_Final.pdf.

[15] Gartner, "Gartner says worldwide information security spending will grow 7 percent to reach $86.4 billion in 2017," 2017 [Online]. Available: https://www.gartner.com/newsroom/id/3784965