ADAPTIVE HIERARCHICAL CYBER ASSUELT IDENTIFICATION AND LOCALIZATION

Chandrashekar B
Department of MCA
AMC Engineering College, Banglore
chandrashekar7766@gmail.com

Ms.Barnali Chakarobathy
Associate Professor
Department of MCA
AMC Engineering College,Banglore

Abstract

Cyber Physical Systems (CPS), one of the fundamental technologies for implementing the Internet of Things (IoT), have become more and more important in recent years. We try to combine the real and virtual worlds in which we live, and the CPS is a new paradigm that does this. However, the CPS has a few issues that could immediately endanger our lives, and the CPS environment, including its many layers, is linked to immediate threats, prompting CPS security research. A thorough analysis of the vulnerabilities, threats, and assaults is therefore necessary for CPS security and privacy for IoT.

In this paper, we look at the security issues, threats, and remedies for IoT-CPS as well as previous studies. The CPS erects a number of barriers through the security markets that already exist and security issues. The paper also highlights issues with CPS as well as assaults and vulnerabilities. We conclude by providing solutions to the CPS security risks for each system and outlining strategies for dealing with potential future issues.

Keywords: *Cyberattacks, IOT, Security, and CPS.*

I. INTRODUCTION

A new paradigm called the Cyber real System (CPS) aims to combine the real and digital worlds in which we live. It is a system that is deeply connected with numerous physical and cybernetic systems on both a scale and level. In the CPS, a digital environment that is calculated, transferred, and managed by a world made by computer programs is referred to as the "cyber environment." The physical environment uses a variety of sensors across time, as well as the Internet of Things (IoT). As a result, the CPS is made up of hardware, software, sensors, actuators, and embedded systems that are connected to multiple systems and human-machine interfaces.

A complex system for gathering, processing, computing, and analyzing information about the physical environment and applying the results to the physical environment is built using a network to connect a number of sensors, actuators, and control devices. It is a next-generation network-based distributed control system called the CPS that incorporates a physical system with sensors and actuators as well as a computational element that controls it. The CPS is a technology that is closely related to the Internet of Things. The development of information and communication technology (ICT) has brought attention to the many linkages between the physical and virtual worlds. A variety of applications in the energy, transportation, medical, and manufacturing sectors increasingly depend on the CPS.

II. LITERATURE SURVEY

The three layers of the CPS are the application layer, the data transmission layer, and the perceptual layer [1]. The recognition and sensor are included in the first layer, also known as the perception layer, together with the GPS, RFID, sensor, actuator, camera, and IoT. Through node cooperation in local and wide-area network domains, the sensor may generate real-time data from data such as sound, light, mechanical, chemical, thermal,

electrical, biological, and location [2]. Because of this, the perception layer recognizes and collects data, transmits it to the communication layer, and interacts with the network's IoT nodes [3,4].

Data processing and transport between the sensor and the application are handled by the communication layer. This layer communicates via a range of technologies, including wired (LAN, WAN), wireless (Bluetooth, ZigBee, WiFi, 4G, and 5G), and network hardware (Switch, Router). One of the most crucial features of the CPS, which typically varies from local to global [5], is this. The majority of communications are incredibly accessible and economical because they can initially analyze and handle enormous volumes of data through the Internet. Real-time transmission is made possible by the communication layer, which is also in charge of reliability [6].

Problem Statement:

We tested the efficacy of machine learning (ML) methods for identifying backdoor, command, and SQL injection attempts in water storage systems, including K-Nearest Neighbour (KNN), Random Forest (RF), DT, Logistic Regression (LR), ANN, Nave Bayes (NB), and SVM. According to the comparative brief, the RF algorithm has the best attack detection, with a recall of 0.9744; the ANN is the fifth-best methodology, with a recall of 0.8718; and the LR is the worst-performing method, with a recall of 0.4744.

Using the KNN on the balanced dataset, they reported accuracy of 97%, precision of 0.98, recall of 0.92, and an f-measure of 0.95. In order to extract patterns and rules from sensor data, the authors of described a Logical Analysis of Data (LAD) approach. They then used these patterns and rules to build a two-step anomaly detection system. In the first stage, a system is classified as stable or unstable, and in the second, the presence of an attack is established. The DNN technique was used by the authors to locate false data injection attacks in power systems. Their analysis, which used two datasets, produced results that showed 91.80% accuracy.

Fig 1.Proposed Flow

III. PROPOSED METHODOLOGY

The two stages of the proposed assault detection approach are representation learning and detection. An unbalanced dataset and a standard unsupervised DNN produced a DNN model that learned majority class patterns but ignored minority class features. The majority of studies have made an effort to get around this problem by creating new samples or removing particular samples to balance the dataset before feeding the data to a DNN.

In ICS/IIoT security applications, however, creating or removing samples is not a workable solution. Due to the sensitivity of ICS/IIoT systems, manufactured samples must be reviewed in a real network, which is not possible because the attack samples produced during the generation process may be harmful to the network and have negative effects on the environment or human life. Additionally, validating the samples that have been created takes time. Furthermore, removing normal data from a dataset is not the ideal course of action since, in

ICS/IIoT datasets, the proportion of attack samples is frequently less than 10%, and by removing 80% of the dataset, the majority of the dataset's information is lost.

This work established a revolutionary deep representation learning approach that enables the DNN to deal with imbalanced datasets without altering, creating, or removing samples, thus resolving the issues with handling unbalanced datasets as mentioned above. A single class of patterns were identified by each of the two unsupervised stacked auto encoders that made up this model. Each model aims to isolate abstract patterns of one class without taking into account another, thus the output of each model closely matched its inputs. In the stacked auto encoders, there were three decoders and encoders with input and final representation levels. A higher, 800-dimensional space, a 400-dimensional space, and finally a 16-dimensional space were created from the input representation by the encoder layers.

IV. Model

The collection, testing, and analysis of functional and non-functional software requirements in these many industries is difficult. Overall, testing has become more difficult as a result of a lack of suitable testing methods or tools as well as issues with the CPS. Development and testing should therefore be able to recognize a variety of scenarios, engage with a variety of customers, and communicate effectively across a range of industries. complexity of design and implementation: The aforementioned difficulties and constraints may make the software design for the target CPS very complex. Additionally, a variety of requirements imposed by other aspects, including the components, application logic, different development environments, programming languages and interface techniques, and external constraints, must be addressed by the CPS.

In industrial applications with control systems that are in charge of the technological activities, safety is frequently considered as a crucial advantage. Computer systems should be built so that environmental hazards are avoided and equipment failure doesn't result in fatalities, serious injuries, or large financial losses when computer software or hardware fails. Security: The CPS divides security into three categories: data information security, control system security against cyberattacks, and encryption. The three main aspects of security are these issues.

The prevention, detection, and blocking of network attacks on the data exchanged between sensors and actuators or controllers should be taken into account by CPS. The high availability of the CPS aims to provide services constantly without compromising compute, control, or communications due to hardware issues, system updates, or DoS/DDoS attacks.

V. Result

The system illustrates how an auto encoder functions. The decoder layers worked in reverse, starting with the 16-dimensional new representation and mapping it to the 400-dimensional, 800-dimensional, and input representations in an effort to reproduce the input representation. The decoder function of an auto encoder is shown in Equation 2. Trial and error led to the selection of these hyperparameters, which have the best f-measure performance with the least amount of architectural complexity.

The proposed two-stage assault detection component has been put into practice.2) Since unsupervised models do not necessitate a thorough comprehension of cyber-threats, they can be used as a supplement to system monitoring.

Providing Services

The Service Provider must enter a valid user name and password to log in to this module. He can perform certain tasks after successfully logging in, including logging in, training with and testing cyber data sets, View Prediction Of Cyber Attack Type, View Prediction Of Cyber Attack Type Ratio, View Cyber Datasets Trained Accuracy in Bar Chart, View Cyber Datasets Trained Accuracy Results, Download Predicted Datasets, View the results of the cyberattack type ratio for all remote users.

Check out and Authorize Users

The list of people who have registered can be seen by the administrator in this module. The admin may examine the user's information in this, including user name, email address, and address, and admin can also authorize users.

Remote person

There are n numbers of users present in this module. Before doing any operations, the user should register. Once a user registers, the database will record their information. After successfully registering, he must log in using an authorized user name and password. After successfully logging in, the user can perform a number of actions, including REGISTER AND LOGIN, PREDICT CYBER ATTACK TYPE, and VIEW YOUR PROFILE.

VI. CONCLUSION

There hasn't been much research done in this area because CPS security is a brand-new field that is distinct from the current network environment. The CPS is a transmission medium that may include a wide range of sensors, different data types, in-the-moment data, process analysis, and different application interactions. This article groups the various risks, cures, and CPS security initiatives that are pertinent to the challenges and threats facing the CPS and offers answers. In addition to illustrating the current security industry and CPS-related surveys, the CPS notion and security raised concerns and challenges. The CPS security team investigated potential future research topics as well as the risks and solutions for each tier. We looked into open issues and the relationship between CPS security hazards and solutions.

REFERENCES

Computers & Security, vol. 68, pp. 81–97, Mahmoud, "Cyber Physical Systems Security: Analysis, Challenges, and Solutions," 2017.

[2] D. R. Patel and J. S. Kumar, "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] "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] S. Khan, 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," Proceedings of the 2010 47th ACM/IEEE Design Automation Conference (DAC), Anaheim, CA, 2010, pp. 731–736.

[7] "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. Y. Peng, T. Lu, J. Liu, Y. Gao, X. Guo, and F. Xie. [8] B. Zhang, X. X. Ma, and Z. G. Qin, "Security architecture on the trusting internet ofthings," 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, no. 4, 2015, pp. 517–527.

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.