DETECTION AND ATTRIBUTION OF CYBER ATTACKS IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS

#1JOGULA AJAY,
#2Dr.P.VENKATESHWARLU, *Associate Professor,*
#3Dr.V.BAPUJI, *Associate Professor& HOD,*
Department of Master of Computer Applications,
VAAGESWARI COLLEGE OF ENGINEERING, KARIMNAGAR, TELANGANA

ABSTRACT: The Internet of Things has opened up novel avenues of development and application. The study's goal is to identify the causes of and solutions to cyber-attacks on cyber-physical systems. Cyberphysical systems (CPS) based on the Internet of Things (IoT) provide a security challenge because safeguards developed for conventional information technology (IT) and operational technology (OT) infrastructures may not be adequate for CPS. As a result, this study provides an architecture for the detection and attribution of ensemble attacks in the context of cyber-physical systems (CPS) operating within industrial control systems (ICS). In order to detect attacks in an imbalanced industrial control system (ICS) environment, a decision tree and a new ensemble deep representation learning model are employed. The second phase of assault attribution makes use of an ensemble of deep neural networks. Data collected from the water treatment plant and the gas distribution pipelines are used to validate the suggested model. The results of the investigation show that the proposed model outperforms other strategies that need the same amount of computer resources.

Keywords: *Cyber-attacks, Deep representation learning, Cyber threat detection, Cyber threat attribution.*

1. INTRODUCTION

Cyber-physical systems (CPS) and Internet of Things (IoT) technology are increasingly being incorporated at dams and power facilities. Integration of Internet of Things (IoT) devices into Industrial Control Systems (ICS) is becoming increasingly widespread due to the critical role they play in ensuring the secure operation of infrastructure. Systems that use PLCs and Modbus protocols, as well as Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA), are all types of Industrial Control Systems (ICS). Connecting ICS or IIoT-based systems to public networks increases the attack surface and the likelihood that hackers may target these systems. The Stuxnet attack, largely believed to have been launched in 2010 against Iranian centrifuges used for nuclear enrichment, caused extensive damage to the targeted machinery. Another instance is the 2011 closure of a water treatment plant in Illinois due to a broken pump. Another attack on Ukraine's power grid, known as BlackEnergy3, occurred that year. In this case, the attack caused a power outage that affected over 230,000 people. During the month of April 2018, news emerged of allegedly successful cyberattacks on three different American gas pipeline firms. The electronic customer communication services were temporarily disrupted for several days as a result of these attacks. It's possible that the direct applicability of ICS security solutions to IT and OT systems is restricted, despite the fact that these solutions have been shown to be effective in assuring the security of these systems. The possibility of this happening arises from the tight integration of cyber technologies and the carefully managed real world. System-level security techniques are required for efficient physical activity monitoring and system upkeep. Industrial Control Systems (ICS) prioritize security objectives in a way that is distinct from most IT/OT systems. Availability, Integrity, and Confidentiality are the Three T's of ICS. In contrast, most IT/OT systems put a premium on data security, availability, and integrity. Successful attacks on Industrial Control Systems (ICS) can have serious societal and environmental repercussions due to the close link between physical processes and feedback control loop variables. Because of this, it's more important than ever to set up foolproof safety and security processes to detect and prevent attacks on ICS.

2. LITERATURE SURVEY

Observing the harbor and preparing for a defensive strategy against the impending threat. The SANS Institute was established in 2001. The individual in question is Christopher. Port scanning is a commonly employed technique for the purpose of network resource discovery. All computers that are linked via modem to a local area network or the Internet utilize standardized or unspecified port services. Port scanning can enable an attacker to ascertain the services being utilized by users, identify network services that necessitate authentication, and determine the presence of anonymous logins.

The authors J. A. Stanford and J. A. Hoagland. In the year 2002, M. McAlerney published an article titled "Practical Automated Port Detection" in the Computer Security Journal. The article may be found in volume 10, issues 1-2, on pages 118-124. The practice of scanning for open ports is well recognized and considered to be a fundamental aspect of network security. Hostile software is commonly employed for the purpose of categorizing hosts and networks. System administrators and other network proponents encounter difficulties in employing port scans as an initial means of categorizing more severe attacks as a consequence of this. Network defenders often assess danger by utilizing their own networks. Consequently, it becomes upon the perpetrators to ascertain whether network proponents engage in regular scanning activities. However, irrespective of the presence of attackers, defenders typically exhibit little inclination to conceal their ports from scanning. In the subsequent sections, we will examine both individuals who endeavor to authenticate and individuals who conduct network searches, encompassing both supporters and adversaries. The ongoing discourse over the ethical implications of port scanning is a prominent topic of discussion on several internet platforms, including discussion boards and forums. Engaging in the act of scanning a remote network port without the explicit knowledge of the owner might be considered both ethically and legally permissible.

The subject matter under consideration exhibits a lack of clear legal boundaries in the majority of jurisdictions. Nevertheless, based on our empirical observations, it is evident that a significant proportion of instances involving illegal remote scanning originate from host systems that possess the ability to cause harm or exhibit malicious behavior. Consequently, it is justifiable to deem a port inhospitable and duly inform the remote network administrators on its source. Subsequently, following the provision of contextual information, we present our algorithms. In conclusion, we engage in speculation regarding the potential uses and future trajectories of this study.In addition to possessing fundamental comprehension of Internet protocols, network intrusion detection, and digital analysis, it is also anticipated that readers possess a functional familiarity with probability, information theory, and linear algebra. When conducting a port scan, an intrusive party will typically have two main objectives in focus. The primary aim is to document pertinent details on the identified IP addresses, including the associated ports (TCP or

UDP) to which they are linked, as well as the current state of their connections.

The other objective is to activate flood-intrusion detection systems to identify network proponents with the intention of discouraging or redirecting their activities. The primary objective of this study is to examine the collection of information pertaining to portscans, with a particular emphasis on the identification of flood portscans. Although this article does not particularly address ICMP scans, the general concepts discussed herein can be extrapolated to this area of investigation. However, in the process of developing algorithms, it is crucial to possess a substantial and comprehensive understanding of the subject matter, even including potentially harmful or excessive volumes of information. The Port and IP address range chosen by the attacker will be denoted as a scan base print. Distinguishing between the tangible footprint of a scan and the document now being accessed by the attacker holds practical value. The temporal sequence is primarily concerned with the chronological order of events. The size of the sample is not influenced by factors such as the speed of the script, its randomization, or other special qualities.

3. SYSTEM DESIGN

We've developed a novel two-phase ensemble approach that can detect both common and uncommon forms of assaults on ICS. We will also demonstrate that the suggested strategy outperforms competing strategies in terms of accuracy and f-measure. With the proposed deep representation learning, this strategy can better handle unevenly distributed data.

Using a deep neural network (DNN) framework, we propose a novel two-phase assault attribution method that automatically adjusts between various deep one-versus-all classifiers. The purpose of this technique is to lessen the occurrence of unwarranted alarms. The proposed method has proven its capacity to accurately identify those responsible for assaults with striking similarities. To our knowledge, this is the first time that a machine learning-based attack attribution mechanism has been applied to ICS and the IIoT.

The feasibility of the proposed technique for locating assaults and identifying their perpetrators is investigated. The findings demonstrate that despite the system's improved performance, its computing cost is comparable to that of previously described approaches based on deep neural networks (DNNs).

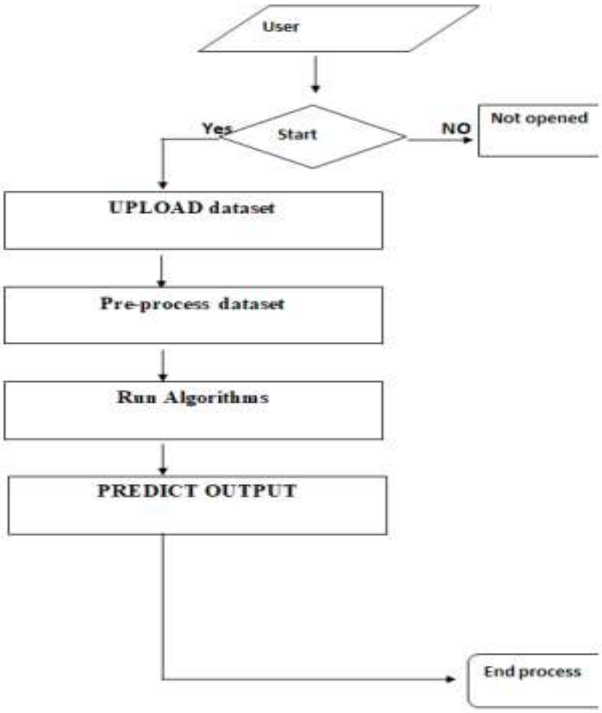


Fig 1:Working Architecture

4. SYSTEM ANALYSIS

Upload SWAT Water Dataset:

The module's goal is to make it easier for users to import data into the software, run necessary data reading activities, and then identify any instances of attacks within the imported data.

Preprocess Dataset:

If you don't fill in a value, this module will automatically fill it in with 0. The normalized feature values will be scaled using the MINMAX method. In addition, we'll split the dataset in two, with 80% of the data used for training and 20% used for testing.

Run AutoEncoder Algorithm:

In this section, we will train a deep neural network using the AutoEncoder technique and then extract features from the trained network.

Run Decision Tree with PCA:

Principal Component Analysis (PCA) will be used to compress the features extracted by the AutoEncoder before they are used in decision tree training. The signatures in the dataset are used by the decision tree method to create predictions about the labels for each record.

Run DNN Algorithm:

In order to recognize and assign blame for cyberattacks, deep neural networks (DNNs) will be used to train the decision tree label. **Detection & Attribute Attack Type**:

This component allows for the submission of test data that has not been annotated or is otherwise unfamiliar, and the prediction of the type of attack using a deep neural network (DNN).

Comparison Graph:

This component makes it easy to create a comrehensive algorithm comparison graph.

5. RESULTS

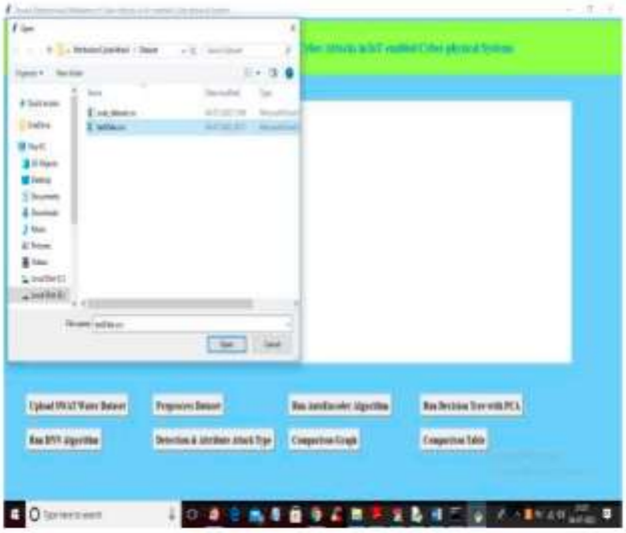
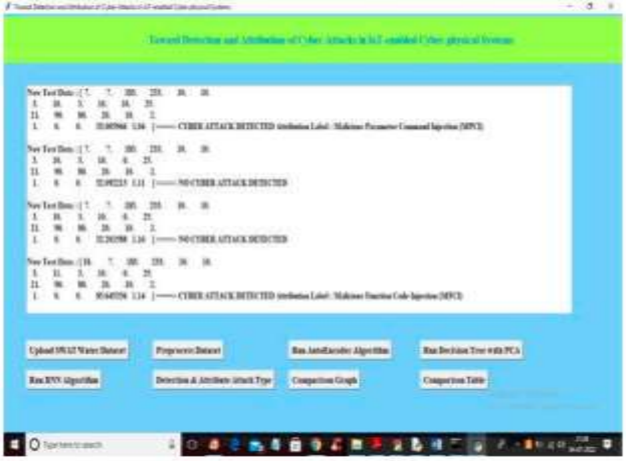

ber Attacks in IoT enabled Cyber physical Systems
Open
Cancel
Upload SWAT Water Dataset
Preprocess Dataset
Run AutoEncoder Algorithm
Run Decision Tree with PCA
Run DNN Algorithm
Detection & Attribute Attack Type
Comparison Graph
Comparison Table

Fig 2: The "TEST DATA" document can be obtained by selecting the "Open" button on the aforementioned page.


Toward Detection and Attribution of Cyber Attacks in IoT enabled Cyber physical Systems
Upload SWAT Water Dataset
Preprocess Dataset
Run AutoEncoder Algorithm
Run Decision Tree with PCA
Run DNN Algorithm
Detection & Attribute Attack Type
Comparison Graph
Comparison Table

```
New Test Data : [ [illegible]
[illegible] |-----> CYBER ATTACK DETECTED Attribution Label : Malicious Parameter Command Injection (MPCI)
New Test Data : [ [illegible]
[illegible] |-----> NO CYBER ATTACK DETECTED
New Test Data : [ [illegible]
[illegible] |-----> NO CYBER ATTACK DETECTED
New Test Data : [ [illegible]
[illegible] |-----> CYBER ATTACK DETECTED Attribution Label : Malicious Function Code Injection (MFCI)
```

Fig 3: Select an assault case from the 'Detected' portion of the interface, and then click the 'Comparison Graph' button to be taken to the aforementioned visualization.

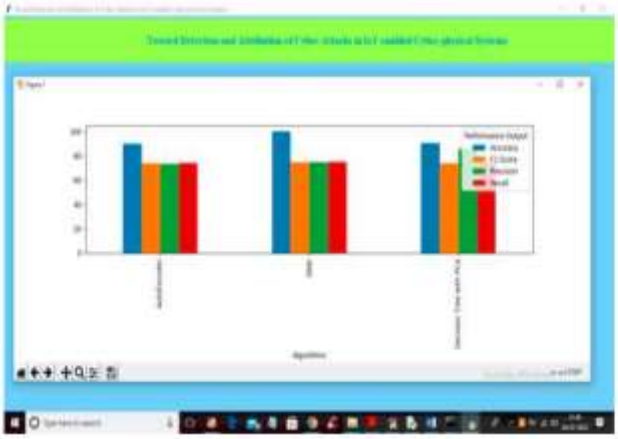


Fig 4: The x-axis of the following graph shows the names of the algorithms, while the y-axis shows other metrics.

6. CONCLUSION

Problems may arise when attempting to secure cyber-physical systems (CPS) that make use of Internet of Things (IoT) features, as security solutions designed for traditional information technology and operational technology (IT/OT) may not be as effective in this new setting. This study proposes a methodology for identifying and assigning blame for cyber-physical system (CPS) intrusions that target industrial control systems (ICS). At the first stage of analysis, a decision tree and a novel ensemble deep representation-learning model are developed to detect attacks in an unbalanced ICS environment. By creating an ensemble deep neural network, we are able to tackle the problem of attributing attacks at the second level. The proposed model is tested with information gathered from operational sources including water purification facilities and gas distribution networks. The results of this study show that the proposed model outperforms competing methods with comparable computing complexity.

REFERENCES

[1] K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.

[2] R. Christopher, "Port scanning techniques and the defense against them," SANS Institute, 2001.

[3] M. Baykara, R. Das¸, and I. Karado ˘gan, "Bilgi g ¨uvenli ˘gi sistemlerinde kullanilan arac¸larin incelenmesi," in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp. 231–239.

[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "Practical automated detection of stealthy portscans," Journal of Computer Security, vol. 10, no. 1-2, pp. 105–136, 2002.

[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in high bandwidth environments," in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1. IEEE, 2003, pp. 130–138.

[6] K. Ibrahimi and M. Ouaddane, "Management of intrusion detection systems based-kdd99: Analysis with lda and pca," in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1–6.

[7] N. Moustafa and J. Slay, "The significant features of the unsw-nb15 and the kdd99 data sets for network intrusion detection systems," in Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS), 2015 4th International Workshop on. IEEE, 2015, pp. 25–31.

[8] L. Sun, T. Anthony, H. Z. Xia, J. Chen, X. Huang, and Y. Zhang, "Detection and classification of malicious patterns in network traffic using benford's law," in Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864– 872.

[9] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system using naive bayes and pca algorithm," in Convergence in Technology (I2CT), 2017 2nd International Conference for. IEEE, 2017, pp. 565–568.

[10] M. C. Raja and M. M. A. Rabbani, "Combined analysis of support vector machine and principle component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5