International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/10
DOI: https://doi.org/10.5281/zenodo.19132088

CYBER ATTACK DETECTION AND ATTRIBUTION IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS

[#1]**G. LAKSHMI,** ***Associate Professor,***
[#2]**K. ASHOK,** ***Assistant Professor,***
[#3]**SD. KHAJA PASHA,** ***Assistant Professor,***
[#4]**P. LAVANYA,** ***Assistant Professor,***
Department of AIML,
TRINITY COLLEGE OF ENGINEERING AND TECHNOLOGY, PEDDAPALLY, TG.

ABSTRACT: The development of new application and development routes has been made easier by the Internet of Things. Intrusions on cyber-physical systems are the focus of the inquiry, which aims to determine their origins and possible remedies. There is cause for concern over the security of cyberphysical systems (CPS) built on the Internet of Things (IoT), as the safeguards designed for more conventional IT and OT infrastructures might not be sufficient for CPS. Therefore, within the framework of cyber-physical systems (CPS) functioning within industrial control systems (ICS), this article presents an architecture for the detection and assignment of collective assaults. To identify intrusions in an imbalanced industrial control system (ICS) setting, a decision tree and a new ensemble deep representation learning model are utilized. Second, an ensemble of deep neural networks is used for attack attribution. To verify the suggested model, we used data acquired from the water treatment facility and the gas distribution conduits. According to the research's findings, the suggested approach beats competing tactics that call for the same amount of processing power.

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

1. INTRODUCTION

Power plants and dams are increasingly implementing cyber-physical systems (CPS) and Internet of Things (IoT) technology. Due to their critical importance in ensuring the safe operation of infrastructure, more and more individuals are integrating Internet of Things (IoT) devices into Industrial Control Systems (ICS). Systems that are based on PLCs and Modbus, as well as Distributed Control Systems (DCS), and Supervisory Control and Data Acquisition (SCADA) are all instances of ICS. Hackers are more likely to target ICS and IIoT systems that are linked to public networks.

The Stuxnet attack, which heavily damaged Iranian nuclear enrichment centrifuges, began in 2010, according to most estimates. In addition, a broken pump forced the closure of an Illinois water treatment facility in 2011. In the same year, another attack known as BlackEnergy3 was launched on Ukraine's electrical grid. The attack resulted in more than 230,000 people losing power. Allegedly, in April 2018, successful attacks were launched against three different American gas pipeline

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/10
DOI: https://doi.org/10.5281/zenodo.19132088

companies. These attacks made electronic consumer communication services unavailable for a few days. Although there is proof that IT and OT systems can be safeguarded by industrial control system (ICS) security solutions, it is unlikely that these systems can be directly integrated with ICS security solutions.

Cyber technologies rely on the strictly regulated physical environment, thus this might happen. System-level security measures are essential for effective system maintenance and the oversight of physical activities. Most information technology and operational technology systems do not emphasize security measures as industrial control systems do. Privacy, integrity, and availability constitute the Three T's of ICS. The predominant focus of IT/OT systems is on the availability, security, and integrity of data. The intimate connection between physical processes and variables in feedback control loops means that successful attacks on Industrial Control Systems (ICS) can cause considerable damage to both humans and the environment. The establishment of reliable security measures to identify and thwart ICS attacks is paramount.

2. SYSTEM DESIGN

A new two-phase ensemble method that can identify both common and uncommon ICS attacks has been created by our team. In terms of f-measure and accuracy, we will also demonstrate that the suggested strategy outperforms existing approaches. This strategy becomes even more adept at dealing with unevenly distributed data when using the suggested deep representation learning.

A unique two-phase assault attribution methodology that autonomously transitions among a variety of deep one-versus-all classifiers within a deep neural network (DNN) architecture is proposed. The goal of this approach is to reduce the occurrence of false alarms. Proof of concept for the proposed strategy is in its ability to distinguish between visually identical attackers. We are unaware of any previous usage of a machine learning-based attack attribution technique on ICS and the IIoT. The efficacy of the proposed method for tracing attacks to their source is assessed. The results show that the system outperforms competing systems using deep neural networks (DNNs), while having similar running costs.

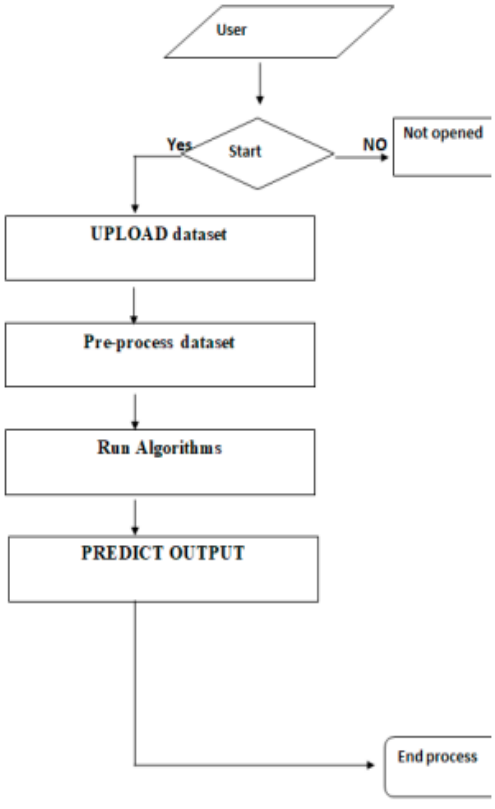

Fig 1: Working Architecture

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/10
DOI: https://doi.org/10.5281/zenodo.19132088

3. LITERATURE SURVEY

Observing the harbor while preparing to repel the impending threat. In 2001, the SANS Institute was founded. Christopher is the person in issue here. Scannable ports allow users to discover resources within a network. Standard or unnamed port services are utilized by every computer that has an Internet or local area network modem connection. Port scanning allows an attacker to discover user services, password requirements, and anonymous logins on a network.

Jos. A. Hoagland and Stanford wrote it. Article "Practical Automated Port Detection," published in 2002 by the Computer Security Journal, was authored by M. McAlerney. Volume 10, issues 1-2, pages 118–124, include the article. One of the most important aspects of network security is checking for open ports, as is well known. It is common practice to sort hosts and networks using malicious malware. This makes it difficult for network defenders and system administrators to use port scans as an initial step in identifying more serious threats. Network security professionals frequently use their own networks to scan for potential dangers. Thus, it is the responsibility of the offenders to determine the frequency of scanning by network advocates. Even in the absence of attackers, defenders typically prefer not to conceal their ports from surveillance. In the parts that follow, we shall examine both friends and enemies. Among these are those seeking networks and those attempting authentication. The moral implications of port scanning have been the subject of much debate on various internet forums and message boards. Legally and ethically, it may be acceptable to scan a remote network port without the owner's agreement.

The matter under investigation lacks explicit legal boundaries in the majority of jurisdictions. But our research shows that malicious host systems are the root cause of many unauthorized remote scanning situations. This is why it is prudent to inform the other network administrators about the source of an inaccessible port. We lay out our process after providing some context. Finally, we offer some speculation regarding potential future applications and uses of this research.Internet usage, intrusion detection in networks, and digital analytic skills are required, in addition to knowledge of probability, information theory, and linear algebra. Intruders often have two primary goals when they do a port scan. Noting critical details about the discovered IP addresses, such as the ports they are connected to (TCP or UDP) and the status of those connections, is the primary goal.

A further goal is to activate flood-intrusion monitoring systems in order to track out network supporters and either halt or redirect their actions. Examining the process for gathering data relevant to portscans, specifically flood portscan identification, is the primary purpose of this research. Although this article doesn't cover ICMP scans in depth, the broad concepts discussed can be applied to this field of research. But even if it involves handling potentially harmful or excessive amounts of data, it is essential to know a great deal about the issue while developing algorithms. The hacker's chosen port and

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/10
DOI: https://doi.org/10.5281/zenodo.19132088

range of IP addresses can be seen in a scan base print. Differentiating between the actual page an attacker is viewing and the physical trace of a scan is useful. The most important thing about the chronological sequence is the order in which events occurred. Speed, randomization, and other script-specific characteristics have no bearing on the sample size.

4. SYSTEM ANALYSIS

Upload SWAT Water Dataset:

The purpose of the module is to simplify data loading, reading, and the detection of attacks in the provided data for the benefit of the program's users.

Preprocess Dataset:

This module will input 0 if no value is entered. To adjust the magnitude of the normalized feature values, we shall apply the MINMAX technique. In addition, we will divide the dataset in half, with 80% going into training and 20% into testing.

Run Auto Encoder Algorithm:

The current section will focus on training a deep neural network using the AutoEncoder approach. Features will thereafter be retrieved from the network.

Run Decision Tree with PCA:

The features obtained by the AutoEncoder will first be Principal Component Analysis (PCA) compressed before being utilized to train a decision tree. The decision tree approach makes educated guesses about the labels for each item based on the signatures in the dataset.

Run DNN Algorithm:

The decision tree label will be trained using deep neural networks (DNNs) to identify and categorize cyberattacks.

Detection & Attribute Attack Type:

A deep neural network (DNN) is used to guess what kind of attack the test data is. The test data doesn't need to be named or known.

Comparison Graph:

Crafting an understandable graph for the purpose of comparing algorithms becomes a breeze with this component.

5. RESULTS

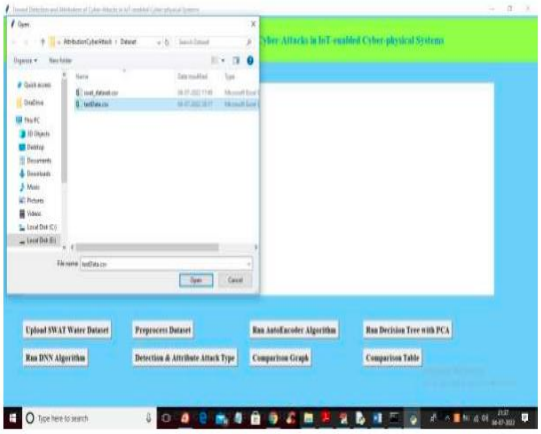

Fig 2: The "TEST DATA" document can be accessed by clicking the "Open" button on the specified page.

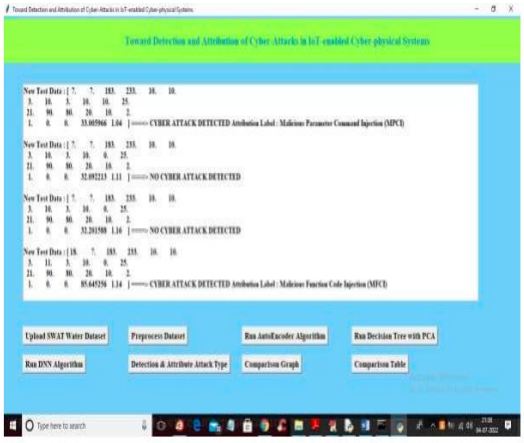

Fig 3: Choose an attack case from the 'Detected' section of the interface, and thereafter click the 'Comparison Graph' button to access the specified visualization.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/10
DOI: https://doi.org/10.5281/zenodo.19132088

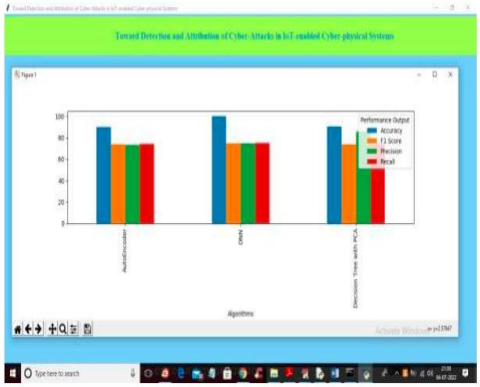

Fig 4: The x-axis of the subsequent graph represents the names of the algorithms, and the y-axis denotes various measures.

6. CONCLUSION

Cyber-physical systems (CPS) with Internet of Things (IoT) components may be challenging to secure since security techniques that are effective for traditional IT/OT may not be as effective in this new environment. The purpose of this article is to offer a way for determining who is responsible for cyber-physical system (CPS) attacks on industrial control systems (ICS). To identify attacks in an imbalanced ICS setting, the analysis starts by building a decision tree and a one-of-a-kind ensemble deep representation-learning model. We apply an ensemble deep neural network to the second-level attack blame assignment problem. To validate the model, we use information gathered from real-world sources, such as water treatment facilities and gas distribution systems. The research's findings demonstrate that the suggested model outperforms alternative models with comparable computational 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.

International Journal of Technovation and Business Insights
Volume 02, Issue 01, January-March 2026
ISSN: 3107-7900, P.CODE: 26/2-1/10
DOI: https://doi.org/10.5281/zenodo.19132088

[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