Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 16, Issue. 1: 2025
ISSN : **1906-9685**

Journal of Nonlinear Analysis and Optimization : Theory & Applications

Editors-in-Chief :

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

K. JAYA KRISHNA [1], K. ABHINASH [2]

[1]Associate Professor, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

[2]PG Scholar, Dept. of MCA, QIS College of Engineering and Technology, Ongole, Andhra Pradesh.

ABSTRACT— Securing Internet of Things (IoT)-enabled cyber physical systems (CPS) can be challenging, as security solutions developed for general information / operational technology (IT / OT) systems may not be as effective in a CPS setting. Thus, this paper presents a two-level ensemble attack detection and attribution framework designed for CPS, and more specifically in an industrial control system (ICS). At the first level, a decision tree combined with a novel ensemble deep representation learning model is developed for detecting attacks imbalanced ICS environments. At the second level, an ensemble deep neural network is designed for attack attribution. The proposed model is evaluated using real-world datasets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.

Index Terms – Internet of things, Cyber Physical System, Machine learning, Deep Neural Network.

I. INTRODUCTION

Popular attack detection and attribution approaches include those based on signatures and anomalies. To mitigate the known limitations in both signature-based and anomaly-based detection and attribution approaches, there have been attempts to introduce hybrid-based approaches. Although hybrid based approaches are effective at detecting unusual activates, they are not reliable due to frequent network upgrades, resulting in different Intrusion Detection System (IDS) typologies . Beyond this, conventional attack detection and attribution techniques mainly rely on network metadata analysis (e.g. IP addresses, transmission ports, traffic duration, and packet intervals). Internet of Things (IoT) devices are increasingly integrated in cyber-physical systems (CPS), including in critical infrastructure sectors such as dams and utility plants. In these settings, IoT devices (also referred to as Industrial IoT or IIoT) are often part of an Industrial Control System (ICS), tasked with the reliable operation of the infrastructure.

ICS can be broadly defined to include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and systems that comprise programmable logic controllers (PLC) and Modbus protocols. The connection between ICS or IIoT-based systems with public networks, however, increases their attack surfaces and risks of being targeted by cyber criminals. One high profile example is the Stuxnet campaign, which reportedly targeted Iranian centrifuges for nuclear enrichment in 2010, causing severe damage to the equipment. Another example is that of the incident targeting a pump that resulted in the failure of an Illinois water plant in 2011 BlackEnergy3 was another campaign that targeted Ukraine power grids in 2015, resulting in power outage that affected approximately 230,000 people. In April 2018, there were also reports of successful cyber-attacks affecting three U.S. gas pipeline firms, and resulted in the shutdown of electronic customer communication systems for several days. Although security solutions developed for information technology (IT) and operational technology (OT) systems are relatively mature, they may not be directly applicable to ICSs.

This reinforces the importance of

designing extremely robust safety and security measurements to detect and prevent intrusions targeting ICS. Popular attack detection and attribution approaches include those based on signatures and anomalies. To mitigate the known limitations in both signature-based and anomaly-based detection and attribution approaches, there have been attempts to introduce hybrid-based approaches.

II. LITERATURE SURVEY

The network of entities is a crucial idea that is incorporated into a wider range of networked items and digital sensors, according to Tobby (2017). This technologies has resulted in a flood of available apps, a large change in how people use the Internet, and both advantages and disadvantages, notably when it comes to national infrastructure. For example, attackers have broken into security systems using IoT devices like printers, thermostats, and conference technology. Home automation, power management, smart homes, internet drug delivery systems, smart cars, interconnected transportation infrastructure, road and bridge sensors, and technologies in agricultural, industrial, and energy production and distribution have all been made possible by Web facilities. Even though this has increased performance in many ways, the unchecked growth of the IoT creates a number of concerns about people's confidentiality and protection, telecom networks, and companies. This is a result of unauthorised intrusions into the networks supporting infrastructural facilities, as the effectiveness of Wireless internet also increases the sensitivity to security breaches caused by improper use of IoT data. Whereas an ICS is air-gapped and therefore a closed environment, it is still subject to physical access assaults, such as those launched from infected portable devices, even though it might not be sensitive to digital attack. Because of the expanded interconnection, a breakdown in one system may result in a disturbance in another, making vital infrastructure more susceptible to hackers. Arash and Stuart (2015) claim that CPS integrates, monitors, or controls its activities, allowing structural components to be managed using cyber-based commands. A CPS creates a feedback signal for each of the platform's physical components by connecting controllers, central processing elements, detectors, and communications. Distributed control system (DCS), and logic model processor are the three main parts of a CPS . The SCADA systems collect and manage regionally scattered resources, from managing sensors inside a factory to managing electricity distribution across a nation. They play a significant role in many crucial infrastructures, including petroleum refining, water distribution networks, and power generation grids. The achievement of a company's goals is heavily reliant on the Usage of Information Systems (CIS) that supports the objective, according to Lange et al. (2016) in their article. Cyber attacks on CIS consequently hinder or impair the execution and fulfilment of the related mission capabilities. An electrical grid's primary operating goal is to transport electricity from producers to customers. They are linked to CIS for reasons of surveillance and management. An application's functionality, efficiency, or dependability may be reliant on a number of wireless services that span numerous network gadgets and inter - and intra of an infrastructure. Attackers may take advantage of flaws in desktop applications or online programs to leak user information or copyrights through the dangers associated with susceptible technology installed in enterprises today. Lack of consistent, proactive measures to address Bring Your Own Device (BYOD) trend-related risks. The safety of all vital information is a big challenge that smart apps present, and the proliferation of these devices increases the risk of accidental and malicious cyber security incidents.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

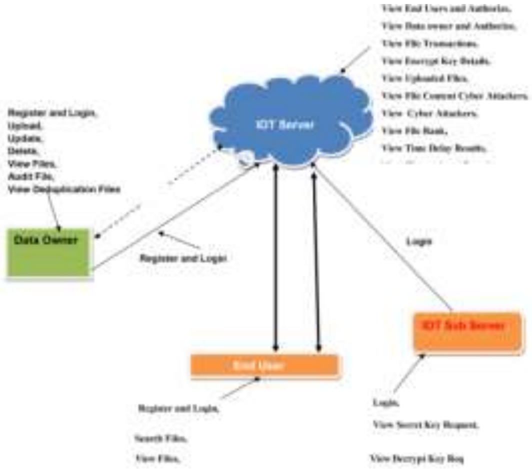

Fig. 1: System Overview

Implementation Modules

IOT Server

- The IOT Server enormous storage space, and supplies storage services and downloading services for users. In order to improve storage efficiency, the IOT Server performs deduplication for duplicated files.
- In other words, the IOT Server keeps only a single copy of any duplicated le and its corresponding authenticators, and provides user with a link to the corresponding file.

User

- The user is divided into two categories. One is the initial user who uploads files that did not exist in the cloud previously. The other one is the subsequent users who upload files that the IOT Sub Server kept. The initial user generates the authenticators for each encrypted file, then uploads the encrypted file, its corresponding authenticators and the file tag to the IOT Server.
- The subsequent user does not need to generate the data authenticators and upload the above messages to the IOT Server. Later, both the data owner and the End user can recover their data after downloading the data from the cloud. In addition, users are able to verify the integrity of the cloud data by executing

the cloud storage auditing protocol with the cloud.

IOT Sub Server

- The IOT SUB SERVER is responsible for helping users generate the file index and the file label with his private key. With the file index, the cloud can verify whether the file uploaded by the user is duplicated or not. With the file label, the user can generate some keys for encryption and authenticator generation.

IV. RESULTS

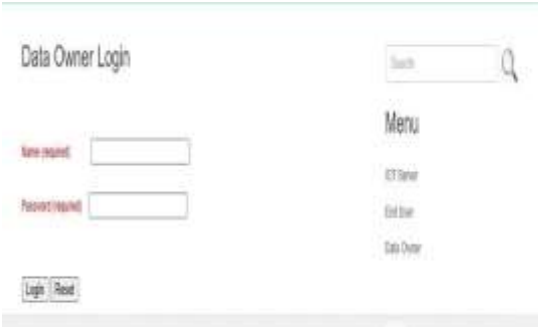

Fig.2: Data Owner Login

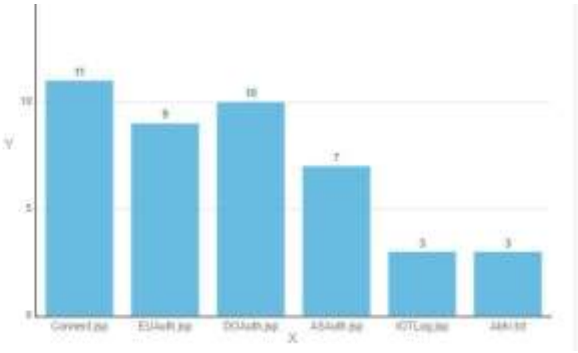

Fig.3: Results

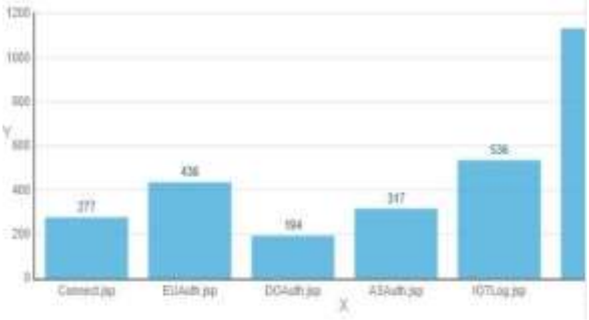

Fig.4: Connected Results

V. CONCLUSION

This project proposed a novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS data. The attack detection stage uses deep representation learning to map the samples to the new higher dimensional space and applies a DT to detect the attack samples. This stage is robust to imbalanced datasets and capable of detecting previously unseen attacks. The attack attribution stage is an ensemble of several one-vs-all classifiers, each trained on a specific attack attribute. The entire model forms a complex DNN with a partially connected and fully connected component that can accurately attribute cyber attacks, as demonstrated. Despite the complex architecture of the proposed framework, the computational complexity of the training and testing phases are respectively O(n4) and O(n2), (n is the number of training samples), which are similar to those of other DNN-based techniques in the literature. Moreover, the proposed framework can detect and attribute the samples timely with a better recall and f measure than previous works.

REFERENCES

1. F. Zhang, H. A. D. E. Kodituwakku, J. W. Hines, and J. Coble, "Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data," IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4362–4369, (2019).

2. R. Ma, P. Cheng, Z. Zhang, W. Liu, Q. Wang, and Q. Wei, "Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber Physical System," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9783–9793, (2019).

3. Mohammed Ali Shaik, Praveen Pappula, T. Sampath Kumar, Battu Chiranjeevi, "Ensemble model based prediction of hypothyroid disease using through ML approaches", International Conference on Research in Sciences, Engineering, and Technology, AIP Conf. Proc., 2971, 020038 (2024), https://doi.org/10.1063/5.0196055

4. J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly Detection Based on Zone Partition for Security Protection of Industrial Cyber-Physical Systems," IEEE Transactions on Industrial Electronics, vol. 65, no. 5, pp. 4257–4267, (2018).

5. Mohammed Ali, P. Praveen, Sampath Kumar, Sallauddin Mohmmad, M. Sruthi, "A survey report on cloud based cryptography and steganography procedures", International Conference on Research in Sciences, Engineering, and Technology, AIP Conf. Proc. 2971, 020040-1–020040-8; https://doi.org/10.1063/5.0196050

6. J.F.Clemente, "No cybersecurity for critical energy infrastructure,"Ph.D. dissertation, Naval Postgraduate School, (2018).

7. Mohammed Ali Shaik, P. Praveen, T. Sampath Kumar, Masrath Parveen, Swetha Mucha, "Machine learning based approach for predicting house price in real estate", International Conference on Research in Sciences, Engineering, and

Technology, AIP Conf. Proc. 2971, 020041-1–020041-5; https://doi.org/10.1063/5.0196051

8. Y. Bengio, A. Courville, and P. Vincent, “Representation learning: A review and new perspectives,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798–1828,(2013).

AUTHORS Profile

Mr. K. Jaya Krishna is an Associate Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Anna University, Chennai, and his M.Tech in Computer Science and Engineering (CSE) from Jawaharlal Nehru Technological University, Kakinada (JNTUK). With a strong research background, he has authored and co-authored over 90 research papers published in reputed peer-reviewed Scopus-indexed journals. He has also actively presented his work at various national and international conferences, with several of his publications appearing in IEEE-indexed proceedings. His research interests include Machine Learning, Artificial Intelligence, Cloud Computing, and Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

Mr. K. Abhinash has revived has received her BCA (computers) And Degree From ANU 2023 Pursuing MCA Qis College Of Affiliated to Engineering and technology JNTUK 2023-2025