Cyber-Attacks in IoT-enabled Cyber-physical Systems

Latha SS, K. Mani Sai Goud, P. Muni Sai Chetan Reddy, P. Surendra Reddy and P. Bharath Arun

Department of Information Science and Engineering, New Horizon College of Engineering Bangalore, India

Abstract - Cyber physical systems (CPS) that are Internet of Things (IoT) enabled might be difficult to secure since security measures designed for general data / value through the development (IT / OT) systems may not work as well in a CPS environment. Consequently, this research provides a two-level ensemble attack detection and attribution framework created for CPS, and more particularly in an industrial control system (ICS). For identifying assaults in unbalanced ICS environments, a decision tree integrated to an unique ensemble deep representation learning model is created at the first extent. An ensemble deep neural network is created for assault features at the second level. Applying actual data collections from the gas pipeline and water treatment system, Findings show that the suggested type is more effective than other competing methods with a similar level of computational complexity. ***Keywords:*** *IOT, CPS, IT, OT, ICS, ML, DNN.*

1. INTRODUCTION

Cyber-physical systems (CPS) have become more and more integrated with Internet of Things (IoT) technology, including key infrastructure sectors like dams and utilities plants. Smart gadgets, also known as Industrial IoT or (IIoT) devices, is frequently a component of an Industrial Control System (ICS) in these environments, which is responsible for the safe foundation maintaince. ICS can be widely classified to cover systems that use programmable logic controllers (PLC) and Modbus protocols, distributed control systems (DCS), and supervisory control and data acquisition (SCADA) systems. Approaches are based on signatures and anomalies are frequently used for attack citation and detecting. There are already initiatives to propose based on hybrid systems in order to lessen the acknowledged drawbacks for both exceptional situation and handwriting detecting and labelling methods. Although hybrid-based methods are good at spotting odd activity, they are unreliable since networks are frequently upgraded, leading to many Intrusion Detection System (IDS) classifications. In addition, traditional attacker identification and recognition methods generally depend on network information analysis (such as IP port number, transmission ports, traffic volume, and package break). The use of attacker recognization and reporting based on machine learning (ML) or deep neural networks (DNN) has therefore recently

attracted significant attention. Additionally, network-based and host-based attack detection methodologies can be classified. Techniques that are frequently used for identifying attacks in internet activity include supervised clustering, single-class or multi-class Support Vector Machine (SVM), fuzzy logic, Artificial Neural Network (ANN), and DNN. These methods use serious traffic data analysis to quickly identify malicious attacks. Detection mechanism that solely takes network and host data into account, though, may miss more considered at high risk or insider attacks. Since unsupervised models don't require in-depth expertise of the cyber-threats, they can supplement system monitoring by incorporating process/physical data. in general Robust protective measures may be defeated by a knowledgeable attacker with enough time and information, like a complex persistent risk operator from a national government.. Additionally, the majority of current techniques represent a system's only usual behaviour and report variances from that behaviour as occurrences, ignoring given ICS content's unbalanced quality. This may be because there aren't many attack examples in real-world circumstances and datasets currently available. Whereas employing positive class data is an excellent way to prevent problems brought on by unbalanced information, the training set won't be able to see the patterns evidence of the assault. In additional lines, a method is inaccurate with a higher percentage of misclassification undetected threats .As a result, efforts have been made to use DL techniques, for instance, to assist automatic training to predict from attribute (expression) difficult concepts from smaller ones without relying for human-made attributes **.**

2 SURVEY OF RESEARCH

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 cybersecurity incidents. As a result, it is now a corporate responsibility to confirm the privacy of the program being installed to those systems. This is significant since systems like Google's Android do only rudimentary security checks on programmes before allowing users to download them via respective Mobile app.

3 EXISTING SYSTEM

The comparison report indicated that the RF algorithm, with a recall of 0.9744, has the greatest detection mechanism, the ANN, in a recall of 0.8718, is the fifth-better method, and the LR, with a recall of 0.4744, is the lowest-performing algorithm. The authors also said that the ANN mistakenly identified 0.03% of the regular samples as attacks and was unable to identify 12.82% of the attacks. Additionally, most assault samples were processed as test set by LR, SVM, and KNN, and these ML techniques are reactive to unbalanced data. They cannot be used for ICS attack detection, in those other terms. The developers of presented a KNN technique to find gas pipeline cyberattacks. They oversampled the dataset to attain equality in order to reduce the impact of utilising an unbalanced information in the algorithms. They obtained efficiency of 98%, precision of 0.97, recall of 0.93, and an f-measure of 0.96 by using KNN on the information with balance. They evaluated the suggested LAD theory's efficiency to that of the DNN, SVM, and CNN approaches. According to these tests, in LAD technique scored good in recall and f-measure, but the DNN scored higher in the precise metric.

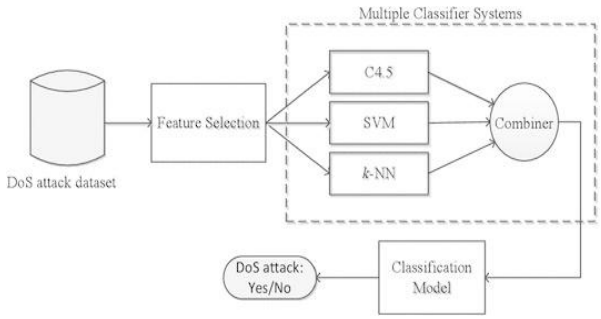

Fig. 1. Framework of attack detection using MCS

DRAW BACK OF EXISTING SYSTEM: Considering unsupervised algorithms don't require indepth information of the cyber-threats, we can supplement system monitoring by incorporating workflow data. In generally, a knowledgeable hacker with enough time and information, such a national or high-level persistent threat actor, may be able to get through strong protection measures. Additionally, the majority of current techniques analyze only a system's usual behaviour and record deviation from that behaviour as irregularities, ignoring

the unbalanced nature of ICS information. This may be because there aren't many attack examples in the data that already available and in real - world scenarios.

4 PROPOSED SYSTEM

In this system, a clustering algorithm and an array of unsupervised DNNs are used to analyse the ICS input features as part of the attack detection technique. The sample is sent to a number of DNNs for thorough study if an attack is discovered. The hidden attacker sensor would pick it up and classify it as an invisible strike if it had never been seen or known before. For a rigorous security evaluation, this will be forwarded. Unless something prevents it, the assault credit technique recognises the attack attribute.

a. Ensemble Attack Detection Method

The two phases of a suggested attacker detection technique are the supervised learning period and the prevention strategies. A standard unsupervised DNN in an unbalanced sample produced a DNN type that mostly acquired patterns specific to the majority class while missing attributes specific to the minority class. The majority of researchers have attempted to overcome this problem by creating additional samples or eliminating particular data to normalize the dataset before feeding the data to a DNN. However, producing or removing samples are not useful strategies in ICS/IIoT application areas. The created threat examples should be verified in a real network given the severity of ICS/IIoT systems, however this is hard because they may be detrimental to the network and have serious negative effects either on the environmental or on people’s existence. Additionally, validating the produced data requires time. The amount of attacker items in ICS/IIoT data is typically less than 10.0 % of the set of data, and eliminating 80% set of data discards the majority of the datasheet information. As a result, eliminating the summary statistics from a data source is not the best course of action.

b. Self-Tuning Attack Attribution Method

There are two parts to the suggested self-tuning assault attribution mechanism. A one-vs-all classifier is learned for each characteristic in the initial stage. Attacking data from a collection are divided into many groups considering this characteristics and one DNN type is built for each set in order to develop these classifications. The final product training algorithm is the Convolutional value, and the obscured state input layer is the Convolution Unit (ReLU) function. The input of all of the initial phase DNNs are then sent to the second stage, where one vs-all DNNs are used to assign the examples. The one vs-all classifiers and a DNN evolutionary algorithm are integrated to create a more complicated DNN in the second step. This DNN is divided into two parts: a partly attached elements made up of numerous onevs-all classifications and a networked part that combines the traits of the samples and the outputs of the first part to create various classes. The ensemble DNN's hidden layers employ the Activation functions, and its output activation function uses the learning algorithm. This technique doesn't to provide because it can adjust itself from altering the attack patterns this is the outcome of utilising the approach of gradient descent to the aggregation framework and all one-vs-all classifications' scores are updated sequentially. When an attack patterns component is found and introduced to the attack attribution technique, this functionality is helpful. The synthetic data, which includes the fresh attacking quality, is run into to the suggested attack identification technique to complete this task.

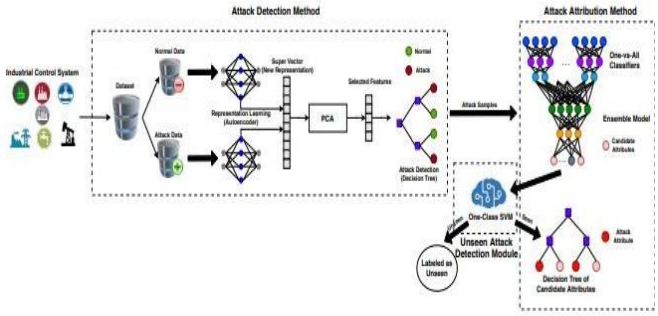

Fig. 2. Proposed attack detection and attribution framework

ADVANTAGE OF PROPOSED SYSTEM: The Network of Things (IoT), which allows its users to enhance the activities and efficiently stay with the latest breakthroughs in the cyber-physical sector, has attracted a lot of interest in current history. In regards to the hardware they are based on and the memory file types they employ, Network edge equipment are different. When delivering the content, those gadgets must authorize each other by utilizing high security mutually secure protocols. Provider connectivity has authentication process as a key component. These tool systems can authenticate one another thanks to encrypted secret key. A device can be authorised and given access to common resources after it has successfully authorization. To prevent data privacy violations, it is necessary to validate a gadget making a data transmission proposal.

4 METHODOLOGY

The two stages of the recommended security attacks are the information retrieval stage and the prevention strategies. A DNN system that mostly learnt positive class patterns and overlooked minority class characteristics was produced by applying a typical unsupervised DNN to an unbalanced dataset. The majority of researchers have attempted to overcome this problem by creating additional samples or eliminating particular samples to balance the dataset before feeding the info to a DNN. Yet, producing or deleting examples are not useful strategies in ICS/IIoT security systems. The created attacker sampling must be tested in a network system due to the sensitive nature of ICS/IIoT systems, however this is difficult because they may be detrimental to the network and have serious consequences for the environment or humankind. The amount of attacked instances in ICS/IIoT records is typically below 10% of the information, and eliminating 80% of the information discards the majority of the database information. As a result, deleting the training dataset from a set of data is not the best course of action. This paper explains a novel classification algorithm techniques to enable the DNN to handle datasets without modifying, producing, or eliminating sampling in order to solve the aforementioned issues with managing outliers.

Two unsupervised layered automatic encoders made up this model, each of which was in charge of looking for sequences from a single class. The result of such models accurately reflected its inputs since every strategy seeks to discover visuals of one class without taking into account another. Three decoders and transceivers with incoming and finish representational layers made up the stackable auto encoders. A larger, 700 area with dimensions, a 400 area with dimensions, and finally a 15-dimensional space were all transferred to by the encoder layers from the input data. The automatic encoder's encoder operation. By beginning with the 15-dimensional new feature space and translating it to the 400- area with dimensions, 800- area with dimensions and original expressions, the decoder

layers attempted to restore the initial information. the auto encoder's decoder feature. Utilizing trial-and-error, those variables were chosen to have the optimum f-measure efficiency and the least amount of builds on existing model.

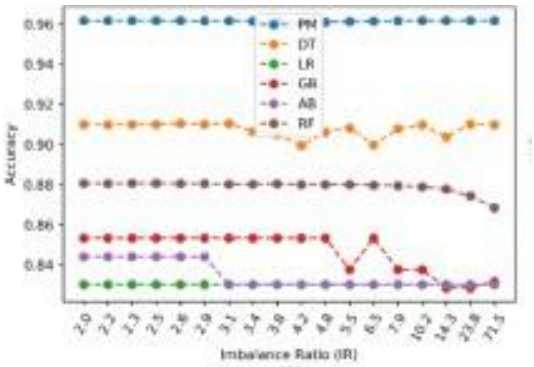

Fig. 3. Output results with attacks**.**

Predicated on its past knowledge, the detecting aspects evaluate it as a regular or an attack (Experimental details). If the data presented is recognised as being realistic, It will be given to an OCSVM interface for additional analysis by comparison to the patterns of typical data. The identification portion will be contacted to collect the attack's attribution if the recognition portion identifies the samples as an attack. The surveillance system is then given access to all the results. samples as an attack. The surveillance system is then given access to all the results.

Algorithm	Training	Testing
DT	$O(n^3)$	$O(n)$
PCA	$O(n^3)$	$O(1)$
OCSVM	$O(n^3)$	$O(n^2)$
DNN	$O(n^4)$	$O(n^2)$

Fig. 4. Computational complexity of used algorithms

5 CONCLUSION

A unique two-stage ensemble deep learning-based attack detection and attack attribution paradigm for unbalanced ICS data was created in this study. The attacker detection phase performs a DT to identify the attacker instances after mapping the information to the newly larger dimensional space using deep representation learning. This stage can identify previously unexplored assaults and is resistant to large datasets. Each one-vs-all classifier in the attack attribution stage has been developed on a different attack attribute. As shown, the existing model creates a complicated DNN with a feature that is both completely and linked and can correctly identify cyberattacks. Considering the suggested framework's intricate design Identical to other DNN-based algorithms used in the literature, the computational complexity of the training and testing is O(n 4) and O(n 2), correspondingly (n represents the number of training set). Furthermore, the suggested system outperforms earlier research in

terms of recall and f- measure for timely detection and attribution of data. The construction of a cyber-threat hunters feature is a possible development that will help with the discovery of anomalies that are hidden from the detection component, for example by creating a class attribute from over entire network and the components.

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. G. Falco, C. Caldera, and H. Shrobe, "IIoT Cybersecurity Risk Modeling for SCADA Systems," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4486– 4495, (2018).
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. S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 252–260, (2016).
6. J.F.Clemente, "No cybersecurity for critical energy infrastructure,"Ph.D. dissertation, Naval Postgraduate School, (2018).
7. C. Bellinger, S. Sharma, and N. Japkowicz, "One class versus binary classification: Which and when in 2012 11th International Conference on Machine Learning and Applications, vol. 2, 2012, pp. 102–106.
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).
9. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822– 6834,(2019).
10. I. A. Khan, D. i, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," IEEE Access, vol. 7, pp. 89 507– 89 521, (2019).
11. T. K. Das, S. Adepu, and J. Zhou, "Anomaly detection in industrial control systems using logical analysis of data," Computers & Security, vol. 96, p. 101935, (2020).
12. J. J. Q. Yu, Y. Hou, and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3271–3280,(2018).
13. M. M. N. Aboelwafa, K. G. Seddik, M. H. Eldefrawy, Y. Gadallah, and M. Gidlund, "A machine learning-based technique for false data injection attacks detection in industrial iot," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8462–8471, (2020)