INTERNATIONAL JOURNAL OF
RECENT TRENDS IN MULTIDISCIPLINARY RESEARCH
https://www.doi.org/10.59256/ijrtmr.20240401003
January-February 2024, Vol 4(01), 17-20.
ISSN No: 2583-0368

Towards Detection and Attribution of Cyber Attacks in IoT Enabled Cyber-Physical Systems

Dr .X.S. Asha Shiny[1], B.Vaishnavi[2], V.Shreya[3], K.Siddarth[4], D.Harika[5]

[1]*Associate professor, Department of Information Technology, CMR Engineering College (UGC Autonomous), Hyderabad, Telangana, India.*

[2,3,4,5] *B.Tech IV-Year, Department of Information Technology, CMR Engineering College (UGC Autonomous), Hyderabad, Telangana, India.*

OPEN ACCESS

Article Citation:
Dr .X.S. Asha Shiny[1], B.Vaishnavi[2], V.Shreya[3], K.Siddarth[4], D.Harika[5], "Towards Detection and Attribution of Cyber Attacks in IoT Enabled Cyber-Physical Systems", International Journal ofRecent Trends In Multidisciplinary Research, January-February 2024, Vol 4(01), 17-20.

Published by 5th Dimension Research Publication.

Abstract: Internet of Things (IoT) enabled cyber physical systems such as Industrial equipment's and operational IT to send and receive data over internet. This equipment's will have sensors to sense equipment condition and report to centralized server using internet connection. Sometime some malicious users may attack or hack such sensors and then alter their data and this false data will be report to centralized server and false action will be taken. Due to false data many countries equipment and production system got failed and many algorithms was developed to detect attack, but all these algorithms suffer from data imbalance (one class my contains huge records (for example NORMAL records and other class like attack may contains few records which lead to imbalance problem and detection algorithms may failed to predict accurately). To deal with data imbalance, existing algorithms were using OVER and UNDER sampling which will generate new records for FEWER class only. Securing Internet of Things (IoT)-enabled cyberphysical 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 connection between ICS or IIoT-based systems with public networks, however, increases their attack surfaces and risks of being targeted by cyber criminals.To overcome from this issue, we are introducing novel technique without using any under or oversampling algorithms. The proposed technique consists of 2 parts.

Auto encoder: It will get trained on imbalanced dataset and then extract features from it and these extracted features will get trained with DECISION TREE algorithm to predict label for known or unknown attacks. Decision tree get trained on reduced number of features obtained from PCA (principal component analysis) algorithm.

Deep Neural Network (DNN): In this level, DNN algorithm get trained on known and unknown attacks.

Key Word: Cyber Physical Systems (CPS), Industrial Control System (ICS).

1. Introduction

Sensors are most commonly used in numerous applications ranging from body-parameters' measurement to automated driving. Moreover, sensors play a key role in performing detection- and vision-related tasks in all the modern applications of science, engineering and technology where the computer vision is dominating. An interesting emerging domain that employs the smart sensors is the Internet of Things (IoT) dealing with wireless networks and sensors distributed to sense data in real time and producing specific outcomes of interest through suitable processing. In IoT-based devices, sensors and artificial intelligence (AI) are the most important elements which make these devices sensible and intelligent. In fact, due to the role of AI, the sensors act as smart sensors and find an efficient usage for a variety of applications, such as general environmental monitoring [1].

Monitoring a certain number of environmental factors; weather forecasting; satellite imaging and its use; remote sensing based applications; hazard events' monitoring such as landslide detection; self-driving cars; healthcare and so on. In reference to this latter sector, recently the usage of smart devices has been hugely increased in hospitals and diagnostic centers for evaluating and monitoring various health conditions of affected patients, remotely as well as physically [2]. Practically, there is no field of science or research which performs smartly without using the modern sensors. The wide usage and need of sensors; and IoT employed in remote sensing, environment and human health monitoring make the applications as intelligent. In the last decade, the agriculture applications have also included [3] the utilization of many types of sensors for monitoring and controlling various types of environmental parameters such as temperature, humidity, soil quality, pollution, air quality, water contamination, radiation, etc.

This paper also aims to highlight the use of the sensors and IoT for remote sensing and agriculture applications in terms of extensive discussion and review. In recent years, SHM of civil structures has been a critical topic for research. SHM helps to detect the damage of a structure, and it also provides early caution of a structure that is not in a safe condition for usage. Civil infrastructure like [4] bridges get damaged with time, and the reason for the damage is heavy vehicles, loading environmental changes, and dynamic forces such as seismic. These types of changes mainly occur at existing structures constructed long ago, and various methods will detect that damage. The strategy of SHM involves observing the structure for a certain period to notice the condition of the structure and the periodic measurements of data will be collected, and the features of data will be extracted from these computation results, and the process of analysis can be done with the help of a featured data to find out the present-day health of the structure.

The information collected from the process can be updated periodically to monitor the structure and based on the data collected through monitoring a structure, and the structure can be strengthened and repaired, and rehabilitation and maintenance can be completed [5] As IoT devices often have limited resources, implementing lightweight security protocols and leveraging machine learning algorithms for real-time threat analysis are crucial. Continuous monitoring, encryption, and regular updates are essential components of a comprehensive cyber security strategy in the IoT landscape.

2. Deep Neural Network (DNN)

A deep neural network, or DNN, is an artificial neural network sketched for processing structured arrays of data such as portrayals.

1. DNN used to extract relevant features from IoT network traffic and device telemetry data to capture patterns indicative of cyber attacks.

2. DNN Implement transfer learning to leverage pre-trained models, enhancing efficiency and performance.

3. Deep neural networks support continuouslearning, enabling them to adapt to changes in the IoT environment and incorporate new knowledge about emerging cyber threats.

4. Deep neural networks can model complex relationships between different IoT devices and their interactions within a Cyber-Physical System.

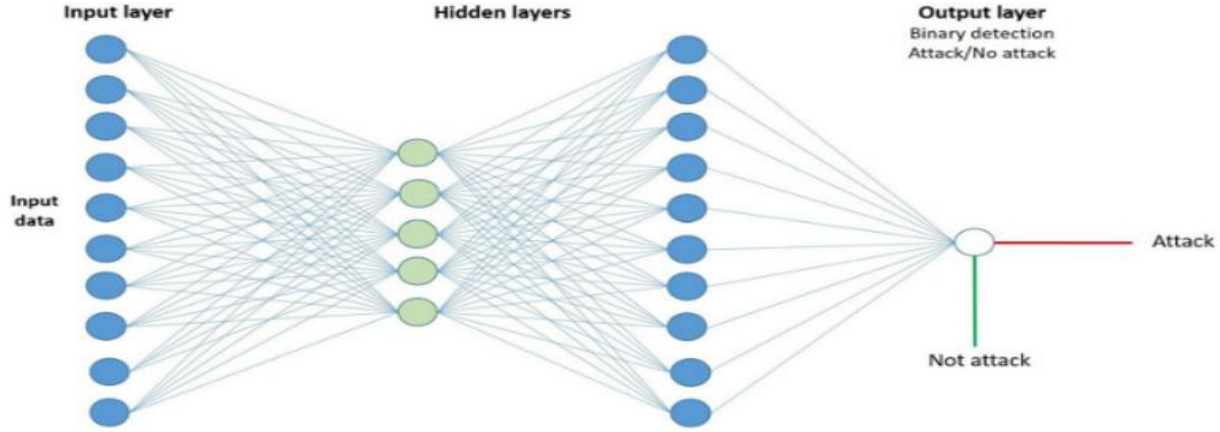
5. Combining multiple deep neural networks using ensemble techniques improves the overall robustness and accuracy of cyber attack detection.

6. Deep neural networks excel at recognizing intricate patterns and anomalies within large datasets, making them well-suited for identifying subtle cyber attack patterns in the complex and dynamic environment of IoT-enabled Cyber-Physical Systems (CPS).

7. Networks like Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks can capture temporal dependencies.

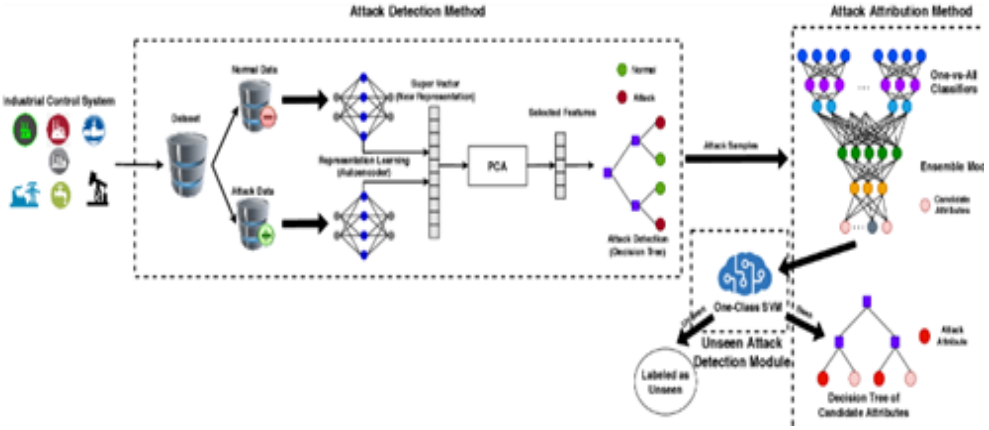
8. Integration of deep neural networks with attribution mechanisms enables the tracing of detected anomalies back to specific IoT devices or network segments.

9. Deep neural networks can leverage transfer learning by pre-training on a large dataset from a related domain.



3. System Architecture

We need to upload the dataset of selected feature values where feature extraction is done from the Cyber attacks and non-Cyber attacks which is called as trained data set. This is used to train the DNN model. Dataset of selected feature values is given as input to the DNN model and output is generated whether the given input is detected or Not detected. Accuracy is generated based on the DNN Model.It's essential to choose an architecture and parameters that are suitable for the specific task and dataset to achieve the best results.



4. Input Design

The input design for detecting and attributing cyber attacks in IoT-enabled cyber-physical systems is a critical aspect of developing a robust cybersecurity framework. It involves the careful consideration of various elements to ensure effective monitoring, analysis, and response to potential threats.The first step in the input design is to determine the types of data to be collected from IoT devices and cyber-physical systems. This includes network traffic data, system logs, device behavior, and any other relevant information that can provide insights into the normal functioning of the system.

IoT devices are equipped with sensors that generate valuable data. The input design should incorporate mechanisms to integrate and interpret data from these sensors. This may involve standardizing data formats and ensuring compatibility across diverse sensor types.Establishing standardized communication protocols is crucial for consistent data exchange between IoT devices. This helps in creating a unified and coherent dataset that can be analyzed effectively for anomalies or suspicious activities.Including metadata in the collected data is essential for contextualizing information. Metadata may include device information, timestamps, and geographical location, providing a comprehensive understanding of the environment in which the IoT-enabled cyber-physical systems operate.

5. Output Design

The output design for detecting and attributing cyber attacks in IoT-enabled Cyber-Physical Systems (CPS) involves a multifaceted approach to ensure comprehensive security. Firstly, a robust intrusion detection system (IDS) is imperative. Employing anomaly-based detection mechanisms, the IDS monitors network traffic and device behavior, identifying deviations from established baselines. Signature-based detection complements this by recognizing known attack patterns.To attribute cyber attacks, a forensics-oriented output framework is essential. Logging and timestamping network activities facilitate post-incident analysis. The output design includes a centralized repository for storing forensic data,

aiding investigators in reconstructing the timeline of events. Utilizing blockchain technology enhances the integrity and immutability of these logs, ensuring the credibility of the attribution process.

6. Modules

1. Upload SWAT water Dataset
2. Read &split Dataset To Train & Test
3. Execute autoencoder algorithm
4. Execute decision tree with PCA Algorithm
5. Execute DNN Algorithm
6. Display detected attack type
7. Predict Accuracy

7. Result

In fig(a) , in square bracket, we can see TEST data values and after arrow -> symbol we can see detected ATTACK TYPE.

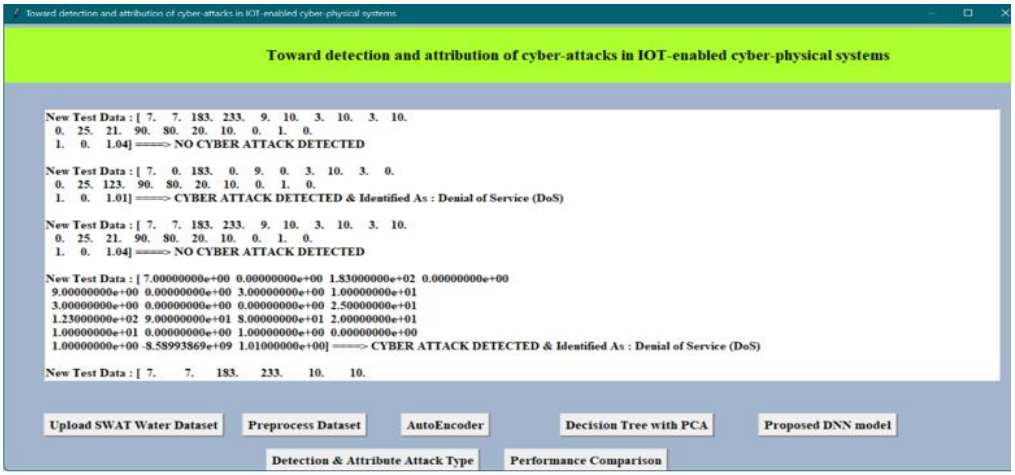


Fig (a)

Below screen Fig(b) we can see algorithm names and its metrics values such as accuracy and precision and other.

Algorithm Name	Accuracy	Precision	Recall	FSCORE
AutoEncoder	90.0	73.14281070224018	73.58689458689459	73.29616654463219
Decision Tree with PCA	90.4779411764706	85.75313833952161	74.62748067246231	73.96952834086689
DNN	100.0	100.0	100.0	100.0

Fig (b)

8. Acknowledgement

- We are extremely grateful to Dr. A. Srinivasula Reddy, Principal and Dr. Madhavi Pingili, HOD, Department of IT, CMR Engineering College for their constant support.
- We are extremely thankful to Dr. X.S. Asha Shiny, Associate Professor, Internal Guide, Department of IT, for her constant guidance, encouragement and moral support throughout the project.
- We express our thanks to all staff members and friends for all the help and co-ordination extended in bringing out this project successfully in time.

References

1. *Dazhe Zhao, Kaijun Zhang, Yan Meng, Zhaoyang Li, Yucong Pi, Yujun Shi, Jiacheng You, Renkun Wang, Ziyi Dai, Bingpu Zhou, Junwen Zhong, Untethered triboelectric patch for wearable smart sensing and energy harvesting, Nano Energy, Volume 100, 2022, 107500, ISSN22112855 htts://doi.org/10.1016/j.nanoem.2022.107500*
2. *Carminati, M.; Sinha, G.R.; Mohdiwale, S.; Ullo, S.L. Miniaturized pervasive sensors for indoor health monitoring in smart cities. Smart Cities 2021, 4, 146–155.*
3. *Sivasuriyan, A., Vijayan, D.S., LeemaRose, A., Revathy, J., Gayathri Monicka, S., Adithya, U.R. and Jebasingh Daniel, J., 2021. Development of smart sensing technology approaches in structural health monitoring of bridge structures. Advances in Materials Science and Engineering, 2021.*

4. *Ullo, S.L. and Sinha, G.R., 2021. Advances in IoT and smart sensors for remote sensing and agriculture applications. Remote Sensing, 13(13), p.2585.*
5. *Kayad, A.; Paraforos, D.; Marinello, F.; Fountas, S. Latest advances in sensor applications in agriculture. Agriculture 2020, 10, 362.*
6. *Elahi, H.; Munir, K.; Eugeni, M.; Atek, S.; Gaudenzi, P. Energy harvesting towards self-powered IoT devices. Energies 2020, 13, 5528.*
7. *Ullo, S.L.; Sinha, G.R. Advances in smart environment monitoring systems using IoT and sensors. Sensors 2020, 20, 3113.*
8. *A. Verma, S. Prakash, V. Srivastava, A. Kumar and S. C. Mukhopadhyay, "Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review," in IEEE Sensors Journal, vol. 19, no. 20, pp. 9036-9046, 15 Oct.15, 2019.*
9. *Z. Hu, Z. Bai, Y. Yang, Z. Zheng, K. Bian and L. Song, "UAV Aided Aerial-Ground IoT for Air Quality Sensing in Smart City: Architecture, Technologies, and Implementation," in IEEE Network, vol. 33, no. 2, pp. 14-22, March/April 2019.*