International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Toward Detection and Attribute of Cyber - Attacks in IoT - Enabled Cyber-Physical Systems

K. Sirisha I, Saragadam Sridhar

[1, 2]Department of Master of Computer Science, Miracle Educational Society Group of Institutions, Vizianagram– 535216 (AP) India
[1]Email: *sirishakanuru4g[at]gmail.com*
[2]Email: *sridharmagnus[at]gmail.com*

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 articlepresents a two-level ensemble attack detection and attribution framework designed forCPS, 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 to facilitate attack attribution. The proposed model is evaluated using real-world data sets in gas pipeline and water treatment system. Findings demonstrate that the proposed model outperforms other competing approaches with similar computational complexity.***

Keywords: Internet of Things (IOT), CPS (Cyber Physical Systems), information/operational technology (IT/OT)

1. Introduction

I NTERNET 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 (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 (PLCs) 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 attackers. One high-profile example is the Stuxnet campaign, which reportedly targeted Iranian centrifuges for nuclear enrichment in 2010, causing severe damage to the equipment [1], [2]. Another example is that of the incident targeting a pump that resulted in the failure of an Illinois water plant in 2011 [3]. BlackEnergy3 was another campaign that targeted Ukraine power grids in 2015, resulting in a power outage that affected approximately 230 000 people [4]. 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 [1]. Although security solutions developed for information technology (IT) and operational technology (OT) systems are relatively mature, they may not be directly applicable to ICS. For example, this could be the case due to the tight integration between the controlled physical environment and the cyber systems. Therefore, system-level security methods are necessary to analyze physical behavior and maintain system operation availability [1]. ICS security goals are prioritized in the order of availability, integrity, and confidentiality, unlike most IT/OT systems (generally prioritized in the order of confidentiality, integrity, and availability) [5]. Due to close coupling between variables of the feedback control loop and physical processes, (successful) cyber-attacks on ICS can result in severe and potentially fatal consequences for the society and our environment. This reinforces the importance of designing extremely robust safety and security measurements to detect and prevent intrusions targeting ICS [1]. 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 [6]. 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). Therefore, there has been renewed interest in utilizing attack detection and attribution solutions based on machine learning (ML) or deep neural networks (DNNs) in recent times. In addition, attack detection approaches can be categorized into network-based or host-based approaches. Supervised clustering, single-class or multiclass support vector machine (SVM), fuzzy logic, artificial neural network (ANN), and DNN are commonly used techniques for attack detection in network traffic. These techniques analyze real-time traffic data to detect malicious attacks in a timely manner. However, attack detection that considers the only network and host data may fail to detect sophisticated attacks or insider attacks. Unsupervised models that incorporate process/physical data can complement a system's monitoring since they do not rely on detailed knowledge of the cyber-threats. In general, a sophisticated attacker with sufficient knowledge and time, such as a nation state advanced persistent threat actor, can potentially circumvent robust security solutions. Furthermore, most of the existing approaches ignore the imbalanced property of ICS data by modeling only a system's normal behavior and reporting deviations from normal behavior as anomalies. This is, perhaps, due to limited attack samples in existing data sets and real-world scenarios. Although using majority class samples is a good solution to avoid issues due to imbalanced data sets, the trained model will have no view of the attack samples' patterns. In other words, such an approach fails to detect unseen attacks and suffers from a high false-positive

Licensed Under Creative Commons Attribution CC BY

rate [7]. Thus, there have been attempts to utilize DL approaches, for example, to facilitate automated feature (representation) learning to model complex concepts from simpler ones [8] without depending on human-crafted features [9]. Motivated by the above observations, this article presents our proposed novel two-stage ensemble deep-learning-based attack detection and attack attribution framework for imbalanced ICS data set\s. In the first stage, an ensemble representation learning model combined with a decision tree (DT) is designed to detect attacks in an imbalanced environment. Once the attack is detected, several one-versus-all classifiers will ensemble together to form a larger DNN to classify the attack attributes with a confidence interval during the second stage. Moreover, the proposed framework is capable of detecting unseen attack samples. A summary of our approach in this study is as follows. 1) We develop a novel two-phase ensemble ICS attack detection method capable of detecting both previously seen and unseen attacks. We will also demonstrate that the proposed method outperforms other competing approaches in terms ofaccuracy and f-measure. The proposed deep representation learning results in this method being robust to imbalanced data. 2) We propose a novel self-tuning two-phase attack attribution method that ensembles several deep one-versus all classifiers using a DNN. Architecture for reducing false alarm rates. The proposed method can accurately attribute attacks with high similarity. This is the first ML-based attack attribution method in ICS/IIoTat the time of this research. 3) We analyze the computational complexity of the proposed attack detection and attack attribution framework, demonstrating that despite its superior performance, its computational complexity is similar to that of other DNN-based methods in the literature. The remainder of this article will be organized as follows. Section II will introduce the relevant background and related literature. Section III will describe the proposed framework, followed by the experimental setup in Section IV. In Section V, the evaluation findings based on two real-world ICS data sets demonstrate that the proposed framework outperforms several other systems. Finally, Section VI concludes this article.

2. Proposed System

We develop a novel two-phase ensemble ICS attack detection method capable of detecting both previously seen and unseen attacks. We will also demonstrate that the proposed method outperforms other competing approaches in terms of accuracy and f- measure. The proposed deep representation learning results in this method being robust to imbalanced data.

We propose a novel self-tuning two-phase attack attribution method that ensembles several deep one-versusall classifiers using a DNN architecture for reducing false alarm rates. The proposed method can accurately attribute attacks with high similarity. This is the first ML-based attack attribution method in ICS/IIoT at the time of this research.

We analyze the computational complexity of the proposed attack detection and attack attribution framework, demonstrating that despite its superior performance, its computational complexity is similar to that of other DNN-based methods in the literature

Auto Encoder: auto encoder deep learning will get trained on imbalanced dataset and thenextract features from it and this extracted featured 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. If any records contains attack signature then DNN will identify attack labelor class and attribute them.

3. Literature Survey

Girish L, Rao SKN (2020) "Quantifying sensitivity and performance degradation of virtual machines using machine learning.", Journal of Computational and Theoretical Nanoscience , Volume 17, Numbers 9-10, September/October 2020, pp.4055-4060(6) https://doi.org/10.1166/jctn.2020.901

Virtualized data centers bring lot of benefits with respect to the reducing the high usage of physical hardware. But nowadays, as the usage of cloud infrastructures are rapidly increasing in all the fields to provide proper services on demand. In cloud data center, achieving efficient resource sharing between virtual machine and physical machines are very important. To achieve efficient resource sharing performance degradation of virtual machine and quantifying the sensitivity of virtual machine must be modeled, predicted correctly. In this work we use machine learning techniques like decision tree, *K* nearest neighbor and logistic regression to calculate the sensitivity of virtual machine. The dataset used for the experiment was collected using collected from open stack cloud environment. We execute two scenarios in this experiment to evaluate performance of the three mentioned classifiers based on precision, recall, sensitivity and specificity. We achieved good results using decision tree classifier with precision 88.8%, recall 80% and accuracy of 97.30%.Madala, S. R., & Rajavarman, V. N. (2018). Efficient Outline Computation for Multi View Data Visualization on Big Data. International Journal of Pure and Applied Mathematics, 119(7), 745-755

In Big data analysis, representation of data in different views with respect to visualization for handling large scale data. Continuous parallel co-ordinate framework is effective data visualization tool to analyze each attribute without any change or update in their values, without change in continues information structures and present data in structural orientationbased on attributes to handle high amount of data. To present data in multi attribute evaluation, traditionally use Similarity Measure Centered with Multi Viewpoint (SMCMV) approach and related clustering approaches to represent data based on multi view data visualization procedure with different attributes. For multi dimensional and large scale data have different types of attributes to process and evaluate data based on different values in high amount of data. For efficient data processing to evaluate each attribute in separate manner to represent data in different factor with respect to returning of interest points in large scale data. So that in this paper, we present and develop novel

Licensed Under Creative Commons Attribution CC BY

Hybrid machine learning with sorting algorithm to evaluate data based on different attributes with respect to interest points from high amount of data. Sorting algorithm consists two basic steps in evolution of data, first step evaluates sorted positional index, second step exploits sorted positional index and then evaluate computational with selective and sequential data into table formation. Our implemented approach performs on real world UCI repository mostly used data sets with sorting to exploit results comparison of existing algorithms with respect to time, memory and table index evaluation for sorted data.

Vivek, T. V. S., Rajavarman, V. N., & Madala, S. R. (2020). Advanced graphical-based security approach to handle hard AI problems based on visual security. International Journal of Intelligent Enterprise, 7(1-3), 250-266

Security is the main aspect to explore human data from different web oriented applications present in artificial intelligence (AI). It is very difficult to use different web applications without security to access data in various places. So that various types of security related approaches were introduced to use services in securely in outside environment, but they have some limitations to protect data from outside attackers (hackers). So that in this paper, we propose and introduce a novel and advanced security model to provide security from outside attackers in AI related web oriented applications. In this approach, we follow the basic features related to Captcha as a graphical password to enable security services in our proposed approach. Using Captcha graphical passwords in our approach, we describe pushing attacks, pass-on attacks and guessing attacks in web applications with random selection of Captcha passwords to use web services. Our experimental results show efficient security relations when compare to existing security approaches in terms of Captcha generation, time and other parameters present in web security applications.

Madala, S. R., Rajavarman, V. N., & Vivek, T. V. S. (2018). Analysis of Different Pattern Evaluation Procedures for Big Data Visualization in Data Analysis. In Data Engineering and Intelligent Computing (pp. 453-461). Springer, Singapore

Data visualization is the main focusing concept in big data analysis for processing and analyzing multi variate data, because of rapid growth of data size and complexity of data. Basically data visualization may achieve three main problems, i.e. 1. Structured and Unstructured pattern evaluation in big data analysis. 2. Shrink the attributes in data indexed big data analysis. 3. Rearrange of attributes in parallel index based data storage. So in this paper we analyze different techniques for solving above three problems with feasibility of each client requirement in big data analysis for visualization in real time data stream extraction based on indexed data arrangement. We have analyzed different prototypes in available parallel co-ordinate and also evaluate quantitative exert review in real time configurations for processing data visualization. Report different data visualization analysis results for large and scientific data created by numerical simulation in practice sessions analysed in big data presentation.

4. Results

Internet of Things 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 got failed and many algorithms was developed to detect attack but all this algorithms suffers 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 but this technique improve accuracy but not up to the mark.

To overcome from this issue author is introducing novel technique without using any under or oversampling algorithms and this technique consists of twoparts

1) Auto Encoder: auto encoder deep learning will get trained on imbalanced dataset and then extract features from it and this extracted featured 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.
2) Deep Neural Network (DNN): in this level DNN algorithm get trained on known and unknown attacks. If any records contains attack signature then DNN will identify attack label or class and attribute them.

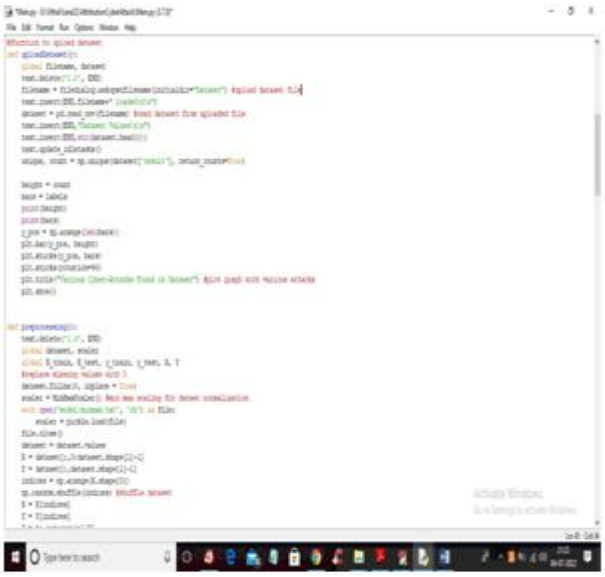
To implement this project author has used SWAT (secure water treatment) and this dataset contains IOT request and response signature and associate each dataset with unique attack label and dataset contains below cyber-attack labels **'Normal', 'Naive Malicious Response Injection (NMRI)', 'Complex Malicious', 'Response Injection (CMRI)', 'Malicious State Command Injection (MSCI)', 'Malicious Parameter Command Injection (MPCI)', 'Malicious Function Code Injection (MFCI)', 'Denial of Service (DoS)'**

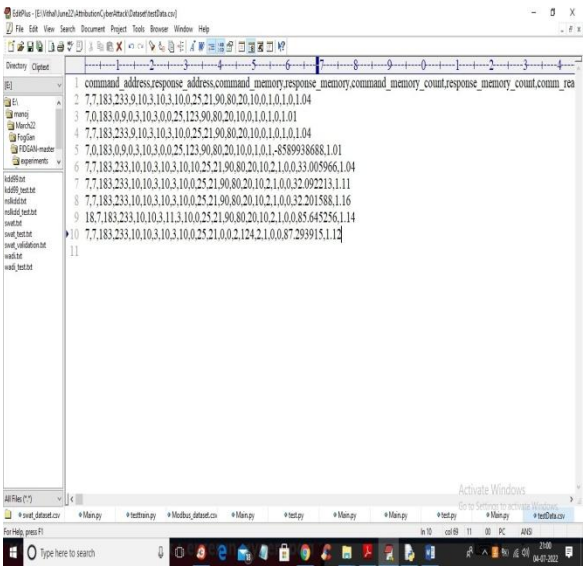
Above are the attacks found in dataset and dataset contains above labels as integer value of its index for example NORMAL label index will be 0 and continues up to 8 class labels. Below screen showing dataset details

In above dataset screen first row contains dataset column names and remaining rows contains dataset values and in last column we have attack type from label 0 to 7. We will used above dataset to train propose Auto Encoder, decision tree and DNN algorithms.

In below screen we are using NEW test data which contains only signature and there is no class label and propose algorithm will detect and attribute class labels.

Licensed Under Creative Commons Attribution CC BY





In above test data we have IOT request signature without class labels. To implement this project we have designed following modules

Upload SWAT Water Dataset: using this module we will upload dataset to application and then read dataset and then find different attacks found in dataset

Preprocess Dataset: using this module we will replace all missing values with 0 and then apply MIN-MAX scaling algorithm to normalized features values and then split dataset into train and test where application used 80% dataset for training and 20% for testing

Run AutoEncoder Algorithm: using this module we will trained AutoEncoder deep learning algorithm and then extract features from that model.

Run Decision Tree with PCA: extracted features from AutoEncoder will get transform using PCA to reduce features size and then retrain with Decision tree. Decision tree will predict label for each record based on dataset signatures

Run DNN Algorithm: predicted decision tree label will further train with DNN (deep neural network) algorithm to detect and attribute attacks

Detection & Attribute Attack Type: using this module we will upload unknown or un-label TEST DATA and then DNN will predict attack type

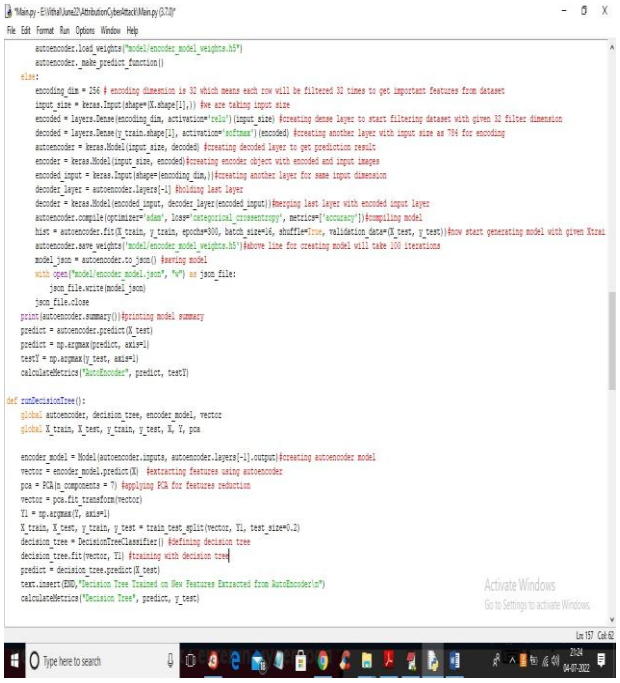
Comparison Graph: using this module we will plot comparison graph between all algorithms

Comparison Table: using this module we will display comparison table ofall algorithms which contains metrics like accuracy, precision, recall and FSCORE.

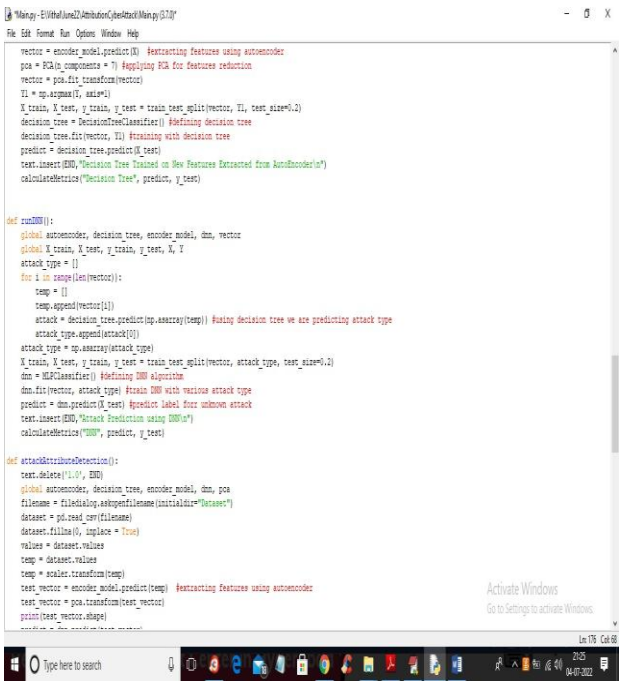
In below screen you can read red colour comments to know about algorithmsimplementation

In above screen read red colour comments to know about dataset loading andmin-max normalization

Licensed Under Creative Commons Attribution CC BY



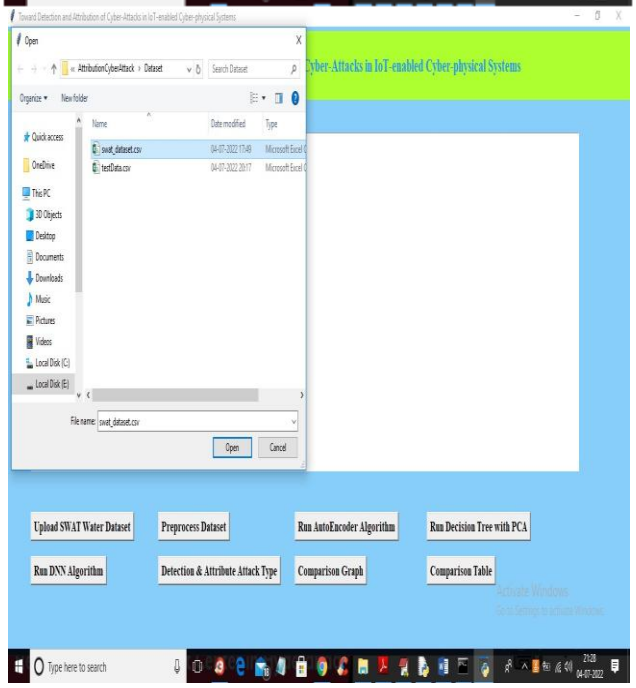
In above screen you can see we are using AutoEncoder, PCA and decision tree to train dataset and in below screen we are using DNN algorithms to train



In above screen we are training dataset with DNN algorithms SCREEN SHOTS

To run project double click on 'run.bat' file to get below screen

In above screen click on 'Upload SWAT Water Dataset' button to uploaddataset to application and get below output

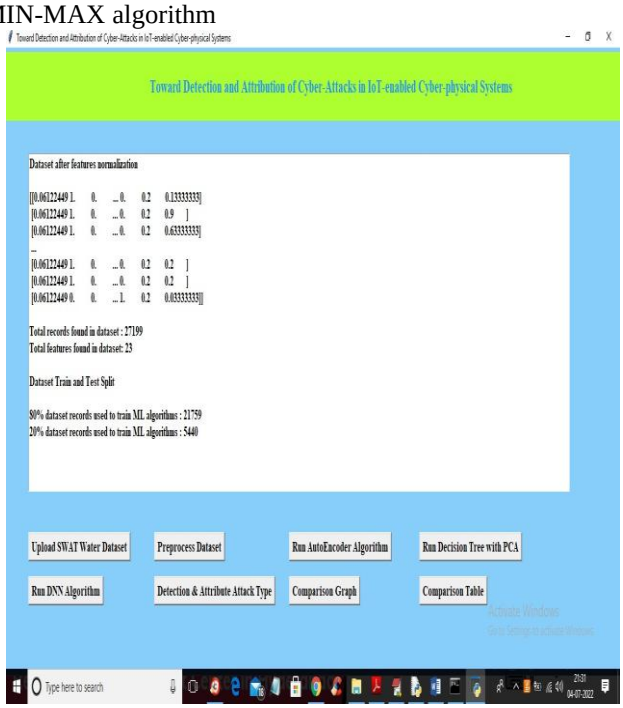


In above screen selecting and uploading SWAT dataset file and then click on 'Open' button to load dataset and get below output

In above screen dataset loaded and in graph x-axis contains ATTACK NAMEand y-axis contains count of those attacks found in dataset and we can see 'NORMAL' class contains so many records and other attacks contains very few records so it will raise data imbalance problem which can be solved using AutoEncoder, Decision Tree and DNN. Now close above graph and then click on 'Preprocess Dataset' button to remove missing values and then normalized values with

Licensed Under Creative Commons Attribution CC BY

MIN-MAX algorithm



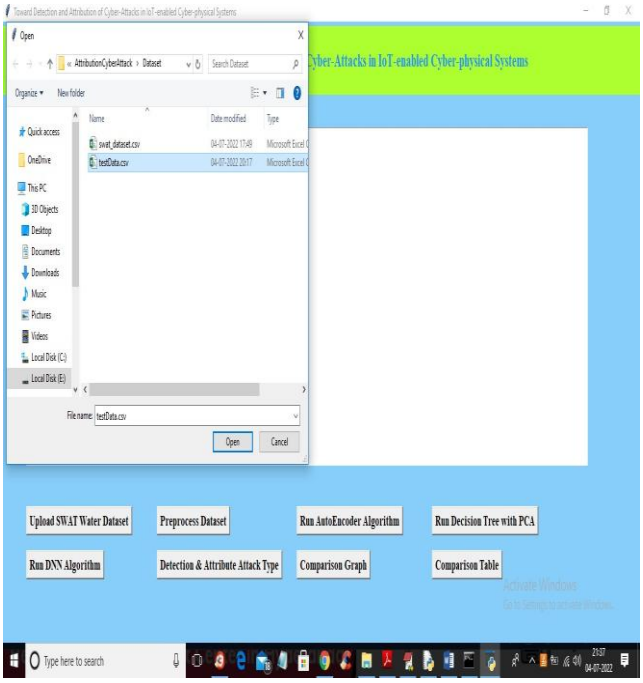
In above screen all values are normalized (converting data between 0 and 1 called as normalization) and then we can see total records in dataset and then dataset train and test split records count also displaying. Now dataset is ready and now click on 'Run AutoEncoder Algorithm' button to train dataset with AutoEncoder and get below accuracy

In above screen with AutoEncoder we got 90% accuracy and this accuracy canbe enhance by implementing Decision Tree with PCA algorithm and now click on 'Run Decision Tree with PCA' button to get below output

In above screen we can see with decision tree accuracy and precision value is enhanced and now click on 'Run DNN Algorithm' button to further enhance accuracy and get below output

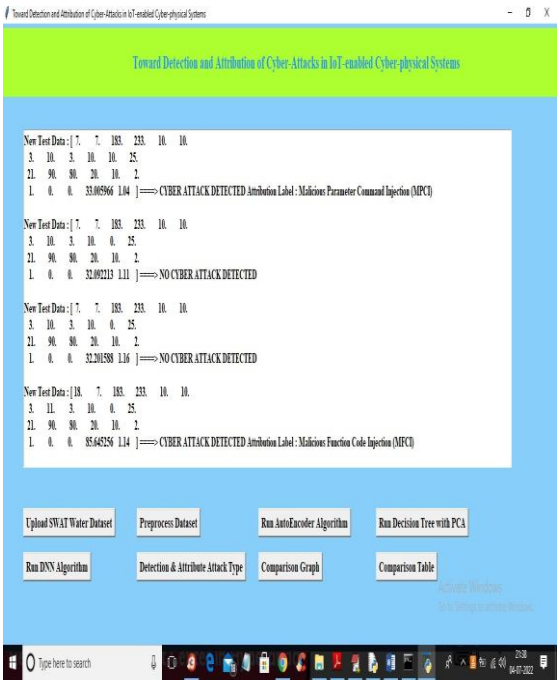
In above screen with DNN we got 99% accuracy and now click on 'Detection & Attribute Attack Type' button to upload test DATA and detect attack attributes

Licensed Under Creative Commons Attribution CC BY



In above screen selecting and uploading 'TEST DATA' file and then click on'Open' button to get below output

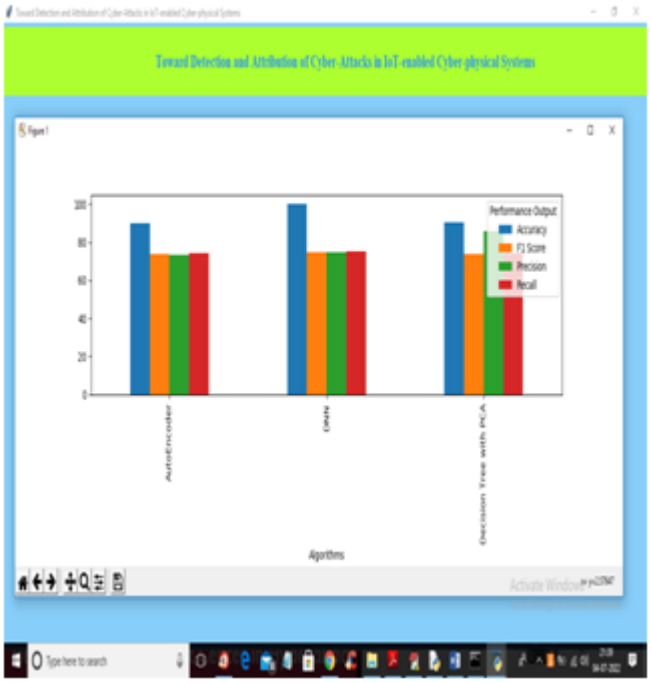
In above screen in square bracket we can see TEST data values and after arrow=□ symbol we can see detected ATTACK TYPE and scroll down above textarea to view all detection



In above screen we can see detected various attacks and now click on 'Comparison Graph' button to get below graph

In above graph x-axis represents algorithms names and y-axis represents different metric values such as precision, recall, accuracy and FSCORE with different colour bars and in all algorithms DNN got high accuracy and now close above graph and then click on 'Comparison Table' to get below comparison table of all algorithms

In above table we can see algorithm names and its metrics values such asaccuracy and precision and other.



5. Conclusion

This article proposed a novel two-stage ensemble deep learning-based attack detection and attack attribution framework for imbalanced ICS data. The attack detection stage uses deeprepresentation learning to map the samples to the new higher dimensional space and appliesa DT to detect the attack samples. This stage is robust to imbalanced data sets and capable of detecting previously unseen attacks. The attack attribution stage is an ensemble of severalone-versus-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 cyberattacks, as demonstrated. Despite the complex architecture of the proposed framework, the computational complexity of the training and testing phases is, 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. The future extension includes the design of a cyber-threat hunting component to facilitate the identification of anomalies invisible to the detection component for example bybuilding a normal profile over the entire system and the assets.

Licensed Under Creative Commons Attribution CC BY

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 GatheringExperience 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.
[11] S. Aljawarneh, M. Aldwairi, and M. B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," Journal of Computational Science, vol. 25, pp. 152–160, 2018.
[12] Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." in ICISSP, 2018, pp. 108–116.
[13] D. Aksu, S. Ustebay, M. A. Aydin, and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm," in International Symposium on Computer and Information Sciences. Springer, 2018, pp. 141–149.
[14] N. Marir, H. Wang, G. Feng, B. Li, and M. Jia, "Distributed abnormal behavior detection approach based on deep belief network and ensemble svm using spark," IEEE Access, 2018.
[15] P. A. A. Resende and A. C. Drummond, "Adaptive anomaly-based intrusion detectionsystem using genetic algorithm and profiling," Security and Privacy, vol. 1, no. 4, p. e36, 2018.
[16] C. Cortes and V. Vapnik, "Support-vector networks," Machine learning, vol. 20, no. 3,pp. 273–297, 1995.
[17] R. Shouval, O. Bondi, H. Mishan, A. Shimoni, R. Unger, and A. Nagler, "Application of machine learning algorithms for clinical predictive modeling: a data-mining approach in sct," Bone marrow transplantation, vol. 49, no. 3, p. 332, 2014.

Licensed Under Creative Commons Attribution CC BY