International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

SECURING SMART SENSING PRODUCTION SYSTEM

Ms. M. ANITHA[1], Mr. CH. SATYANARAYANA REDDY[2], Ms. K. NIKITHA SREE [3]
#1 Assistant professor in the Department of Master of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District
#2 Assistant professor in the Department Master of Computer Applications SRK Institute of Technology, Enikepadu, Vijayawada, NTR District
#3 MCA student in the Department of Master of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District.

ABSTRACT The internet of things allows cyber-physical systems such as commercial equipment and operational IT to ship and get hold of records over the internet. Those devices will have sensors to experience the circumstance of the system and file to a centralized server through internet connection. Sometime a few malicious customers may additionally attack or hack such sensors and then alter their facts and these fake facts might be pronounced to centralized server and wrong actions may be taken.
Because of fake facts many nations system and production gadget were given failed and lots of algorithms became evolved to come across attack however most of these algorithms be afflicted by information imbalance one class can also incorporate huge data (for instance normal information and different class like attack can also incorporate few facts which lead to imbalance problem and detection algorithms might also didn't are expecting appropriately). To address facts imbalance, existing algorithms have used OVER and below sampling, which generates new statistics for the fewer elegance, but this method improves accuracy however now not up to the mark

1.INTRODUCTION

INTERNET OF THINGS(IoT) gadgets are an increasing number of included in cyber–bodily structures (CPS), along with in important infrastructure sectors, along with dams and application vegetation. In those settings, IoT gadgets [also referred to as Industrial IoT (IIoT)] are frequently a part of an business manipulate device (ICS), tasked with the dependable operation of the infrastructure. ICS can be extensively defined to encompass supervisory control and information acquisition (SCADA) structures, dispensed manage systems (DCS), and systems that contain programmable good judgment controllers (%) and Modbus protocols.

The connection among ICS or IIoT-based totally systems with public networks, however, increases their assault surfaces and risks of being targeted with the aid of cyber attackers. One high-profile example is the Stuxnet campaign, which reportedly targeted Iranian centrifuges for nuclear enrichment in 2010, causing extreme damage to the system. Some other examples is that of the incident focused on a pump that resulted within the failure of an Illinois water plant in 2011. Black Energy became another campaign that centered Ukraine power grids in 2015, ensuing in a power outage that affected approximately 230 000 humans.
In April 2018, there had been additionally reviews of a hit cyber-attack affecting 3

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

U.S. Fuel pipeline corporations, and resulted inside the shutdown of electronic patron conversation structures for numerous days. Despite the fact that safety solutions advanced for information generation (IT) and operational generation (OT) structures are fantastically mature, they'll no longer be without delay applicable to ICS. As an instance, this can be the case due to the tight integration among the controlled bodily environment and the cyber systems.

Therefore, system-stage safety strategies are vital to analyze physical conduct and preserve gadget operation availability. ICS safety desires are prioritized within the order of availability, integrity, and confidentiality, unlike maximum IT/OT structures (normally prioritized in the order of confidentiality, integrity, and availability). Because of near coupling between variables of the comments manage loop and bodily approaches, (successful) cyber-assaults on ICS can bring about extreme and probably fatal outcomes for the society and our surroundings.

This reinforces the significance of designing extraordinarily strong safety and safety measurements to come across and save you intrusions targeting ICS. Famous attack detection and attribution approaches consist of the ones based on signatures and anomalies. To mitigate the known limitations in both signature-primarily based and anomaly primarily based detection and attribution strategies, there were attempts to introduce hybrid-primarily based strategies.

Although hybrid-based totally approaches are effective at detecting unusual activates, they're now not reliable because of common community improvements, resulting in extraordinary intrusion detection machine (IDS) typologies. Past this, traditional assault detection and attribution strategies specially rely upon community metadata analysis (e.g., IP addresses, transmission ports, traffic period, and packet intervals). Consequently, there was renewed interest in utilizing assault detection and attribution answers primarily based on gadget gaining knowledge of (ML) or deep neural networks (DNNs) in recent times.

In addition, attack detection techniques can be categorized into community-based totally or host-based totally methods. Supervised clustering, unmarried-magnificence or multiclass assist vector system (SVM), fuzzy good judgment, synthetic neural network (ANN), and DNN are typically used techniques for assault detection in community site visitors.

These techniques analyze actual-time site visitors' facts to stumble on malicious attacks in a timely manner. But assault detection that considers the simplest community and host facts can also fail to detect state-of-the-art assaults or insider attacks. Unsupervised fashions that contain manner/physical information can supplement a device's tracking on account that they do now not depend upon specific knowledge of the cyber-threats.

In popular, a sophisticated attacker with enough know-how and time, which includes a country advanced chronic risk actor, can potentially keep away from robust protection answers. Furthermore, maximum of the existing methods ignores the imbalanced belongings of ICS

information by means of modeling handiest a gadget's normal behavior and reporting deviations from regular conduct as anomalies.

This is, possibly, because of limited attack samples in existing statistics units and real-international situations. Although the usage of majority elegance samples is a good technique to keep away from issues because of imbalanced information units, the skilled version will don't have any view of the assault samples' patterns. In other phrases, such an technique fails to detect unseen assaults and suffers from a excessive fake-high-quality charge.

As a result, there were tries to utilize DL procedures, for instance, to facilitate computerized function (representation) learning to model complicated standards from simpler ones [8] without relying on human-crafted functions. Inspired by using the above observations, this article gives our proposed novel -degree ensemble deep-gaining knowledge of-based totally attack detection and assault attribution framework for imbalanced ICS information units.

Within the first degree, an ensemble representation studying model mixed with a decision tree (DT) is designed to discover assaults in an imbalanced surrounding. As soon as the attack is detected, several one-as opposed to-all classifiers will ensemble together to form a bigger DNN to categories the assault attributes with a self-belief interval for the duration of the second level. Furthermore, the proposed framework is able to detecting unseen assault samples.

2.LITERATURE SURVEY

2.1 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 centres 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 centre, 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 modelled, predicted correctly. In this work we use machine learning techniques like decision tree, *K* nearest neighbour 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%.

2.2 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

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

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 orientation based on attributes to handle high amount of data. To present data in multi attribute evaluation, traditionally use Similarity Measure Centred 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 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.

3.PROPOSEDWORK

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 of accuracy 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-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.

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.

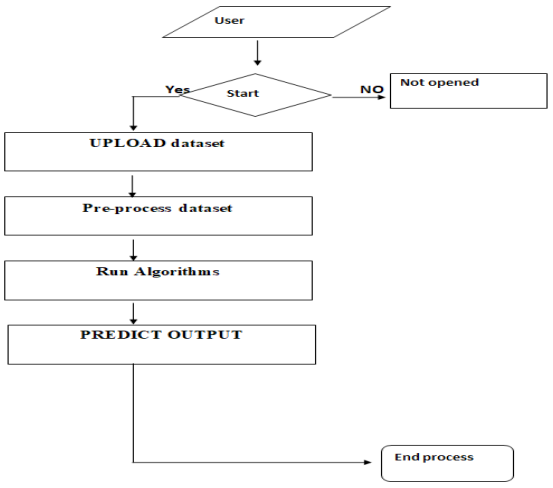

Fig 1: Working Architecture

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

3.1 IMPLEMENTATION

3.1.1 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

3.1.2 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

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

3.1.4 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

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

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

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

4.RESULTS AND DISCUSSION

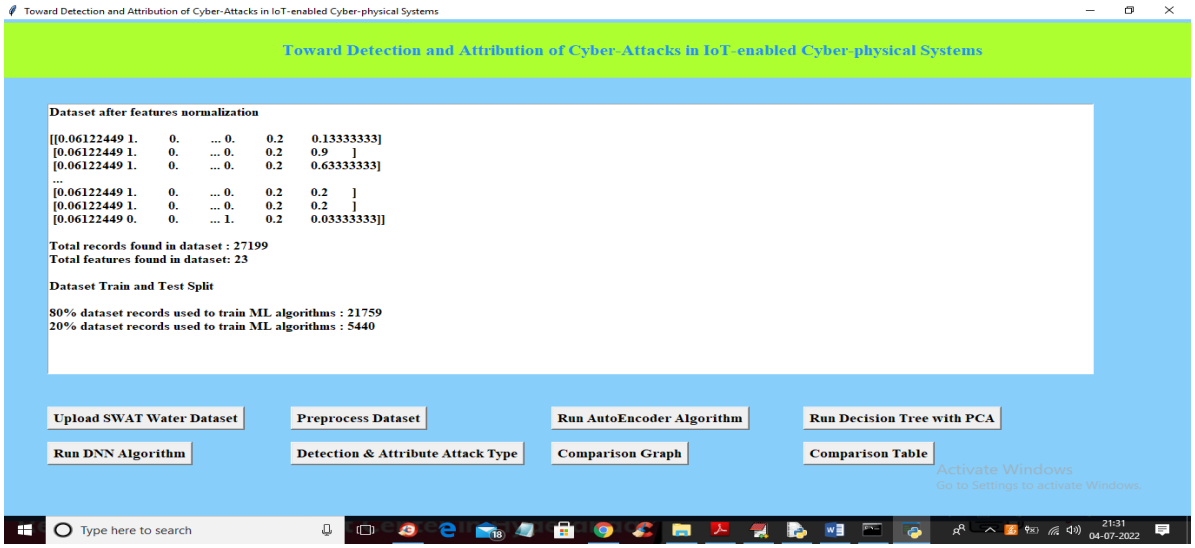

Fig 2: preprocess dataset

In above display all values are normalized (changing statistics between 0 nd 1 called as normalization) after which we will see total facts in dataset after which dataset educate and test split statistics depend also displaying.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

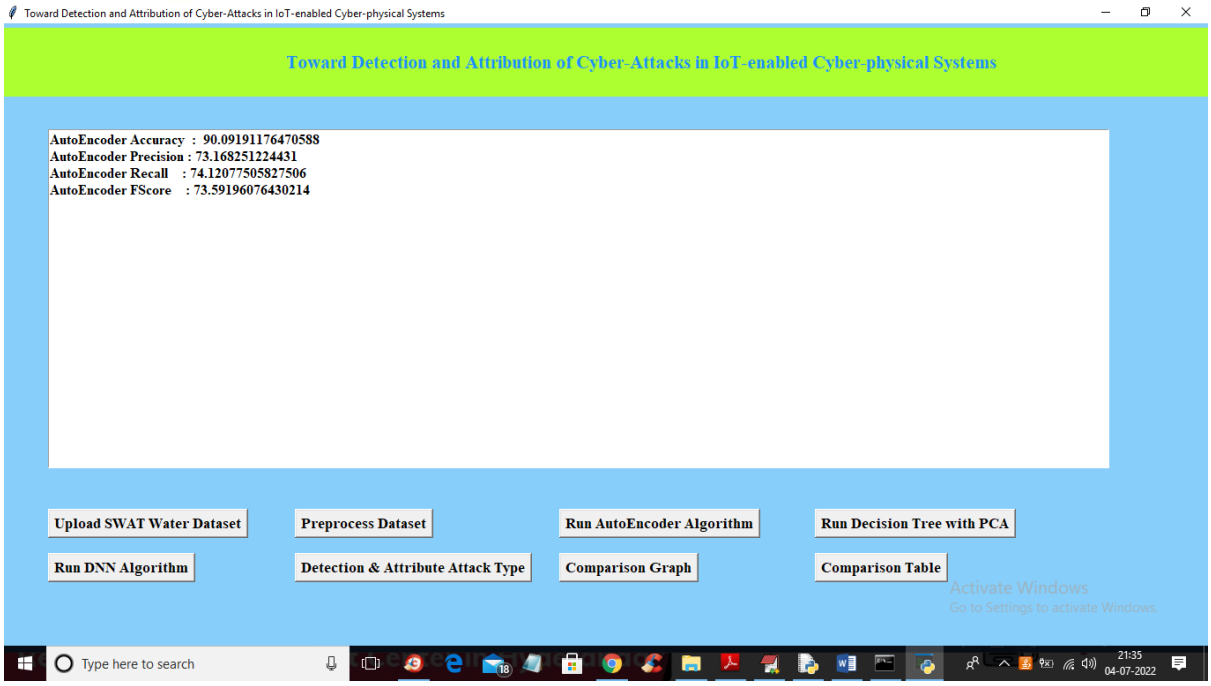

Fig3: Run Autoencoder

In above display screen with Autoencoder we were given ninety% accuracy and this accuracy may be beautify by using enforcing choice Tree with PCA algorithm and now click on 'Run decision Tree with PCA' button to get under output

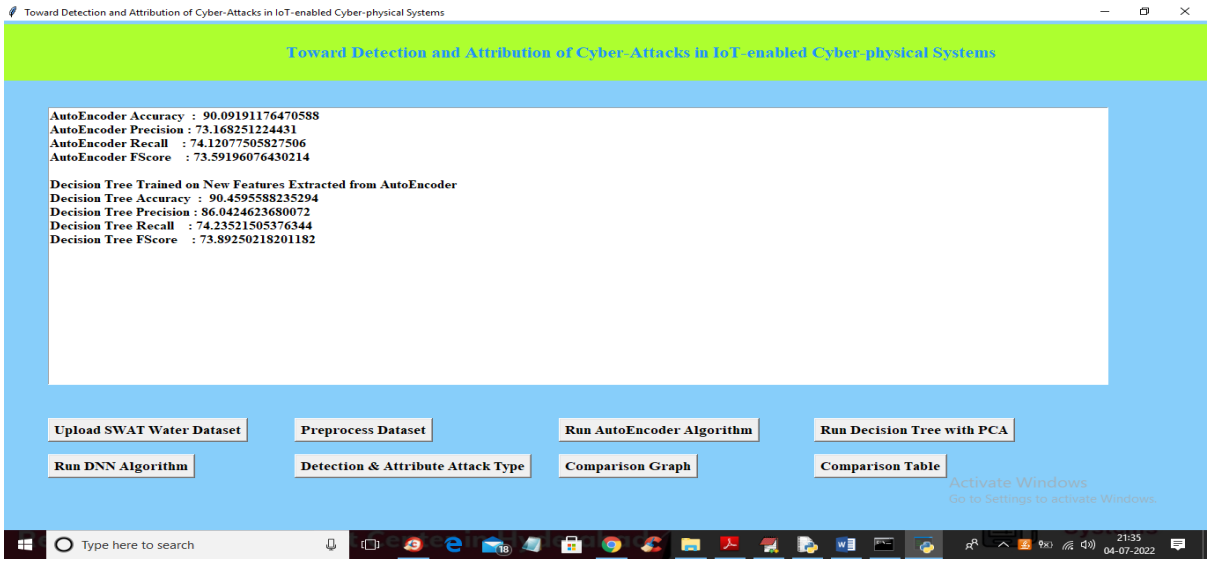

Fig 4: Decision tree with pca

In above display we will see with choice tree accuracy and precision fee is improved and now click on on 'Run DNN set of rules' button to similarly enhance accuracy and get beneath output

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

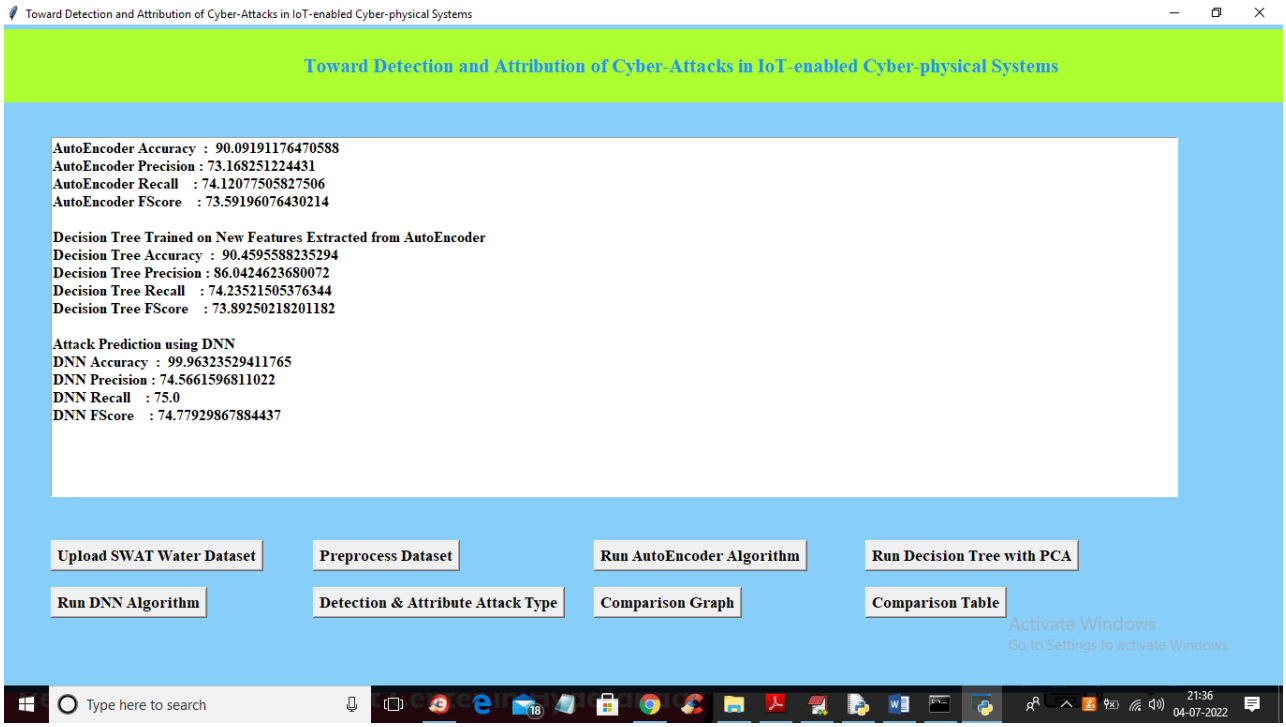

Fig 5:Run DNN

In above display with DNN we were given ninety 99% accuracy and now click on 'Detection & attribute attack type' button to add check facts and stumble on assault attributes

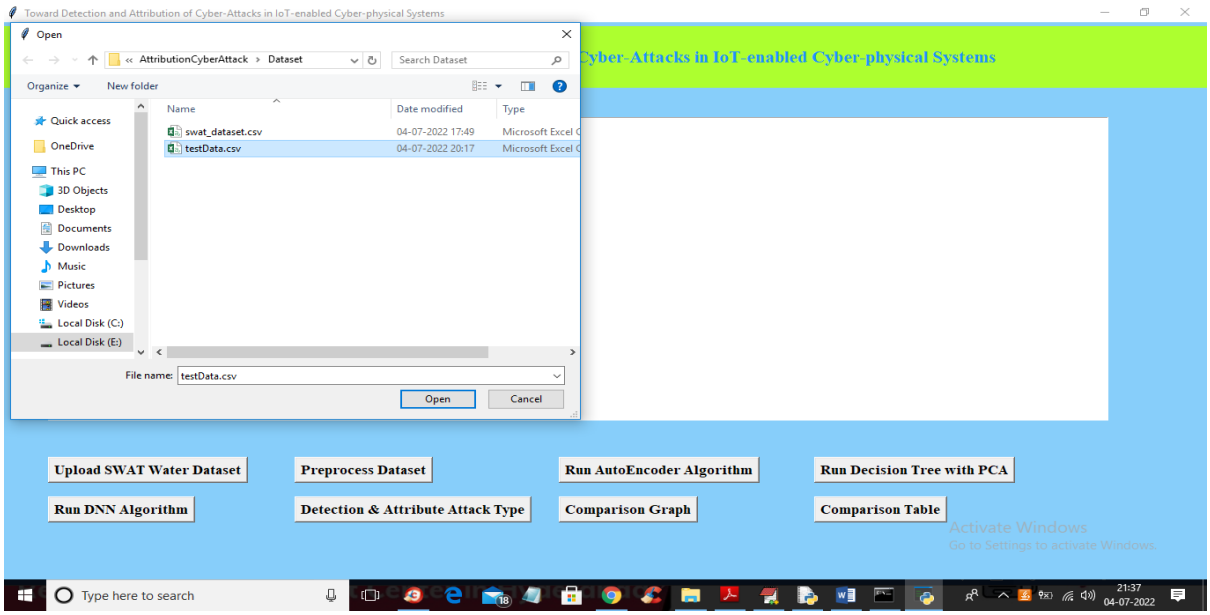

Fig 6: upload test dataset

In above display deciding on and uploading 'take a look at statistics' file and then click on on 'Open' button to get underneath output

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362
IJARST

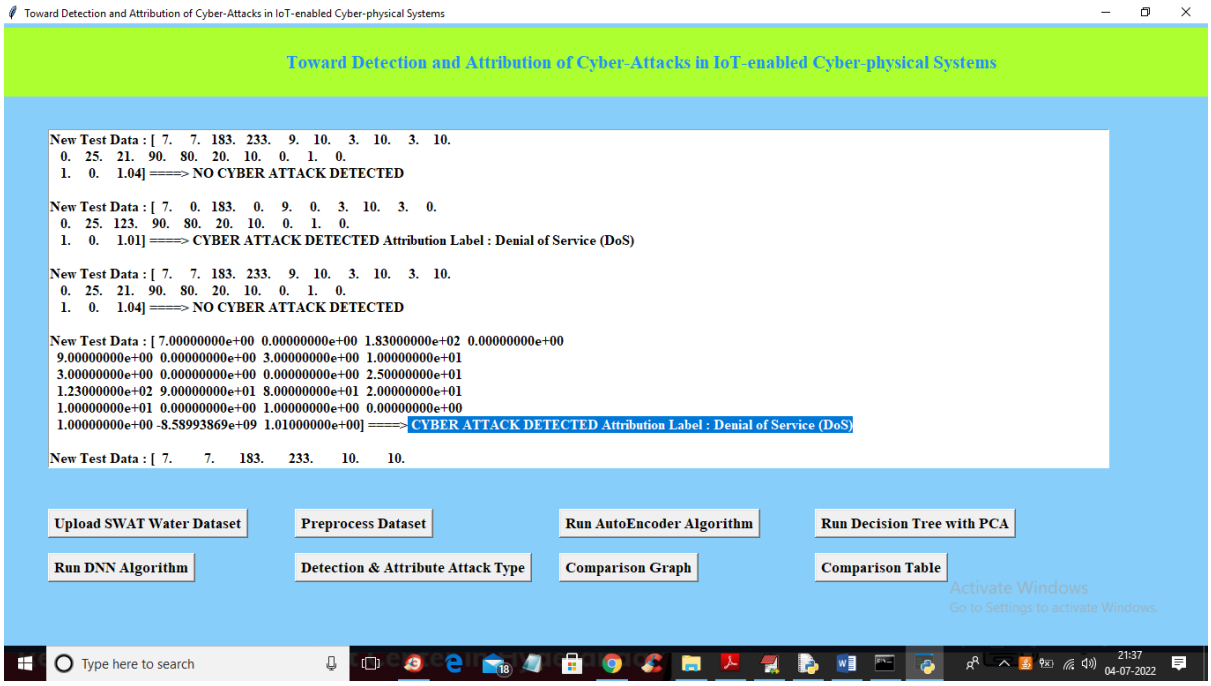

Fig 7: attack detection

In above display screen we will see detected various assaults and now click on on 'Comparison Graph' button to get below graph

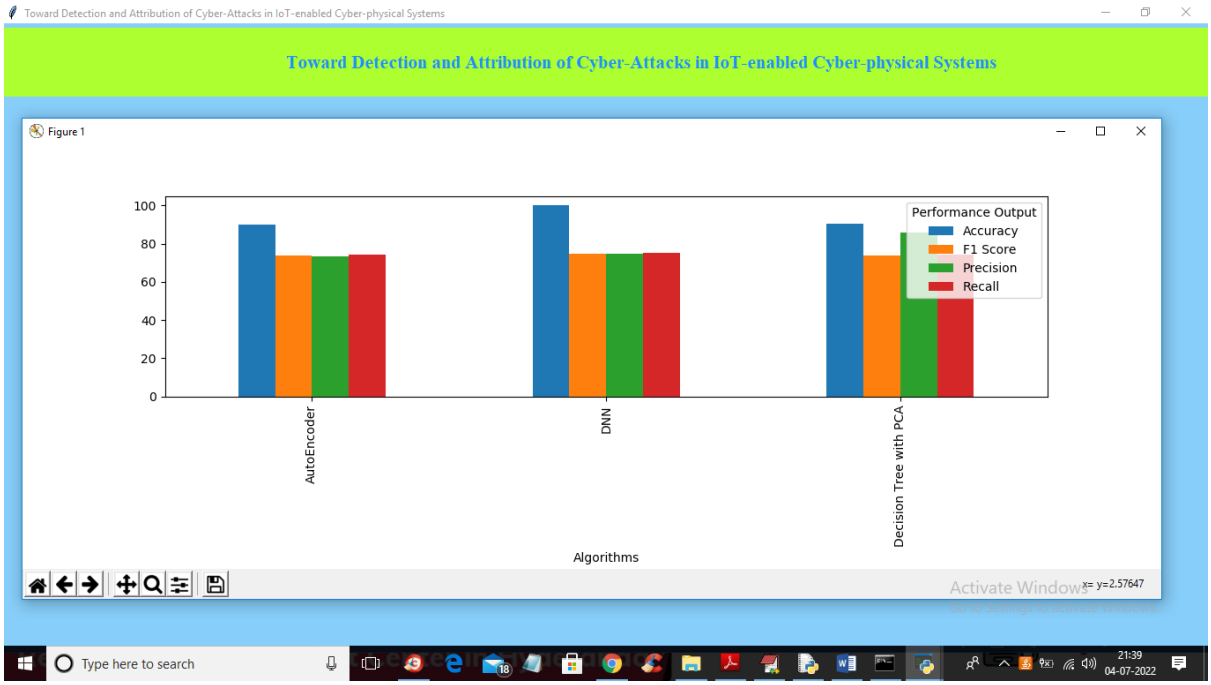

Fig 8: comparison graph

In above graph x-axis represents algorithms names and y-axis represents distinct metric values consisting of precision, don't forget, accuracy and FSCORE with unique coloration bars and in all algorithms DNN were given high accuracy and now near above graph and then click on on 'comparison table' to get below comparison desk of all algorithms

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

5. CONCLUSION

This paper proposes a novel two-stage ensemble deep learning-based attack detection and attack attribution framework for unbalanced 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 is capable of detecting previously unseen attacks. The attack attribution stage is an ensemble of multiple one-versus-all classifiers, each trained on a specific attack attribute. The entire model forms a complex DNN with a partially connected and a 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 is O(n4) and O(n2), respectively, where n is the number of training samples, which is similar to other DNN-based techniques in the literature. Furthermore, the proposed framework can detect and attribute the samples in a timely manner with 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 by building a normal profile over the entire system and assets.

REFERENCES

[1] ok. Graves, Ceh: reputable licensed ethical hacker overview manual: exam 312-50. John Wiley & Sons, 2007.

[2] R. Christopher, "Port scanning strategies and the defense in opposition to them," SANS Institute, 2001.

[3] M. Baykara, R. Das¸, and i. Karado ˘gan, "Bilgi g ¨uvenli ˘gi sistemlerinde kullanilan arac¸larin incelenmesi," in 1st worldwide Symposium on digital Forensics and safety (ISDFS13), 2013, pp. 231–239.

[4] S. Staniford, J. A. Hoagland, and J. M. McAlerney, "sensible automated detection of stealthy portscans," journal of computer security, vol. 10, no. 1-2, pp. One hundred and five–136, 2002.

[5] S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, "Surveillance detection in excessive bandwidth environments," in DARPA facts Survivability convention and Exposition, 2003. Court cases, 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.

[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 principal component analysis for ids," in IEEE International Conference on Communication and Electronics Systems, 2016, pp. 1–5.

AUTHOR PROFILES

Ms. M. ANITHA completed her Master of Computer Applications and Master of Technology. Currently working as an Assistant professor in the Department of Master of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr. CH. SATYANARAYANA REDDY Completed his Bachelor of Computer Applications at Acharya Nagarjuna University. He completed his Master Computer Applications at Acharya Nagarjuna University. Currently working as an Assistant professor in the Department of Master of Computer Applications SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. His areas of interest include Networks, Machine Learning & Artificial Intelligence.

Ms. K. NIKITHA SREE is an MCA student in the Department of Master of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She has a Completed Degree in B.Sc.(computers) from sri durga malleswara siddhartha mahila kalasala, Vijayawada. Her areas of interest are DBMS, C, Python and Machine Learning with Python.