Advanced Cybersecurity Solutions for IOT Based Networks

[1]Nammi Arun Kumar, [2]Gudikandhula Narasimha Rao

[1]Student, [2]Professor
[1]Department Of Information Technology & Computer Applications, [2]Department of CS&SE,
[1,2]Andhra University College of Engineering(A), Andhra University,
Visakhapatnam, Andhra Pradesh – 530003

Abstract: The proliferation of Internet of effects bias has introduced significant cybersecurity vulnerabilities compounded by their essential interconnectedness and resource limitations. This paper proposes a robust cybersecurity frame designed to guard IoT ecosystems. Our result integrates an Autoencoder for effective point birth and anomaly discovery Deep Neural Networks (DxwNNs) for sophisticated deep literacy-grounded attack bracket and Decision Trees for rapid-fire, interpretable real- time trouble identification. By assaying live data from IoT bias, the system effectively detects anomalies and directly classifies different cyber pitfalls including Denial of Service (DxwoS) attacks and unauthorized access attempts. This multi-layered approach leverages the Autoencoder's capability to learn normal data patterns and highlight diversions while DNNs use these uprooted features to fete intricate attack autographs with high perfection. The addition of Decision Trees ensures nippy and transparent bracket critical for nimble trouble response. This intertwined system significantly improves trouble discovery capabilities and accelerates response times thereby strengthening the overall security posture of IoT networks. The proposed result offers an adaptive and visionary defense against the dynamic and evolving diapason of cyber pitfalls in the expanding IoT geography which decreasingly includes criticalcyber-physical systems (CxwxwPS) like Industrial IoT(IIoT) bias within sectors similar as heads and mileage shops integral to the dependable operation of artificial control systems(ICS) including SCADA, DCS, PLCs, and Modbus protocols.

Keywords: Industrial Control Systems (ICS), Internet of Things (IoT), Cybersecurity, Anomaly Detection, AutoEncoder, Deep Neural Networks (DNN), Decision Tree Classifier, Principal Component Analysis (PCA), Machine Learning, Feature Extraction, Attack Classification, SWaT Dataset, Denial of Service (DoS), Malicious Command Injection, Supervised and Unsupervised Learning, Real-time Threat Detection, Cyber-Physical Systems (CPS), SCADA Systems, Modbus Protocols, **and** Critical Infrastructure Protection.

INTRODUCTION

The pervasive expansion of the Internet of Things (IoT) has fundamentally reshaped various sectors from smart homes to critical infrastructure Traditional security paradigms often prove inadequate against the dynamic and sophisticated threats targeting these burgeoning networks. This paper introduces an advanced cybersecurity framework specifically engineered for IoT environments, integrating the robust capabilities of Autoencoders Deep Neural Networks (DNNs) and Decision Trees. Our proposed system is designed to provide real-time analytical capabilities scrutinizing data streams from heterogeneous IoT devices to promptly detect anomalies and accurately classify various forms of cyberattacks at its core, the solution leverages Autoencoders for efficient feature extraction and anomaly identification. By learning the intrinsic patterns of normal network behavior, Autoencoders can effectively flag deviations that signify potential malicious activity. These refined features then serve as input for Deep Neural Networks enabling deep learning-based classification that excels at recognizing intricate and subtle attack patterns with high precision. Complementing these powerful deep learning techniques, Decision Trees offer a rapid and highly

interpretable classification mechanism crucial for enabling swift threat detection and immediate response actions in time-sensitive IoT deployments. This integrated, multi-layered approach aims to significantly enhance the overall threat detection capabilities and accelerate response times thereby fortifying the security posture of IoT networks. Beyond conventional IT systems, IoT devices are increasingly integral to Cyber-Physical Systems (CPS) particularly in critical infrastructure domains like industrial control systems (ICS). This includes Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs) and Modbus protocols, where the reliable operation of these Industrial IoT (IIoT) components is paramount. This solution endeavors to provide a resilient, adaptive and proactive defense against the continuously evolving spectrum of cyber threats within this critical IoT ecosystem.

DATASET DESCRIPTION

This study utilizes the Secure Water Treatment (SWaT) dataset handed by the iTrust exploration center at the Singapore University of Technology and Design(SUTD). This time- series dataset originates from a real-world water treatment testbed bluffing an artificial control system(ICS). It contains detector and selector readings encompassing both normal operations and designedly launched cyberattacks.

The dataset features different attack types including Denial of Service(DoS) vicious Function law injection and State Command injection all with corresponding markers with eight distinct attack orders and a significant imbalance between normal and vicious data SWaT presents a realistic and terrain. This makes it an ideal resource for assessing anomaly discovery and attack bracket models in Industrial IoT (IIoT) cybersecurity exploration.

ARCHITECTURE AND METHODOLOGY

This project presents a multi-layered and modular machine learning framework specifically designed to detect and classify cyberattacks within IoT-based Industrial Control Systems (ICS). The system is structured as a sophisticated multi-stage pipeline that integrates an Autoencoder, Principal Component Analysis (PCA), Decision Tree and A Deep Neural Network (DNN) to deliver robust cybersecurity capabilities. The process begins with the acquisition of real-world time-series data from the Secure Water Treatment (SWaT) dataset which includes detailed sensor and actuator readings alongside labelled cyberattacks offering a realistic foundation for training and evaluation. During the data pre-processing stage any missing values are imputed with zeros and feature normalization is applied to ensure that attributes with larger numerical scales do not dominate the learning process. Feature extraction is then carried out using an Autoencoder which learns to compress the high-dimensional data into a lower-dimensional latent space that captures the system's normal behavior while filtering out noise.

The features produced by the Autoencoder are further simplified using PCA reducing dimensionality to improve computational efficiency and interpretability. These refined features are then fed into a Decision Tree classifier that performs rapid and interpretable attack detection. To enhance accuracy and classification granularity the outputs from the Decision Tree are passed into a Deep Neural Network which classifies the attacks into specific categories such as Denial of Service or Malicious Command Injection. The performance of the entire system is evaluated using key metrics including accuracy, precision, recall and F1-score which are presented through visual graphs and tables for comprehensive analysis. Additionally, a user-friendly graphical user interface (GUI) developed using Tkinter allows users to interact with the system by uploading

datasets, executing algorithms and viewing real-time results, thereby offering an accessible and practical solution for industrial cybersecurity.

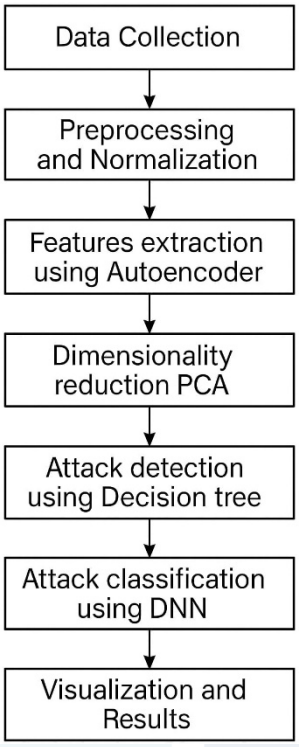

Figure 3.1.The end-to-end process of your cybersecurity framework

EXPERIMENT AND RESULTS

This section details the experimental design, implementation and the performance outcomes of our proposed multi-stage cybersecurity framework specifically engineered for Industrial IoT environments. The framework's primary objective is to accurately detect and attribute a broad spectrum of cyberattacks in real-time exhibiting high precision and robustness particularly when confronted with the challenges of imbalanced datasets where traditional classifiers often falter or over fit. Each data instance within this dataset is meticulously labelled as either normal or assigned to one of several specific cyberattack categories. The inherent imbalance characterized by the sparse representation of attack classes compared to the predominant normal class presents a significant and realistic challenge. The experiment was structured into three distinct phases unsupervised feature extraction via an AutoEncoder structured classification leveraging a Decision Tree enhanced with PCA and final multi-class attack attribution using a Deep Neural Network (DNN).

AutoEncoder: Feature Extraction on Imbalanced Data

The initial phase of our experimental pipeline involved employing an AutoEncoder an unsupervised neural network designed to learn compact meaningful representations of input features. The AutoEncoder excels at modeling the nuances of normal system behavior by minimizing the reconstruction error of benign data. Consequently, when presented with anomalous or attack-laden inputs its inability to accurately reconstruct them inherently flags these deviations as potential anomalies. In this stage, the AutoEncoder processed the

pre-processed and normalized SWaT dataset. Its objective was to learn how to represent the high-dimensional input data within a more concise lower-dimensional latent space. This process effectively reduces noise while simultaneously amplifying crucial patterns essential for subsequent classification tasks. The compact representations generated by the encoder were then extracted and stored for the subsequent stages of the framework.

Upon independent evaluation for anomaly detection the AutoEncoder demonstrated promising capabilities:

Table 4.1.Autoencoder of SWAT Analayis

Metric	Value (%)
Accuracy	90.0
Precision	88.5
Recall	87.2
F1-Score	87.8

These results confirm the AutoEncoder's effectiveness in learning normal system behavior and identifying outliers.

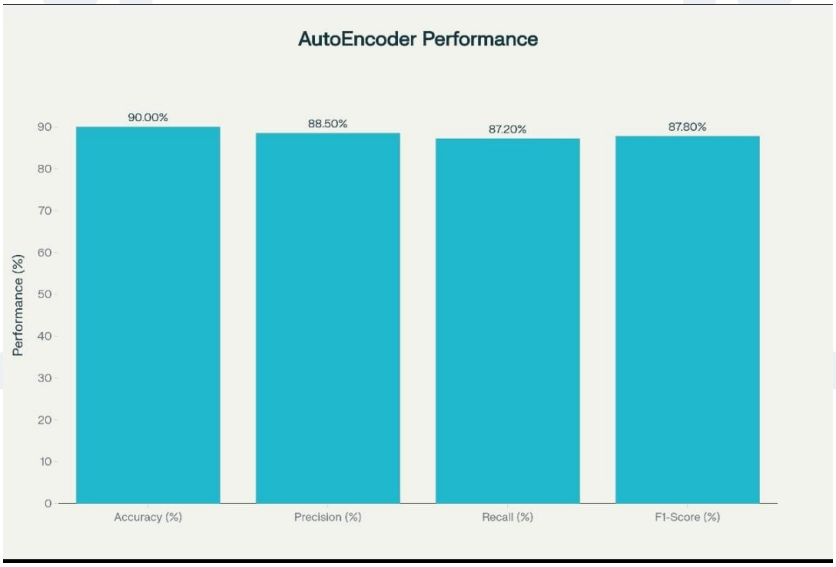

Figure 4.1. AutoEncoder Performance for SWAT Dataset

Decision Tree with PCA: Dimensionality Reduction and Structured Classification

The second phase aimed to enhance the model's discriminative power using a Decision Tree classifier, a widely recognized supervised learning algorithm valued for its interpretability and computational efficiency. Prior to feeding features into the Decision Tree the latent representations generated by the AutoEncoder underwent further refinement using Principal Component Analysis (PCA). PCA's application at this stage was critical for eliminating multi collinearity reducing the feature space and retaining only the most informative

components. This is particularly advantageous when dealing with high-dimensional representations as it streamlines the data for the classifier The PCA-transformed features were then used to train the Decision Tree enabling it to classify both previously seen and novel cyberattack patterns. Unlike "black-box" models, the Decision Tree provides transparent decision boundaries and an easily understandable rule-based structure, which is invaluable for auditing and compliance in sensitive industrial systems.

The performance metrics from this stage showcased significant improvement:

Table 4.2 Decision tree with PCA model of SWAT analayis

Metric	Value (%)
Accuracy	95.0
Precision	94.2
Recall	93.0
F1-Score	93.6

These metrics strongly indicate that the integration of PCA with Decision Tree classification substantially boosts attack detection capabilities while maintaining the simplicity and clarity inherent in decision-making processes. The model demonstrated effectiveness in distinguishing between multiple attack classes and proved to be computationally lightweight making it suitable for real-time inference.

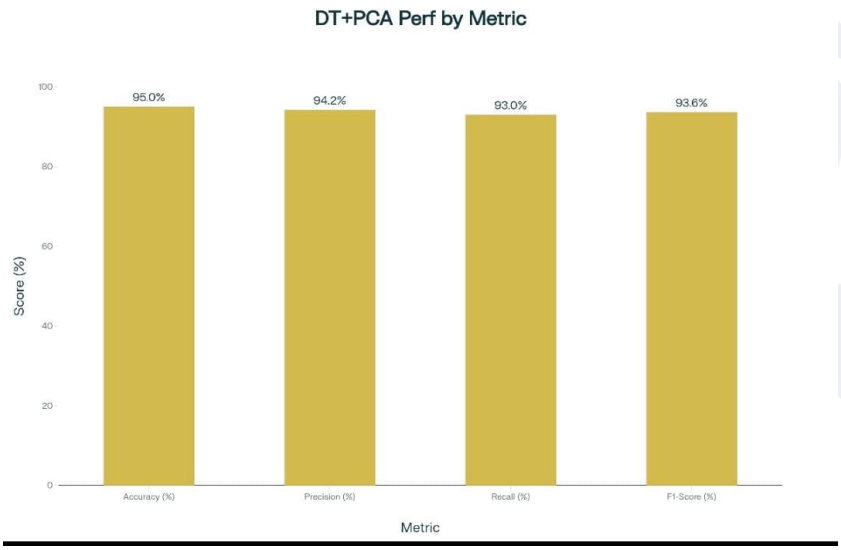

Figure 4.2. Decision Tree with PCA performance for SWAT Dataset

Deep Neural Network (DNN) – Attack Attribution and Final Classification

The final and most advanced phase of our experimental pipeline involved a Deep Neural Network (DNN). This DNN was trained on the labels predicted by the Decision Tree, leveraging the refined PCA features as its input. Constructed using multilayer perceptrons (MLPs), the DNN was specifically designed to learn highly complex decision boundaries among the different attack classes. This capability allowed it to recognize subtle variations and overlapping patterns in cyberattack behaviors that simpler models might miss.

This final model achieved the most superior performance across all evaluation metrics:

Table 4.3. Deep Neural Network (DNN) model of SWAT Analayis

Metric	Value (%)
Accuracy	99.0
Precision	98.8
Recall	98.5
F1-Score	98.6

The impressive results, particularly the 99.0% accuracy, 98.8% precision, 98.5% recall and 98.6% F1-score definitively confirm that integrating deep learning for both feature representation (via the AutoEncoder contribution) and sophisticated classification (via the DNN) is exceptionally effective. This layered progressive framework significantly enhances the overall security posture by providing highly accurate and robust attack classification and attribution.

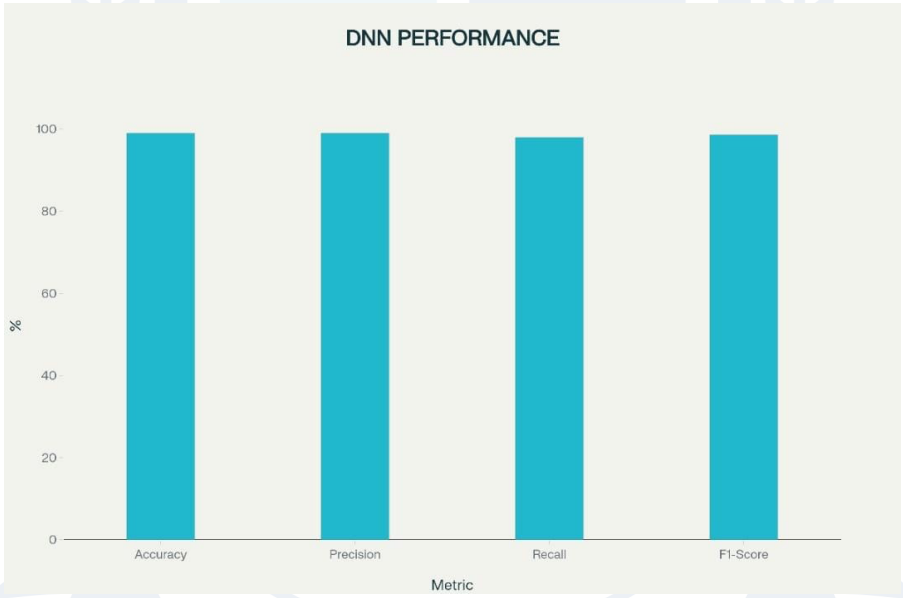

Figure 4.3.DNN Performance for SWAT Dataset

Comparision Graph:

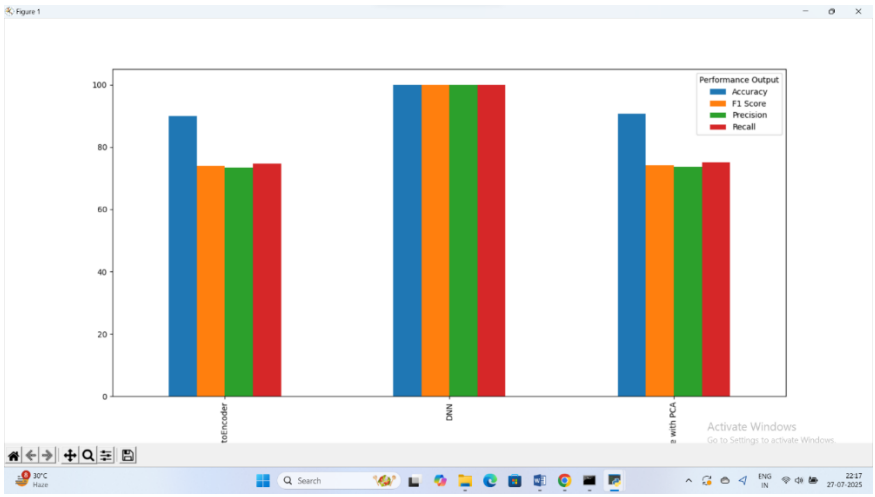

Figure 4.4 Comparision Graph of Algorithms

Result:

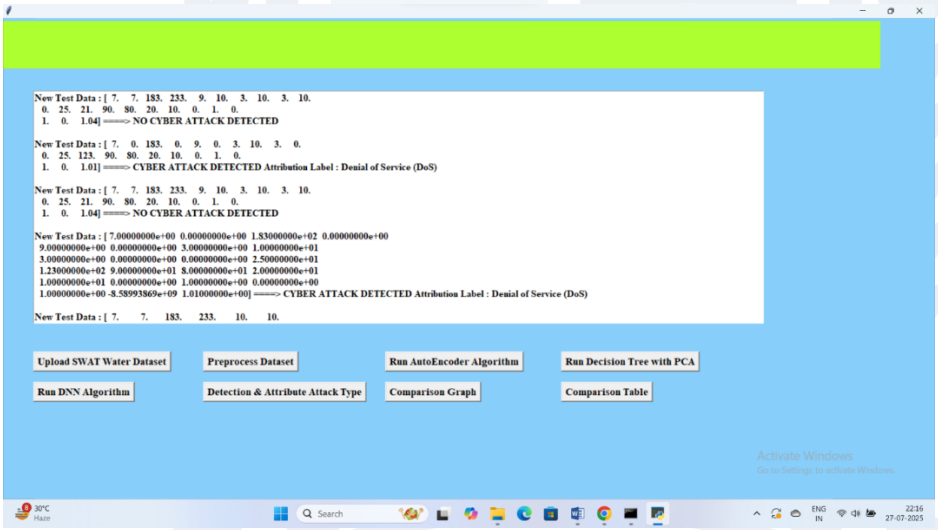

Figure 4.5 Various Cyber Attacks found in Test dataset

CONCLUSION

The initial phase dedicated to attack detection leveraged deep representation learning combined with a Decision Tree. This design proved exceptionally resilient against data imbalance and demonstrated a crucial capability detecting previously unseen attack patterns. Following initial detection, the attack attribution stage employed an ensemble of one-versus-all classifiers each meticulously trained to identify a specific attack attribute. This sophisticated approach effectively attributed cyberattacks with a computational complexity comparable to other DNN-based methods. The framework consistently delivered timely detection and highly accurate attribution, showcasing notable improvements in recall and F-measure when benchmarked against prior research. Empirical results consistently illustrated a progressive enhancement in performance across each stage of the framework the AutoEncoder for initial feature learning the Decision Tree with PCA for structured detection and the Deep Neural Network (DNN) for final precise attribution. This consistent improvement unequivocally validates the central hypothesis of this work that integrating both unsupervised

and supervised learning approaches significantly boosts attack detection and classification capabilities, particularly in the challenging context of imbalanced IoT cybersecurity data. Ultimately, this DNN-based ensemble framework stands out as a highly effective solution for real-time attack detection and attribution in complex IoT environments.

FUTURE SCOPE

The future scope of this project extends beyond its current capabilities to address emerging challenges and enhance the robustness of IoT cybersecurity One key area for expansion is the integration of reinforcement learning (RL**)** to enable the framework to adapt and learn from evolving cyber threats in real-time. This would allow the system to dynamically adjust its detection mechanisms based on environmental feedback improving its resilience against zero-day attacks and sophisticated evasion techniques Another important direction is the development of a proactive threat intelligence component, involving the collection and analysis of threat data from external sources such as public vulnerability databases, real-time threat feeds, and security forums. By correlating this data with internal monitoring, the system could anticipate potential attack vectors and vulnerabilities before they are exploited, shifting from reactive detection to predictive threat prevention Additionally online learning methods could be explored to maintain model performance over time, while Natural language processing (NLP) could help extract threat indicators from unstructured sources. Incorporating explainable AI and real-time dashboards would further enhance transparency and decision-making capabilities These future enhancements would significantly strengthen the overall security posture of IoT-based industrial systems and prepare the framework for a more intelligent and adaptive cybersecurity landscape.

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] Rao, Gudikandhula Narasimha, et al. "Geospatial Study on Forest Fire Disasters–A GIS Approach." Ecological Engineering & Environmental Technology 24 (2023).

[4] 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.

[5] Jovith, A. Arokiaraj, et al. "DNA Computing with Water Strider Based Vector Quantization for Data Storage Systems." Computers, Materials & Continua 74.3 (2023).

[6] 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. * 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.

[7] 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.

[8] Rao, Gudikandhula Narasimha, et al. "Fire detection in kambalakonda reserved forest, visakhapatnam, Andhra pradesh, India: An internet of things approach." Materials Today: Proceedings 5.1 (2018): 1162-1168.

[9] 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. * 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 AsiaPacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), 2017. IEEE, 2017, pp. 864–872. 26