

Cyber Attack Detection for Industrial IoT using ML Techniques

Firoz Ahmed Mansuri¹ and Dr. Anita Seth²

^{1,2}Department of Electronics & Telecommunication, IET DAVV, Indore, India
Email: firoz55@gmail.com, aseth@ietdavv.edu.in

Abstract—The industrial sector is seeing a rapid expansion of the Industrial Internet of Things (IIoT), and protecting IIoT systems against cyber threats is essential. This study suggests a machine-learning-based intrusion detection solution for the Industrial Internet of Things. The suggested system classifies incoming network data as malicious or benign using two separate machine classifier algorithms: Decision Tree and Support Vector Machine. The Edge-IIoTset-dataset, which comprises 157,800 samples—133499 attack samples and 24301 normal samples was utilized in this study. To train and evaluate the suggested intrusion detection system, the dataset underwent preprocessing and features were extracted. The accuracy, recall, precision, and F1-score were used to assess the suggested system's performance. The experiments' findings demonstrate that the suggested system successfully identified malicious traffic in the IIoT network with high recall, accuracy, and precision. With 96.27% accuracy, the Decision Tree algorithm was the most accurate, followed by the support vector machine with 74.88% accuracy. It is anticipated that the suggested cyber-attack detection system will improve IIoT system security and lessen the possibility of cyberattacks in the industrial sector. To increase their efficacy and offer a security solution, it is advised to integrate the suggested system with the current IIoT security systems.

Keywords—IIoT, cyber-attack detection, decision tree, SVM, edge-IIoTset dataset, intrusion detection systems.

I. INTRODUCTION

The Internet of Things (IoT) has spurred modernization and rapid progress in wireless and communication technologies. It enables seamless interaction between people and objects by connecting numerous embedded devices, often referred to as 'things,' to the Internet. With its widespread adoption, IoT is now integral to various sectors, including manufacturing, smart factories, smart homes, and industrial applications [1]. The Industrial Internet of Things (IIoT) is a growing segment of IoT-driven contemporary production systems. When properly executed, IIoT provides significant practical and economic benefits, improving system configuration, ease of use, dependability, adaptability, and interoperability [2]. However, IoT-enabled automation devices have introduced numerous new risks to industrial and residential areas. Malicious activities can lead to electronic communication disruptions or security breaches. Attackers can easily steal or delete information from computers and network infrastructure, promoting the use of cyber warfare [3]. Various attacks, such as port scans, network scans, address sweeps, Man-in-the-Middle (MitM) attacks, port sweeps, vulnerability scans, information theft, and botnet assaults, are documented.

On May 1, 2020, Formosa Petrochemical Corporation (FPCC) and CPC Corporation, two regulated oil companies in Taiwan, experienced malware cyber-attacks. In July 2020, Swvl, a Cairo-based transit booking platform, faced security issues due to unauthorized access to its IT infrastructure. These examples highlight the vulnerabilities in network security. The extensive variety of IoT devices and unsecured Machine-to-Machine (M2M) and Machine-to-People (M2P) connections compromise individual security and the safe use of equipment.

A Cyber Attack Detection with high detection performance and low error rates is considered effective in identifying disruptions, detecting hostile activities, and ensuring internet traffic reliability [4]. A wide range of attacks occur, and machine learning (ML) approaches are employed to create effective security strategies. Additionally, advancements in ML hold promise for identifying and intelligently addressing emerging threats through learning capabilities. Future standards for securing Internet of Things (IoT) devices will enhance the reliability and accessibility of machine learning algorithms [5][6]. This study aims to create an advanced Cyber Attack Detection System for the Industrial Internet of Things (IIoT) using machine learning (ML) techniques. To achieve this, a comprehensive analysis of the Edge-IIoTset dataset is carried out to assess the proposed model's performance. The research evaluates the effectiveness of two different ML models: Decision Tree and Support Vector Machine. The findings demonstrate that the proposed system excels in accuracy, emphasizing its potential to make notable improvements in IIoT security.

The main contributions of this paper are:

- This paper highlights the importance of data preparation and preprocessing techniques in creating effective Cyber Attack Detection systems for IIoT.
- Detection of cyber-attacks or malicious activities by applying the machine learning techniques including DT and SVM using the latest IIoT dataset.

The structure of the paper is as follows:

- Section II reviews relevant existing research.
- Section III explains the methodology for developing the Cyber Attack Detection models.
- Section IV covers the results and discussion.
- Section V offers concluding remarks.

II. RELATED WORK

The domain of expert systems has been widely explored, with numerous studies addressing interference detection through knowledge discovery methods and computer-based techniques. Despite this, there is a gap in research focusing on the application of machine learning (ML) for detecting interference in conventional networks. This study seeks to bridge that gap by applying ML to identify cyberattacks in physical objects. The application of expert systems to physical objects, particularly in data and smart device security, is still emerging, offering significant potential for deriving insights from smart device data.

In smart networks, ML approaches such as anomaly detection, pattern recognition, and behavioural analysis can be employed to detect potential cyberattacks and prevent abnormal activities. This research assesses recent work on cyberattack detection using ML in physical object networks by reviewing various studies. Each study is analysed for its ML algorithms, detection techniques, and datasets. The emphasis is on evaluating the performance of these datasets and algorithms. The findings indicate that ML methods are effective for intrusion detection. The role of ML in IoT security encompasses both unsupervised and supervised detection techniques.

Recent research has investigated the application of machine learning (ML) in diverse areas such as object detection, pattern recognition, text analysis, and image processing. Furthermore, substantial research efforts have focused on leveraging deep learning (DL) methods for security purposes [7]. The author [8] discusses the development of cloud computing (CC) and its role in advancing smart cities through the use of big data. He also introduces a framework designed to manage big data effectively for smart city applications. In study [9], an intrusion detection system (IDS) was developed for IoT environments utilizing devices with limited capacity. The system demonstrated a 99.4% success rate in detecting Denial of Service attacks. However, the specifics of the dataset employed in their research were not provided. The research in [10] applied the NSL-KDD dataset alongside deep learning (DL) techniques for cybersecurity. This study employed a self-supervised DL method, utilizing sparse autoencoders for unsupervised feature learning from the training data. The extracted features were then used to classify the labelled test dataset into categories of attack or normal. Performance was assessed through n-fold cross-validation, and the results were found to be satisfactory. Additionally, two recent studies have explored the application of machine learning (ML) techniques to security challenges in IoT architectures using the KDD99 dataset. Bostani and Sheikhan [11] proposed a modified K-means algorithm aimed at reducing

the training dataset size and balancing the data for training Extreme Learning Machines (ELMs) and Support Vector Machines (SVMs). Their experimental results demonstrated an accuracy of 96.02% and a false alarm rate of 5.92%. The model utilized Clustering with Self-Organized Ant Colony Networks (CSOACN) to classify network traffic into benign or normal categories. The research in [12] introduced an intrusion detection model featuring a two-tiered approach for dimension reduction and classification. This model was designed to identify malicious behaviors, including R2L and U2R attacks. Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) were utilized for dimensionality reduction. The experiments were carried out using the NSL-KDD dataset, and the two-tier classification system employed Naive Bayes (NB) and a Certainty Factor variant of K-Nearest Neighbor (K-NN) to detect suspicious activities.

Most research in the field has concentrated on addressing potential solutions from various angles, including IoT standards and technologies, architectural frameworks, security threats, and best practices. It also covers diverse machine learning methods, datasets, and implementation tools. Most existing research relies on the NSL-KDD and KDDCUP99 datasets for experiments. These datasets are relatively outdated for identifying R2L, DoS, probing, and U2R attacks. In contrast, this research will use the Edge-IIoTset dataset, which is more recent and better suited for detecting a range of threats including exploits, DoS/DDoS attacks, information gathering, man-in-the-middle attacks, injection attacks, and malware.

III. PROPOSED MODEL

This section outlines the detailed approach employed to create a machine learning-based system for detecting cyber-attacks tailored specifically for IIoT networks. Our research aims to improve data security and accurately identify potential cyber threats within the dynamic field of Industrial IoT. The methodology includes several critical steps, which are illustrated in Fig. 1:

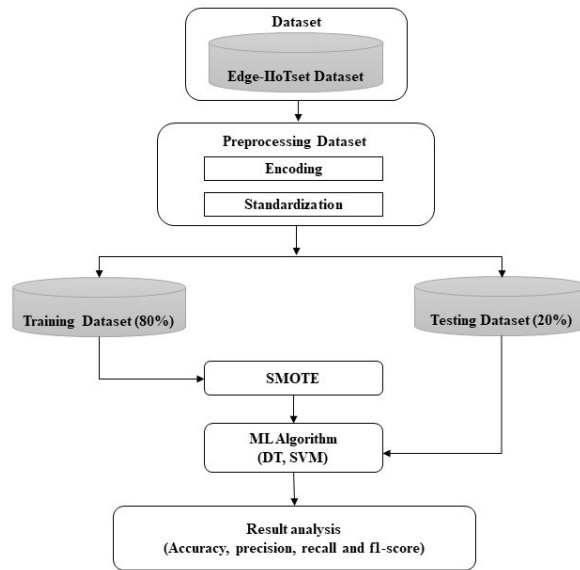


Fig. 1. Proposed methodology overview

Together, these steps establish the basis for our advanced cyber-attack detection system, designed to tackle the key cybersecurity issues encountered by contemporary IIoT networks. The subsequent sections will explore each step in detail, offering a thorough understanding of our approach and its potential to markedly enhance cyber-attack detection in IIoT settings.

A. Dataset and Data Preprocessing

The effectiveness of an intrusion detection system largely depends on the quality and diversity of the datasets utilized for training and assessment. In our study, most updated Edge-IIoTset datasets is selected to provide extensive coverage of network traffic patterns and attack types, thereby improving the reliability and applicability of our results.

In the Edge-IIoTset dataset study [13], 14 distinct cyberattacks were simulated, categorized into five groups: (1) DoS/DDoS, (2) Information Gathering, (3) Man-in-the-Middle (MITM), (4) Injection, and (5) Malware.

In this research the Edge-IIoTset dataset has been utilized to develop detection systems for both binary and multi-class cyberattacks. In the binary classification scenario, all listed attacks are grouped into a single class labelled as "anomalous," while normal traffic is categorized as "normal." For the multi-class classification scenario, the classes are distinguish between 15 classes: 14 for each specific attack and one for normal traffic. Fig. 2 illustrates the distribution of these classes within the dataset. The dataset comprises a total of 157,800 traffic connections (data points).

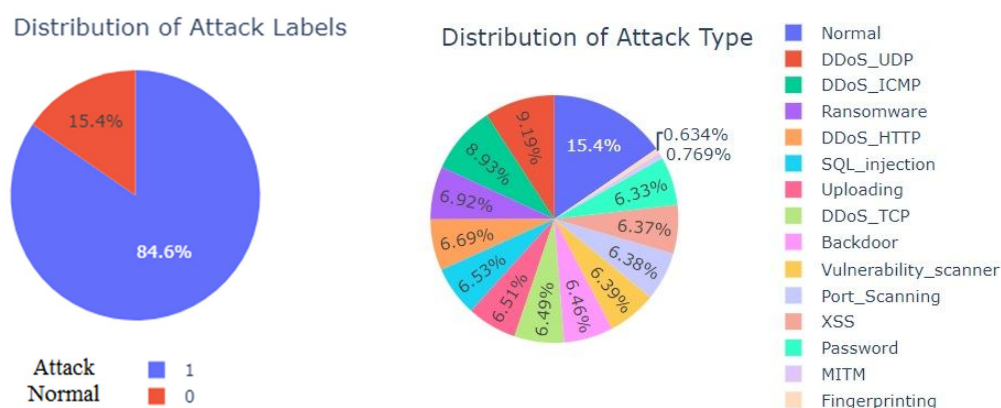


Fig. 2. Percentage of normal vs malicious connections in Edge-IIoT Dataset

Data preprocessing plays a crucial role in developing an effective and precise intrusion detection system (IDS). The challenges of class imbalance, diverse attack types, and feature selection are addressed using advanced methods. Creating a balanced dataset and identifying key features improves the IDS's capability to accurately differentiate between legitimate and malicious network activities.

The study identified a significant issue with class imbalance in the dataset, marked by an insufficient number of examples for certain network attacks. To address this, the Synthetic Minority Over-sampling Technique (SMOTE) [14] was utilized., a well-established method for balancing class distributions. SMOTE generates synthetic examples for the underrepresented class by creating new instances that are similar to existing minority samples. This approach effectively increases the number of minority class samples, thereby improving the balance of the dataset. The datasets are divided into two segments: 80% for training the models and 20% for testing them. The training set is used to develop the models, while the test set is employed to assess their performance on new, unseen data.

B. Machine Learning Algorithms

The learning algorithm identifies relevant information from the training data. Machine learning algorithms fall into two main types: supervised and semi-supervised. Unlike unsupervised learning, which explores unlabelled data, supervised learning relies on labelled examples to build models [15]. Before creating a decision model, the classifier undergoes a training phase. The next section offers a thorough examination of two machine learning classifiers, Decision Tree and Support Vector Machine, which are utilized in this research for detecting network flow attacks.

Decision Tree Algorithm (DT)

Decision tree (DT) algorithms are designed to derive meaningful classifications. A decision tree consists of a root node, several internal nodes, and leaf nodes. The root node is the starting point and has no incoming connections, while internal nodes are intermediate points in the tree, and leaf nodes represent the final classifications. To build a decision tree, various criteria and characteristics are used to evaluate internal nodes. When selecting decision nodes, priority is given to those with the highest information gain. Decision trees are recognized for their accuracy and effectiveness in data classification [16].

Support Vector Machine (SVM)

It is a highly popular and well-established method, primarily used for classification tasks but also applicable to regression. In Support Vector Machines (SVM), data points are plotted in an n-dimensional space, where 'n' denotes the number of features. The algorithm constructs a hyperplane that divides the data into distinct classes [17].

C. Metrics for Evaluation

The models were trained on datasets with different amounts of training data to evaluate their performance metrics, including accuracy, false positive rate, detection rate, and F1-score.

These metrics were derived from counts of true negatives (TN), true positives (TP), false negatives (FN), and false positives (FP).

Specifically, false positives and false negatives correspond to incorrectly classified legitimate and attack instances, respectively, while true positives and true negatives represent correctly identified legitimate and attack instances [18] [19].

Accuracy (ACC) measures the system's ability to correctly identify attack packets as either normal or malicious. It reflects the proportion of correct classifications across all samples. The formula for calculating accuracy is as follows:

$$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} \times 100 \quad (1)$$

Precision (Pre) represents the proportion of correctly identified attacks among all packets labelled as attacks. It is calculated using the following formula:

$$Precision = \frac{TP}{TP+FP} \times 100 \quad (2)$$

The F1-score (F1) is defined as the harmonic mean of precision and recall.

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (3)$$

Recall (Rec) measures the system's effectiveness in identifying attacks during a security breach. It is also referred to as the true positive rate and is mathematically represented as follows:

$$Recall = \frac{TP}{TP+FN} \times 100 \quad (4)$$

D. Experimental Setup

The experiments were performed on a Lenovo Legion equipped with a Windows 11 operating system, i5-11th Gen 11400H Processor, 16GB of memory, and an integrated RTX 3050 graphics card used for dataset training. For data preprocessing, cleaning, and feature selection, the NumPy and Pandas libraries were utilized.

IV. RESULT ANALYSIS

As previously noted, two machine learning algorithms were tested on the Edge-IIoTset dataset: Decision Tree (DT) and Support Vector Machine (SVM).

Cross-validation results indicates that the Decision Tree outperformed the SVM in both training and testing accuracy, achieving a maximum accuracy of 96.27%.

In comparison, the Support Vector Machine achieved an accuracy of 74.88%. The experimental results of our findings of the proposed models are presented in Table I.

TABLE I. PERFORMANCE MEASURES OF THE PROPOSED MODEL

Classifiers	Accuracy	Recall	Precision	F1
DT	96.27	96	96	96
SVM	74.88	75	72	74

V. CONCLUSION

The results demonstrate that supervised machine learning is effective for analysing traffic data and accurately identifying malicious traffic on IIoT devices.

By critically evaluating the Edge-IIoTset dataset using machine learning techniques, it was possible to accurately identify such traffic. This dataset was employed to compare the performance of different frameworks through functions like selection and classification.

The Decision Tree algorithm achieved the highest accuracy at 96.27%, outperforming the Support Vector Machine algorithm. Future work will involve applying deep learning algorithms to the same dataset for further analysis.

REFERENCES

- [1] Nwakanma, C.I., Nwadiugwu, W., Lee, J.M. and Kim, D.S., "Real-Time validation scheme using blockchain technology for Industrial IoT," in Proceedings of 2019 Korean Institute of Communications and Information Sciences Summer Conference pp. 379-382, June, 2019.
- [2] Long, N.B., Tran-Dang, H. and Kim, D.S., "Energy-aware real-time routing for the large-scale industrial Internet of Things," IEEE Internet of Things Journal, 5(3), pp. 2190-2199, 2018.
- [3] Hafeez, I., Antikainen, M., Ding, A.Y. and Tarkoma, S., "IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge," IEEE Transactions on Network and Service Management, 17(1), pp. 45-59, 2020.
- [4] Muna, A.H., Moustafa, N. & Sitnikova, E. , "Identification of malicious activities in the industrial Internet of Things based on deep learning models," Journal of information security and applications, 41, pp.1-11, 2018.
- [5] Vashi S, Ram J, Modi J, Verma S, Prakash C. "Internet of Things (IoT): A vision, architectural elements, and security issues," in 2017 international conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp. 492-496, 2017 .
- [6] Sharma B, Sharma L, Lal C. "Anomaly Detection Techniques using Deep Learning in IoT: A Survey," in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE). 2019; pp. 146-149.
- [7] S. Mendhurwar and R. Mishra, "Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges," Enterprise Information Systems, vol. 15, no. 4, pp. 565–584, Apr. 2021
- [8] K. K. Mohbey, "An Efficient Framework for Smart City Using Big Data Technologies and Internet of Things," in Progress in Advanced Computing and Intelligent Engineering, Singapore, 2019, pp. 319–328
- [9] E. Hodo et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," 2016 Int. Symp. Networks, Comput. Commun. ISNCC 2016, pp. 4–9, 2016.
- [10] Q. Niyaz, W. Sun, A.Y. Javaid, M. Alam, "A deep learning approach for network intrusion detection system," EAI Int. Conf. Bio-inspired Inf. Commun. Technol. 2015.
- [11] H. Bostani, M. Sheikhan, Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach, Comput. Commun. 98 (2017) pp. 52–71
- [12] H.H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, K.- K. Choo, A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks, IEEE Trans. Emerg. Top. Comput. 7 (2) (2019) pp. 314–323
- [13] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," in IEEE Access, vol. 10, pp. 40281-40306, 2022
- [14] Chawla, N.V.; Bowyer, K.W.; Hall, L.O.; Kegelmeyer, W.P. SMOTE: Synthetic Minority over-sampling Technique. J. Artif. Intell. Res. 2002, 16, pp. 321–357.
- [15] M. Almseidin, M. Alzubi, S. Kovacs, and M. Alkasassbeh, "Evaluation of machine learning algorithms for intrusion detection system," presented at the 2017 IEEE 15th international symposium on intelligent systems and informatics (SISY), IEEE, 2017, pp. 000277–000282.
- [16] B. Gupta, A. Rawat, A. Jain, A. Arora, and N. Dhama, "Analysis of various decision tree algorithms for classification in data mining," Int. J. Comput. Appl., vol. 163, no. 8, pp. 15– 19, 2017.
- [17] B. S. Bhati and C. S. Rai, "Analysis of Support Vector Machine-based Intrusion Detection Techniques," Arabian Journal for Science and Engineering, vol. 45, no. 4, pp. 2371–2383, Apr. 2020
- [18] Alsaedi, A.; Moustafa, N.; Tari, Z.; Mahmood, A.; Anwar, A. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. IEEE Access 2020, 8, pp. 165130–165150.
- [19] Rani, D.; Gill, N.S.; Gulia, P.; Chatterjee, J.M. An Ensemble-Based Multi-class Classifier for Intrusion Detection Using Internet of Things. Comput. Intell. Neurosci. 2022, 2022, 1668676.