Securing the Future: Real-Time Intrusion Detection in IIoT Smart Grids through Innovative AI Solutions

Mounir Mohammad Abou-Elasaad[1,*], Samir G. Sayed[2], Mohamed M. El-Dakroury[3]

[1]Department of Electronics & Communications, Faculty of Engineering Egypt, Helwan University, Egypt
[2]Professor, Department of Electronics and communication Engineering, Helwan University, Egypt
[3]Assistant Professor, Department of Electronics and Communications Engineering, Helwan, Egypt

Emails: Mounir_abouelkhair@h-eng.helwan.edu.eg; samir_abdelgawad@h-eng.helwan.edu.eg; mdakroury@h-eng.helwan.edu.eg

Abstract

The world is witnessing an unprecedented boom in the development of information technology, which has come to encompass all aspects of life, Smart networks based on the Industrial Internet of Things (IIoT) are among the latest technologies used in various industries, contributing to improved production efficiency, reduced costs, and enhanced security, With the increasing reliance on this technology, the challenge of complex cyberattacks are also on the rise, These attacks are considered one of the major challenges facing smart networks, as attackers can exploit vulnerabilities in systems to access sensitive data or disrupt industrial operations, To counteract these threats, advanced intrusion detection systems should be developed, leveraging artificial intelligence and big data analytics to effectively detect and respond to attacks in real-time. Therefore, it is imperative to strive towards developing advanced and intelligent security systems to combat cyberattacks, ensuring the safety of industrial operations and data protection. This paper provides two IDS based on AI that are developed to negate the raising sophisticated cyberattacks. IN the first technique, Group of ML techniques such as Decision tree, Random Forest classifiers, support vector classifier, and K_Nearest Neighbor are used with Feature reduction algorithms classifying network traffic subspecies to enhancing the accuracy and efficiency of detection systems. The second proposed technique for specifying the type of intrusion advantage various methodologies, particularly in the context of IoT networks and deep learning, the two algorithms are trained and tested using three well-known datasets to investigate wide domain of cyberattacks targeting the IIoT infrastructure. Results of the simulation show that the algorithm proposed in this work provides high improvement in detection of cyberattacks. The first algorithm achieved an accuracy of 99.9% and a very low false positive rate of just 0.1%. In addition, the second proposed algorithm identifies type of attack with a detection ratio of 99.76%. These results demonstrate how the proposed IDS based on AI algorithms can effectively detect network intrusion, and significantly enhance the security of IIoT system.

Keywords: Industrial Internet of Things (IIoT); Intrusion Detection Systems (IDS); Artificial Intelligence (AI); Machine Learning (ML), Deep Learning (DL)

1. Introduction

Industrial IoT revolutionizes industry through technological advancements., aiming to improve industrial productivity and collect, exchange and analyse data by connecting devices, sensors (temperature, pressure, etc.), and systems together [1]. This connectivity naturally poses significant security challenges, as many IIoT devices do not have significant security protections against unauthorized access, making them attractive targets for cybercriminals, and they often run on outdated firmware. Such vulnerabilities allow attackers to manipulate data, Cause disruption to operations or manipulate physical processes within the network, resulting in substantial financial losses, safety risks and environmental hazards [2]. The incidence of false positives and missed detections escalates when depending on conventional security solutions that are reliant on pre-established rules and signatures, and this creates a challenge in industrial environments, just as false alarms can arise, resulting in

1901. https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

unnecessary downtime, and delayed alarms can occur, which in turn lead to serious security incidents. In addition, many industrial systems are built on the idea of combining legacy infrastructure with modern hardware, which further exacerbates the situation, without prioritizing cybersecurity, risks when these systems were designed [3]. Cyber threats and attacks are becoming more complex, consequently, there is a growing demand for the creation and recommendation of sophisticated and flexible security measures to safeguard industrial activities and guarantee their availability and confidentiality. Furthermore, the massive volume of data generated by IIoT devices further complicates anomaly detection and potential security threats [4]. Addressing these challenges is critical for maintaining secure, uninterrupted operations in industrial settings. Strong protective measures have become of the utmost importance with the increasing use of IIoT in industries. Next generation Artificial Intelligence (AI) - enabled intrusion detection systems have the potential to revolutionize IIoT security and overcome traditional system failings [5]. The integrated artificial intelligence technology and IDS provides a real-time data analysis capability for IIoT devices, thus enabling them to recognize patterns and anomalies that may pose threats. The main advantage of AI-IDS is that it learns from experiences and can adjust to new attacks. It all rests on teaching Machine Learning (ML) algorithm on a sample dataset representing normal operation behaviour to detect any changes signalling a breach. This flexibility becomes invaluable when combined with different types and modes of operation in these mixed IIoT environments. AI technologies can also enable the automation of danger identification and response. Industrialists know that even a minute of idle time could lead to considerable financial losses [6]. With AI-IDS, this detection will be automatic, and real-time notifications will be triggered for security personnel to respond quickly. Apart from reducing the workload of human analysts, such automation ensures that potential hazards receive necessary attention before getting out of hand. Additionally, AI-IDS have broader applications. Pattern and trend analysis of attacks enables a company to learn cyber adversaries' tactics and take measures to improve defences ahead of time [7]. In this decade of increasing cyber threats, proactive security measures safeguarding essential assets must be enrooted in every sector.

Our study's main objectives are AI-IDS and possibilities for improving IIoT network security. Each objective considers the critical challenges identified from the problem statement and investigates the potential of AI in creating impactful security solutions. These objectives are not tasks but important steps towards making IDS safer and more resilient. Our main contributions are:

1- Present State of IIoT Security: This would aim at deeply understanding the inherent vulnerabilities prevailing in an IIoT network [8]. It involves studying current security measures, spotting protection gaps, and assessing how traditional intrusion detection systems are performing.
2- Study of AI-based intrusion detection methodologies: This study will analyze the advantages and drawbacks of various potential remedies for enhancing IIoT security and assess their effectiveness. This includes studying several methodologies and comparing different ML and deep learning techniques to study their effectiveness and ability to detect threats within IIoT environments.
3- Implementation Framework: The aim of our research is to offer a comprehensive understanding of the topic, adaptive, flexible, and scalable implementation framework so that AI-IDSs can be integrated into existing infrastructures and made possible for implementation in any organization with advanced security measures [9].

This paper is structured as follows: Section I introduces the problem and significance of AI-based IDS in securing IIoT environments. Section II presents a comprehensive literature review of previous work. Section III details the methodology and framework used in the study. Section IV outlines the tests and results of the proposed IDS model, and finally, Section V will delve into the conclusions and future work.

2. Related work

Verma et al. [10] discussed the role of IDS in securing IoT to predict and detect Denial of Service (DoS) attacks and using seven ML algorithms, including RF, ada boost, gradient-boosted machines, RF, classification decision trees (DT), and multilayer perceptron to compare them in terms of accuracy, recall, false positive rate to get the optimum algorithm. To optimize the classifiers, random search algorithms were employed to determine the best parameters. They used (The CIDDS-001, UNSW-NB15, and NSL-KDD benchmark datasets) for all classifiers. To find significant differences among classifiers, they depend on the results of all classifiers in terms of (accuracy, precision, recall, f1 score, false positive rate, and AUC) also, Friedman and Nmenyi post-host tests are applied to analyse performance measures. Furthermore, they evaluated all the classifiers' response times using the Raspberry Pi hardware device was used in the study. Based on the performance results and statistical tests, they found that DT and extreme gradient-boosting classifiers are optimal for building anomaly-based IDS suitable for IOT. Khatib et al. [2] presented ML models that can detect and protect systems from attacks. Furthermore, they used many ML classifiers to analyze the effect of data oversampling on ML models by comparing the results of all of them before and after resampling the data using the SMOTE technique. The results showed that Linear Discriminant Analysis

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

(LDA), RF, and DT performed better than others did since they could predict attacks with higher accuracy on many types of attacks (multi-class cases). They found that DT, RF, and Nystrom-SVM techniques performed better in the binary case for detection (normal or attack). They noticed that they could detect attacks more efficiently when they trained their algorithms with balanced data. Tyagi et al. [4] developed an IDS based on extracted features from the BoT-IoT dataset that can accurately and automatically distinguish normal and attack in real time. They use a lightweight feature set, consisting of seven lightweight features, instead of standard feature reduction techniques such as principal component analysis (PCA), which change the primary meaning of features. The study shows that this technique can detect four types of attacks (Distributed DoS (DDoS), DoS, reconnaissance, and information theft). They use many models in their system, such as KNN, LR, SVM, multilayer perceptron (MLP), DTs, and RF, by using (accuracy, precision, recall, F-Score, and receiver operating characteristics (ROC)), to validate the performance of the proposed system. The results show that DT and RF classifiers are the best, having accuracy (99.9%), but in other metrics, RF was the best. Ramadan et al. [5] build an IDS system that detects IoT network attacks. The IDs are based on two phases: pre-processing and classification. The first data preprocessing is performed on the benchmark dataset (NSL-KDD dataset), which performs encoding, scaling, and removing noise. Then, they performed feature selection using Enhanced Shuffled Frog Leaping (ESFL), which was used to extract the most relevant features. The second stage is the classification done using the Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN), which classifies data into standard and attack. Based on the experimental results, the proposed system performed better than the existing methods. Soe et al. [6] also developed an IoT IDS system using ML algorithms to detect the type of traffic used for feature selection, the lightweight and efficient feature selection algorithm CFS, and using (decision trees DT), and the J48 algorithm for classification. They used a benchmark dataset (UNSW-NB15) and implemented it on a Raspberry Pi. During the experiment, the system detected all attacks with high accuracy and at a faster training speed. Moreover, if the feature selection step were not taken, the system would only be able to handle 80% of the attacks. Choudhary et al. [8] built an IDS based on deep learning using SVM and DNN. They used SVM and binary classifiers based on the Cosine similarity measure to extract the most relevant feature. They deployed the proposed work by performing Measurements based on precision, recall, F-measure, and accuracy. They compared the proposed work with other techniques to determine its effectiveness. Compared with other approaches, precision, recall, F-measure, and accuracy improved by 13%, 74%, 71%, and 76%, respectively. Krishnan et al. [9] used many techniques for feature selection to predict any attack traffic against IoT devices using sequential backward processing, sequential forward processing, and recursive feature elimination (RFE) and used three ML models on each of them (Support Vector classifier (SVC), RF and XGBoost) then getting results for each of them. From the results, we found that all of them achieved high accuracy with these techniques. As a result, these techniques can be used in a supervised learning setting to predict an attack on IoT devices. Feature selection on their IDS system to predict any attack on IOT devices. They developed two techniques (information gain (IG) and gain ratio (GR)), and then they extracted the best features using mathematical set theory. They used four ML algorithms) (bagging, multilayer perception, J48, and IBk). To be applied on the Benchmark datasets ((IoTID20) and NSLKDD. Based on the feature extraction methods, they select 13 and 28 relevant features (out of 86) for (IoTID20) and 15 and 25 relevant features (out of 41) for (NSL-KDD), respectively. Based on the comparison with other approaches, they are getting these results: their proposed model scores a very high 99.97% accuracy. Sai et al. [11] used a Raspberry Pi to implement a lightweight intrusion detection technique using an ML approach. They used for feature selection a CFS algorithm applied on the benchmark dataset (UNSWNB 15) that reduced features from 44 to 3 and used them for classification SVM to detect the attack and normal traffic. Their method of classifying attacks and regular traffic was based on an SVM. If we use all 44 features, the Raspberry Pi system will fail. In the evaluation, the DoS attacks are extracted from the UNSWNB 15 dataset to be evaluated by the WEKA application. By reducing the number of features in the system, the CFS algorithm extracts 9 of 30 of the system's weight to enhance detection accuracy. Because of their experiments, they found they could detect DDOS attacks with high accuracy. Addoura et al. [12] performs their IDS through many clustering with reduction, oversampling, and classification using a single-hidden layer feed-forward neural network (SLFN). The development of their paper is how to reduce the data using their technique and oversampling technique to balance the data. The hybrid approach is used to detect intrusion activities. As part of the experiments, the evaluation is done in terms of (accuracy, precision, recall, and G-mean) by dividing into four steps: ensuring reduction of data using clustering, then the impact of over-sampling on results by comparing results before and after it. It is found t SLFN classifications and SVM with Synthetic Minority Oversampling Technique (SVM-SMOTE) and k value 3 for the k-means++ clustering technique produce better results than other classification techniques and other values.

The authors of [13] also evaluated IDS solutions, comparing ML-based and DL-based systems, detailing their functions, advantages, disadvantages, and use cases. Table I shows the analysis of the above works.

AZAM et al. [14], presented the recent IDS taxonomy, a comprehensive review of intrusion detection techniques, and commonly used datasets for evaluation. In this paper, the researchers attempt to explore the latest

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

developments in ML and deep learning-based intrusion detection systems, including methodology, evaluation metrics, and dataset selection, and propose a future research paradigm to address the weaknesses of the methodologies. Decision tree, known for its speed and ease of use, is proposed as a model for anomaly detection by combining the results from a comparative survey. The aim of the research was to provide insights into building an effective decision tree-based intrusion detection framework.

KASONGO in his work titled ‘‘An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms’’ [15] proposed adopting the Genetic Algorithm (GA) for feature selection in the IIoT intrusion detection system and using the Random Forest (RF) model in the fitness function of the genetic algorithm. The proposed algorithm outperformed the existing IDS frameworks, and the experimental results showed that for the binary modelling process, Genetic Algorithm- Random Forest (GA-RF) achieved a test accuracy of 87.61% and an area under the curve of 0.98, using a feature vector containing 16 features.

In [16], Tareq et al. trained two intelligent network models — DenseNet and Inception Time to detect cyberattacks based on a multi-class classification approach using three datasets: ToN-IoT, Edge-IIoT and UNSW2015. The results were then compared for multiple cyberattacks, and extensive experiments were conducted on standard ToN-IoT datasets using the DenseNet multi-class classification model. The best accuracy result was 99.9% for Windows 10 with DenseNet but using the Inception Time approach the highest result was for Windows 10 with the network, with 100% accuracy. Using the Edge-IIoT dataset with the Inception Time approach, the best result was 94.94% accuracy. Attacks were also evaluated on the UNSW-NB15 dataset using the Inception Time model, which had an accuracy rate of 98.4%.

In the research [17], Manderna et al. focused on the security of the vehicular ad hoc network (VANET) and built an Artificial Intelligence (AI) and deep learning-based system for network intrusion detection. The proposed model includes a self-attention-based bidirectional long short-term memory (SA-BiLSTM) for classification and a cascaded convolutional neural network (CCNN) for learning high-level features. The proposed model was able to achieve 99% accuracy on all datasets.

On smart agriculture, the authors in study "Intrusion Detection in Internet of Things Based Smart Farming Using Hybrid Deep Learning Framework" [18] have developed a novel and efficient framework based on deep learning for intrusion detection in smart agriculture systems. The model includes three layers: the first layer is the sensor layer. The second layer is the fog-computing layer (FCL). The last layer is the cloud layer. The proposed system was implemented in Python platform, using ToN-IoT and APA-DDoS attack datasets for evaluation. The proposed system showed superiority over existing methods in accuracy (99.35%), detection rate (98.99%), precision (99.9%), and F-score (99.08%) for APA DDoS attack dataset and achieved accuracy (99.71%), detection rate (99.02%), precision (99.89%), and F-score (99.05%) for ToN-IoT dataset.

Researchers at [19] designed an intrusion detection system using ML and explainable artificial intelligence (XAI) techniques to classify different cyberattacks detected in real-time. By leveraging frameworks such as Apache Kafka and Spark, along with libraries such as Scikit-learn and SHAP, the system is capable of identifying and categorizing normal or abnormal network traffic in real-time. The researchers’ goals were to develop a flexible and scalable intrusion detection system that can provide clear explanations for its decisions as well as compare and analyse different ML models to achieve the best results in terms of accuracy, f1, recall, and precision. The proposed random forest models performed best in learning the key features identified by the XAI model, which include Ct_state_ttl, Sttl, Dmean, and Dbytes from the UNSW-NB15 dataset.

3. Methodology

The main objective of our researches is clear-cut: to Enhance IIoT security with AI-IDS. To navigate this challenge, we have harnessed the ML classification algorithms to build IDS to detect anomalies in IoT devices. These IDS will continuously monitor network traffic for any deviation from normal network profiles based on anomaly detection. Three types of IDSs can be used: signatures, anomalies, and specifications. Due to its ability to detect new attacks, anomaly-based IDS is preferred over signature- or specification-based IDS. However, it comes with a high false alarm rate. The effectiveness of anomaly-based IDS depends on the quality of its detection engine (model or classifier). An anomaly-based ID continuously monitors network traffic for deviations from the standard profile. When a deviation exceeds the threshold, an alarm detects a DoS attack. This study will have several key stages, as the flow chart shows. To train the system, in this stage, the processing of data from three datasets—Bot-IoT, ToN-IoT, and UNSW-NB15—, which encompass a diverse range of attack types targeting IoT networks [20, 21]. In Table 1, we present a comprehensive analysis of prominent datasets currently used in some IIoT cybersecurity research. This comparison aims to identify the unique attributes of the datasets, such as the number of attacks, instances, and other critical characteristics, and gives us an idea of the diversity of available datasets and emphasizes their importance in examining the effectiveness of intrusion detection system solutions specifically designed for IIoT networks.

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

Table 1: Summary of Industrial IoT Cybersecurity Datasets: Key Attributes Comparison

Dataset	Ref	Features	Instances	Threats (attacks)
Edge_ IIoTset	[22]	61	157,800	14
NSL-KDD	[23]	41	148,517	4
UNSW-NB15	[24]	49	2,540,044	9
IoT-Botnet Traffic Dataset	[25]	46	TBD	8
CICIDS2017	[26]	78	2,830,743	14
DS2OS	[27]	13	357,952	7
WUSTL-IIoT-2021	[28]	47	1,194,464	4
CICIoT2023	[29]	46	2,867,734	7

A. Research design

In this study, design of an intelligent intrusion detection system (AI-IDS) to secure IIoT networks will be investigated. To achieve this main objective, our work will be divided into two phases (pre-processing and classification) and use various techniques from deep learning and ML. will resort to quantitative and qualitative data analysis, statistical analysis, and ML algorithms to identify patterns such as correlations in the data and trends.

B. Framework and approach

Our framework ensures a thorough examination of network data that can improve the detection and classification accuracy of expected threats. Deep learning and ML models are evaluated for both phases. It comprises a K-Nearest Neighbors (KNN) approach, Random Forest (RF), decision trees, logistic regression, gradient boost, XGBoost, and a Voting score ensemble. Accuracy, false positive rate, recall, computing time, Area Under the Curve (AUC), and F1-Score are the performance indicators used to assess the models. Two cascading models are used for these IDS. At first, we tried a variety of ML models and deep learning models such as logistic regression, decision trees, KNN, XGBoost, random forest voting score ensemble, and gradient boost methods for determining whether it is regular traffic or any attack. Then, compare each model's result in computing time, accuracy, recall, F1-Score, and false positive. We discovered that using DT models works best for it. The second cascaded model is used to determine types of threats using many ML models as we made the first model and compared them, finding that RF is the best model as shown in the Figure 1.

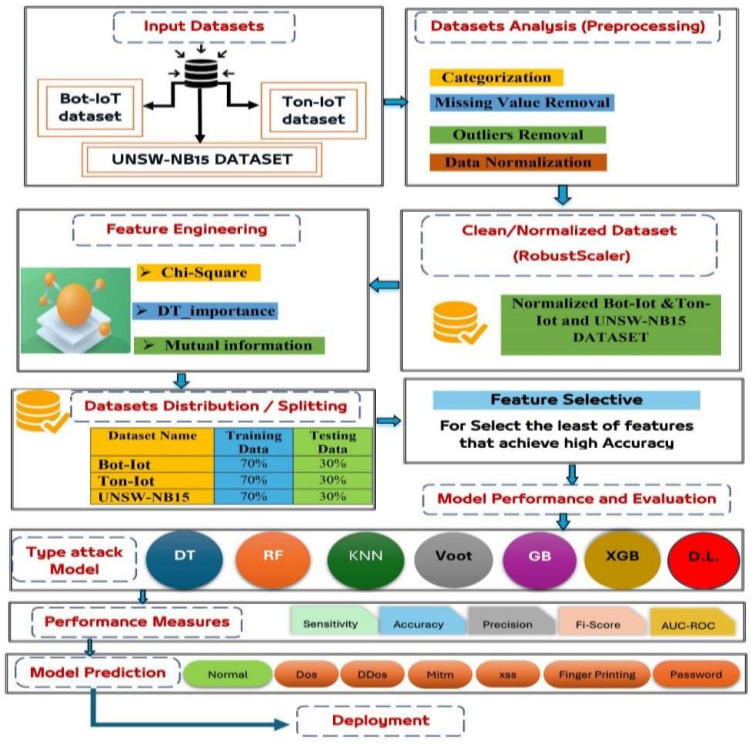


Figure 1. Proposed Framework.

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

C. Data sources

IIoT networks gather data, which is essential for creating successful IDS. It comprises information from various sources, including network traffic, IIoT devices, past attack data, and operational logs. The gathered information includes incident occurrences and typical operating patterns, essential for ML model training [30]. By evaluating the data, researchers can determine several attack methods, including DDoS attacks, spoofing, ransomware, IIoT devices, Programmable Logic Controllers (PLCs), sensors, and actuators, which are devices that perform physical actions in response to commands received from control systems, which are frequently influenced by sensor data [31, 32]. An IDS can determine and classify irregularities in real-time through this data collection process and enhance IIoT security. Data Accessibility is crucial for creating prosperous IDS for IIoT networks. Data sources may include a range of information that offer perceptions of typical operating behavior and possible security risks, such as network traffic (contains packet captures that provide information about the protocols used, communication patterns, and possible efforts at illegal access [33]), operational logs (containing information on system performance, user interactions, and error messages), historical attacks statistics, and intelligence on external threats. IIoT devices, such as sensors and actuators, are essential data sources, because they produce real-time data regarding their operational status and surrounding circumstances. There are a few different ways to do a train test split, but the most common is to split your data into two sets simply. For example, 70% for training and 30% for testing as shown in figure 2.

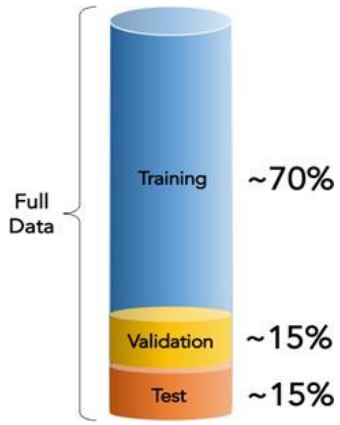


Figure 2. Data Splitting.

This ensures that both sets are representative of the entire dataset and gives you an excellent way to measure the accuracy.

D. Types of attacks

Cyberattacks are a serious threat to the operational integrity and security of networks. Man-in-the-middle (MitM) attacks [34] enable adversaries to intercept and manipulate communications between devices; DDoS attacks [35], in which multiple compromised devices flood a target with excessive traffic, are also common. Attackers exploit vulnerabilities in connected devices to build massive botnets. Logical attacks [36], on the other hand, exploit software vulnerabilities to disrupt operations without requiring physical access. These many attack methods demonstrate how important it is for IIoT setups to have strong security controls in place to protect against evolving cyber threats.

E. Feature selection

Isolating the most consistent, non- redundant and relevant features for model construction. Methodically reducing the size of datasets is essential as the size and variety of datasets continue to grow. The main goal of feature selection is to improve the performance of a predictive model and reduce the computational cost of modeling. There are several types of feature selection, but we focused on three of them (Chi-square, mutual information gain, and feature importance based on DT); so, the techniques selected that achieve high accuracy with the fewest number of features.

1- Chi-square test: It helps in solving the problem of selecting attributes by testing the relationship between them. It is a statistical test used to determine whether there is a significant correlation between two categorical

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

variables. It is also non-parametric, meaning that it does not assume any distribution of the data. The test compares the observed and expected frequencies within a contingency table. The chi-square distribution is defined as the sum of the squares of the k independent standard random variables given by equation (1) [37]:

$$X^2 = \sum \left[\frac{(O_{r,c} - E_{r,c})^2}{E_{r,c}} \right] \quad (1)$$

where: $O_{r,c}$ is the observed frequency number at the level r of the variable A and the level c at the variable B, and $E_{r,c}$ is the expected frequency number at the level r of the variable A and the level c of the variable B.

2- Mutual Information (MI): is a measure of the amount of knowledge between two random variables, X and Y. If X and Y are independent, i.e., X contains no information about Y, and vice versa, then their mutual information is zero. The objective is to maximize the relevance between the input features and the output and to minimize the redundancy of the selected features.

3- Feature importance based on DT: it is determined by how much each feature contributes to reducing the uncertainty in the target variable [38]. This is typically measured by the reduction in the Gini impurity or entropy achieved by splitting on a particular feature (root and leaves) as shown in figure 3.

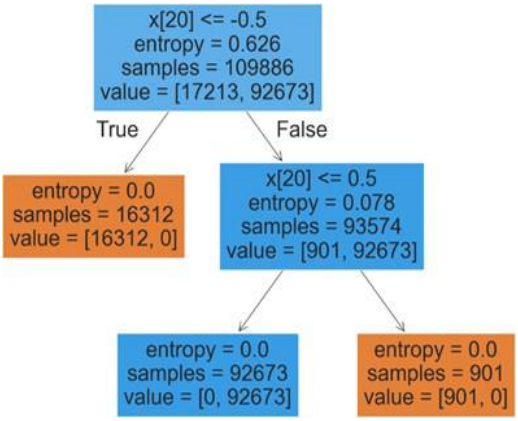


Figure 3. Example for Feature importance based on DT.

4- Techniques Performance Results: In the table 2, make a comparison between these three techniques for feature selection by Applying them on three datasets and getting the least number of features for each one of them that achieving the highest accuracy, and we found that Chi-square is the best technique to be applied.

Table 2: Feature Selection Results

Feature Selection Method	Dataset	Number of Features Selected	Accuracy
CHI_square	BOT-IOT	5	0.99874
CHI_square	UNSW_NB15	23	0.99998
CHI_square	TON_IOT	18	0.996
Features based on DT	BOT-IOT	8	0.99863
Features based on DT	UNSW_NB15	28	0.99973
Features based on DT	TON_IOT	22	0.993
MI	BOT-IOT	7	0.997
MI	UNSW_NB15	25	0.993
MI	TON_IOT	27	0.9953

F. Artificial intelligence techniques

AI-IDSs have improved network security, in terms of their ability to detect and respond to threats in real time, but these measures sometimes fail in the face of the skill of cybercriminals, so more innovative solutions are needed. The interconnectedness of devices in IIOT environments makes them more vulnerable to attacks due to the massive amounts of data. Several AI techniques support detection systems that aim to improve the efficiency of the network and improve its security.

- Exploratory data analysis (EDA) is concerned with exploring data and understanding its nature and relationships, including summary statistics, visualizing data distributions, and identifying potential problems such as missing values or outliers. This method is widely used [39].

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

- Correlation matrix: provides insight into the relationships between different features within a dataset, facilitating an understanding of the critical attributes that are of utmost importance in the anomaly identification process. The strength of the correlation between variables can be assessed using the correlation coefficient, where a correlation coefficient close to 1 indicates a high correlation, while a value less than one or negative indicates a weak relationship between variables.
- Distribution of Label Classes: The dataset's balance can be ascertained by examining a bar plot that exhibits the distribution of the label classes, namely, normal or attack. Considering an imbalanced dataset is crucial when creating a machine-learning model for anomaly detection.
- Data Preprocessing: Which means preparing the raw data to fit the machine-learning model. It is the first and crucial step in creating a machine learning model, and aims to drop null and duplicate values, investigate outliers, and remove all these to make the data clean and suitable for machine learning and increase the accuracy of our model [40].
- Encoding these categorical variables into numbers is essential, using Label Encoder, a technique used to map categorical columns to integers or decimals to be suitable for machine learning [41].
- Feature Scaling: To ensure that no variable dominates the other, we resort to standardizing the independent variables of the dataset to a certain range, which is the last step in data preprocessing in machine learning. There are many types of feature scaling, but we use a robust scaling, which is done by removing the meaning and scaling to unit variance.

G. Evaluation metrics

Evaluation metrics are needed to evaluate the effectiveness of the performance and reliability of the proposed intrusion detection systems. Metrics such as precision, accuracy, recall, and the F1 score, etc.., are essential for evaluating the performance of machine learning models

1- Accuracy: It is calculated as the percentage of accurate results, true positives, and true negatives among all the cases considered. Designers of intrusion detection systems strive for high accuracy as it indicates their high ability to distinguish between benign and malicious activity. The accuracy of the model is calculated using the following formula [42]:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (2)$$

where: TP is the number of true positives, TN is the number of true negatives, FP is the number of false positives, and FN is the number of false negatives.

2- False Positive Rate (FPR): This is a very important metric; it calculates the percentage of harmless actions that are mistakenly classified as attacks. The lower the FPR of the IDS, the more reliable it is and the less likely it is to produce unnecessary alarms. This rate is calculated based on the following equation:

$$FPR = \frac{FP+TN}{FP} \quad (3)$$

3- Precision: It is calculated as the ratio of accurate positive predictions to all positive predictions of the intrusion detection system. It gives an idea about the system's ability to prevent false positives, and is calculated based on the following equation [43]:

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

4- Recall: It is defined as the ratio of all actual positives to the actual positive predictions. The higher the recall ratio, the less chance there is for false negatives. It is calculated based on the following equation [43]:

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

5- F1-Score: The harmonic mean of precision and recall produces the F1-Score, which offers a fair evaluation of the IDS's effectiveness. It is beneficial in situations where datasets are unbalanced, and neither precision nor recall can give a clear picture. An elevated F1-Score suggests that the IDS effectively balances recall and precision [44].

$$F1-score = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (6)$$

4. Model test and results

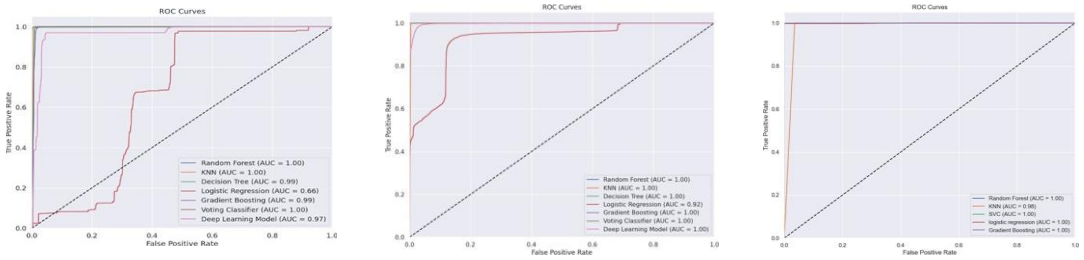
We are applying two cascaded models to predict the type of traffic (normal or any attack). We use two models and get the overall results for them after combining them: 1-Label model 2- Type-Attack-Model.

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

1) Label model

The first model (label model) will be used to predict if the traffic is (attack or normal) which are used to train the selective features (X) and label (Y) by fitting the model on the train data and evaluate it using test data. To get (accuracy, F1 score, precision, recall, AUC, confusion matrix and False positive rate) we try many techniques and compare between them to get the best one (logistic regression, DT, RF, deep learning using RNN, voting score ensemble and XGBoost) we compare all of them and getting the best one as the first cascaded model.

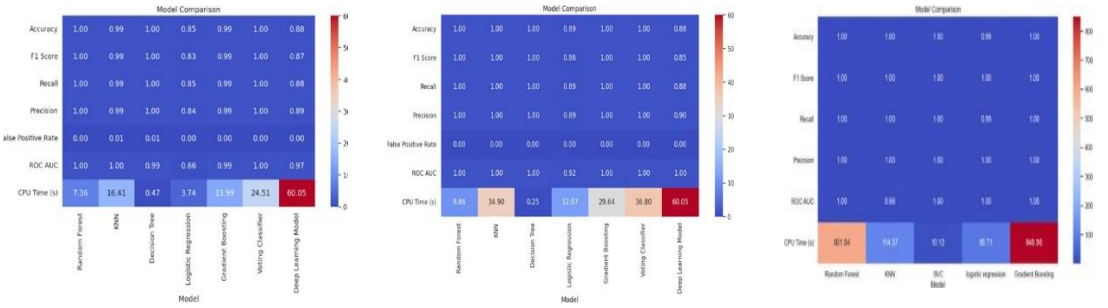
Figure 4 (a,b,c) exhibits a brief about the techniques used and evaluation methods. It represents the comparison between many models and shows AUC for the three mentioned datasets.



(a) AUC for TON-IOT dataset (b) AUC for UNSW-NB15 dataset (c) AUC for Bot-IOT dataset

Figure 4. AUC comparisons across different models for the three datasets.

Figure 5 shows the comparison between models for many terms (recall, precision, accuracy, F1 score and computing time) also for the three datasets.



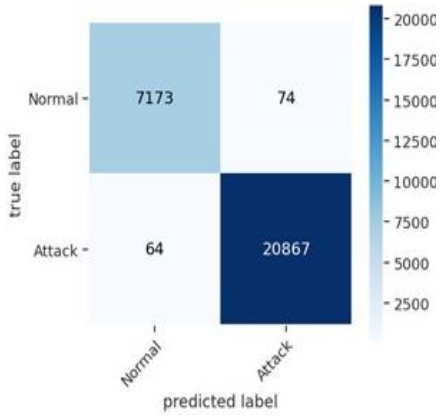
(a) Comparison on TON-IOT dataset (b) Comparison on UNSW-NB15 dataset (c) Comparison on Bot-IOT dataset

Figure 5. Comparison of recall, precision, accuracy, F1-score, and computing time across the three datasets.

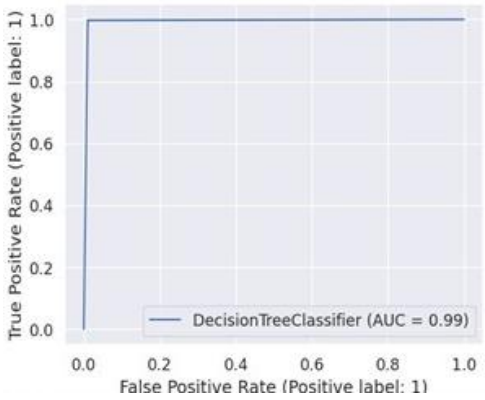
Table 3: Comparison of Models on Ton-IOT Dataset

Model	AUC	False Rate	Accuracy	Recall	F1-score	Precision	CPU Time(s)
RF	1.00	0.00	1.00	1.00	1.00	1.00	7.36
DT	0.9987	0.01	1.00	1.00	1.00	1.00	0.47
Logistic regression	0.66	0.00	0.85	0.8564	0.83	0.84	3.74
Voting classifier	1.00	0.00	1.00	1.00	1.00	1.00	24.51
KNN	1.00	0.01	0.997	0.9932	0.998	0.9946	16.41
Gradient boosting	0.998	0.00	0.994	0.9925	0.9945	0.99785	13.99
Deep learning	0.978	0.00	0.881	0.883	0.8744	0.89724	60.05

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024



(a) Confusion matrix of DT on Ton-IOT dataset

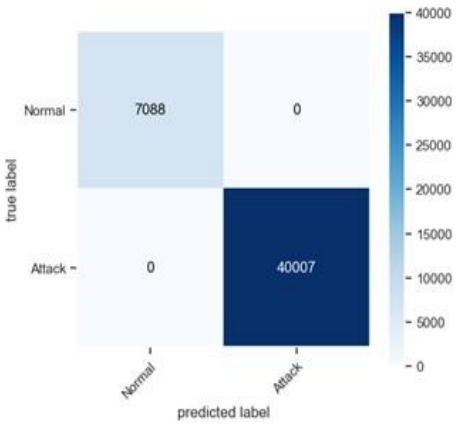


(b) AUC of DT on Ton-IOT dataset

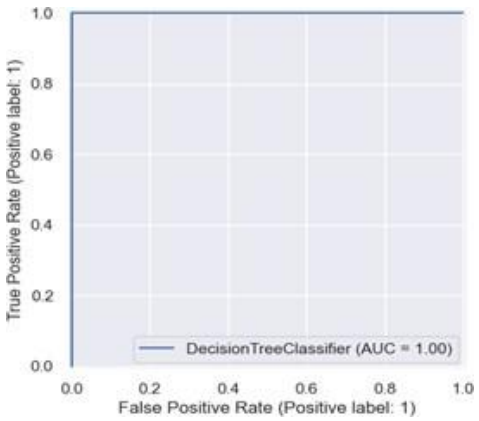
Figure 6. Comparison of DT Model Performance on Ton-IOT Dataset

Table 4: Comparison of Models on UNSW-NB15 Dataset

Model	AUC	False Rate	Accuracy	Recall	F1-score	Precision	CPU Time(s)
RF	1.00	0.00	1.00	0.9964	1.00	1.00	9.86
DT	1.00	0.005	1.00	0.9959	1.00	1.00	0.25
Logistic regression	0.92	0.00	0.887	0.8894 1	0.8855	0.8894	3.74
Voting classifier	1.00	0.00	1.00	1.00	1.00	1.00	36.8
KNN	1.00	0.001	0.9946	0.9954	1.00	1.00	34.9
Gradient boosting	1.00	0.00	1.00	1.00	1.00	1.00	29.64
Deep learning	1.00	0.00	0.88325	0.8835 9	0.8845	0.90468	60.05



(a) AUC of DT on UNSW-NB15 dataset



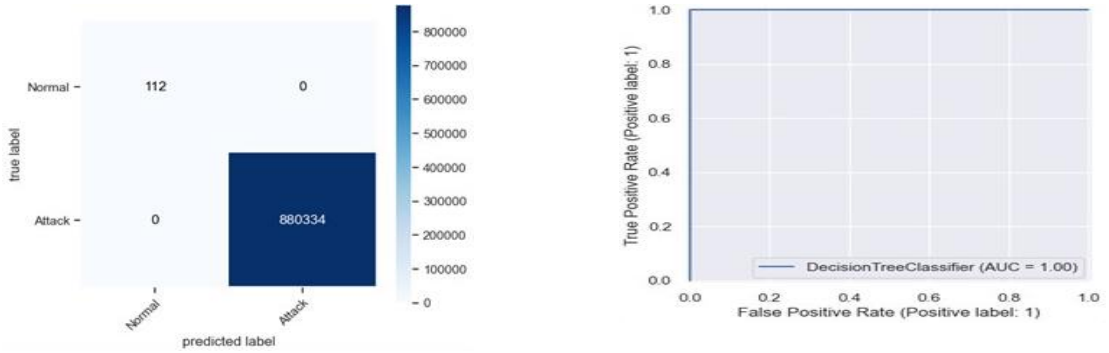
(b) Confusion matrix of DT on UNSW-NB15 dataset

Figure 7. Comparison of DT Model Performance on UNSW-NB15 Dataset

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

Table 5: Comparison of Models on BOT-IOT Dataset

Model	AUC	False Rate	Accuracy	Recall	F1-score	Precision	CPU Time(s)
RF	1.00	0.0015	1.00	0.9985	0.99954	1.00	601.54
DT	1.00	0.0028	1.00	0.9978	0.9857	1.00	0.49
Logistic regression	1.00	0.001	0.99	0.99	0.987	0.99	85.71
KNN	0.995	0.0025	0.9975	0.9948	0.9964	1.00	114.5
SVC	0.9975	0.0045	0.9996	0.9912	0.99815	1.00	10.12
Gradient boosting	0.9986 5	0.001	0.9957	0.9974	0.9963	0.9998	848.56

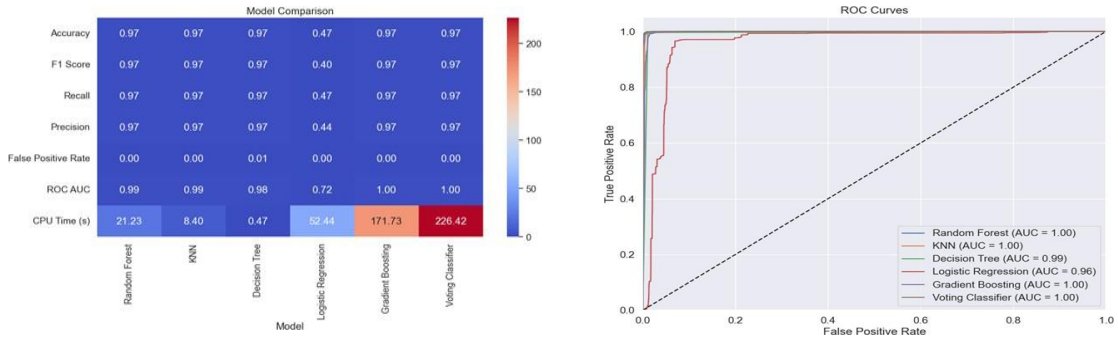


(a) Confusion matrix of DT on BOT-IOT dataset

(b) AUC of DT on BOT-IOT dataset

Figure 8. Comparison of DT Model Performance on BOT-IOT Dataset

As we can see from the results above (Figure 6,7,8 and Table 3,4,5), DT is the best model to be used in Label model for the three datasets. DT achieves high accuracy, recall, and precision, nearly equal to 1. It also has a low false positive rate on all the datasets, approximately 0.001. DT takes less computing time to fit the dataset and make a decision about whether the traffic is normal or an attack. After obtaining the results, as shown in the figures below, we select the best performing algorithm to integrate into the system, see figures (9, 10, 11).

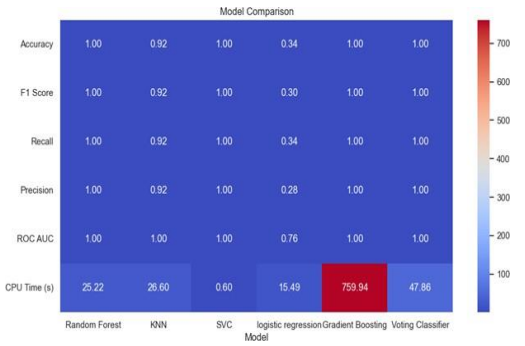


(a) Comparison of ML Algorithms on Ton-IOT

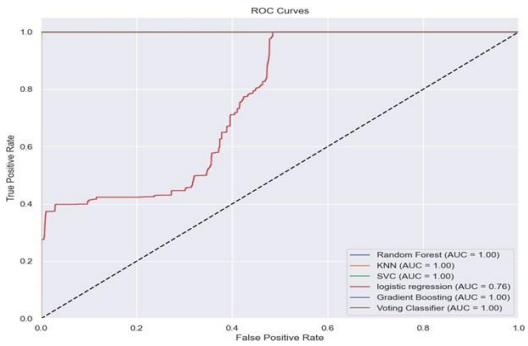
(b) AUC on Ton-IOT

Figure 9. Results on Ton-IOT Dataset

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

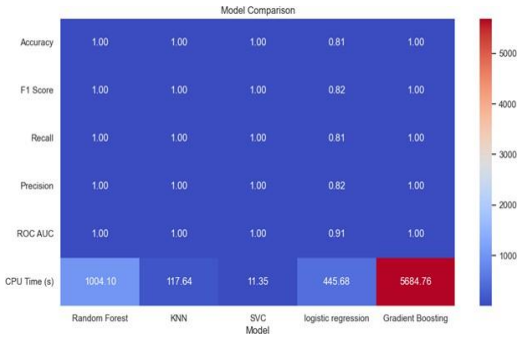


(a) Comparison of ML Algorithms on BOT-IOT dataset

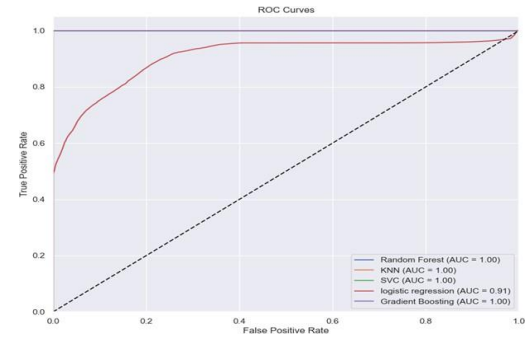


(b)) AUC on BOT-IOT dataset

Figure 10. Results on UNSW-NB15 Dataset



(a) Comparison of ML Algorithms on BOT-IOT dataset



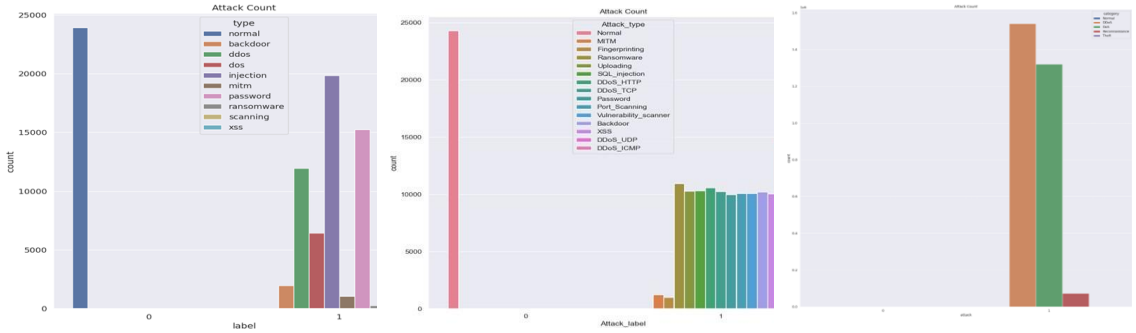
(b)) AUC on BOT-IOT dataset

Figure 11. Results on BOT-IOT Dataset

Next, the second model deploying in our cascade system to predict the type of attack.

2) Type-Attack-Model

After deploying the label model of our cascade system and obtaining the results, the performance of various algorithms will be compared to identify which model most effectively detects different types of attacks. As previously noted, this analysis incorporates three distinct datasets. Figure 12 illustrates the types of attacks detected in each dataset.



(a) Types of Attacks Detected in Ton-IOT dataset

(b) Types of Attacks Detected in UNSW- NB15 Dataset

(c) Types of Attacks Detected in BOT-IOT Dataset

Figure 12. Comparison of Types of Attacks Detected in Three Different Datasets

Various machine-learning algorithms will be used, similar to those used in the label model, on the dataset. Here, X represents the features selected using the feature selection technique, while Y represents the attack types based

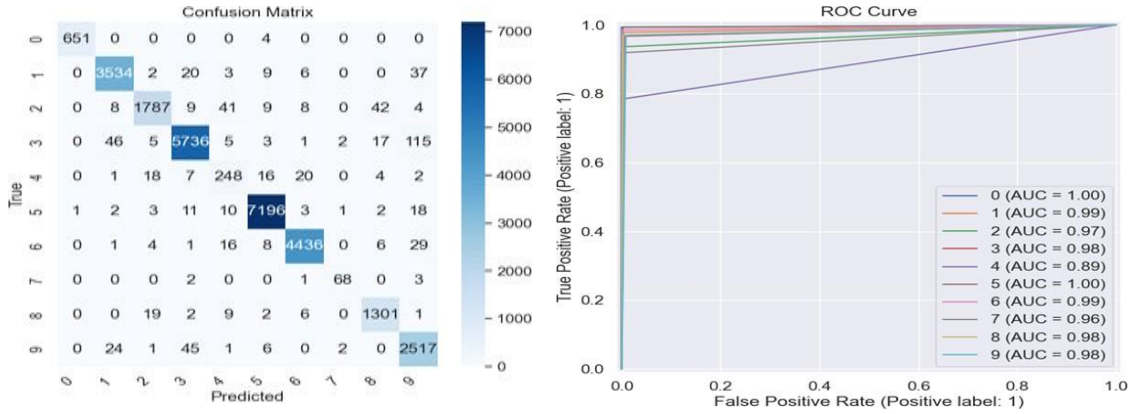
DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

on the dataset. The goal is to determine the best algorithm to use as the second model in our cascade system. We try several techniques, including RF, DT, KNN, Gradient Boosting, SVC, and deep learning algorithms.

Table 6: Summarizes the number of attack types and the specific attack types present in each dataset.

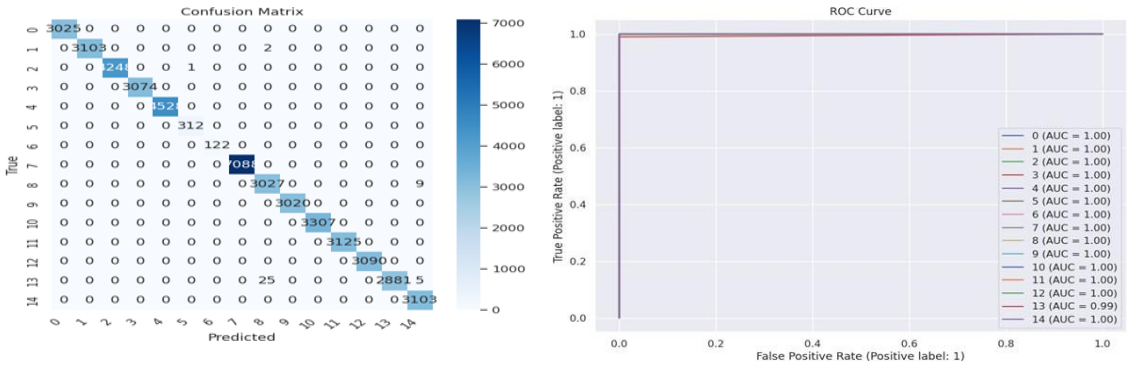
Dataset	N. of Attack Types	Attacks
Ton-IOT	10	Normal, DDOS, DOS, Backdoor, Injection, Scanning, MITM, Password, Ransomware, XSS
UNSW-NB15	15	Normal, MITM, Fingerprinting, Uploading, Port Scanning, DDOS HTTP, DDOS TCP, DDOS UDP, DDOS ICMP, Password, XSS, Vulnerability Scanner, SQL Injection, Ransomware, Backdoor
BOT-IOT	5	Normal, DOS, DDOS, Reconnaissance, Theft

All comparisons possible on the three datasets and got results as shown in figure 13,14,15.



(a) Confusion Matrix of RF on Ton-IOT (b) AUC of RF on Ton-IOT

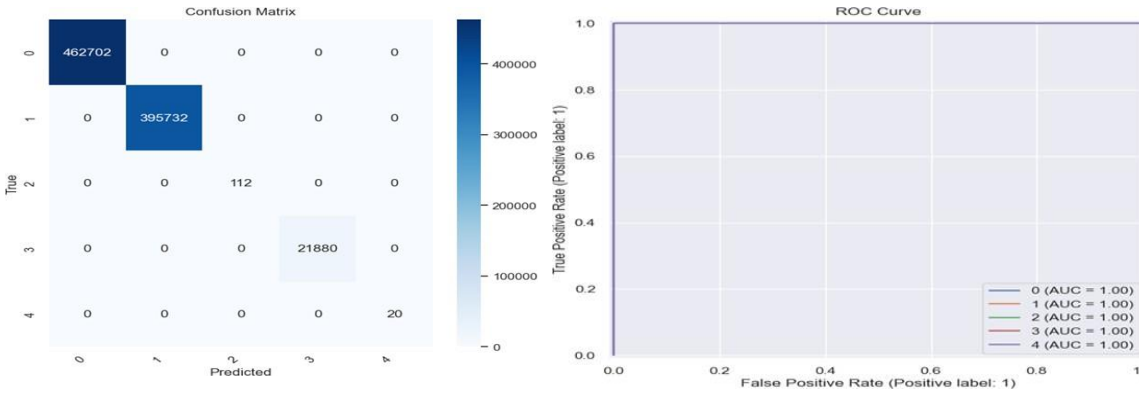
Figure 13. Results of RF Model on Ton-IOT Dataset



(a) Confusion Matrix of RF on UNSW-NB15 (b) AUC of RF on UNSW-NB15

Figure 14. Results of RF Model on UNSW-NB15 Dataset

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024



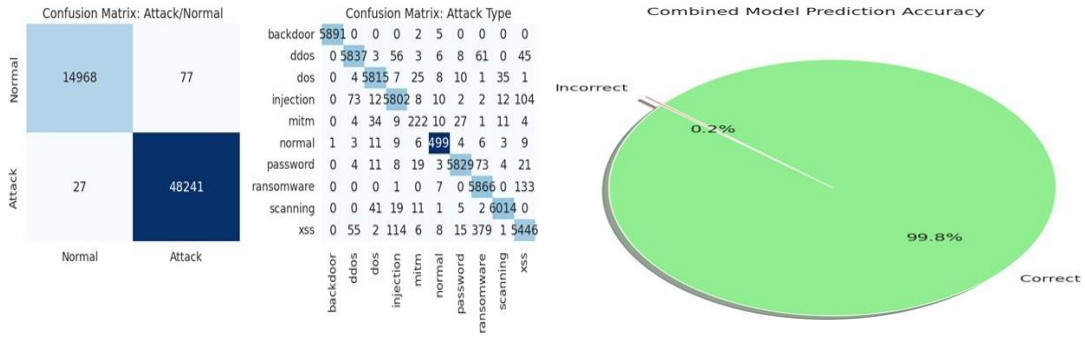
(a) Confusion Matrix of RF on BOT-IOT (b) AUC of RF on BOT-IOT

Figure 15. Results of RF Model on BOT-IOT Dataset

We can see that RF is the best technique to be used in the type of attack model. We first used grid search for the best parameters of RF to get the best results in terms of (accuracy, recall, precision, f1 – score, and CPU time). We use RF with parameters (an estimators =500, max iteration=200, max depth=30), getting the best results.

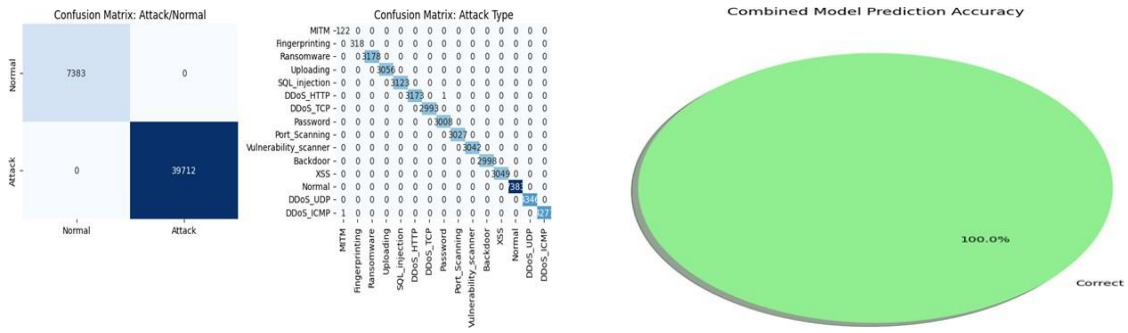
3) The cascaded model

After we choose DT to be used as the label model to detect if the traffic is normal or an attack and RF as the type-attack- model to detect the type of attack, we combine the results of the two models to get the overall results for both, as shown in figure 16 and figure 17. Results are ready to be deployed for real-world applications.



(a) Results of Two Models on TON-IOT (b) Combined Model Results on TON-IOT

Figure 16. Results of the DT and RF Models on TON-IOT



(a) Results of Two Models on UNSW-NB15 (b) Combined Model Results on UNSW-NB15

Figure 17. Results of the DT and RF Models on UNSW-NB15

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

5. Conclusion

In our work, we present a comprehensive framework for enhancing IIoT security based on AI intrusion detection systems. Our research highlights the impact of increased interconnectivity between devices and systems on increasing vulnerabilities in all IIoT settings. Traditional intrusion detection methods cannot handle complex attacks in such an environment, and often lead to high false positives and undetected threats since their monitoring of malicious activities is tied to predefined rules and signatures. Leveraging AI-powered techniques such as machine learning and deep learning has helped demonstrate marked improvements in increasing the intrusion detection rate while reducing the false positive rate and allowing anomaly detection in real-time. The proposed cascading model approach, which integrated DT and RF, has been able to classify with greater efficiency in the detection of a wide range of attacks on several datasets, including the BOT-IoT, UNSW- NB15, and TON-IoT datasets. It achieved very high accuracy, recall, and precision with low false positive rates. Thus, it was a robust solution for the challenges of IIoT security. Moreover, the flexibility and adaptability of AI-IDS would ensure their continuous evolution with emerging threats, turning them into a vital part of the future regarding industrial cybersecurity. This generally will respond to the urgent updating of security in the IIoT environment and provide an automated proactive security framework for industries against ever-evolving cyber threats. Although this study has presented the efficacy of AI- driven IDS for IIoT environments, some of these areas require further consideration to pick up the findings and progress towards making the system more robust such as Integration with Block chain Technology for decentralized and tamper-proof security. Using edge computing for real-time security is also another area to improve our work results, which aims to reduce detection times and enhance the system's ability to respond in real time. Although our proposed framework will efficiently detect intrusions in IIoT networks, using cloud-based analysis may introduce some latency issues. Our research areas could also expand to include adversarial machine learning, which may include the development of resilient models to poisoning, evasion, and other data manipulation techniques employed by attackers. While this work has focused on IIoT environments, future work could extend the research to other domains, such as smart cities, healthcare, or agriculture, where IIoT is gaining momentum.

References

[1] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, "The industrial internet of things (IIoT): An analysis framework," Elsevier, 2018.

[2] A. Khatib, M. Hamlich, and D. Hamad, "Machine learning based intrusion detection for cyber-security in iot networks," E3S Web of Conferences, vol. 297, p. 01057, 2021.

[3] H. Tyagi and R. Kumar, "Attack and anomaly detection in iot networks using supervised machine learning approaches," Revue d'Intelligence Artificielle, vol. 35, p. 11–21, Feb 2021.

[4] B. Alotaibi, "A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities," Sensors 2023.

[5] R. A. Ramadan and K. Yadav, "A novel hybrid intrusion detection system (ids) for the detection of internet of things (iot) network attacks," Annals of Emerging Technologies in Computing, vol. 4, p. 61–74, Dec 2020.

[6] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Implementing lightweight iot-ids on raspberry pi using correlation-based feature selection and its performance evaluation," Advances in Intelligent Systems and Computing, p. 458–469, Mar 2019.

[7] E. Seid, O. Popov, and F. Blix, "Security Attack Behavioural Pattern Analysis for Critical Service Providers,", J. Cybersecur. Priv., 4, 55–75, 2024

[8] S. Choudhary, N. Kesswani, S. Majhi, "An ensemble intrusion detection model for internet of things network," 2021.

[9] S. Krishnan, A. Neyaz, and Q. Liu, "Iot network attack detection using supervised machine learning," 2021.

[10] A. Verma and V. Ranga, "Machine learning based intrusion detection systems for iot applications," Wireless Personal Communications, vol. 111, p. 2287–2310, Nov 2019.

[11] K. M. Sai, B. B. Gupta, C.-H. Hsu, and D. Perakovi´c, "Lightweight intrusion detection system in iot networks using raspberry pi 3b+.," in SysCom, pp. 43–51, 2021.

[12] R. Qaddoura, A. M. Al-Zoubi, I. Almomani, and H. Faris, "A multi-stage classification approach for iot intrusion detection based on clustering with oversampling," Applied Sciences, vol. 11, no. 7, 2021.

[13] A. Jamalipour, S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," IEEE Internet Things J., 9, 9444–9466, 2021.

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

[14] Z. AZAM, MD. M. ISLAM, and M. NURUL HUDA, "Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis through Decision Tree," IEEE Access, VOLUME 11, 2023.

[15] S. M. KASONGO, "An Advanced Intrusion Detection System for IIoT Based on GA and Tree Based Algorithms," IEEE Access, VOLUME 9, 2021.

[16] I. Tareq, B. M. Elbagoury, S. El-Regaily, and El-Sayed M. El-Horbaty, "Analysis of ToN-IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT," Appl. Sci., 12, 9572, 2022.

[17] A. Manderna, S. Kumar, U. Dohare, M. Aljaidi, O. Kaiwartya, and J. Lloret, "Vehicular Network Intrusion Detection Using a Cascaded Deep Learning Approach with Multi-Variant Metaheuristic," Sensors, 23, 8772, 2023.

[18] K. Kethineni, G. Pradeepini, "Intrusion Detection in Internet of Things Based Smart Farming Using Hybrid Deep Learning Framework," 2023.

[19] X. Larriva-Novo, C. Sánchez-Zas, V. A. Villagrá, A. Marín-Lopez, and J. Berrocal, "Leveraging Explainable Artificial Intelligence in Real-Time Cyberattack Identification: Intrusion Detection System Approach," Appl. Sci.,13, 8587,2023

[20] B. Khampirat, "The impact of work-integrated learning and learning strategies on engineering students' learning outcomes in thailand: A multiple mediation model of learning experiences and psychological factors," IEEE Access, vol. 9, pp. 111390–111406, 2021.

[21] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (ddos) attack dataset and taxonomy," in 2019 International Carnahan Conference on Security Technol- ogy (ICCST), pp. 1–8, 2019.

[22] 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: Cen- tralized and federated learning," 2022.

[23] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw- nb15 network data set)," in 2015 Military Communi- cations and Information Systems Conference (MilCIS), pp. 1–6, 2015.

[24] S. More, M. Idrissi, H. Mahmoud, and A. T. Asyhari, "Enhanced Intrusion Detection Systems Performance with UNSW-NB15 Data Analysis," Algorithms, 2024.

[25] K. Roshan, A. Zafar, "An Optimized Auto-Encoder based Approach for Detecting Zero-Day Cyber-Attacks in Computer Network," IEEE, 2021.

[26] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. No˜mm, "Medbiot: Generation of an iot botnet dataset in a medium-sized iot network," 02 2022.

[27] F. Aubet, M. Pahl, "DS2OS traffic traces," 2018, Available at: https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces.

[28] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "WUSTL-IIOT-2021 Dataset for IIoT Cybersecurity Research," 2021.

[29] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," Sensors, 2023.

[30] A. Mehto, S. Tapaswi, and K. Pattanaik, "Multi-objective particle swarm optimization-based rendezvous point selection for the energy and delay efficient networked wireless sensor data acquisition," Journal of Network and Computer Applications, vol. 195, p. 103234, 2021.

[31] Z. M. Nayeri, T. Ghafarian, and B. Javadi, "Application placement in fog computing with ai approach: Taxonomy and a state-of-the-art survey," Journal of Network and Computer Applications, vol. 185, p. 103078, 2021.

[32] Z. Tong, X. Deng, J. Mei, B. Liu, and K. Li, "Response time and energy consumption co-offloading with slrta algorithm in cloud–edge collaborative computing," Future Generation Computer Systems, vol. 129, pp. 64–76, 2022.

[33] T. A. Akyildiz, C. B. Guzgeren, C. Yilmaz, and E. Savas, "Meltdowndetector: A runtime approach for detecting meltdown attacks," Future Generation Computer Systems, vol. 112, pp. 136–147, 2020.

[34] A. Mallik, "MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE WORDS," Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2019.

[35] A. Singh, B. B. Gupta, "Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions," International Journal on Semantic Web and Information Systems (IJSWIS) 18(1), 2022.

[36] F. Nabi, J. Yong, X. Tao, "Classification of Logical Vulnerability Based on Group Attacking Method," Procedia Computer Science, 170, 2020.

[37] N. S. Turhan, "Karl Pearson's Chi-Square Tests," Educational Research and Reviews, 16(9), 575-580, 2020

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024

[38] Codecademy Team, "Feature Importance," Codecademy. Available at: https://www.codecademy.com/article/fe-feature-importance-final.
[39] M. Komorowski, D.C. Marshall, J.D. Salciccioli, Y. Crutain, "Exploratory Data Analysis. In: Secondary Analysis of Electronic Health Records," Springer, Cham, 2016.
[40] I. D. Acheme, O. R. Vincent, "16 - Machine-learning models for predicting survivability in COVID-19 patients," Data Science for COVID-19, Academic Press, 2021.
[41] M. K.Dahouda, , I. Joe, "A deep-learned embedding technique for categorical features encoding," IEEE Access, 9, 114381-114391, 2021
[42] T. Fawcett, "An introduction to ROC analysis," Pattern recognition letters, vol. 27, no. 8, 2006, pp. 861-874.
[43] D. M. Powers, "Evaluation: from precision, recall and Fmeasure to ROC, informedness, markedness and correlation," Journal of machine learning research, vol. 2, no. 1, 2011, pp. 37–63.
[44] Y. Sasaki, "The truth of the F-measure," Teach Tutor mater, vol. 1, no. 5, 2007, pp. 1-5.

DOI: https://doi.org/10.54216/JCIM.150216
Received: May 15, 2024 Revised: July 14, 2024 Accepted: November 02, 2024