iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78516

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Hybrid Rule-Based and Machine Learning Intrusion Detection System for DDoS Detection in Cyber-Physical Production Systems

T. Dayakar Reddy[1], P. Priyanka[2]
[1]*Assistant Professor, CSE Department, PBR Visvodaya Institute of Technology and Science, Kavali-A.P*
[2]*M. Tech, Computer Science and Engineering, PBR Visvodaya Institute of Technology and Science, Kavali-A.P*

Abstract: ***The industrial system now functions differently as a result of recent developments in communication technology. The process has become more transparent as a result of the better communication between the various entities involved in cyber physical production systems (CPPS), including manufacturers, suppliers, and users. The availability of the production systems may be threatened by the adoption of cutting-edge new technologies in CPPS, which may create weak points that attackers may utilize to conduct complex distributed denial of service (DDoS) assaults. Current machine learning-based intrusion detection systems (IDS) frequently skip the critical testing stage with real-time scenarios since they rely on irrational datasets for training and validation. The ML models' outputs are predicated on predictions made at every stage of the flow and are unable to offer a comprehensive picture of malevolent actors. This study suggested an effective IDS system that employs both rule-based detection and machine learning techniques to identify DDoS attacks that harm CPPS's infrastructure in order to overcome this constraint. We use real-time network traffic taken from an actual industrial setting, known as a Farm-to-Fork (F2F) supply chain system, for system training and validation. CIC-FLOWMETER was used to extract bidirectional features from both attacks and regular traffic. We employ 8 ML supervised and unsupervised techniques to identify the harmful flows. The frequency of the malicious flows is then determined using a rule-based detection mechanism, and the frequency is used to assign varying severity levels.***
Index Terms: Industry 4.0, CPPS, DDoS attacks, IDS solutions, machine learning, and rule-based detection.

I. INTRODUCTION

Factories are now sophisticated cyber-physical production systems (CPPS) thanks to the fourth industrial revolution (4.0), in which people, machines, and goods are connected across the supply chain. CPPS's infrastructure makes use of a number of cutting-edge technologies, including artificial intelligence (AI), cloud computing, edge computing, machine-to-machine (M2M) connectivity, and the Internet of Things (IoT). The basis for smart factories, where the entire chain is connected from the user to the production plant, has been laid by these technologies, which have converted factories into massively networked CPPS. Better product quality, higher productivity, lower costs, and sustainability are the outcomes of this networking, storage, and computing integration, which has improved communication between various manufacturing processes. In the ever-changing operational contexts of CPPS, the utilization of developing technologies has also led to an enhanced security threat landscape. New and significant security issues have arisen as a result of this integration, including a rise in cyberthreats, monetary losses, data breaches, disruptions to operations, and harm to one's reputation. Furthermore, because CPPS is made up of several IoT-based systems, sensors, and smart devices from various suppliers, there is a greater likelihood that it could exhibit additional vulnerabilities, which could put malicious actors at risk. can take advantage of. In actuality, the attacker may use these flaws to interfere with the system's regular functioning, which could lead to dire consequences like stopping the production line, lowering the caliber of the output, and damaging various organizational assets. Then, it is preferable to implement a cutting-edge intrusion detection system (IDS) that can both safeguard the network's perimeter and permit uninterrupted communication between the various industrial system sub-components. The application of CPPS in the farm-to-fork (F2F) supply chain is the main focus of this study. From the producers (farmers) to the final consumer, the F2F supply chain encompasses the full life cycle. The food industry's reliance on new digital technologies makes it far more susceptible to cyberthreats like distributed denial of service (DDoS) attacks, which disrupt the whole supply chain and cause business interruptions. Analyzing the risks and weaknesses related to the food and supply chain system is crucial, as the SecuFood project highlights.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Ransomware and DDoS attacks are the most frequent threats that the food business encounters. Generally speaking, the development of CPPS increases the likelihood of DDoS assaults in the food sector, underscoring the necessity of preventative measures to preserve the food supply chain's continuity and integrity. In order to provide dependable communication, protection against these kinds of attacks is essential. Their impact on the communication infrastructure may be unfavorable. Serious financial losses may result from the various parties participating in the food industry's supply chain experiencing delays or being unable to communicate with one another. The many parts of the communication infrastructure that link the various food supply chain stakeholders can be targeted by the attacker. DDoS assaults have the potential to overload services and resources and jeopardize production lines' availability. The availability of the communication network may be impacted by an abrupt spike in network traffic and resource usage, which could lead to less or, worse, no communication between the various supply chain system sub-components.

II. LITERATURE SURVEY

We provided a brief explanation of each comparable model and the study's closest competitor in the literature review section. For this study, we reviewed the most recent research publications over the previous two years. Additionally, Gozde Karatas et al. suggested a machine learning method for classifying attacks. After experimenting with several machine learning algorithms, they discovered that, in comparison to previous studies, the KNN model performs the best in classification. Machine learning techniques for intrusion detection were proposed by Nuno Martins et al. The KDD dataset, which is accessible through the UCI repository, was utilized. To improve performance, they experimented with various supervised models to balance the unclassification method. Several classification algorithms were used in this work to provide a comparison analysis, and the findings were positive. A systematic review for malware detection using machine learning models was proposed by Laurens D'hooge et al. They contrasted several malware datasets from internet sources and methods for the dataset. In order to make better decisions faster, they discovered that machine learning supervised models are highly successful for malware detection. A comparative study for network traffic classification was proposed by Xianwei Gao et al. They detected intrusions using machine learning classifiers. The CICIDS and KDD datasets were extracted from the UCI repository. When compared to other methods, they discovered support vector machine (SVM) to be among the best. Adaptive learning was suggested by Tongtong Su et al. for intrusion detection. They made advantage of an online repository's KDD dataset. These classifier models are KNN, R-forest, and Dtree. The authors of this study discovered that ensemble and Dtree models produce good classification results. The suggested task has an overall accuracy of 85%. Deep learning methods for intrusion detection were proposed by Kaiyuan Jiang et al. Convention neural network (CNN), BAT-MC, BAT, and recurrent neural network are the models used on the KDD dataset. Overall, the model performed admirably. CNN was deemed the top learning resource by them. The accuracy increased to 85% from 82%. For intrusion detection, Arun Nagaraja et al. suggested a hybrid deep learning approach. In order to classify CNNC LSTM from the RNN model, they integrated two deep learning models. KDD is the dataset used in this study.

They discovered that the suggested accuracy was 85.14% on average. Yanqing Yang et al. suggested a similarity-based method for machine learning-based anomaly identification. They employed the naïve Bayes model for classification and the k mean cluster model for feature similarity identification. Hui Jiang et al. applied deep learning classification models to the KDD dataset using an auto-encoder for labels. Use the adaptive search PSO optimum structure Xgboost after first creating a classification model based on Xgboost. The reference dataset for evaluating the suggested model is NSL-KDD. According to our findings, the PSO-Xgboost model performs exceptionally well in identifying U2R and R2L attacks in terms of precision, recall, and macro-average accuracy. Additionally, this study offers an experimental foundation for the intelligence application group NIDS. A recurrent neural network model for categorization intrusion detection was presented by Maede Zolanvari et al. They contrasted RNN with different deep learning models. Using the KDD dataset, they ultimately discovered that RNN is the most effective model for intrusion detection. A domain that provides a botnet categorization algorithm was proposed by Yijing Chen et al. The problem was one of multiple classification. They tackled various categorization difficulties using sophisticated deep learning LSTM. With an average accuracy of 89%, they discovered promising outcomes for the suggested task. Two benchmark datasets were proposed by Larriva-Novo et al., particularly UGR16 and UNSW-NB15, and the most popular dataset, KDD99, was utilized for evaluation. Scalar and standardization capabilities are used to evaluate the pre-processing approach. Different attribute arrangements are used to apply these pre-processing models. These characteristics are contingent upon the categorization of the four sets of highlights: content quality, fact attributes, basic associated highlights, and, lastly, the generation of highlights based on traffic and traffic quality based on the collection of linked titles.

In order to get the most accurate model, this inspection aims to assess this arrangement using several information pre-processing techniques. Our proposal demonstrates that the accuracy can be increased by up to 45% by using preprocessing techniques and traffic organization order.

III. PROPOSED SYSTEM

The overview of our proposed system is shown in the below figure.

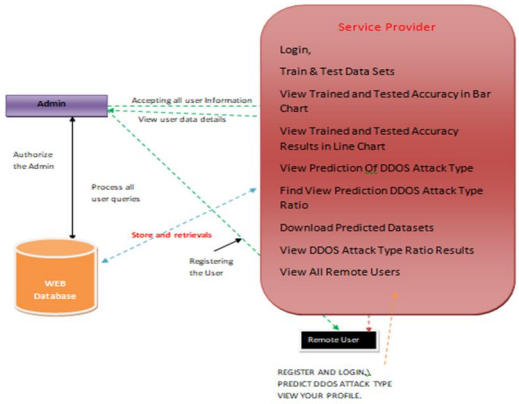


Fig. 1: System Overview

A. *Implementation Modules*

1) Service Provider Module: In this module, the service provider enters a working username and password to access the system. Following a successful login, he can examine the train and test dataset, view the accuracy of the trained and tested data, view the results of the trained and tested accuracy using charts, view the prediction of the type of DDoS assault, find the predicted ratio of the DDoS attack, and view distant users.

2) Train and Test Model: The service provider divided the used dataset in this module into 70% train data and 30% test data, respectively. Thirty percent of the data is regarded as test data, which is used to evaluate the model, and seventy percent is regarded as train data, which is used to train the model.

3) Remote User: The remote user registers for the system in this module and logs in with a valid username and password. He is able to view profiles and predict the type of DDoS assault after successfully logging in

4) Prediction: To determine the type of attack, the remote enters the malicious attack details in this module. This determines the type of DDoS assault and assesses the attack specifics.

5) Graphical Analysis: Show graphs such as the system's accuracy and predicted ratio in this module. The graph analysis takes into account a number of parameters. Plotting charts such as bar charts and others is part of this phase.

B. *Implementation Algorithms*

1) Support Vector Machine

- Support-vector machines (SVMs, also known as support-vector networks) are supervised learning models in machine learning that use related learning methods to examine data for regression and classification. As a non-probabilistic binary linear classifier, an SVM training technique creates a model that allocates new samples to either category.

2) Logistic Regression

- Among the most widely used machine learning algorithms, logistic regression falls under the category of supervised learning. With a given collection of independent factors, it is used to predict the categorical dependent variable.
- A categorical dependent variable's output is predicted by logistic regression. As a result, the result needs to be a discrete or category value. Yes or No, 0 or 1, true or false, etc., can be used, but probabilistic values that fall between 0 and 1 are provided rather than the precise values of 0 and 1.

3) Random forest

- It creates a number of decision trees, each of which makes a prediction based on a portion of the data sample.

- The outcome that the greatest number of trees were able to produce is then regarded as the final forecast.
- Random Forest is an algorithm for supervised learning that employs the ensemble learning approach for regression and classification. A bagging technique, random forests have trees that operate in parallel without interacting with one another.
- During training, a Random Forest builds many decision trees, with the mean of the classes serving as each tree's prediction.

4) Navie Bayes

- Based on the Bayes theorem, the supervised learning technique known as the Naïve Bayes algorithm is used to solve classification issues.
- Text classification using a high-dimensional training dataset is its primary application.
- One of the simplest and most efficient classification techniques for creating quick machine learning models with rapid prediction capabilities is the Naïve Bayes Classifier.
- Because it is a probabilistic classifier, it makes predictions based on an object's likelihood.

IV. RESULTS

Fig. 2: Service Provider Login Page

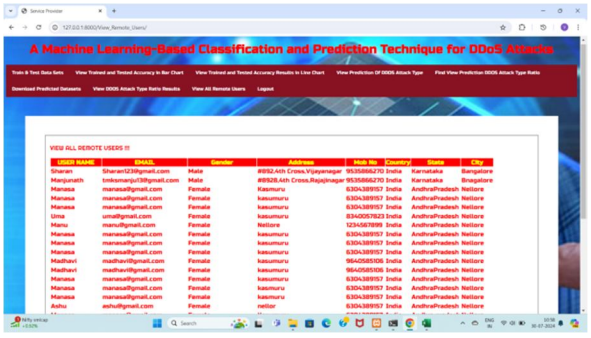


Fig. 3: View Remote Users

Fig. 4: Models Accuracy

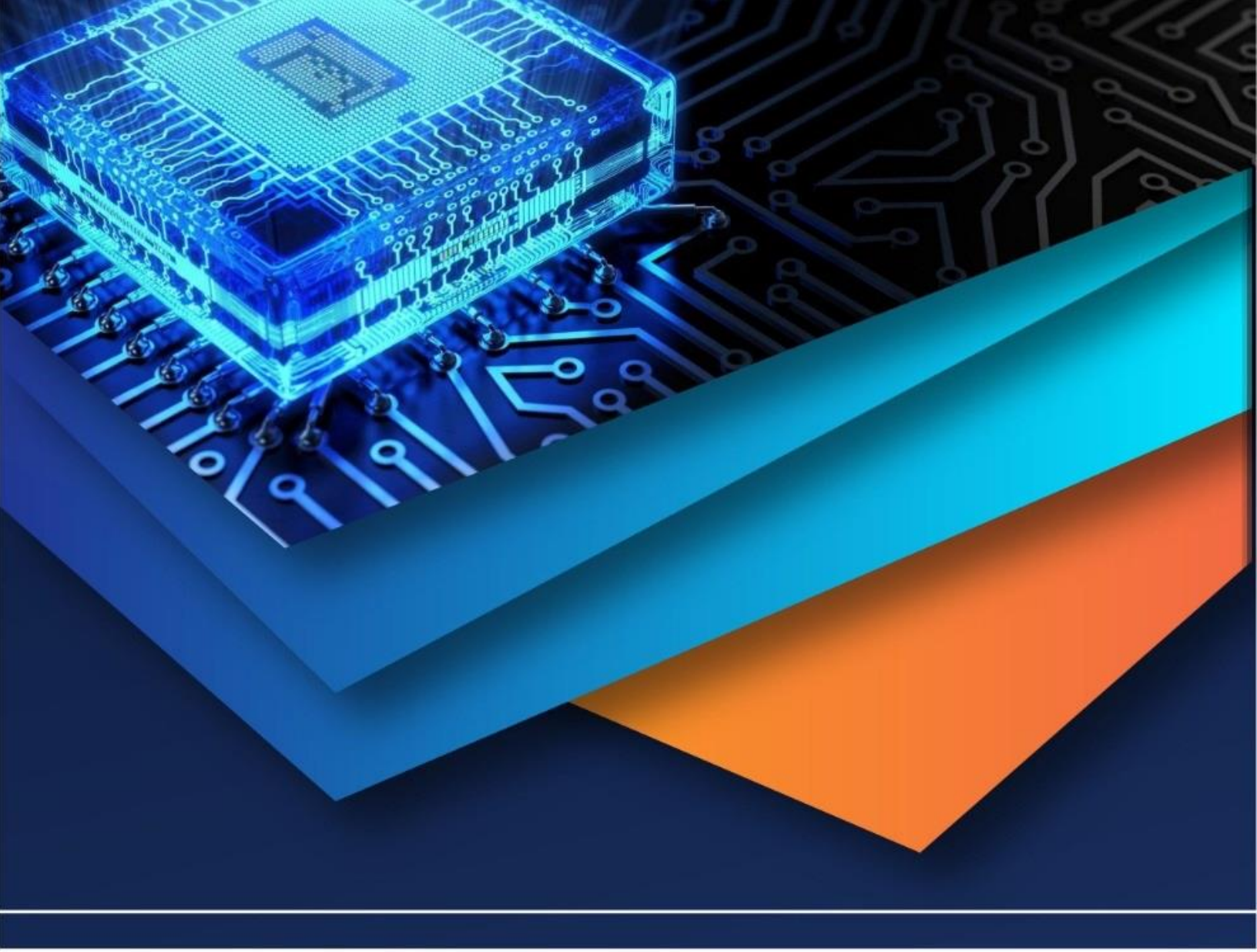
Fig. 5: Accuracy Graph

V. CONCLUSION

In this study, we suggested a comprehensive, methodical approach to DDOS assault detection. The UNSW-nb15 dataset, which includes details on the DDoS attacks, was first chosen from the GitHub source. The Australian Centre for Cyber Security (ACCS) supplied this dataset. Data wrangling was then done using a notebook that included Python and Jupyter. Second, the dataset was separated into two classes: the independent class and the dependent class. For the algorithm, we also normalized the dataset. Following the normalization of the data, we used the suggested supervised machine learning method. The supervised algorithm produced classification and prediction results for the model. Next, we applied the categorization algorithms XGBoost and Random Forest. We found that the Random Forest Precision (PR) and Recall (RE) are both roughly 89% accurate in the initial classification. Additionally, we observed that the suggested model had an average Accuracy (AC) of about 89%, which is very fantastic and sufficient. Keep in mind that the F1 score is 89% based on the average accuracy. We observed that the XGBoost Precision (PR) and Recall (RE) are both roughly 90% accurate for the second classification. We observed an average Accuracy (AC) of almost 90% for the proposed model, which is fantastic and incredibly intelligent. Once more, the F1 score is 90% based on the average Accuracy. The precision of the previous research's flaw determination, which was 85% and 79%, was particularly noteworthy when compared to the planntly improved.

REFERENCES

[1] "Adversarial machine learning applied to intrusion and malware scenarios: A systematic review," by N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, IEEE Access, vol. 8, pp. 3540335419, 2020.
[2] Increasing the performance of machine learning-based intrusion detection systems on an unbalanced and current dataset, G. Karatas, O. Demir, and O. K. Sahingoz, IEEE Access, vol. 8, pp. 3215032162, 2020.
[3] BAT: Deep learning techniques on network intrusion detection using NSL-KDD dataset," IEEE Access, vol. 8, pp. 2957529585, 2020; T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li.
[4] "Network intrusion detection based on PSO-xgboost model," by H. Jiang, Z. He, G. Ye, and H. Zhang, IEEE Access, vol. 8, pp. 5839258401, 2020
[5] "Similarity based feature transformation for network anomaly detection," by A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty, and V. S. Kiran, IEEE Access, vol. 8, pp. 3918439196, 2020.
[6] Classification hardness for supervised learners on 20 years of intrusion detection data, by L. D'hooge, T. Wauters, B. Volckaert, and F. De Turck, IEEE Access, vol. 7, pp. 167455167469, 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY