International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Machine Learning Approach for Detecting DDOS Attack in IoT Network Using Random Forest Classifier

P. Elamparithi[1], S. Kalaivani[2], S. Vijayalakshmi[3], E. Keerthika[4], S. Koteswari[5], R. Sathesh Raaj[6]

Submitted: 15/07/2023 **Revised**: 08/09/2023 **Accepted**: 25/09/2023

Abstract: The Internet of Things (IoT) has seen noteworthy growth and advancement in the last ten years, offering innovative keys to address social and industrial challenges. However, ensuring the safety of IoT devices has become a crucial concern because of their vulnerability to cyberattacks, which poses serious hazards and result in serious harm. Although researchers have made strides in this direction, Multiview feature integration and extensive semantic relationship capturing still need to be completed beyond the purview of existing work. Therefore, these methods may be more secure and better at identifying various threats in actual time. This study proposes a new technique using the Random Forest classifier to overcome these obstacles. By harnessing the potential of ensemble learning, this approach combines numerous decision trees to provide accurate and speedy predictions for the rapid and precise identification of threats in IoT networks. UDP-FLOOD, Smurf, HTTP-FLOOD, and SIDDOS are only some network assaults included in the collection. When applied to network traffic data, the Random Forest classifier is a powerful addition to more traditional machine learning-based categorization methods. The proposed Random Forest classifier enhances intrusion detection efficacy and shortens training time, indicating an enhanced solution for improving the network security in IoTs.

Keywords: *Machine Learning, Internet of Things (IoT), Classification, Security, Accuracy*

1. Introduction

IoT environment combines various network entities, including software's, sensors and other technology. These elements work together to connect systems and devices through the Internet and to enable data exchange. In IoT numerous entities are integrated which can be sensor, human or service [1]. It introduced a new computing architecture that fundamentally changes our daily lives. IoT's are widely used in supply-chain management, healthcare, transportation, industrial production smart homes [2-4].

The technology evolution highly relies on IoT devices, which increases the popularity among the entrepreneurs, researchers, cyber criminals and business people. The services offered by IoT devices are raising the market demand significantly. Potential investors have expressed interest in this requirement. By developing and promoting various IoT apps that improve and simplify our lives, innovators, and businesspeople are increasing the appeal of this industry. However, it has allowed cybercriminals to exploit IoT devices' flaws and vulnerabilities. IoT has been a popular target for cyberattack training because of corporate expansion and financial potential. This is the primary reason for the exponential rise in cyberattacks on IoT devices [5,6].

The IoT is susceptible to various assaults due to its open architecture and ability to self-configure. IoT devices frequently require additional human controls, and their memory and processing resources are constrained. Additionally, IoT's dependency and quick expansion are open for security vulnerabilities, necessitating network security solutions. While certain assaults can be difficult to detect, several systems work well [7,8]. The amount of data being carried across networks is expanding swiftly, increasing the number of network assaults. Due to the growing deployment of IoT technologies, it is essential to provide rapid and efficient means of attack detection and risk reduction. One of the most harmful assaults is a denial of service (DoS), which prohibits reputable consumers from using services. Distributed denial of service attacks can have serious repercussions for essential applications like healthcare, resulting in catastrophic delays in providing medical care.

The present work is structured in a systematic manner as outlined below: Section 1 delivers an overview to the

[1]*Assistant Professor, Department of Computer Science and Engineering, AAA College of Engineering and Technology, Sivakasi 626005, Tamil Nadu, India. Email: parithics@gmail.com*
[2]*Assistant Professor, Department of Computer Applications, B.S.Abdur Rahman Crescent Institute of science and Technology, Vandalur, Tamil Nadu 600048,India. Email: kalaivani@crescent.education*
[3]*Professor, Department of Electronics and Communication Engineering, R.M.K. Engineering College , Kavaraipettai, Tamil Nadu 601206, India. Email: svl.eie@rmkec.ac.in*
[4]*Assistant Professor, Department of Biomedical Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi-626140, Tamil Nadu,India. Email: keerthika@psr.edu.in*
[5]*Department of Electronics and Communication Engineering, Pragati Engineering College, Surampalem, East Godavari District, Andhra Pradesh, India*
[6]*Assistant Professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, 600062, India, Email: satheshraaj@gmail.com*

topic. Section 2 delves into the pertinent literature, encompassing previous studies and identifying any existing research gaps. Section 3 comprehensively elucidates the suggested methodology, encompassing the research techniques employed. Section 4 focuses on the experimental works conducted, while The results derived from the investigation are presented in Section 5.

2. Related Work

S. Ramakrishnan et al. [9] utilized the KDD Cup 99 dataset in their research to develop an intrusion detection system (IDS) aimed at identifying both intruders and legitimate data. In the first stage, an entropy-based feature selection methodology is used to identify the most crucial attributes. Subsequently, Fuzzy Control Language categorizes data into two distinct groups: regular and attacked. The findings indicated that the suggested method exhibited a statistically significant accuracy. The Densely-ResNet system, known as IDS, was introduced by Peilun Wu et al. in their publication [10]. The researchers employed the correlation function to identify the key features. The UNSW-NB15 dataset was utilized to evaluate the performance of Densely-ResNet. The results obtained from the model demonstrated a remarkable degree of accuracy and a very low percentage of false alarms.

In their study, Latif et al. (2011) proposed the development of an IDS for safeguarding IIoT systems. The IDS was designed using a random neural network approach. The experiment was done using the UNSW NB15 dataset. The dataset underwent analysis to evaluate its possible suitability for use in the context of the IIoT. The findings indicated a lower false alarm rate and improved detection accuracy. According to Prabhat Kumar et al. [12], an IoMT network framework with ensemble learning and a fog-cloud architecture is proposed to identify cyberattacks. The ToN-IoT dataset is taken for observation for accessing the capability of accuracy prediction.

In their study, Roopak et al. [13] focused on specific components of six fundamental goals in order to create distinct hybrid identifiers for the resolution of detecting distributed denial-of-service (DDoS) assaults in IoT settings. The algorithm is constructed by using the deep learning methodology, which takes input from the condensed data produced in the previous step. A quick and effective Artificial Neural Network (ANN) attack recognition technique was developed in [14] to recognize a various attack in IoT data. In the event of an attack, the IoT console classifies malicious packets using ANN technology. There were three levels of neural networks: hidden, input and output. According to the immunity concepts such as clonal selection, danger theory and adverse selection, a unique AIS-based DDoS IDS system has been proposed [15].

Shareena and her colleagues [16] developed an intrusion detection system (IDS) that use deep learning techniques to detect distributed denial-of-service (DDoS) botnet attacks in the context of the Internet of Things (IoT). Deep Neural Network (DNN) has the capability to create and test for accurate IoT botnet attack detection. The findings demonstrate that the DNN's potential for accurately identifying IoT DDoS botnet attacks compared to current systems with high levels of precision and accuracy. In their work, Alghanam et al. give a better way to choose features for intruder detection. For detection, the system takes advantage of ensemble learning. These modes employ a straightforward architecture and dataset [17]. An RNN-based intrusion detection system in IoT networks is presented by Syed et al. The models created on the minimum dataset exhibited more excellent recall rates without sacrificing their ability to differentiate between the classes to trained systems on the entire feature set [18].

Saba et al. [19] created a deep learning-based approach that uses a CNN-based and anomaly-based IDS to improve the security of the Internet of Things. The suggested method carefully examines every IoT communication to find potential intrusions and odd traffic patterns. The method receives 92.85% on the BoT-IoT datasets [19]. in order to increase ML's estimates' clarity and the precision with which IDS identifies threats. Li et al. provide an ML-based IDS method in [20] that builds ensemble trees from RF and DT classifiers. The IoTDS20, NF-ToN-IoT-v2, and NF-BoT-IoT-v2 datasets [20] examine the method using a net flow meter feature set. Because sensor nodes may arrange themselves in unforeseen ways, securing Wireless Sensor Networks (WSN) has become more challenging in recent years. The popularity of Wireless Sensor Networks (WSNs) has grown as a result of its self-organizing characteristics, low power needs, and cheap cost. The Wireless Sensor Network (WSN) is increasingly replacing conventional technologies used in businesses and factories due to significant advancements in processing capabilities, communication efficiency, and low-power consumption of embedded computer systems. The widespread use of Wireless Sensor Networks (WSNs) in corporate and commercial contexts may be attributed to advancements in processing capabilities, communication technologies, and energy-efficient embedded computer systems [22-26]. The Internet of Things (IoT), an emerging technology, makes it easy and advantageous to share data with additional devices across wireless networks. However, due of their continual development and technological advancements, IoT systems are more vulnerable to cyberattacks, which could result in strong assaults [27-29].

2.1 Problem Statement:

- Traditional machine learning techniques do not handle a wide variety of traffic effectively.

- The accuracy of intrusion detection is inadequate
- Low-performance accuracy classification and lengthy computation

2.2 Research Contribution:

This work aims to create ML-based Random Forest algorithms for Internet of Things applications. The suggested Random Forest classifier addresses the flaws mentioned in the preceding publications. The dataset with many types of attacks was used in this study to evaluate discovery algorithms that blend real-world and simulated IoT network traffic with diverse attacks to become better at detecting malicious activity. The weights of various variables, particularly those retrieved during preprocessing, can be adaptively updated to help the Random Forest classifier recognize attack types more accurately in real time.

3. Proposed Methodology

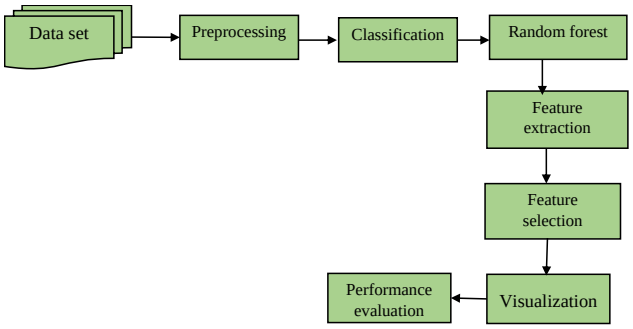

Fig. 1. Proposed Architecture

3.1 Data set

The collection includes around 2,100,000 records from network assaults of different types. The network attacks are of various types, such as Normal traffic, Smurf, HTTP-FLOOD, UDP-Flood, and SIDDOS. https://www.kaggle.com/datasets/jacobvs/ ddos-attack-network-logs?resource=download

3.2 Preprocessing

Data preparation is a critical stage in the machine learning pipeline that entails preparing raw data for training models by cleaning, converting, and organizing it. The caliber of the input data directly influences machine learning algorithms' efficiency and dependability. Better model results are anticipated due to this approach, which tries to improve the data's consistency, correctness, and accuracy.

3.3 Tools used

The Classification Learner program is employed in data classification for training the model. With the help of several categorization algorithms, this system enables supervised machine learning exploration. These tools are widely used for data processing, training the model, selecting the features, and evaluating the results. Automatic training determines the best model among several candidates, including neural network classification, Bayes naive, kernel approximation, discriminant analysis, support vector machines, logistic regression, decision trees, closest neighbors, and ensemble classifications. The trained model is then exported to the workspace, utilized with fresh data through MATLAB code, or used to go further into programmatic sort.

3.4 Random Forest classifier

Random Forest classifiers are an effective machine learning strategy for solving regression and classification issues. It uses an ensemble learning technique to mix many decision trees and provide precise predictions. Each decision tree makes its prediction after being trained on a different random subset of the dataset. Combining the bagging method with feature randomization yields an uncorrelated forest of decision trees; hence, it is an extension of the bagging methodology. The training process begins with the establishment of the random forest algorithms and their three important hyperparameters: tree count, sampling feature count, and node size. An ensemble of decision trees is the basis of the random forest algorithm. Each tree in this ensemble is built using a replacement on a data sample taken from the training set. The bootstrap sample is a method of sampling. Each decision tree is combined for the classification task and regression job. The most frequent categorical indicator provides overwhelming support for the anticipated class. Combining each tree's forecasts, the Random Forest generates a final prediction. Then, cross-validation with the oob sample is used to make the final prediction.

3.5 Classification attributes

3.5.1 Black Hole Attack

One kind of cyber hazard that might harm communication networks is a black hole attack. A malicious node or device performs this attack by acting as if it is the quickest way to the target, so diverting traffic from other nodes and devices to itself. As a result, valid nodes are cut off from one another, interrupting the regular flow of communication.

3.5.2 Flooding

Flooding is a communication strategy in WSNs in which data is transmitted to every device in a network, whether they belong to the recipients or not. Important information, such as network upgrades or configuration changes, is frequently transmitted via this technique. Flooding, if improperly handled, can also result in network clogging and inefficiency.

3.5.3 Gray Hole Attack

A cybersecurity flaw that attacks computer networks is the gray hole attack, particularly those using wireless

connectivity. In contrast to a black hole attack, which indiscriminately loses all data packets, this particular assault entails a hostile node selectively rejecting or modifying a subset of the packets. This dishonest conduct results in inconsistent network performance, which might result in data manipulation and communication interruption.

3.5.4 TDMA (Time Division Multiple Access):

In WSNs and other networks, TDMA is a communication technique that allows several devices to utilize a single communication channel. Each device participating in TDMA is given a certain time slot within which the data can be transmitted. This technique enables effective utilization of the interaction channel and avoiding collisions.

4.Experimental Results

Description of the Terms:

- Positive (P): A positive observation
- Negative (N): An observation that does not exhibit a favorable or optimistic quality.
- A true positive (TP) refers to an observation that is characterized by being positive in nature and is accurately expected to be positive.
- A false negative (FN) refers to an instance when an observation, which is initially categorized as positive, is incorrectly forecasted or classified as negative.
- A true negative (TN) refers to an observation that exhibits a negative outcome and is accurately expected to have a negative outcome.
- A false positive (FP) refers to an instance when an observation is classified as positive despite being negative according to the prediction.

4.1 Recall

The total sample count of positive instances in each category is used to calculate recall. Low FN and high recall levels determine an accurate identification. Its definition is;

$$Recall = \frac{TP}{TP + FN}$$

4.2 Precision

Comparing the total number of correctly classified positive samples to the total number of anticipated positive samples yields an estimate of precision. The likelihood of a favorable outcome is high and is as follows:

$$Precision = \frac{TP}{TP + FP}$$

4.3 F-measure

The F-measure is a metric that is determined by evaluating both accuracy and recall. It is a well-defined measure. The use of Harmonic Mean in the F-measure is justified due to its superior ability to handle high values. The F-measure is consistently lower than both Precision and Recall. It is defined as;

$$F - measure = \frac{2 * Recall * Precision}{Recall + Precision}$$

Table 1 Attack types in WSN

	Black hole	Flooding	Gray hole	Normal	TDMA
Black hole	0	1	1	1	1
Flooding	1	0	1	1	1
Gray hole	1	1	0	1	1
Normal	1	1	1	0	1
TDMA	1	1	1	1	0

Table 1 presents the many forms of assaults seen in the Wireless Sensor Network (WSN) dataset used in the proposed implementation.

The time required to construct the model was 0.03 seconds.

=== Evaluation of training set ===

=== Summary ===

Table 2 Evaluation of training set

Correctly Classified Instances	24	96	%
Incorrectly Classified Instances	1	4	%
Kappa statistic	0.8718		
Mean absolute error	0.0305		
Root mean squared error	0.1234		
Relative absolute error	18.315 %		
Root relative squared error	46.5242 %		
Total Number of Instances	25		

Table 2 presents the assessment measures used on the training set, indicating that 96% of occurrences were properly identified whereas 4% were classified incorrectly. The kappa statistic yielded a value of 0.8718, indicating a strong level of agreement. The MAE was 0.0305, showing the average absolute difference between expected and actual values. The square root of the mean (RMSE) of the squared discrepancies between the anticipated and actual values was 0.1234. The Relative Absolute Error (RAE) is

calculated to be 18.31%, while the Root Relative Squared Error (RRSE) is determined to be 46.52%.

Table 3 Detailed Accuracy by Class

TP Rate	FP Rate	Precision	Recall	F-Measure	ROC	Area Class
1	0.2	0.952	1	0.976	0.9	Normal
0.667	0	1	0.667	0.8	0.848	UDP-Flood
1	0	1	1	1	1	Smurf
0	0	0	0	0	0	SIDDOS
0	0	0	0	0	0	HTTP-FLOOD
0.96	0.16	0.962	0.96	0.956	0.902	

Table 3 describes the detailed accuracy determined through the experiment. The factors determining the accuracy are F – measure, Precision, ROC, Recall, TP rate, and FP rate. Each type of attack is mentioned as an area class and obtained values concerning the factors described in the above table.

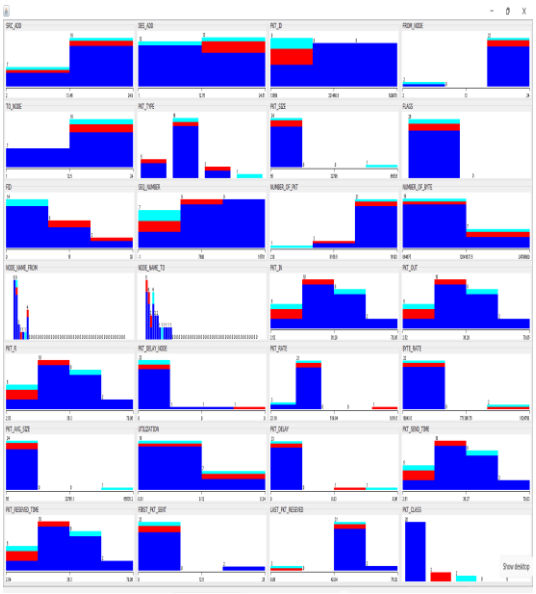

Fig. 2 Network parameters visualization

Figure 2 shows the visualization result of the parameters such as SRC_ADD, NODE_NAME_TO, PKT_SIZE, PKT_RATE, TO_NODE, FROM_NODE, SEQ_NUMBER, FLAGS, NUMBER_OF_PKT, FID, NODE_NAME_FROM, DES_ADD, PKT_IN, NUMBER_OF_BYTE, PKT_DELAY_NODE, PKT_OUT, PKT_ID, PKT_R, PKT_TYPE, PKT_RESEVED_TIME, BYTE_RATE, PKT_DELAY, UTLIZATION, FIRST_PKT_SEND, LAST_PKT_RESEVED, PKT_AVG_SIZE, PKT_SEND_TIME, PKT_CLASS.

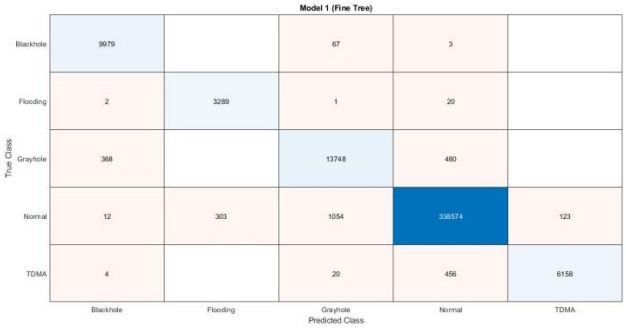

Fig. 3 Confusion matrix for the number of observations

Figure 3 shows the dataset confusion matrix. The execution uses Blackhole, floods, Grayhole, Normal, and TDMA attacks. The x-axis shows the expected class and the y-axis the actual class.

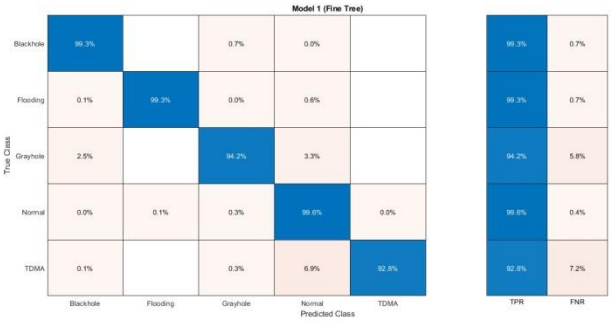

Fig. 4 Confusion matrix for TPR and FNR

Figure 4 shows the confusion matrix observations for the dataset's true positive rate (TPR) and false negative rate (FNR). The execution uses Blackhole, floods, Grayhole, Normal, and TDMA attacks. The x-axis shows the expected class and the y-axis the actual class.

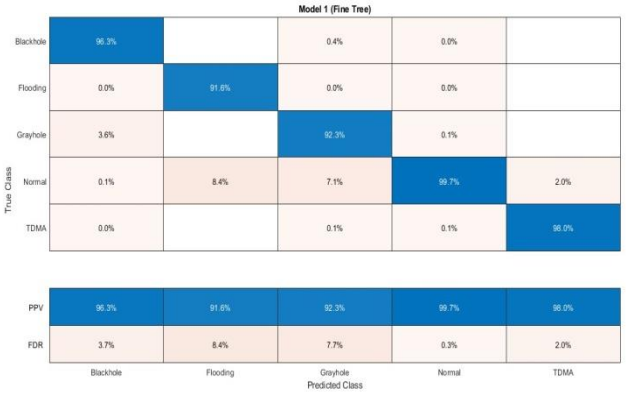

Fig. 5 Confusion matrix for PPV and FDR

Figure 5 presents the recorded observations of the confusion matrix pertaining to the positive predictive value (PPV) and false discovery rate (FDR) on the provided dataset. The execution encompasses many forms of assaults, including Blackhole, floods, Grayhole, Normal, and TDMA. The x-axis represents the anticipated class, while the y-axis represents the genuine class.

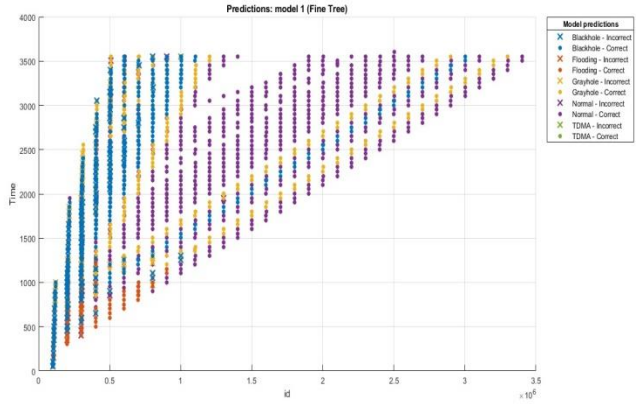

Fig. 6 Scatter plot for Node id vs. time

Figure 6 shows the scatter point observation of node ID with time. The scatter points denote the correct and incorrect attacks of Blackhole, flooding, Grayhole, Normal, and TDMA. The x-axis represents the variable of ID, while the y-axis represents the variable of time taken.

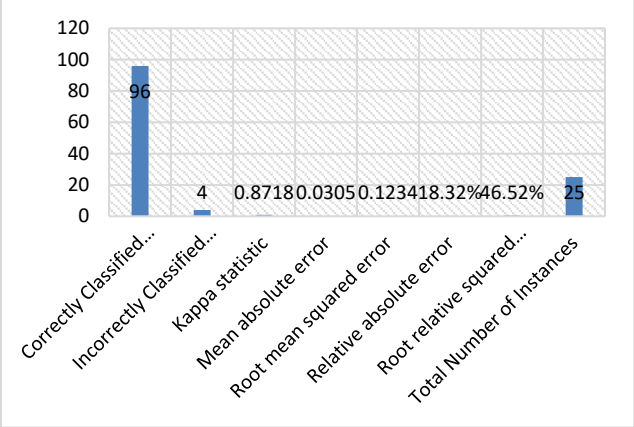

Fig. 7 Classification parameter results comparison

Figure 7 is the graphical representation of classification parameters and their obtained values, described in Table 2.

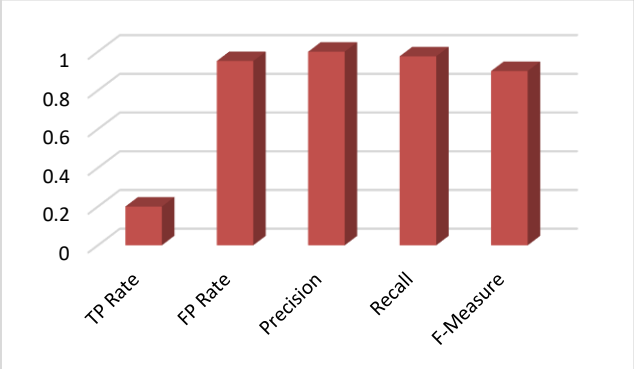

Fig. 8 classification parameter results comparison.

Figure 8 shows the comparison of classification results. The classification parameters taken for the comparison are F-measure, TP Rate, Recall, Precision, and FP Rate.

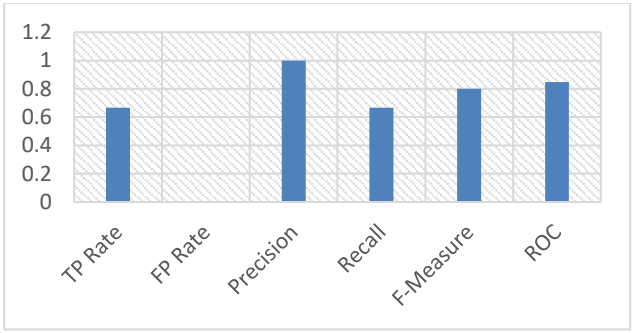

Fig. 9. Classification parameter results comparison.

Figure 9 displays the comparison of classification results. The classification parameters taken for the comparison are F-measure, TP Rate, Recall, Precision, and FP Rate.

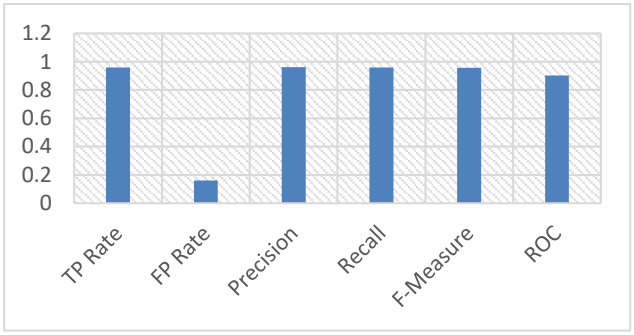

Fig. 10 classification parameter results comparison.

Figure 10 shows the comparison of classification results. The classification parameters taken for the comparison are F-measure, TP Rate, Recall, Precision, and FP Rate.

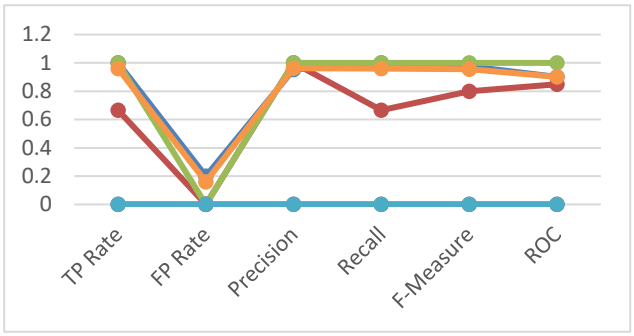

Fig. 11 classification parameter results comparison.

Figure 11 shows the comparison of classification results. The classification parameters taken for the comparison are F-measure, TP Rate, Recall, Precision, and FP Rate.

Table 12: Comparison among the classifiers

Classifiers	Achieved Accuracy level in %
Proposed Random Forest (RF)	99.53
Artificial Neural Network (ANN)	91
Deep Neural Network (DNN)	87

Table 12 displays a comparative study that was conducted to evaluate the efficacy of the proposed Random Forest (RF) in contrast to the well-established ANN [14] and DNN [16]. The suggested Random Forest (RF) model demonstrated a remarkable accuracy rate of 99.53%. In comparison, the Artificial Neural Network (ANN) earned an accuracy of 91%, while the Deep Neural Network (DNN) achieved an accuracy of 87%. The classification accuracy achieved by the suggested Random Forest (RF) model is superior than that of previous models.

5. Conclusion

In this work, we assessed the variety of network assaults, such as HTTP-FLOOD, UDP-FLOOD, SIDDOS, and Smurf, through the proposed Random Forest classifier. Data preprocessing is an essential component of the suggested methodology, as it assumes a crucial role in the preparation of raw data for model training. The process includes the cleansing, transformation, and structuring of the data. Furthermore, the random forest methodology is constructed based on an amalgamation of decision trees, which collaboratively give a conclusive prediction. The performance metrics used for evaluating the level of precision are F-measure, Precision, Receiver Operating Characteristic (ROC), Recall, True Positive (TP) rate, and False Positive (FP) rate. The results indicate that the suggested methodology has achieved a superior degree of accuracy in classifying assaults inside network traffic.

Reference:

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Computer Networks 54, no. 15 (2010): 2787-2805.

[2] Faruqui, N.; Yousuf, M.A.; Whaiduzzaman, M.; Azad, A.; Barros, A.; Moni, M.A. LungNet: A hybrid deep-CNN model for lung cancer diagnosis using CT and wearable sensor-based medical IoT data. Comput. Biol. Med. 2021, 139, 104961. [CrossRef]

[3] Wójcicki, K.; Biega ´nska, M.; Paliwoda, B.; Górna, J. Internet of Things in Industry: Research Profiling, Application, Challenges and Opportunities—A Review. Energies 2022, 15, 1806. [CrossRef]

[4] Hasan, M.K.; Akhtaruzzaman, M.; Kabir, S.R.; Gadekallu, T.R.; Islam, S.; Magalingam, P.; Hassan, R.; Alazab, M.; Alazab, M.A. Evolution of industry and blockchain era: Monitoring price hike and corruption using BIoT for smart government and industry 4.0. IEEE Trans. Ind. Inform. 2022, 18, 9153–9161. [CrossRef]

[5] Soldatos, J.; Gusmeroli, S.; Malo, P.; Di Orio, G. Internet of Things applications in future manufacturing. In Digitising the Industry Internet of Things Connecting the Physical, Digital and Virtual Worlds; River Publishers: Delft, The Netherlands, 2022; pp. 153–183.

[6] Sharma, R.; Arya, R. Security threats and measures in the Internet of Things for smart city infrastructure: A state of the art. Trans. Emerg. Telecommun. Technol. 2022, 1, e4571. [CrossRef]

[7] Balaji, R.; Deepajothi, S.; Prabaharan, G.; Daniya, T.; Karthikeyan, P.; Velliangiri, S. Survey on Intrusions Detection System using Deep learning in IoT Environment. In Proceedings of the 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 7–9 April 2022; IEEE: Manhattan, NY, USA; pp. 195–199.

[8] Alsamiri, J.; Khalid, A. Internet of Things cyber-attacks detection using machine learning. Int. J. Adv. Comput. Sci. Appl. 2019, 10, 627–634. [CrossRef]

[9] S. Ramakrishnan1 and S. Devaraju, "Attack's Feature Selection-Based Network Intrusion Detection System Using Fuzzy Control Language," Taiwan Fuzzy Systems Association and Springer-Verlag Berlin Heidelberg (2016).

[10] P. Wu, N. Moustafa, S. Yang, and H. Guo, "Densely Connected Residual Network for Attack Recognition," IEEE 19th International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom) (2020).

[11] S. Latif, Z. Idrees, Z. Zou, and J. Ahmad. Drain, "A deep random neural network model for intrusion detection in industrial IoT," International Conference on UK-China Emerging Technologies (UCET) IEEE (2020).

[12] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fogcloud architecture-driven cyber-attack detection framework for IoMT networks," Computer Communications (2021).

[13] Roopak, M.; Tian, G.Y.; Chambers, J. An intrusion detection system against DDoS attacks in IoT networks. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; IEEE: Manhattan, NY, USA; pp. 562–567.

[14] Hanif, S.; Ilyas, T.; Zeeshan, M. Intrusion detection in IoT using artificial neural networks on UNSW-15 dataset. In Proceedings of the 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT and AI (HONET-ICT), Charlotte, NC, USA, 6–9 October 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 152–156.

[15] Prathyusha, D.J.; Kannayaram, G. A Cognitive Mechanism for Mitigating DDoS Attacks Using the Artificial Immune System in a Cloud Environment. Evol. Intell. 2021, 14, 607–618. [CrossRef]

[16] Gurung, S.; Chauhan, S. A dynamic threshold-based approach for mitigating black hole attack in MANET. Wirel. Netw. 2017, 24, 2957–2971. [CrossRef]

[17] Shareena, J.; Ramdas, A. APH Intrusion detection system for IoT botnet attacks using deep learning. SN Comput. Sci. 2021, 2, 205.

[18] Alghanam, O.A.; Almobaideen, W.; Saadeh, M.; Adwan, O. An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning. Expert Syst. Appl. 2023, 213, 118745. [CrossRef]

[19] 20. Syed, N.F.; Ge, M.; Baig, Z. Fog-cloud based intrusion detection system using Recurrent Neural Networks and feature selection for IoT networks. Comput. Netw. 2023, 225, 109662. [CrossRef]

[20] Le, T.T.; Kim, H.; Kang, H.; Kim, H. Classification and explanation for intrusion detection system based on ensemble trees and SHAP method. Sensors 2022, 22, 1154. [CrossRef]

[21] Hemanand, D., Reddy, G. ., Babu, S. S. ., Balmuri, K. R. ., Chitra, T., & Gopalakrishnan, S. (2022). An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs). International Journal of Intelligent Systems and Applications in Engineering, 10(3), 285–293.

[22] P. Satyanarayana, U. D. Yalavarthi, Y. S. S. Sriramam, M. Arun, V. G. Krishnan and S. Gopalakrishnan, "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR)Algorithm to Improve Network Lifetime in WSN's," 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6,

[23] Yaseen, M., Hayder Sabah Salih, Mohammad Aljanabi, Ahmed Hussein Ali, & Saad Abas Abed. (2023). Improving Process Efficiency in Iraqi universities: a proposed management information system. Iraqi Journal For Computer Science and Mathematics, 4(1), 211–219. https://doi.org/10.52866/ijcsm.2023.01.01.0020

[24] Aljanabi, M. ., & Sahar Yousif Mohammed. (2023). Metaverse: open possibilities. Iraqi Journal For Computer Science and Mathematics, 4(3), 79–86. https://doi.org/10.52866/ijcsm.2023.02.03.007

[25] Atheel Sabih Shaker, Omar F. Youssif, Mohammad Aljanabi, ABBOOD, Z., & Mahdi S. Mahdi. (2023). SEEK Mobility Adaptive Protocol Destination Seeker Media Access Control Protocol for Mobile WSNs. Iraqi Journal For Computer Science and Mathematics, 4(1), 130–145. https://doi.org/10.52866/ijcsm.2023.01.01.0011

[26] Hayder Sabah Salih, Mohanad Ghazi, & Aljanabi, M. . (2023). Implementing an Automated Inventory Management System for Small and Medium-sized Enterprises. Iraqi Journal For Computer Science and Mathematics, 4(2), 238–244. https://doi.org/10.52866/ijcsm.2023.02.02.021

[27] Perumal, G., Subburayalu, G., Abbas, Q., Naqi, S. M., & Qureshi, I. (2023). VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions. Systems, 11(8), 436. MDPI AG. Retrieved from http://dx.doi.org/10.3390/systems11080436

[28] Satyanarayana, P., Diwakar, G., Subbayamma, B. V., Phani Sai Kumar, N. V., Arun, M., & Gopalakrishnan, S. (2023). Comparative analysis of new meta-heuristic-variants for privacy preservation in wireless mobile adhoc networks for IoT applications. Computer Communications, 198, 262–281. https://doi.org/10.1016/j.comcom.2022.12.006

[29] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2023) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, 18:3, 402-420, DOI: 10.1080/19361610.2021.2002118

[30] Yadav, R. ., & Singh, R. . (2023). A Hyper-parameter Tuning based Novel Model for Prediction of Software Maintainability. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 106–113. https://doi.org/10.17762/ijritcc.v11i2.6134

[31] Hiroshi Yamamoto, An Ensemble Learning Approach for Credit Risk Assessment in Banking , Machine Learning Applications Conference Proceedings, Vol 1 2021.

[32] Anand, R., Ahamad, S., Veeraiah, V., Janardan, S.K., Dhabliya, D., Sindhwani, N., Gupta, A. Optimizing 6G wireless network security for effective communication (2023) Innovative Smart Materials Used in Wireless Communication Technology, pp. 1-20.