iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77454

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 II Feb 2026- Available at www.ijraset.com

Ensemble Machine Learning Models for Real-Time Intrusion Detection in Heterogeneous IoT Environments

Jaswanth Syam Sundar Garugu

Abstract: ***The high rate of IoT devices proliferation has considerably augmented the attack space of the current networks, making effective intrusion detection critical in supporting the security and reliability of the Internet of Things environment. Complex and diverse attack patterns in real time cannot easily be detected with the standard security measures, so clever detecting methods are required. A complete analysis of the network traffic using 80 extracted features was performed using the RT-IoT2022 dataset which contained both the normal and malicious network activity of devices such as ThingSpeak-LED, Wipro-Bulb and MQTT-Temp as well as the simulated attacks of Brute-force SSH, DDoS and Nmap scan. ML classifiers such as KNN, Gradient Boosting, XGBoost, SVM, RF, DT and Extremely randomized Trees were used to identify bad behavior. In accuracy, precision, recall, and F1-score, we found that RF and Extremely Randomized Trees worked better than the rest with a 99.9% score on all the scores. Such an approach demonstrates that the level of accuracy in determining intrusions in complex IoT networks can be extremely high and real-time. It is an important milestone towards a proactive mitigation of threats and intelligent implementation of network security.***

"Index Terms: Accuracy, Internet of Things (IoT), intrusion detection systems (IDS), machine learning classifiers."

I. INTRODUCTION

The IoT is the next upscale of the internet, which links physical objects to sensing, communication and computing services to enable it to be feasible that smart cities, healthcare, industrial processes and home management can all cooperate without issues [1]. This unified ecosystem relies on an architecture of multiple levels, which comprises perceptual, network, and application levels. A combination of these layers allows one to gather, transmit, and distribute data and services [2]. The rapid introduction of the IoT has simplified the operations significantly, making them much more convenient, but has also increased the digital attack surface greatly. Security and privacy problems have become complex due to emergence of devices with restricted resources and limited processing capabilities with poor authentication mechanisms [3]. Consequently, securing Internet of Things systems has emerged as a priority at the global level. Cybercriminals are also coming after these systems exploiting vulnerability on any level of architecture.

Although the importance of IoT is increasing in critical fields, the aspect of ensuring the safety of the IoT environments remains an issue which has not been addressed. Security vulnerabilities are categorized differently and each layer of the IoT architecture is susceptible to them such as eavesdropping, spoofing, denial-of-service, and malware propagation [4]. According to recent research, there has been a sharp rise in cyberattacks connected to the IoT, which has impacted millions of devices globally and cost economies billions of dollars in various industries [5]. Not only do these threats jeopardize the integrity of the system, but also the privacy of users, confidentiality of their data, and the reliability of the services are jeopardized [6]. IDS that are traditional have been employed to monitor and identify oddities occurring on networks. However, conventional techniques that are based on pre-determined signatures do not detect new or more advanced attacks with ease [7]. There are also high false positive rates and lack of scalability that makes it difficult to implement such systems in very dynamic and diverse IoT networks [8]. Thus, a considerable gap exists in the research on the development of adaptive and efficient intrusion detection mechanisms tailored to the complexity of the nature of the IoT ecosystems. The present work is aimed to address these issues by performing an in-depth evaluation of intelligent intrusion detection algorithms that were developed in the context of IoT. This research paper aims at assessing the data-driven methods, which are capable of detecting anomalous network traffic and distinguishing between normal and suspicious network activities [9]. The aim of the work is to build a comparative idea of various learning paradigms by applying large datasets of IoT traffic to identify the capability of these paradigms to enhance intrusion detection accuracy and maintain computational efficiency. In addition, the experimental methodology used in this trial will ensure reproducibility and transparency, which will enhance additional development of the research of IoT cybersecurity.

©IJRASET: All Rights are Reserved

The results of this study make the IoT systems more resilient to emerging threats of cyberattacks. The article provides empirical evidence of the effectiveness of smart intrusion detecting strategies, therefore, contributing to the development of proactive defense strategies that can be implemented into real IoT infrastructure [10]. The findings can have implications on designing secure IoT systems capable of supporting massive deployments at minimal security vulnerabilities. Finally, this publication seeks to influence future developments in smart cybersecurity systems that promote trustworthy, dependable, and privacy-sensitive IoT systems in different fields of applications.

II. LITERATURE REVIEW

The recent advancements in ML have contributed greatly to the development of intelligent IDS capable of making networks safer in the IoT environments. Several researches have investigated different ML strategies to improve the accuracy and customizability of intrusion detection systems models. Dina and Manivannan [11] examined the possibility of using ML in the detection of intrusions on normal computer networks. They emphasized that signature-based attacks are not as effective in detecting attacks that have never been seen previously as data-driven models. They limited their research to the classic network designs and did not measure performance in a resource-constrained IoT setting whose dynamic traffic patterns offer additional challenges. A comprehensive research on various ML algorithms of IDS was also conducted by Saranya et al. [12], in terms of the accuracy of classification of their data, and the speed at which they could perform it. Their exploration gave a useful insight into the operation of algorithms but failed to examine the manner in which they respond to changes in real-time and how energy-efficient they can be which are highly significant in terms of the IoT-based applications.

The recent years have seen an increase in the popularity of using a IoT-specific dataset in the IDS research. The RT-IoT2022 dataset was published by Nagapadma [13], and it is a free benchmark that facilitates easy conducting reproducible tests on IoT threat detection. Such data set can enable standardized assessment of all studies but it is not investigated sufficiently in comparative studies based on ML. Similarly, Inuwa and Das [14] conducted a comparative study of anomaly detection strategies in the IoT networks and demonstrated that hybrid models that combine the use of statistical and ML methods enhance the effectiveness of detection. Nevertheless, they indicated that the trade-off between model complexity and processing cost existed, and it was difficult to scale up in large installations of IoT. Bacha et al. [15] addressed this limitation by proposing an anomaly-based IDS that employed extreme ML based on kernel. This system could locate problems more precisely and using less time. Most of the performance of the model was tested using small-scale data which casts doubts on its resilience in the real-world IoT environments.

There have been efforts to develop hybrid and intelligent IDS structures in the IoT applications that are specific to a field. HIIDS described by Saif et al. [16] is an IoT-based healthcare system intrusion detector that is a hybrid system, based on machine learning and metaheuristic algorithms to detect complex patterns of assaults in the system. The system was highly flexible and precise, yet it required a tremendous amount of computing capabilities, which are not suitable with tiny IoT gadgets. Ahmad et al. [17] researched intrusion detection using the supervised ML model and features of applications and transport layer using the UNSW-NB15 dataset. The accuracy of their research was substantial but they revealed limitations on cross-layer generalization and model scalability within the environment of various IoT systems.

Recent research has also improved the performance of the IDS by addressing the issue of the imbalance of data and augmenting the generalization of the model. Talukder et al. [18] introduced the MLSTL-WSN, which is a ML-based intrusion detection system based on SMOTETomek wireless sensor networks, which reduced false positives by a significant margin and increased the detection rates. However, it was a technique designed to support traffic patterns that are specific to the WSNs, rather than the IoT systems, in general. Saran and Kesswani [19] reviewed supervised ML classifiers to intrusion detection in the IoT. They discovered that decision tree models performed well and could overfit when trained on a small size of data. Awajan [20] proposed a DL based IDS of the IoT networks, which was very successful in detecting but not very easy to comprehend and expensive to operate.

III. MATERIALS AND METHODS

The proposed solution aims to build a robust framework of intrusion detection of IoT networks through the use of ML techniques that should accurately identify malicious activity in real-time. Network traffic and system logs of IoT devices such as ThingSpeak-LED, Wipro-Bulb and MQTT-Temp are available in the RT-IoT2022 dataset. It further has a total of nine attack scenarios including DDoS, Brute-force SSH and Nmap scans. The system represents bidirectional network properties assimilated through Zeek and Flowmeter which have 80 attributes in each session. It can be described as the workflow involving preprocessing of the received traffic, features extraction, and training of a few classifiers, including KNN, Gradient Boosting, XGBoost, SVM, DT, RF and Extremely Randomized Trees.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

In order to determine the optimal detection model, we test it with accuracy, precision, recall, and F1-score determinants. This is aimed at producing an extremely accurate intrusion detection system, where the detection rates of RF and Extremely Randomized Trees are near perfect. This will render the IoT infrastructures more resistant and secure to advanced cyberattacks.

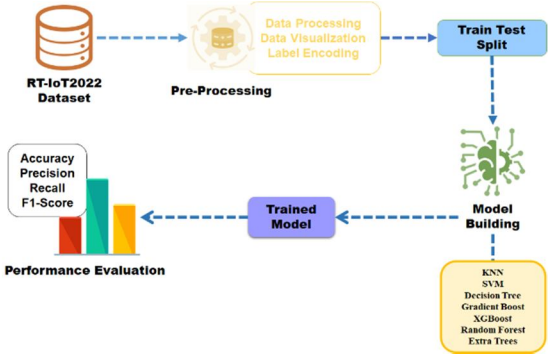


Fig.1 Proposed Architecture

The overall design of the IoT-based intrusion detection system is demonstrated in Figure 1. The first in the process is the RT-IoT2022 dataset. It has marked normal and attack network traffic. Pre-processing entails data cleansing, visualization and coding of the labels to convert the raw traffic into a format that is analyzable. The dataset is then divided into training and testing to allow performance to be measured without bias. ML classifiers We train and test a few ML classifiers. The trained models are then tested to determine how they are able to find things.

A. Dataset Collection

The study uses the RT-IoT2022 dataset that was downloaded in the Kaggle repository. It is a total standard of intrusion detecting in IoT. The collection contains 123,117 records of network traffic, and all of them consist of 85 features demonstrating various statistical, flow-based, and temporal characteristics of IoT communications. There are numerous variations of its forms of attack such as [24] DoS, DDoS, ARP poisoning, and scanning processes, and these are all processes that occur on real networks. The dataset is ideal in testing ML models that can identify complex IoT incursions as it contains a combination of various types of data, a balanced form, and bad and good traffic.

	no	id.orig_p	id.resp_p	proto	service	flow_duration	fwd_pkts_tot	bwd_pkts_tot	fwd_data_pkts_tot	bwd_data_pkts_tot	...	active.std	idle.min
0	0	38667	1883	tcp	mqtt	32.011598	9	5	3	3	...	0.0	2.972918e+07
1	1	51143	1883	tcp	mqtt	31.883584	9	5	3	3	...	0.0	2.985528e+07
2	2	44761	1883	tcp	mqtt	32.124053	9	5	3	3	...	0.0	2.984215e+07
3	3	60893	1883	tcp	mqtt	31.961063	9	5	3	3	...	0.0	2.991377e+07
4	4	51087	1883	tcp	mqtt	31.902362	9	5	3	3	...	0.0	2.981470e+07

5 rows × 85 columns

Fig.2 RT-IoT2022 Dataset

B. Pre-Processing

The preprocessing stage prepares the RT-IoT2022 dataset to be powerfully investigated using strong intrusion detection techniques through data cleaning, visualization, scale, data identification of valuable characteristics, class balance, and data partitioning. This ensures that the model training is correct and reliable.

1) *Data Cleaning:* The cleaning of the dataset was quite high, and the missing or no value found and eliminated, and the duplication of the records was eliminated to ensure that the data was precise. The step is significant because it eliminates inconsistency and duplication that may render training and testing the model inaccurate. Ensuring that the data is clean, unique, causes the learning process to be more credible and reduces noise and makes the intrusion detection system more resilient and capable of generalization.
2) *Exploratory Data Visualization:* A visualization procedure was carried out to examine the manner in which the various categories of attacks were distributed within the data. It was easy since large imbalances of classes would be noticed using bar charts to demonstrate the frequency of each class. This will be highly significant in determining the data characteristics that will be used in resampling or balancing activities, feature selection and model building. The visualization provides you with a glance of the patterns and situations that the data can have.

3) *Feature Scaling:* The whole numerical data were put into the same scale to ensure they had the same ranges. This ensures that models that are sensitive to feature magnitude such as distance-based or gradient-based models are also treated equally as all input variables. Standardization assists in models coming together, rendering them more precise as well as preventing the features of big numbers to exert excessively big influence on the learning process. This is what results in predictability and stability of model performance.

C. Training and Testing

To simplify the testing of the model, the selected feature dataset of balanced and selected data were divided into training and testing sets. To train the models, an 80-20 split was used to sample the data to a representative portion. One more section was reserved to perform a neutral testing. This is required to ensure that the model is applicable in other contexts, preventing it to overfit, and giving a realistic depiction of the ability of the intrusion detection system to predict an aspect in the real world.

D. Algorithms

1) K-Nearest Neighbors (KNN): KNN is a supervised learning method that does not make use of parameters. It predicts what will occur by using the distance between instances. [25]. It considers the closest similar points around based on a distance measure in order to make a prediction on what class a piece of data falls under hence simplifying the process of making a decision. KNN is able to better assist the system in that it can accommodate irregular decision boundaries and patterns of data with minimal training demands of its own. It particularly works well at identifying unusual objects in feature spaces that are hard to understand, as it is simple and understandable.

$$distance(x, X_i) = \sqrt{\sum_{j=1}^{d} \left(x_j - X_{i_j}\right)^2} \quad (1)$$

2) Support Vector Machine (SVM): SVM is a controlled instructional approach which applies an optimal hyperplane to assign classes by maximizing the separation between information. It is applicable to high-dimensional high-dimensional linearly non-separable feature spaces, thus it is useful with non-separable problems of complicated classification. [26]. SVM is useful in terms of robustness and generalization because it minimizes the amount of erroneous classification and achieves high accuracy of the prediction. It operates by mapping features into a high dimensional space and discovering boundaries that are a clear separation between instances. This ensures that trends can be accurately discovered in various datasets.

$$minimize\ \frac{1}{2}\ ||W||^2 + C\sum_{i=1}^{n} \xi_i \quad (2)$$

3) Decision Tree: DT, a supervised learning model, is a model that repeatedly splits data according to the values of features forming a tree structure with decision nodes and decision leaves which display the results. Its method considers features individually and selects those features that best divide the data to render it less uncertain. The decision logic of decision trees has the advantage of being easier to understand the importance of various features as they are hierarchically determined. [27]. They are useful in accuracy and efficiency when classifying characteristics by systematically modeling correlations between these characteristics. That makes them useful in searching patterns and anomalies that do not require a great deal of preprocessing.

$$I\ (i) = 1 - \sum_{i=1}^{k} p_i^2 \quad (3)$$

4) Gradient Boosting: Gradient Boosting is a learning technique that involves a combination of many models. New models correct the errors of the previous ones. It enhances the accuracy of prediction because it tends to reduce the error on the basis of the gradient and thus it is possible to model complex and non-linear relationships between features. Gradient Boosting is able to achieve classification that is more accurate, stronger and general by combining a large number of weak learners into a strong predictor. The advantages of its structured sequential learning methodology are that it effectively balances and removes noise on data, and can find subtle patterns in heterogeneous or high dimensional data.

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x) \quad (4)$$

5) XGBoost: XGBoost is a quick gradient boosting framework which establishes a collection of decision trees with the help of a regularised objective function to prevent excessively overfitting them. Its algorithm is to train trees sequentially, correct the errors of the last tree and increase the performance that it predicts. [29]. XGBoost is more efficient, accurate and scalable because it can work with large and high-dimensional data and compute in parallel. It is also quite resistant to missing values and feature interactions so the model is more versatile and reliable. This has given it a particular advantage when performing real time classification tasks that require rapid and accurate predictions in high dimensional feature spaces.

$$\hat{y}_i = \sigma\left(\sum_{k=1}^{K} f_k(x_i)\right), f_k \in F \quad (5)$$

6) Random Forest: RF, is an ensemble method of learning which constructs numerous decision trees and then pools the prediction of the decision trees to produce a classification relying on the majority of votes. It has a methodology that involves training various trees with random feature subsets then combining the results to reduce variance and overfitting. [30]. RF enhances accuracy, strength, and generalization through the combination of the decision-making. This renders predictions to be stable and consistent in datasets that are not the same. It is capable of characterizing complex interactions, and operating with a wide variety of features, and hence is effective at classification tasks, and yet remains easy to comprehend and can process high-dimensional or noisy data.

$$Gini = 1 - \sum_{i=1}^{C} (Pi)^2 \quad (6)$$

7) Extra Trees (Extremely Randomized Trees): Extra Trees is a related ensemble learning algorithm which is similar to the RF except that it selects the split thresholds randomly. Its strategy constructs numerous random decision trees and uses their outputs to create a more general model to decrease variance. Extra Trees enhances faster speed, stability and performance by mitigating overfitting and high-dimensional data. Its randomizing system is such that it makes quick predictions and is yet precise. It is good in scenarios where real-time detection and practical classification over a wide range of feature space are required.

IV. EXPERIMENTAL RESULTS

1) Accuracy: The accuracy of the test is the capacity of the test in distinguishing between people who are sick and those who are healthy. We would determine the accuracy of a test by computing the number of the cases we considered that were true positives and true negatives. This is mathematically expressed and is:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} (7)$$

2) Precision: Precision is a measure that determines the ratio between the number of correctly classified cases or samples and the number of those that are declared positives. Therefore, the formula of determining the accuracy is:

$$Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} (8)$$

3) Recall: Recall is used in machine learning to determine how the model identifies all the instances of a particular class that matter. The proportion of the accurately estimated positive observations to the number of actual positives demonstrates the extent of a model that captures all the cases of a particular category.

$$Recall = \frac{TP}{TP + FN} (9)$$

4) F1-Score: F1 score is a metric that can be used to measure the effectiveness of a machine learning model. It combines the model precision and recall. Measure of accuracy indicates the number of times that a model made a valid guess on the entire dataset.

$$F1\ Score = 2 * \frac{Recall\ X\ Precision}{Recall + Precision} * 100 \quad (10)$$

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Table.1 Performance Evaluation Table

ML Model	Accuracy	Precision	Recall	F1-Score
KNN	0.996	0.996	0.996	0.996
SVM	0.974	0.978	0.974	0.973
Decision Tree	0.998	0.998	0.998	0.998
Gradient Boost	0.993	0.993	0.993	0.993
XGBoost	0.998	0.998	0.998	0.998
Random Forest	0.999	0.999	0.999	0.999
ExtraTrees	0.999	0.999	0.999	0.999

Table 1 shows that the machine learning models that are most accurate are the Random Forest and the Extra Trees.

Fig.3 Comparison Graph

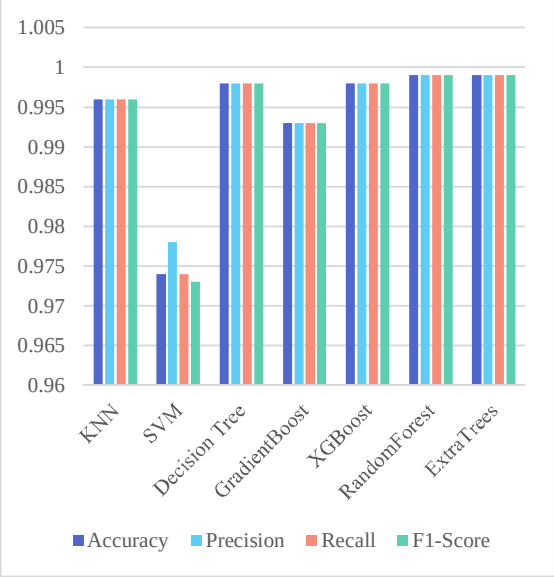


Figure 3 indicates that the best algorithm is the Random Forest. It is clear that there are differences in the metrics the accuracy is presented in purple, precision in blue, recall in orange and F1-score in green.

V. CONCLUSION

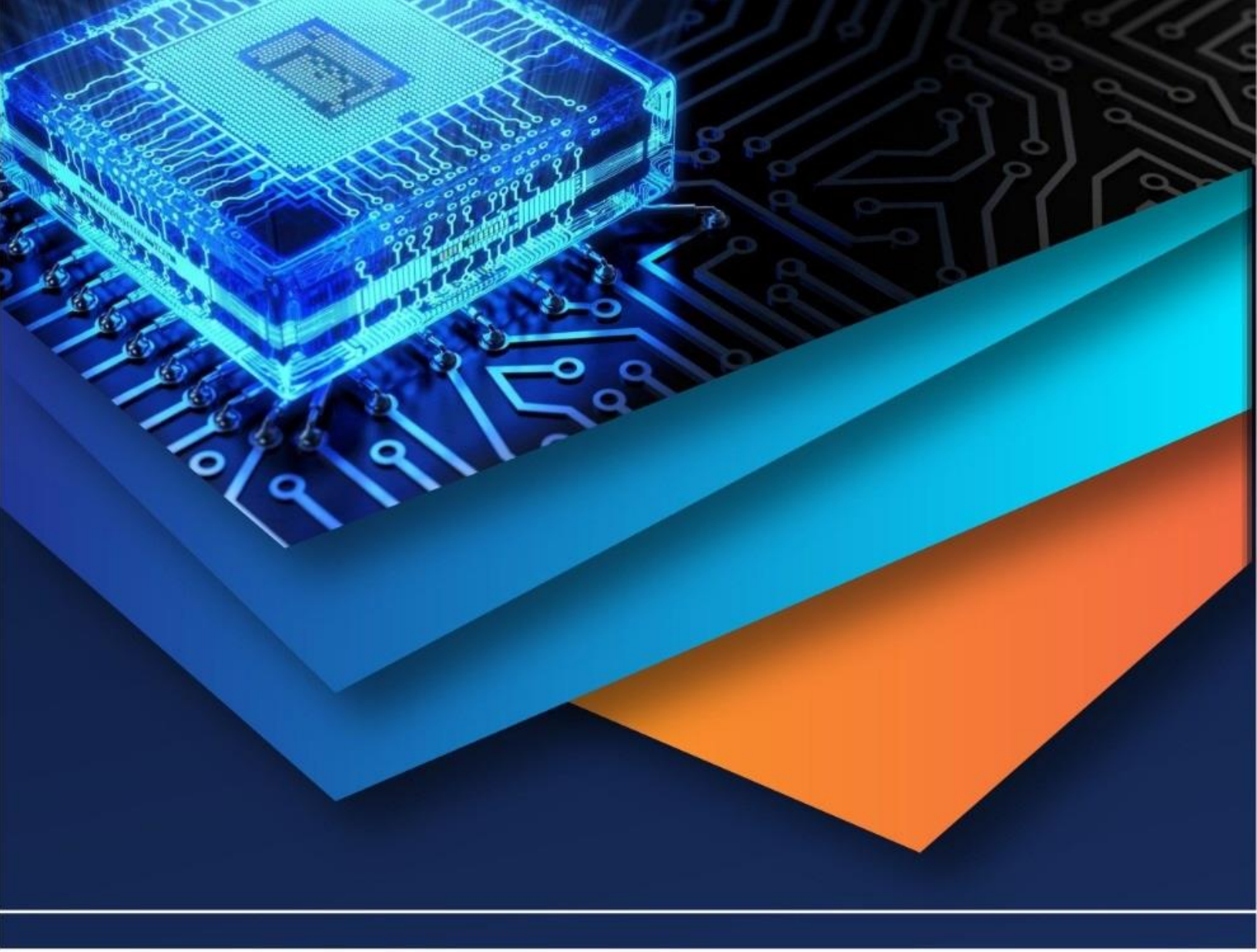
In large-scale IoT networks, advanced cyberattacks are difficult to identify and prevent, and therefore, these networks need to be secured to protect their networks and ensure a smooth operation. Intelligent intrusion detection framework was developed using RT-IoT2022 dataset. This data contains realistic normal traffic of devices such as ThingSpeak-LED, Wipro-Bulb, MQTT-Temp, and adversarial traffic such as Brute-force SSH, DDoS and several scans using Nmap with 80 features extracted network traffic each. We used KNN, Gradient Boosting, XGBoost, SVM, DT, RF and Extremely Randomized Trees in finding the best classifier to identify IoT threats. RF and Extremely Randomized Trees were the strongest and most generalizable and had an accuracy, precision, recall, and F1-score of 99.9%. These findings indicate that ensemble learning is a strong and consistent method of categorizing complex IoT traffic. The developed intrusion detection system is a stable and scalable security system that can automatically identify threats and enhance real-time decision-making process to a strong, robust IoT network infrastructures.

The future development can focus on the application of deep learning models, such as LSTM and Transformer-based models, to enhance the detection of temporal attacks in dynamic IoT traffic.

The inclusion of XAI practices would make the automated decision more comprehensible and credible. Real-time detection can be done with less lag time using lightweight edge-computing frameworks to be deployed. In addition, the presence of testing under various conditions of IoT uses and zero-day attacks would also render large-scale, real-life network structures more flexible, scalable, and robust.

REFERENCES

[1] Benamor, Z., Seghir, Z. A., Djezzar, M., & Hemam, M. (2023). A comparative study of machine learning algorithms for intrusion detection in IoT networks. Revue d'Intelligence Artificielle, 37(3), 567-576.
[2] Almotairi, A., Atawneh, S., Khashan, O. A., & Khafajah, N. M. (2024). Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. Systems Science & Control Engineering, 12(1), 2321381.
[3] Kaddour, H., Das, S., Bajgai, R., Sanchez, A., Sanchez, J., Chiu, S. C., ... & Fouda, M. M. (2024, April). Evaluating the performance of machine learning-based classification models for iot intrusion detection. In 2024 IEEE Opportunity Research Scholars Symposium (ORSS) (pp. 84-87). IEEE.
[4] Amouri, A., Al Rahhal, M. M., Bazi, Y., Butun, I., & Mahgoub, I. (2024, October). Enhancing Intrusion Detection in IoT Environments: An Advanced Ensemble Approach Using Kolmogorov-Arnold Networks. In 2024 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.
[5] Sharma, S. B., & Bairwa, A. K. (2025). Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study. IEEE Access.
[6] J.Fox,TopCybersecurityStatistics for 2024. USA: Cobalt, 2023. [Online]. Available: https://www.cobalt.io/blog/cybersecurity-statistics-2024
[7] A. Marton and S. Systems, IoT Malware Attacks up by 37% in the First Half of 2023. IoTAC Association: EU Research and Innovation Programme, 2023.
[8] S. M. Muzammal, R. K. Murugesan, and N. Z. Jhanjhi, ‘‘A comprehen sive review on secure routing in Internet of Things: Mitigation methods and trust-based approaches,’’ IEEE Internet Things J., vol. 8, no. 6, pp. 4186–4210, Mar. 2021.
[9] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, ‘‘Realizing an Internet of Secure Things: A survey on issues and enabling technologies,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1372–1391, 2nd Quart., 2020.
[10] O. H. Abdulganiyu, T. A. Tchakoucht, and Y. K. Saheed, ‘‘A systematic literature review for network intrusion detection system (IDS),’’ Int. J. Inf. Secur., vol. 22, no. 5, pp. 1125–1162, Oct. 2023.
[11] A. S. Dina and D. Manivannan, ‘‘Intrusion detection based on machine learning techniques in computer networks,’’ Internet Things, vol. 16, Dec. 2021, Art. no. 100462.
[12] T.Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, ‘‘Per formance analysis of machine learning algorithms in intrusion detection system:Areview,’’Proc.Comput.Sci.,vol.171,pp. 1251–1260,Jan.2020.
[13] B.S.A.R.Nagapadma,RT-IoT20222024:UCIMachineLearningRepos itory, USA, 2024.
[14] M. M. Inuwa and R. Das, ‘‘A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks,’’ Internet Things, vol. 26, Jul. 2024, Art. no. 101162.
[15] S. Bacha, A. Aljuhani, K. B. Abdellafou, O. Taouali, N. Liouane, and M. Alazab, ‘‘Anomaly-based intrusion detection system in IoT using ker nel extreme learning machine,’’ J. Ambient Intell. Humanized Comput., vol. 15, no. 1, pp. 231–242, Jan. 2024.
[16] S. Saif et al., ‘‘HIIDS: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in IoT based healthcare,’’ Microprocess. Microsyst., 2022, Art. no. 104622.
[17] M. Ahmad, Q. Riaz, M. Zeeshan, H. Tahir, S. A. Haider, and M. S. Khan, ‘‘Intrusion detection in Internet of Things using supervised machine learn ing based on application and transport layer features using UNSW-NB15 data-set,’’ EURASIPJ.WirelessCommun.Netw.,vol.2021,no.1,pp. 1–23, Dec. 2021.
[18] M. A. Talukder, S. Sharmin, M. A. Uddin, M. M. Islam, and S. Aryal, ‘‘MLSTL-WSN: Machine learning-based intrusion detection using SMOTETomek in WSNs,’’ Int. J. Inf. Secur., vol. 23, no. 3, pp. 2139–2158, Jun. 2024.
[19] N. Saran and N. Kesswani, ‘‘A comparative study of supervised machine learning classifiers for intrusion detection in Internet of Things,’’ Proc. Comput. Sci., vol. 218, pp. 2049–2057, Jan. 2023.
[20] A. Awajan, ‘‘A novel deep learning-based intrusion detection system for IoT networks,’’ Computers, vol. 12, no. 2, p. 34, Feb. 2023.
[21] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, ‘‘Intrusion detection system using feature extraction with machine learn ing algorithms in IoT,’’ J. Sensor Actuator Netw., vol. 12, no. 2, p. 29, Mar. 2023.
[22] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, ‘‘Anomaly-based intrusion detection system for IoT application,’’ Discover Internet Things, vol. 3, no. 1, p. 5, May 2023.
[23] B. S. Sharmila and R. Nagapadma, ‘‘Quantized autoencoder (QAE) intru sion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset,’’ Cybersecurity, vol. 6, no. 1, p. 41, Sep. 2023.
[24] T. S. Othman, K. R. Koy, and S. M. Abdullah, ‘‘Intrusion detection systems for IoT attack detection and identification using intelligent techniques,’’ Networks, vol. 5, p. 6, Jan. 2023.
[25] S. Yaras and M. Dener, ‘‘IoT-based intrusion detection system using new hybrid deep learning algorithm,’’ Electronics, vol. 13, no. 6, p. 1053, Mar. 2024.
[26] H. Nandanwar and R. Katarya, ‘‘Deep learning enabled intrusion detec tion system for industrial IoT environment,’’ Exp. Syst. Appl., vol. 249, Sep. 2024, Art. no. 123808.
[27] N. Islam, F. Farhin, I. Sultana, M. Shamim Kaiser, M. Sazzadur Rahman, M. Mahmud, A. S. M. Sanwar Hosen, and G. Hwan Cho, ‘‘Towards machine learning based intrusion detection in IoT networks,’’ Comput., Mater. Continua, vol. 69, no. 2, pp. 1801–1821, 2021.
[28] V.Choudhary, S. Tanwar, T. Choudhury, and K. Kotecha, ‘‘Towards secure IoT networks: A comprehensive study of metaheuristic algorithms in conjunction with CNN using a self-generated dataset,’’ MethodsX, vol. 12, Jun. 2024, Art. no. 102747.
[29] V. Choudhary et al., ‘‘Towards secure IoT networks: A comprehensive study of metaheuristic algorithms in conjunction with CNN using a self generated dataset,’’ MethodsX, vol. 12, 2024, Art. no. 102747.
[30] A. R. Gad, A. A. Nashat, and T. M. Barkat, ‘‘Intrusion detection system using machine learning for vehicular ad hoc networks based on ToN-IoT dataset,’’ IEEE Access, vol. 9, pp. 142206–142217, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)