JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-19, No.-8, August (2024) pp 191-206 ISSN (Print) 0973-8975

AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS

Sadia Saif[1], Hamayun Khan[2], Arshad Ali[3], Sami Albouq[4], Muhammad Zunnurain Hussain[5], Muhammad Zulkifl Hasan[6] Irfan Uddin [7], Shahab Khan[8], Mohammad Husain[9]

[1,2,7]Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan.

[3,4,9]Faculty of Computer and Information Systems, Islamic University of Madinah, Al Madinah Al Munawarah, 42351, Saudi Arabia.

[5]Department of Computer Science, Bahria University Lahore Campus, Lahore, 54000, Pakistan.

[6]Faculty of Information Technology, Department of Computer Science
University of Central Punjab, Lahore, 54000, Pakistan.

[8]Department of Chemistry, University of Malakand, Chakadara, Dir Lower, Malakand, 18800, Pakistan.

Email: [1]sadiasaif.official01@gmail.com, [2]hamayun.khan@superior.edu.pk, [3]a.ali@iu.edu.sa, [4]salbouq1@iu.edu.sa, [5]Zunnurain.bulc@bahria.edu.pk, [6]zulkifl.hasan@ucp.edu.pk,[7]irfan@superior.edu.pk, [8]shahabkhan262@gmail.com, [9]dr.husain@iu.edu.sa

Corresponding Author: **Sadia Saif**

https://doi.org/10.26782/jmcms.2024.00.00014

(Received: June 10, 2024; Revised: July 27, 2024; Accepted: August 10, 2024)

Abstract

The dangers that Internet of Things (IoT) devices pose to large corporate corporations and smart districts have been dissected by several academics. Given the ubiquitous use of IoT and its unique characteristics, such as mobility and normalization restrictions, intelligent frameworks that can independently detect suspicious activity in privately linked IoT devices are crucial. The IoTs have led an explosion in traffic through the network, bringing information processing techniques for attack detection. The increase in traffic poses challenges in detecting attacks and differentiating traffic that is harmful. In this work, we have proposed a mechanism that uses the standard algorithms in a system that is designed to detect, track, measure and identify online traffic from organizations with malignant transmission: Random Forest (RF), gradient-boosted decision trees (GBDT), and support vector *machines (SVM) gives an optimal accuracy of 80.34%,87.5%, and 88.6% while the random forest-based supervised approach is 5.5% better than the previous techniques. To facilitate comparisons between training time, prediction time, specificity, and accuracy, the proposed approach leverages the NSL KDD dataset accuracy.*

Keywords: NSL-KDD dataset distribution, IoT Security, Fog Computing, Deep Learning, Random Forest (RF) machine learning.

I. Introduction

The Internet of Things (IoT) has revolutionized technology by connecting smart devices, offering remarkable opportunities but also presenting complex security challenges. Cybersecurity is now a critical focus, especially for intrusion detection systems (IDS)[I]. Intrusion detection systems (IDS) analyze network data traffic patterns to mitigate these threats. However, processing raw data within IDS is computationally demanding carefully [II]. Data generated by IoT devices typically reside in the Cloud Computing (CC) ecosystem, which is characterized by robust processors and abundant memory. Pair with progressions in IoT innovation, the cloud layer has developed quickly. To address the challenges posed by IoT organizations, the concept of haze to things arises. Intrusion datasets are essential for identifying, validating, and testing effective detection methods [III, IV].

Devices can process a lot of data locally in the fog layer before sending important data to the cloud layer. Power consumption, bandwidth requirements, network congestion, and data storage and communication issues are all minimized with this strategy. In addition, the design of mist-to-things aims to facilitate information handling close to endpoints and provide swift responses to metropolitan IoT applications. In terms of going after location, the mist-to-things layer provides two significant advantages [V, VI].

Offers a detailed description of deep learning models and their mathematical foundations commonly utilized in cybersecurity using ML. To begin with, when organization assaults are identified at this layer, both organization heads and web access suppliers can go to precautionary lengths to restrict the potential for boundless harm. Second, these tactics don't interfere with people's smooth daily lives [VII].

Utilizing the similarity between fog-to-things connections and conventional IoT devices, the model examines web traffic that moves through each fog-to-things node. This vicinity empowers more effective recognizable proof of organization assaults at the haze-to-things layer contrasted with the cloud layer [VIII].

Fog computing is an architectural model for distributed computing characterized by constrained resources, notably in terms of storage and computational capacity [IX]. Network controllers can quickly notify IoT device operators of attacks thanks to immediate detection, allowing them to evaluate and protect their systems from potential threats [X]. The joining of AI (artificial intelligence) advancements, especially AI (ML), works with extensive assessment and examination of organization trafficAnomalies and patterns that are indicative of malicious activity can be quickly identified by machine learning algorithms, allowing for prompt responses to reduce risks and guarantee residents' safety [XI]. Assault discovery instruments commonly fall into two classifications, signature-based and abnormality-based. While anomaly-based approaches examine the behavioral patterns of normal traffic to identify deviations indicative of potential attacks or crimes, signature-based solutions match incoming traffic against predefined attack signatures stored in a database [XII, XIII].

II. Related Work

The researcher in [XIV] does a careful assessment of haze figuring asset the executive's strategies, offering a deliberate scientific classification, and underlining significant parts like burden adjusting, planning, designation, provisioning, and work offloading. In the direction of cybersecurity. In the meantime, researchers in [XV, XVI] depicted the improvements in the web of things (WoT's), availability, and remote sensor organizations (RSN).

These improvements no doubt help in the formation of stronger and more organized frameworks that can gather and send information in various settings. Within the framework of mist-based open distributed computing, the authors first presented the concept of an Unknown and Secure Total Plan (ASAS) in [XVII].

The cloud provides sophisticated information regarding open cloud servers through this innovative approach. ASAS possesses the capacity to improve the security and effectiveness of distributed computing systems by facilitating the sharing of data between fog devices and Public Cloud Services (PCS). Furthermore researchers in [XVIII] compared ML methods with deep-learning neural networks using a dataset that was made accessible to the general public to concentrate on the identification of assaults in FOG design [XIX].

Presented deep neural networks as a unique way to identify assaults, in an effort to reinforce security protocols in these increasingly networked settings. Furthermore, researchers in [XX] made a profound learning-based network interruption identification framework (NIDS), maybe utilizing complex calculations to work on the framework's ability to distinguish and kill assaults. To distinguish dangers without past information.

Another philosophy that mixes dynamic learning methods with confinement timberlands and One-Class Backing Vector Machines (OCSVM). This demonstrates novel strategies for enhancing cybersecurity defenses [XXI, XXII]. The researcher in [XXIII] utilized a two-stage methodology to further develop assault recognition capacities by joining fast preprocessing or separating approaches with a variety of autoencoders.

Using sophisticated methods, enabled the improvement of detection accuracy in machine learning framework to detect attacks in IoT as data innovation continues to converge and different data devices are becoming increasingly confused[XXIV]. Connected to one another, they continue to create and save substantial amounts of digital data, ushering in an era of big data. Using machine learning to address threats. In ML, there are numerous primary approaches: Using labeled data to train models, and supervised learning is used to identify malware in files by using prior classifications. Unsupervised learning: makes use of unlabeled data so that the model may recognize patterns and abnormalities on its own using the characteristics of the data [XXV].

Another name for this is the data-driven strategy. Employing strategies for both supervised and unsupervised learning, semi-supervised learning is especially helpful whenever a dataset contains data that is both labeled and unlabeled park [XXVI]. Reinforcement learning: It adjusts behavior in response to environmental input and works well in dynamic settings. Formerly referred to as the environment-driven strategy. Active learning: Similar to a teacher supporting learning processes, it directs the model to rectify mistakes and modify behaviors in response to environmental changes and belongs to the subclass of reinforcement learning. [XXVII].

II.i. Support Vector Machine

Support vector machine (SVM) is a well-known and widely used machine learning technique. It is exceptionally respected for its flexibility to both relapse and arrangement issues, though it is generally utilized for the last option. Conceptually, SVM works by projecting data points into an n-dimensional space, where each point represents a feature being analyzed. Through this method, SVM can draw the shape of a hyperplane here and spot it such that it best partitions the information into discrete gatherings. The hyperplane enables SVM to classify newly acquired data points based on their position on the hyperplane, serving as the discriminatory border [XXVIII].

The underpinning of this procedure is expanding the edge, or the hole between the hyperplane and the nearest data of interest from each class, to give solid detachment. By maximizing this margin, SVM hopes to increase its generalizability, making it possible to correctly classify data even when there is noise or overlap SVM is a useful instrument for many fields, including cybersecurity, where it is essential to distinguish between illegal and harmful activity because of this feature [XXIX].

II.ii. G-B Decision Tree

GBDTs are powerful AI calculations that stand out for their capacity to make use of the assets of choice trees through a technique known as support. As opposed to disconnected choice trees, GBDT makes a strong group of feeble choice trees by constantly further developing frail choice trees, which when consolidated structure a powerful expectation model. Choice trees are organized iteratively utilizing distinct informational subsets, with each unused tree noteworthiness to address the botches accomplished by the past ones [XXX]. The GBDT can successfully utilize the characteristics of person choice trees while minimizing their inalienable imperfections through consecutive arrangement, guaranteeing that the demonstrate persistently makes strides in its figure exactness with each accentuation. Additionally, GBDT excels at managing large datasets, making it an excellent choice for tasks where scalability and efficiency are important considerations [XXXI].

With regards to different fields, including online protection, where the distinguishing proof of irregularities and vindictive action requires the utilization of solid and compelling prescient models, GBDT's ability to recognize complex examples inside information and give exact expectations makes it a crucial and versatile apparatus [XXXII].

II.iii. Random Forest

Given the ideas of arbitrary subspace and sacking, Irregular woodland as referenced in [XXXIII], utilizes order and relapse trees (Truck) as its center procedure. This adaptable strategy might be applied to both relapse and grouping applications, exhibiting its materialness in a few fields. Outstandingly, RF utilizes processing assets to help equal tutoring. One of the critical qualities of support learning (RF) is the purposeful presentation of irregularity in the preparation and testing phases of the educational experience.

Consequently, unconventionality overfitting is diminished and variety is cultivated because each choice tree in the group is exceptional from the others. To limit difference and work on the model's general execution, the joined result of these many trees is used during forecasts, as made sense of in [XXXIV].

Since RF can successfully coordinate the information from different randomized choice trees, it is an integral asset for prescient examination that is supposed to perform well in various certifiable situations, like online protection, where the ability to dependably recognize irregularities and order dangers is basic.

II.iv. Data Sets

The NSL KDD dataset was used as the fundamental data focal point for this assessment. The model's turn of events and assessment were made more straightforward with the assistance of this dataset, which can be downloaded in CSV or JSON designs as indicated by [XXXV], the NSL KDD dataset was outstanding for its flexibility, expandability, and consistency. It gave adequate slack to testing and assessment, taking into account adjustments, increases, and discoveries.

III. Examination of Gaps

These are important difficulties that have been identified from previous research:

I. Ineffectiveness of the fog layer assault detection.

II. Employing a range of classifier techniques with smaller datasets.

IV. Proposed Methods

We propose a novel technique for cyber attack detection based on several machine-learning approaches. The most important phase in our framework is to examine the cyber threats and attacks on the IoTs using the renowned NSL-KDD dataset. At this point, the data was thoroughly examined in order to identify its different qualities. Then, in the preparation phase of the information, stringent cleaning methods were when combined with astute visualization strategies and the use of feature engineering, which included vectorizations, resulting in the conversion of the data into feature vectors. After NSL-KDD dataset analyzed, the assaults were divided into four main categories:

I. Unauthorized remote system access (R2L)

II. Port scanning reconnaissance (Probe)

III. Denial-of-service (DoS)

IV. Unauthorized attempts to get root super user access (U2R attack).

IV.i. Algorithm: NSL-KDD Implementation technique.

The following covers the algorithmic stages.

Step I. Load the dataset Import necessary libraries, Scikit-learn.

Step II. Standardize mathematical features.

Step III. Load the dataset NSL-KDD dataset into a data frame using pandas.

Step IV. Train each classifier on the training subset.

Step V. Data Pre-processing by addressing any missing values by either removing them or filling them inappropriately.

Step VI. Convert categorical features to numerical representations using methods like one-hot encoding.

Step VII. Split the Dataset Input using scikit-learn's train_test_split function to separate the dataset into training (80%) and testing (20%) subsets.

Step VIII. Apply feature selection techniques such as recursive feature elimination (RFE), Analysis of Principal Components (PCA), or feature importance from models like Random Forests.

Step IX. Select the most significant features that contribute to model performance.

Step X. Choose three different classifiers (e.g., Random Forest, Support Vector Machine, and Decision Tree).

Step XI. Use the trained classifiers to make predictions on the test subset.

Step XII. Calculate the True-Positive-Rate (TPR), False-Positive-Rate (FPR), specificity, and accuracy for each classifier using the predictions and actual labels from the test subset.

Step XIII. Utilize the subsequent for evaluation:

$$\text{Accuracy: Accuracy} = A = \frac{\mathrm{TP+TN}}{\mathrm{TP+TN+FP+FN}} \tag{1}$$

$$\text{True Positive Rate (Recall): } \mathrm{TPR} = \frac{\mathrm{TP}}{\mathrm{TP+FP}} \tag{2}$$

$$\text{False Positive Rate: } \mathrm{FPR} = \frac{\mathrm{TP}}{\mathrm{FP+TN}} \tag{3}$$

$$\text{Specificity: Specificity} = \frac{\mathrm{TN}}{\mathrm{TN+FP}} \qquad (4)$$

IV.ii. Classifiers and Trainings

We choose to use the Random Forest (RF) machine learning approach supervised for our model training. By adding more trees, the variance may be reduced without noticeably increasing bias. RF has been successfully used in a range of traffic datasets, such as traffic flow-based analysis for the identification of in-network traffic abuse and Command and Control (C&C) IoT attacks.

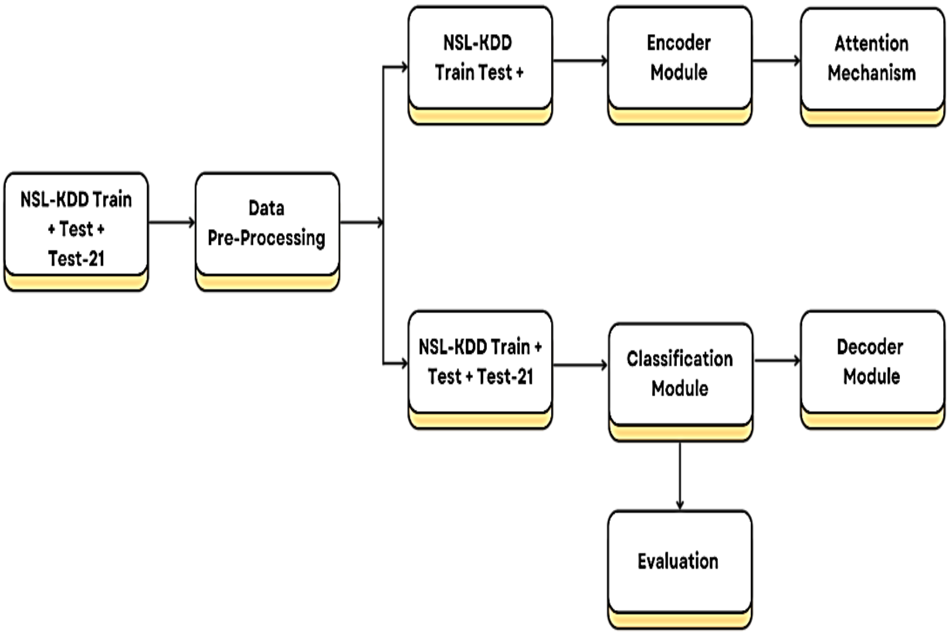

Fig. 1. NSL-KDD dataset evaluation training

IV.iii. Performance Measures

The following four performance measures were assessed under the suggested framework: Precision= A, Genuine Positive= Θ, Wrong Positive= $\bar{\xi}$, Genuine Negative= ω, Untrue Negative= Π

The algorithm's precision measures how well it can segregate between authentic and noxious associations

$$A = \frac{\Theta+\omega}{\Theta+\xi+\omega+\Pi} \qquad (5)$$

$$S = \frac{\omega}{\xi+\omega} \qquad (6)$$

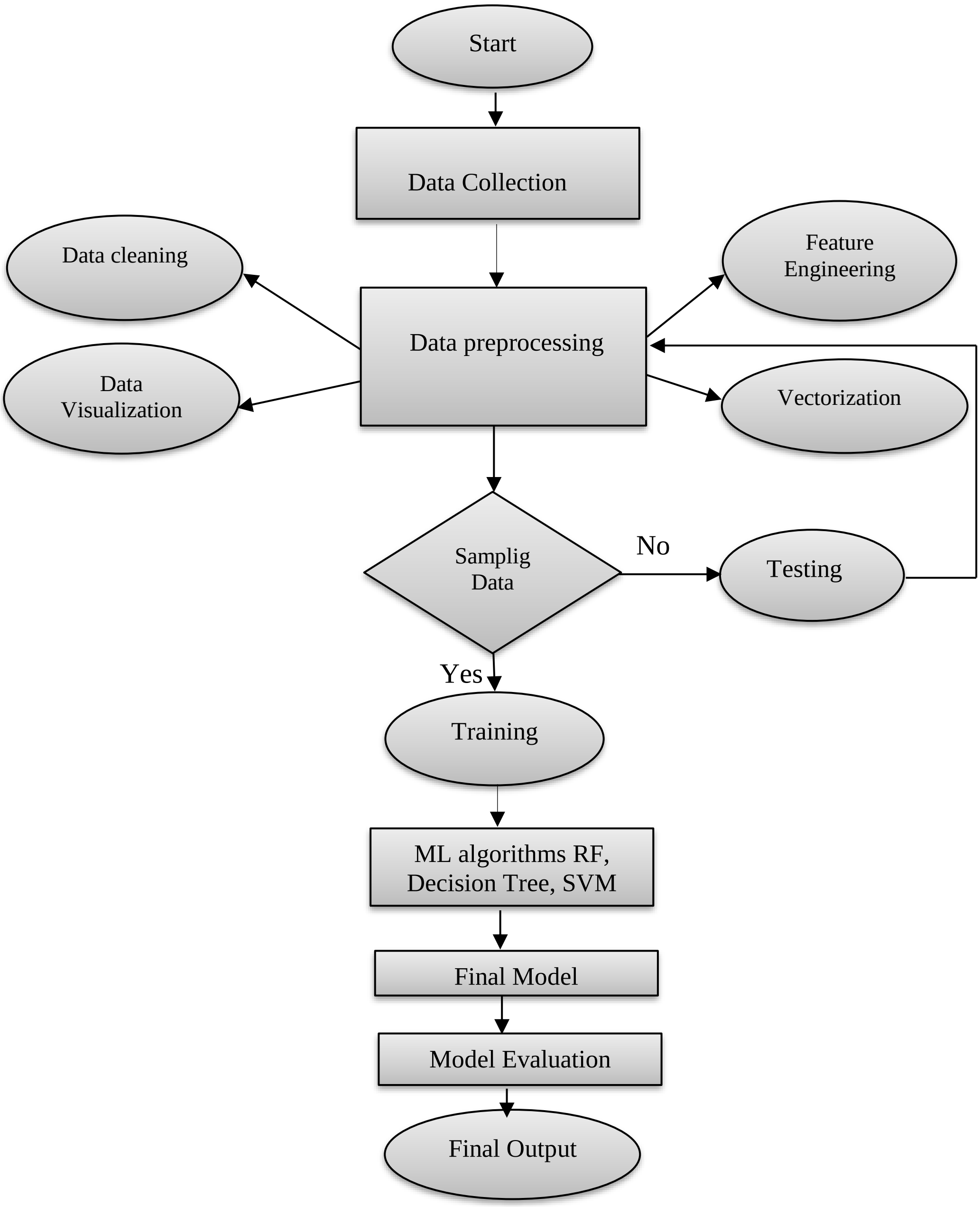

Fig 2. Flow Chart that addresses cyber threats detection in IoT's using ML

It shows how the threshold varies in connection to True-Positive-Rate (TPR) and False-Positive-Rate (FPR). For each class, different thresholds are used to choose the appropriate algorithms.

$$FPR = \frac{\xi}{\xi + \omega} \tag{7}$$

$$TPR = \frac{\Theta}{\xi+\Theta} \tag{8}$$

The anticipated outcome for every one of the anticipated categories is represented by the threshold. ROC curves are usually created for categories that are binary. The range of values for the True-Positive-Rate (TPR) and False-Positive-Rate (FPR) is 0 to 1.

V. Results

The performance metrics that were used to compare the results and the dataset that was employed in the experiment are both discussed in this section. Finally, a variety of choices and classifications are used to conduct a comprehensive analysis of the proposed model. The recommended model was assessed utilizing three unmistakable AI methods, considering an extensive assessment of its viability.

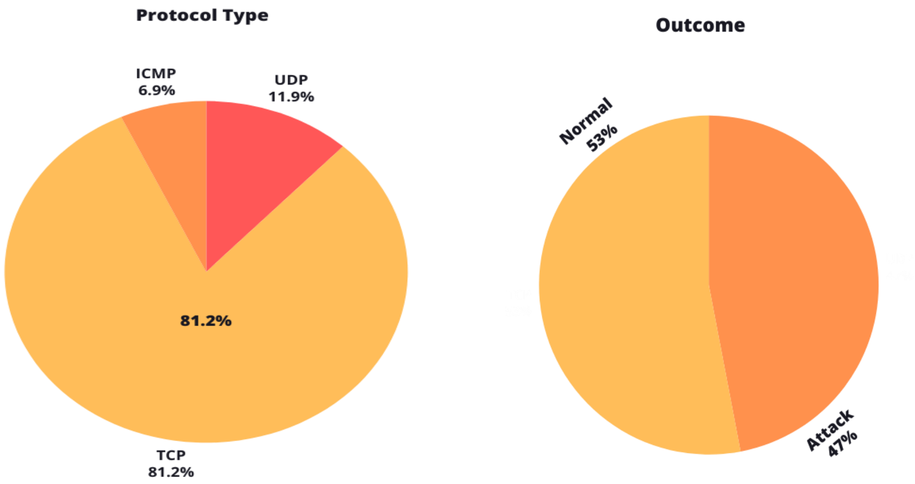

Fig. 3. General description of NSL-KDD

Table 1. Nsl-Kdd Train Set

Type	Authentic (R)	Diverse (R)	Decrease in rate
Threat Attacks	4,926,640	382,178	83.3%
Normalize	874,582	713,114	17.88%
Sub Total	3,748,441	1,555,191	80.05%

Table 2. Nsl-Kdd Test Set

Type	Authentic (R)	Diverse (R)	Decrease in rate
Threat Attacks	240,136	27,178	90.26%
Normalize	70,281	57,911	28.12%
Sub Total	299,927	75,185	75.25%

As shown in Tables I–II, we divided the dataset into training and testing sets after converting our data into feature vectors, allocating 80% for training and 20% for testing. To train our final model, we used a boosting strategy with the training dataset. The distribution of data between the training and testing groups is displayed in Fig 3 and 4, 5, 6 & 7.

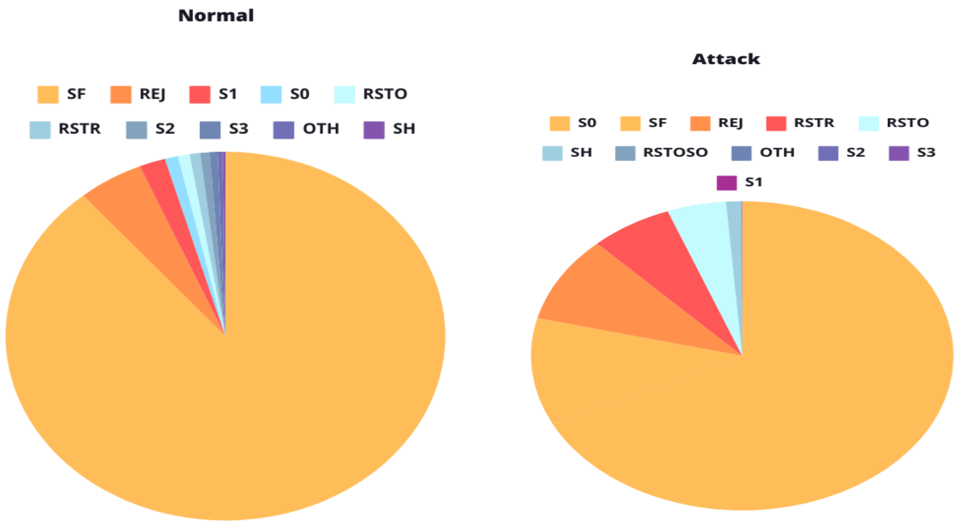

Fig. 4. Flags of normal and attack classes in the dataset.

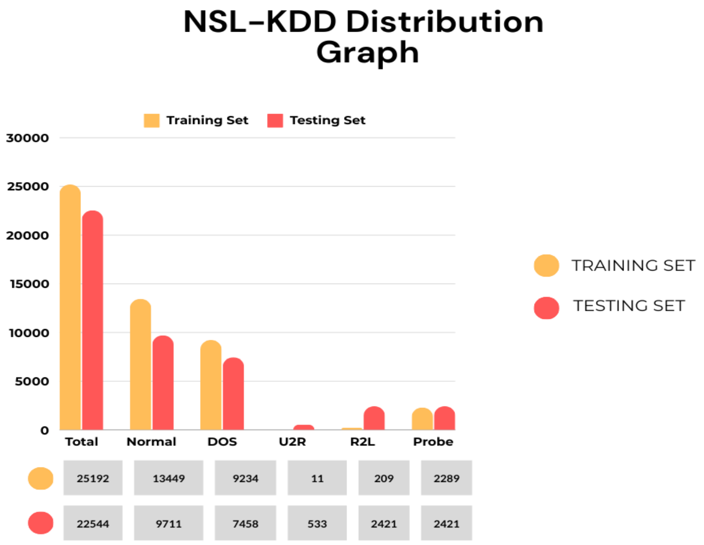

Fig 5. NSL-KDD dataset distribution

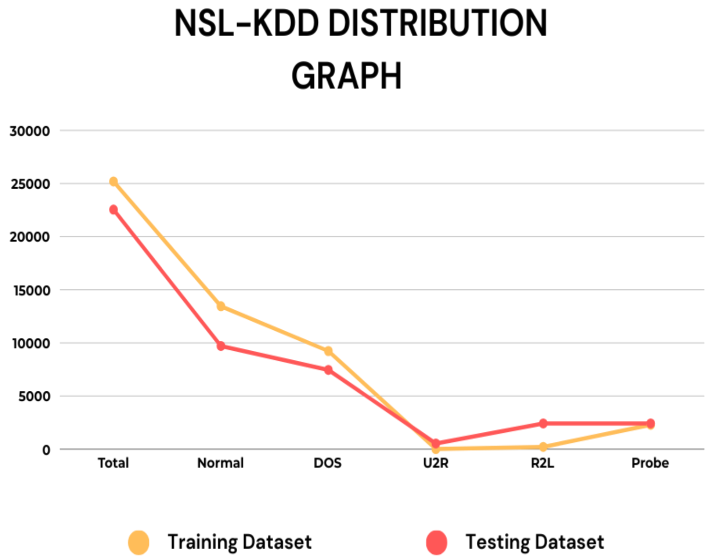

Fig 6. NSL-KDD dataset

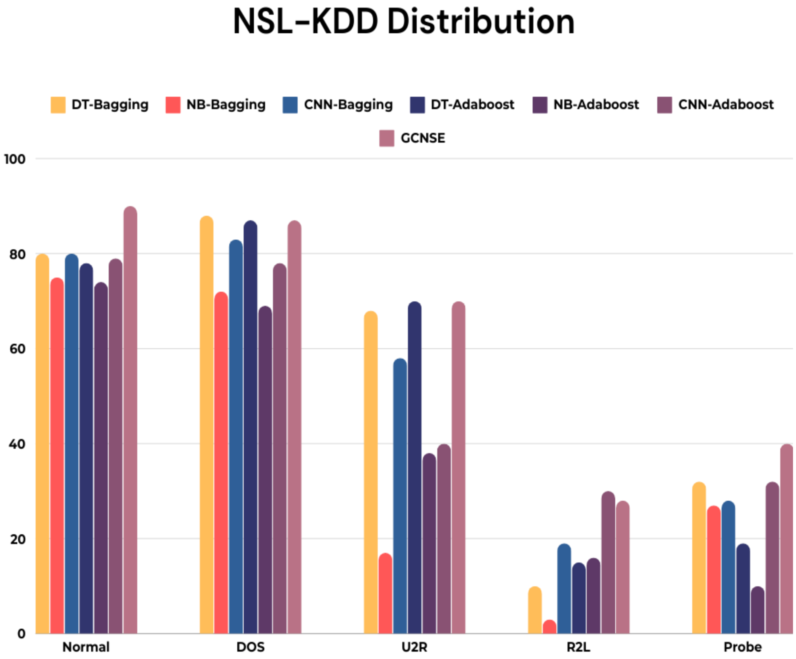

Fig 7. NSL-KDD dataset distributin adopting different methods

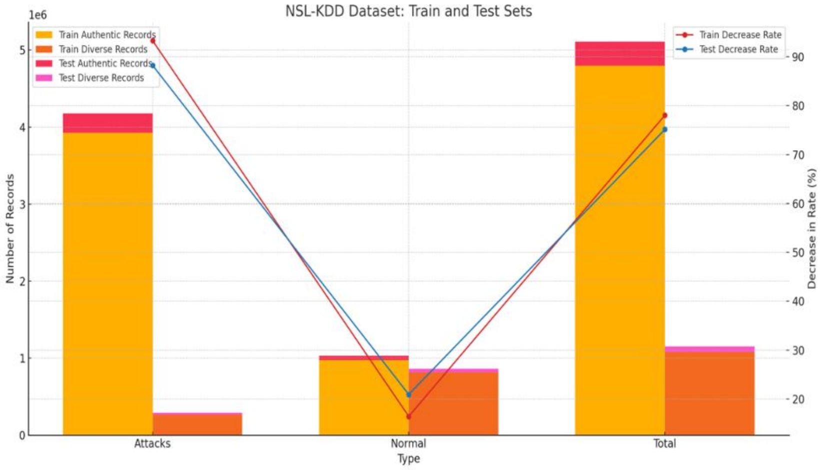

Fig 8. NSL-KDD dataset Rate

The above graphs depict the NSL-KDD dataset for train and test sets, with bars showing the count of records for each category (Attacks, Normal, Total) and lines indicating decreased rates. This dual-axis plot effectively visualizes both record counts and decrease rates across categories.

V.i. Experimental Setup

A Lenovo Thinkpad running Ubuntu 20.04, with a 60000U processor, 16GB of Smash, and an inbuilt AMD illustrations card (with an associated NVIDIA card) utilized for dataset preparation, was utilized for the testing. To clean, highlight choice, and information arrangement, numpy and pandas libraries were utilized.

V.ii. Result Analysis

The NSL-KDD dataset was subjected to three techniques of machine learning, as previously described Random Forest (RF), Slope Boosted Choice Trees (GDBT), and Bolster Vector Machine (SVM). After cross-validation, RF performed best in terms of preparing and testing exactness. With a specificity of 97.02%, GDBT fared better than SVM and RF, which had specificities of 2.02% and 95.09%, respectively. A thorough performance evaluation of these algorithms is shown in Table III, which includes the metrics A (accuracy), TT (training accuracy), PT (testing accuracy), and S (specificity).

Table 3. Assessment Results

Method	Accuracy	Specificities	Training Accuracy
SVM, Random Forest	32.38	2.02	10.87
Gradient Boosted Trees	78.01	97.02	7.78
Random Forest	85.34	95.09	6.10

VI. Conclusion & Future Work

The findings check the feasibility of supervised ML for the analysis of online traffic, specifically for the identification of malicious data that is moving between IoTs using functions like classification.

The techniques were used to thoroughly evaluate the NSL KDD dataset using the Random Forest (RF) method and a few other renowned methods but RF performed the best, with improved accuracy while on the fog layer. In the future, to expand the research on a wider range of using IoTs that are based on remote sensing devices and conducting tests across a few real-time datasets that include sensors that gets affected due to malware and vulnerable cyberattacks.

Conflict of Interest

There is no conflict of interest regarding this article.

References

I. Asish Mitra, Numerical Simulation Of Laminar Convection Flow And Heat Transfer At The Lower Stagnation Point Of A Solid Sphere., J. Mech. Cont.& Math. Sci., Vol.10, No.1, Pp 1469-1480, 2015

II. A. Belabed, E. Aïmeur And A. Chikh, "A Personalized Whitelist Approach For Phishing Webpage Detection", 2012 Seventh International Conference On Availability, Reliability And Security, Prague, Pp. 249-254, 2012

III. A. Naz, H. Khan, I. U. Din, A. Ali, M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Engineering, Technology & Applied Science Research, Vol.14, No.4, pp. 15957-15962, 2024

IV. Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE), Vol.12, No.4, pp. 264-273, 2023

V. H. Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua, Vol.74, No.1, pp. 965-981, 2023

VI. H. Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE), Vol. 12, No.4, pp. 447-453, 2023

VII. Hammad. A , E. Zhao, "Mitigating link insecurities in smart grids via QoS multi-constraint routing", In 2016 IEEE International Conference on Communications Workshops (ICC)", pp. 380-386. 2016

VIII. H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC" Computers, Materials & Continua, Vol.74, No.1, pp. 2097-2113, 2023

IX. Hammad, A. A., Ahmed, “Deep Reinforcement Learning for Adaptive Cyber Defense in Network Security”, In Proceedings of the Cognitive Models and Artificial Intelligence Conference, pp. 292-297, 2016

X. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems," IJCSNS Int. J. Comput. Sci. Netw. Secur, Vol.18, No.12, pp 125-130, 2018

XI. Hossein Shirazi, Bruhadeshwar. B,"Kn0w Thy Doma1n Name": Unbiased Phishing Detection Using Domain Name Based Features. In Proceedings Of The 23nd Acm On Symposium On Access Control Models And Technologies (Sacmat '18). Association For Computing Machinery, New York, Ny, Usa, pp. 69-75, 2018

XII. Hussain, S., Rajput, U. A., Kazi, Q. A., & Mastoi, S, “Numerical investigation of thermohydraulic performance of triple concentric-tube heat exchanger with longitudinal fins”, J. Mech. Cont. & Math. Sci, Vol. 16, No. 8, pp 61-73, 2021.

XIII. H. Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors" Int. J. Sci. Eng. Res, Vol.9, No.12, pp 6-10, 2018

XIV. H. Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers" In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1-7, 2020

XV. Hammad, M., Jillani, R. M., Ullah, S., Namoun, A., Tufail, A., Kim, K. H., & Shah, H, “Security framework for network-based manufacturing systems with personalized customization”, An industry 4.0 approach, Sensors, vol. 23. No. 17-55, 2022

XVI. H. Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems" In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1-8, 2018

XVII. H. Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors", Journal Of Mechanics Of Continua And Mathematical Sciences, Vol.6, No.14, pp. 956-972, 2019

XVIII. H. Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers" In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE, pp 1-7, 2020

XIX. H. Huang, J. Tan And L. Liu, "Countermeasure Techniques For Deceptive Phishing Attack", International Conference On New Trends In Information And Service Science, Beijing, pp. 636-641, 2009

XX. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems" IJCSNS Int. J. Comput. Sci. Netw. Secur, Vol.18, No.12, pp 125-130, 2018

XXI. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol" IJCSNS Int. J. Comput. Sci. Netw. Secur, Vol.18, No.12, pp 181-185, 2018

XXII. J. Chen; J. Tan, C. Chang, F. Feng, "A New Cost-Aware Sensitivity-Driven Algorithm for the Design of FIR Filters", IEEE Transactions on Circuits and Systems I, Vol. 64, No. 6 pp: 1588 - 1598, 2017

XXIII. M. Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System" Journal of Mechanics of Continua and Mathematical Sciences, Vol.14, No.1, pp 276-288, 2019

XXIV. M. Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies, Vol.3, No.2, pp 13-23, 2020

XXV. M. Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies, Vol.2, No.2, pp 1-6, 2019

XXVI. M. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool" In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, pp 1-6, 2019

XXVII. M. Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)," In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, pp 1-7, 2020

XXVIII. M. Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip" Sukkur IBA Journal of Emerging Technologies, Vol.2, No.2, pp 46-53,2019

XXIX. M. U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems" Journal of Mechanics of Continua and Mathematical Sciences, Vol.14, No.4, pp 442-452, 2023

XXX. M. Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller" Engineering, Technology & Applied Science Research, Vol.9, No.2, pp 3900-3904, 2019

XXXI. R. Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications" Bulletin of Business and Economics (BBE), Vol.13, No.2, pp 200-206, 2024

XXXII. S. Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives" Reviews in Inorganic Chemistry, Vol.44, No.3, pp 1-29, 2024.

XXXIII. S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea their characterization, antibacterial activity and catalytic reduction ability" Zeitschrift für Physikalische Chemie, Vol.238, No.5, pp 931-947, 2024

XXXIV. T. M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant" In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, pp 1-9, 2019