Enhancing Network Security: A Study on Classification Models for Intrusion Detection Systems

Abeer Abd Alhameed Mahmood, Azhar A. Hadi, and Wasan Hashim Al-Masoody

Original scientific article

Abstract*—Computer users face a constant influx of internet packets, ranging from legitimate ones to those sent by malicious entities. With the exponential growth in user numbers and evolving attack types, traditional countermeasure methods are becoming ineffective. Artificial intelligence (AI) techniques offer a promising solution to address these challenges. This study leverages AI methods to develop nine classification models using supervised machine learning classifiers. The author has implemented several machine learning models, including bagging, multi-layer perceptron, logistic regression, extreme gradient boosting, and random forest. The authors utilize three datasets (Knowledge Discovery in Databases 1999 dataset, used for network intrusion detection research), UNSW-NB15 (a dataset capturing contemporary network attack patterns generated at the University of New South Wales), and CICIDS2017 (Canadian Institute for Cybersecurity Intrusion Detection System dataset, containing modern attack scenarios)(KDD99, UNSW NB15, and CICIDS2017) with varying train-test ratios to train the classifiers. The author employs accuracy and F1 score metrics to evaluate the model's performance. The Extreme Gradient Boosting classifier exhibits the highest performance across all three datasets, especially with an 80% feature reduction. Various oversampling and undersampling techniques balance the dataset to improve false-negative rates. Performance metrics show improvements across all dataset types, with extreme gradients boosting accuracy. The meta-ensemble learning model does better at sub-multiclass classification than decision trees, random forests, and extreme gradient boosting. It also does better than logistic regression and multi-layer perceptron in multiclass classification. Two hidden layers achieved the highest accuracy for binary classification on the KDD99 dataset. Multiclass classification presents challenges with identifying minor classes, but performance improves with additional hidden layers. Random Forest outperforms other classifiers in accuracy, which is consistent with simulation results.

***Index Terms*—Intrusion Detection Systems (IDS), Machine Learning, Balanced Dataset, Network Security.**

I. Introduction

With the continued expansion of the Internet, concern for information security is crucial for organizations and individuals. The role of network system administrators is to protect communication tools from diverse threats and attacks [1]. Cryptography, firewalls, and access control are essential methods for preserving privacy in an organization and counteracting malicious activities. Currently, distress over new challenges from attackers has forced these traditional methods to become less effective [2]. For example, the significance of sniffer threats and their prevalence in advanced attack mechanisms demonstrate the limitations of conventional security measures.

An Intrusion Detection System (IDS), which automatically detects intrusion and monitors the system state and information flows, ensures confidentiality, integrity, and availability within a network [3]. When it detects suspicious activities, it notifies system administrators to prevent potential threats. These traditional security strategies have not proven fully effective in the modern world, as many organizations remain vulnerable to attacks. Despite using various security measures, it is evident that attacks are increasing continuously. Many network experts have engaged in developing IDS that involve machine learning to improve detection accuracy and reduce false alarms [4]. As a result, the academic community and other organizations, such as Google, Facebook, and Intel, are focusing on researching and developing powerful IDS that can predict, detect, and analyze attacks more accurately. Network security is critical research in the digital world.

This paper examines various techniques, with machine learning emerging as a viable solution to mitigate network threats. However, other challenges, like imbalanced training datasets, affect the performance of the machine-learning-based IDS, making it inefficient, especially for less frequent attack types. Past research has proposed numerous innovative methods to enhance the efficiency of IDS [5]–[8]. A few hybrid variant model techniques are available to use. These involve choosing which features to use, comparing various machine learning algorithms, reducing features using deep learning autoencoders and principal component analysis and finding outliers with ensemble classifiers. This paper contributes to the field by:

- The authors are setting up an operational and scalable IDS that can predict, detect, and analyze attacks as efficiently as possible and reduce false alarm rates.
- The authors are enhancing the effectiveness of the classifier in handling unbalanced intrusion data and decreasing the rate of false negatives.
- The authors are developing a unique ensemble classifier

Manuscript received October 14, 2024; revised December 19, 2024. Date of publication May 12, 2025. Date of current version May 12, 2025. The associate editor prof. Miljenko Mikuc has been coordinating the review of this manuscript and approved it for publication.

Authors are with the University of Babylon, Iraq (e-mails: {eng.abeer.abd, azhar, eng.wasan.hashim.lec}@uobabylon.edu.iq).

Digital Object Identifier (DOI): 10.24138/jcomss-2024-0064

capable of identifying minor classes and reducing false-negative rates in binary and non-binary datasets.
- The authors are proposing various machine learning classifiers, enhancing the selection of attributes, addressing class imbalances, and incorporating performance metrics.
- They have identified Extreme Gradient Boosting as the most effective classifier and are in the process of developing a new meta-ensemble learning approach for IDS optimization and effective cyber threat detection.

The breakdown of the findings, along with the realistic representation of the models and conditions, strengthens the study's contributions and benefits to researchers and practitioners. The structure of the paper is as follows: The current section serves as an introduction, and An exposition of the literature review is given in section II. Section III delves into the methodology, covering the datasets (KDD99, UNSW NB15, and CICIDS2017), feature selection methodologies and classifiers used. The results and analysis subheading displays the evaluation measures of the classifiers in section IV, highlighting Extreme Gradient Boosting as the standout classifier. This underscores the importance of feature selection and dataset balancing. In the last section V, the conclusion briefly reiterates the study's findings, major contributions, and the research implications for future studies.

II. Literature Review

Intrusion detection systems are fundamentally vital for computer network security, effectively detecting and responding to malicious activities and security breaches. In this way, security mechanisms actively monitor network traffic and system activities, identifying potential unauthorized penetrations, malware infiltration, and other deviant behaviors [9]. Traditional intrusion detection systems (IDS) work with pre-established signatures and rules for finding threats that are known beforehand. Using machine learning and artificial intelligence, modern frameworks identify anomalies in patterns that denote cyberattacks [10].

IDS systems provide early alerts through network and system log monitoring, allowing the organization to take quick action. This enhances the management of security risk, thereby necessitating the need for robust protection for secure information [2]. The increasing sophistication of cyber threats necessitates a dynamic and robust IDS, indicating the need for a comprehensive security strategy across diverse sectors. Innovatory research in network security, mainly focusing on the Internet of Things (IoT), further takes IDS capabilities to an entirely different level. For example, this study [21] suggested a custom deep-learning-based IDS model for IoT security. Similarly, [2] developed a unique IDS designed explicitly for IoT settiThe authors also talked about a Golden Jackal Optimization algorithm that makes networks safer when deep learning is used with them.

The author [4] go into more detail about the Anomaly-Based IDS for UAV Swarm Networks. rks. Further, the study [5] proposed an AI-based IDS approach to detect intrusions in IoT, while in paper [6] used machine learning and federated learning to secure IoT networks in the healthcare domain. This paper [7] conducted a study on the function of self-directed learning as a countermeasure against DDoS attacks in IoT environments. Further, Windows 10 has served as the base platform for security-related works, Also, this author [8] use of Snort for intrusion detection systems and the critical research works of this papers [9]–[11].

The paper [12] investigate deep learning IDS for IoT security improvements. Some other studies include the one by this paper [22] called MidSiot—a multistage IDS for IoT—and this paper [23], an IDS tailor-made for IoT traffic to improve data engineering practices. the author [24] proposed a technique to generate datasets for botnets in IoT networks. this study [6] propose a green machine learning-based intrusion detection system for medical IoT networks using federated learning, named GEMLIDS-MIOT.

The study in [25] introduce an IDS system learning from both tabular and textual information, while this study [26] investigate how deep learning and big data analytic techniques could be fused into a database to offer security services. Investigating, the author [21], and many more took an analytical approach to examine the effectiveness of real-time IDS defenses against adversarial attacks. the study [27] assess the effectiveness of IDS in enhancing security in the Internet of Things (IoT) and provide strategies for effectively implementing IDS to mitigate risks. The shared research brings out several strategies and technologies meant to strengthen network security through IDS in light of the changing cyber threat landscape and increased complexities within the IoT environment.

In this article, the methods employed in the analysis are founded on solutions and procedures from the cited literature. In particular, this study combines both signature-based and anomaly-based detection techniques, as noted in previous scientific literature, to possibly improve the functionalities of IDSs. Such strategies as machine learning classifiers, balancing of datasets by oversampling and undersampling, and feature selection of information are used and improved. These methods are derived from previous studies but adapted given the nature of imbalanced data and multiple classes for developing minor attack classes. This foundation helps in establishing the relationship between the reviewed literature and methodologies described in subsequent chapters presenting the cause-and-effect relationship between the research area and this study, the comparision of the related work shown in Table I.

III. Methodology

Recently, there has been a significant increase in internet-based attacks, leading to declines in network performance. This rise is evident in both the number and complexity of the attacks [28]. To cope with this, new detection techniques are required especially the ones that use Artificial Intelligence techniques such as machine learning-based intrusion detection and prevention systems [29]. The following techniques are used to enhance the performance of Intrusion Detection Systems based on Supervised Machine Learning Classifiers: first, the influence of Train-Test ratios and Feature Selection

TABLE I
COMPARISON OF THE RELATED WORK

Ref.	Motivation	Objective	Achievement
Bakhsh et al. (2023) [1]	The motivation is to enhance IoT network security using deep learning-powered Intrusion Detection Systems (IDS).	The objective is to develop an IDS capable of effectively detecting and mitigating security threats in IoT environments.	The achievement involves the implementation of a deep learning-powered IDS tailored for IoT networks, enhancing their security posture.
Bediya et al. (2023) [2]	The motivation is to address the security challenges in IoT network by introducing a novel intrusion detection system.	The objective is to design and implement an intrusion detection system specifically tailored for IoT network security.	The achievement includes the development of a novel IDS framework aimed at bolstering security in IoT environments.
Aljehane et al. (2024) [3]	The motivation is to improve network security using the golden jackal optimization algorithm combined with deep learning for intrusion detection.	The objective is to develop an intrusion detection system utilizing advanced optimization algorithms and deep learning techniques.	The achievement involves the integration of the golden jackal optimization algorithm and deep learning for enhanced intrusion detection capabilities.
Da Silva et al. (2023) [4]	The motivation is to enhance in-flight and network security in UAV swarm through an anomaly-based intrusion detection system.	The objective is to design and implement an intrusion detection system capable of detecting anomalies in UAV swarm networks.	The achievement involves the development of an anomaly-based IDS tailored for UAV swarm networks, improving their security.
Sabitha et al. (2023) [5]	The motivation is to detect IoT attacks using the AIS-IDS model for network-based detection.	The objective is to implement an IDS model specifically for IoT networks to detect and prevent attacks effectively.	The achievement includes the implementation of the AIS-IDS model for network-based detection of IoT attacks, enhancing network security.
Ioannou et al. (2024) [6]	The motivation is to strengthen medical IoT network security through a machine learning intrusion detection system based on federated learning.	The objective is to develop a machine learning-based IDS using federated learning to enhance security in medical IoT networks.	The achievement involves the creation of a federated learning-based IDS tailored for medical IoT networks, improving their security posture.
Almaraz-Rivera et al. (2023) [7]	The motivation is to enhance IoT network security against DDoS attacks using self-supervised learning.	The objective is to develop a self-supervised learning-based approach to mitigate DDoS attacks in IoT networks.	The achievement involves the implementation of self-supervised learning techniques to improve the resilience of IoT networks against DDoS attacks.
Putri et al. (2023) [8]	The motivation is to implement network security using a Snort-based intrusion detection system on Windows 10.	The objective is to deploy a Snort-based IDS on the Windows 10 platform for network security.	The achievement includes the successful implementation of a Snort-based IDS on Windows 10, enhancing network security.
Haricharan et al. (2023) [9]	The motivation is to enhance network security through machine learning and behavioral analysis.	The objective is to develop a network security solution leveraging machine learning and behavioral analysis techniques.	The achievement involves the development of an enhanced network security solution integrating machine learning and behavioral analysis for improved threat detection.
Abdulganiyu et al. (2024) [10]	The motivation is to develop an efficient model for network intrusion detection systems (IDS) through a systematic literature review.	The objective is to identify and synthesize existing literature to propose an efficient model for network IDS.	The achievement involves the synthesis of existing literature to propose a comprehensive model for network intrusion detection systems, enhancing their efficiency.
Kumar et al. (2024) [11]	The motivation is to enhance intrusion detection systems using deep residual convolutional neural networks.	The objective is to develop an efficient technique for intrusion detection leveraging deep residual convolutional neural networks.	The achievement involves the development of a novel technique using deep residual convolutional neural networks to enhance the efficiency of intrusion detection systems.
Alkahtani & Aldhyani (2021) [12]	The motivation is to advance IoT infrastructure based deep learning algorithms for intrusion detection systems.	The objective is to improve IoT security by advancing deep learning algorithms for intrusion detection.	The achievement involves the advancement of IoT infrastructure based deep learning algorithms to enhance the effectiveness of intrusion detection systems.
Khudhair (2021) [13]	The motivation is to review existing laws to enhance competence in cybercrime, including intrusion detection systems.	The objective is to assess existing laws related to cybercrime and their impact on intrusion detection system competence.	The achievement involves the review and analysis of existing laws to identify opportunities for enhancing competence in cybercrime, particularly related to intrusion detection systems.
Indrasiri et al. (2022) [14]	The motivation is to detect malicious traffic in IoT and local networks using a stacked ensemble classifier.	The objective is to develop a detection system capable of identifying malicious traffic in IoT and local networks.	The achievement involves the implementation of a stacked ensemble classifier to effectively detect malicious traffic, improving network security.
Alonazi et al. (2022) [15]	The motivation is to secure smart homes using an SDN architecture integrated with machine learning and deep learning techniques.	The objective is to design an architecture capable of enhancing security in smart homes through machine learning and deep learning.	The achievement involves the development of an SDN architecture incorporating machine learning and deep learning for improved smart home security.

Ref.	Motivation	Objective	Achievement
Sharma et al. (2024) [16]	The motivation is to utilize machine learningbased intrusion detection technologies for network security.	The objective is to leverage machine learning techniques to develop effective intrusion detection technologies for enhancing network security.	The achievement involves the utilization of machine learning-based intrusion detection technologies to bolster network security.
Javanmardi et al. (2024) [17]	The motivation is to develop a mobility and impersonationaware IDS for mitigating DDoS UDP flooding attacks in IoT-Fog networks.	The objective is to design an IDS capable of mitigating DDoS UDP flooding attacks in IoTFog networks by considering mobility and impersonation.	The achievement involves the development of an IDS that effectively mitigates DDoS UDP flooding attacks in IoTFog networks, considering mobility and impersonation.
Kabilan et al. (2024) [18]	The motivation is to implement an unsupervised intrusion detection system for invehicle communication networks.	The objective is to develop an unsupervised IDS for detecting intrusions in invehicle communication networks.	The achievement involves the implementation of an unsupervised IDS for effectively detecting intrusions in invehicle communication networks.
Cengiz et al. (2024) [19]	The main aim is to provide an introduction to a novel intrusion detection system using artificial neural networks and genetic algorithms and a new dimensionality reduction that is specifically a new dimensionality reduction method for the UAV communication problem.	The proposed system is an advanced intrusion detection system based on artificial neural networks and genetic algorithms, together with a new dimensionality reduction scheme custom-tailored for communication networks in UAVs.	The contribution was in the form of an innovative intrusion detection system that harnesses artificial neural networks, genetic algorithms, and a novel dimensionality reduction technique so that it can become viable for use in UAV communication networks for better security.
Sadia et al. (2024) [20]	The motivation is to develop a machine learning-based intrusion detection system for wireless sensor networks.	The objective is to design an intrusion detection system leveraging machine learning techniques for enhancing security in wireless sensor networks.	The achievement involves the development of a machine learning-based intrusion detection system capable of improving security in wireless sensor networks.

on Classifier performance is investigated; second, the model performance has been improved for each model by using the optimal tuning parameters. In the end, the performance of the classifiers is assessed using various input features chosen for each dataset.

The Python programming language is used to build the previously mentioned procedures; binary datasets are utilized for designing bagging, multi-layer perceptron, logistic regression, extreme gradient boosting, and random forest classifiers. In this work Random Forest Classifier on imbalanced multiclass datasets utilized to emulate real-world datasets. The performance of the proposed Extreme Gradient Boosting and Random Forest models has been evaluated using metrics like accuracy, precision, recall, and F1 score. Figure 1 illustrates the overall procedure.

Three feature selection methods information gain is used, Pearson, and ANOVA F test to reduce the dimensional input feature of the KDD99 dataset. The KDD99 dataset comprises 41 features, including attributes like connection duration, protocol type, and byte statistics. The full list of these features is provided in the Appendix. The performance of the Extreme Gradient Boosting, Bagging, Random Forest, Multi layer Perceptron, and Logistic Regression classifiers has been evaluated, leveraging datasets like KDD99, UNSW NB15, and CICIDS2017, under various feature selection and sampling scenarios. Figure 1 presents an overview of the proposed classifier model, comprising several blocks: the dataset (KDD99[1], UNSW_NB15[2], and CICIDS2017[3]), preprocessing, model training, test set, IDS classifier, and model evaluation.

The results of the Extreme Gradient Boosting, Bagging, Multi layer Perceptron, Logistic Regression, and Random Forest models were compared using the KDD99, UNSW NB15,

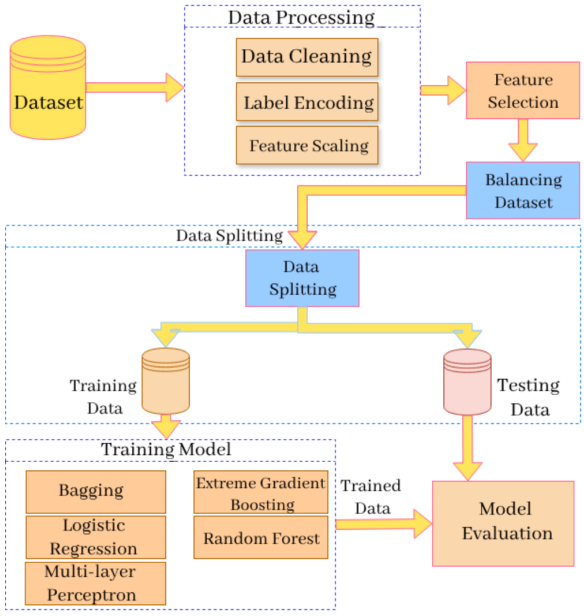

Fig. 1. Overall proposed model.

and CICIDS2017 datasets. Forty one (41) features of the dataset were ranked from the most to the least important using Information Gain, Pearson correlation, and ANOVA F test methods using Information Gain (IG). It could be positive or negative, depending on the linear relationship between the two variables. Regardless of its value, whether positive or negative, features highly correlated to the output response (outcome) are useful for output prediction. In the scikit learn library[4], the F test parameter assists in univariate feature selection. This is helpful given the many features, which are useless in the current scope. A quick way is required to shortlist which ones

[1]https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data
[2]https://research.unsw.edu.au/projects/unsw-nb15-dataset
[3]https://www.unb.ca/cic/datasets/ids-2017.html

[4]https://scikit-learn.org/stable/

are the most useful. Comparing all three methods, the Pearson correlation and F test methods have the same ranking for all input features. The information gained differs from them only in the last two features, src_ bytes and dst_ bytes.

- src_ bytes: The total number of bytes sent from the source to the destination in a network connection.
- dst_ bytes: The total number of bytes sent from the destination to the source during the same network connection.

The results of the classifiers Extreme Gradient Boosting, Bagging, Multilayer Perceptron, Logistic Regression, and Random Forest were obtained after balancing the KDD99, UNSW NB15, and CICIDS2017 datasets using Synthetic Minority Over-sampling Technique (SMOTE) is a data augmentation method used to address class imbalance by generating synthetic samples for minority classes, Tomek Links, and ENN techniques.

An imbalance of datasets used in training the IDS has a major impact on the low performance of IDS that employ machine learning in identifying less frequent attack types. The presence of certain classes like for instance Denial of Service (DoS) attacks makes the learning process of the machine learning models biased . Therefore, models could merely focus on identifying such dominant classes while they misclassify or totally ignore other, but potentially critical classes, such as R2L or U2R attacks. This prejudice leastways affects the general completeness of risk appraisal, decrease the credit of the IDS in the condition where detecting all kinds of danger is imperative. With regards this problem,some of the dataset balancing strategies considered by the study include the Synthetic Minority Oversampling Technique (SMOTE), Tomek Links and the Edited Nearest Neighbors (ENN). These methods were used to adjust the class samples in order to get a better representation of minor types of attack in the training set. The above techniques were assessed based on these metrics: Recall and F1-score and the results are shown before and after class balancing for all classes. The results showed the general enhancement in the ability to approximate for infrequent attack types such that the IDS could quickly identify and categorize the distinct attacks.

In particular, it could be seen that initially, the minority classes (Probe, R2L, and U2R) have low values of recall and F1-scores because of the small number of samples in the training set. As it can be seen from the performance results given in chapter IV, these metrics demonstrated some improvement when balancing techniques were applied. Therefore, these outcomes should be particularly arousing interest in the need to take action for reducing class imbalance to have a better picture of the business risks. Since all these classes are treated equally within the IDS models developed in this study, this offers more credible detection experiences which are crucial for security against diverse forms of cyber threats.

IV. Result and Analysis

Dimensional input feature selection and reduction for binary classification of intrusion detection using different classifier models resulted in getting different performance values. The Bagging Model is implemented with 8 features using information gain by different training and testing sets percentage ratios, 70%, 75% and 80%. Results are shown in Table II.

TABLE II
IG WITH 8 FEATURES

Type	Train 80% Test 20%	Train 75% Test 25%	Train 70% Test 30%
Accuracy	99.9	99.9	99.8
Error Rate	0.06	0.06	0.07
TPR	99.94	99.94	99.94
FPR	0.10	0.13	0.14
Precision	99.9736	99.9681	99.9634
Recall	99.9408	99.9496	99.9464
f1 _ score	99.9572	99.9588	99.9549
Confusion matrix:	[[19333 20] [[47 79405]]	[29154 38] [60 118955]]	[[38919 58] [85 158547]]

Tables II, III, and IV: These tables show findings derived solely from the analyses conducted in this study as part of the work. The authors demonstrate the use of various machine learning classifiers, Which include Bagging, MLP, LR, RF and EG boosting with varying train-test split and feature selection techniques followed by KDD99. Details on the experimental specifications and the procedures employed to establish these results are provided under Methodology. From the study, the datasets used in this work (KDD99, UNSW_NB15, CICIDS2017) have revealed glaring disparities in classes, with some classes having high records and others having very few records. For instance, the KDD99 dataset contains four different classes: DoS, User to Root (U2R), Remote to Local (R2L), and Probes, out of which the DoS class is approximately at 79% while the U2R and R2L class is at less than 1%. As in the CICIDS2017 dataset, benign traffic constituted 50% of the records with some attack types like Shellcode and Worms, not base frequent. Such maturity disparities presented problems for model construction resulting in preferential biases towards majority classes and low discriminative capacities for minor classes, Which often contain important features in practical applications. To overcome these problems, the following data preparation techniques were applied: oversampling and undersampling. To increase density and avoid sample duplication, the SMOTE algorithm (Synthetic Minority Oversampling Technique) was applied which created synthetic samples for oversampling the underrepresented classes from their nearest neighbors, through interpolation. To improve the quality of data, Tomek Links were used to filter out the marginal examples from the dominating class close to the boundary.

Further, the ENN (Edited Nearest Neighbors) technique removed the misclassification samples and thereby removed noise and enhanced class separability. For instance, in the KDD99 the data was balanced using SMOTE integrated with Tomek Links, while in CICIDS2017 SMOTE together with ENN to balance besides eliminate noise in the data. The effectiveness of these techniques is manifested by the enhanced performance corresponding to the minority classes.

TABLE III
F-STATISTIC WITH 8 FEATURES

Type	Train 80% Test 20%	Train 75% Test 25%	Train 70% Test 30%
Accuracy	99.23	99.36	99.23
Error Rate	0.76	0.63	0.76
TPR	99.39	99.30	99.33
FPR	1.42	0.41	1.21
Precision	99.65	99.89	99.70
Recall	99.39	99.30	99.33
f1_ score	99.52	99.60	99.51
Confusion matrix:	[[19078 275] [483 78969]]	[29071 121] [825 118190]]	[[38505 472] [1049 157583]]

Figures 2, 3, 4, 5, 6, and 7, These figures show the techniques used to balance the dataset this study. They represent the initial state of the KDD99, UNSW_ NB15 and CICIDS2017 datasets with imbalance and then show how they achieve balance through the use of SMOTE, Tomek Links and ENN. These numbers are unique to this paper and were obtained after going through the preprocessing and balancing steps highlighted in the Methodology section.

Tables VI, VII, VIII, IX, X, and XI, These tables show the evaluation measures (accuracy, precision, recall, F1-score and the like) of the applied machine learning models on the balanced datasets (KDD99, UNSW_ NB15, CICIDS2017). These were obtained from experiments performed during this research and best represent the performance of the classification models as implemented here. The details of the method and criteria applied to produce these outcomes are described in the methodology and assessment sections of the paper.

Tables II and III have summarized the behaviour of the Bagging model for intrusion detection using the KDD99 dataset at different training to test split ratios (70%, 75% and 80%). We used Information Gain (IG) for feature selection as presented in Table II and the F-statistic as presented in Table III. There is information on feature selection methods and their influence as well as data distribution in both tables based on KPIs such as accuracy, error rate, TPR, FPR, precision, recall, and F1 score. Precisions always stay above the 90% mark and the best outcome is seen with the 80% training ratio. Evaluating Information Gain we can state that this method has a slight advantage in the aspect of accuracy of error rate and therefore is more suitable for feature ranking in this case on this dataset. Moreover, using the precision and F1 score, it is possible to say that the model proposed really works fine for recognizing true positive instances with minor changes in the training ratios. High TPR values are retained in both methods; it approves that the model has high capability to detect the attacks and low FPR in Information Gain, which prevents high false alarms.

These findings will help better understand how to select a good feature ranking approach while paying attention to the fact that the ratio of training and testing data should be reasonable. Raising the training ratio a little more improves the performance of all models and Information Gain is slightly superior to F statistic in the reduction error. This leads to the conclusion that Information Gain should be used to introduce better intrusion detection tasks in datasets similar to KDD99. These findings underscore the call for systematic testing of the proportionality of training data with the ratio used in the testing data set plus feature selection approaches on the data set for improved results in the machine learning intrusion detection model. Table IV shows the results of the proposed models employed with all 41 features with an 80% separation ratio.

Tables IV to VII show that we chose these metrics and models to give a full picture of the classifier's performance, answer the research questions and consider the problems associated with using uneven intrusion detection datasets. We evaluated classification performance using performance measures like accuracy, precision, recall, and F1 score but prioritized precision and recall rate due to their critical role in minimizing false negatives. Accuracy was useful as a measure of overall performance, and the F1 score helped estimate the recall of minor classes and the precision of significant categories. Simultaneously, the F1 score helped to avoid the issue of prioritizing precision over recall or vice versa; the false-positive rate demonstrated the potential for fake alarms. The applied models included both low- and high type models. We used logistic regression as a classifier and then set other classifiers to improve performance and stability; we used the ensemble method for bagging and random forest classifiers. We selected the MLP model for its capacity to capture the non-linearity and non-regularity of the data, while we selected EG boosting due to its rapid speed and effectiveness in handling imbalanced data sets. These metrics and models enabled the assessment of the classifiers' strengths and weaknesses, simultaneously addressing dominant and rare attack classes.

The KDD99, UNSW_NB15, and CICIDS2017 datasets, which are well known and extensively utilized semi-structural datasets, were obtained and prepared for training and testing the performance of the applied models. The performance of all models was assessed across these three datasets, allocating 75% of the data for training and 25% for testing. This training-to-testing ratio was maintained consistently, taking into account the distribution of normal and attack records in each dataset, as illustrated in Table V.

The datasets: KDD99, 10 UNSW_NB15, and CICIDS2017 are balanced using different combinations of 11 oversampling and under-sampling techniques to improve false negative rates. Suitable 12 performance metrics have been used to obtain significant output improvements in all 13 for the three dataset types using the EG Boosting classifier.

The dataset is severely imbalanced among classes, with the DOS (Denial of Service) attack class dominating at 79% of the total samples. KDD99 multiclass dataset has been 5 used with five classes. The normal class accounts for 20% of the dataset, making it the second most prevalent class. The remaining classes (Probe, R2L, and U2R) collectively contribute only 1% to the dataset.

The second dataset is the UNSW_NB15 with 10 classes. It is different from KDD99 12 dataset not only in the number of classes, but also in class ratios as the normal data is 13

TABLE IV
IG WITH ALL FEATURES 41 IG TRAIN 75% TEST 25%

MODEL	ACCURACY	ERROR RATE	TRUE POSITIVE RATE	FALSE POSITIVE RATE	PRECISION	RECALL	F1 SCORE
Bagging	0.870	0.130	0.981	0.070	0.981	0.981	0.981
MLP	0.976	0.024	0.978	0.008	0.998	0.978	0.988
LR	0.991	0.009	0.988	0.039	0.991	0.988	0.989
RF	0.990	0.004	0.993	0.002	0.993	0.992	0.992
EG Boosting	0.997	0.003	0.998	0.001	0.999	0.998	0.999

TABLE V
NUMBER OF NORMAL AND ATTACK RECORDS IN TRAINING AND TESTING SETS

	DATASET	TYPE	TOTAL CLASSES
1	KDD99	Normal	97,278
	Total: 494,021	Attack	396,743
2	UNSW–NB15	Normal	93,000
	Total: 257,673	Attack	164,673
3	CIC—IDS2017	Normal	413,483
	Total: 1,042,557	Attack	629,074

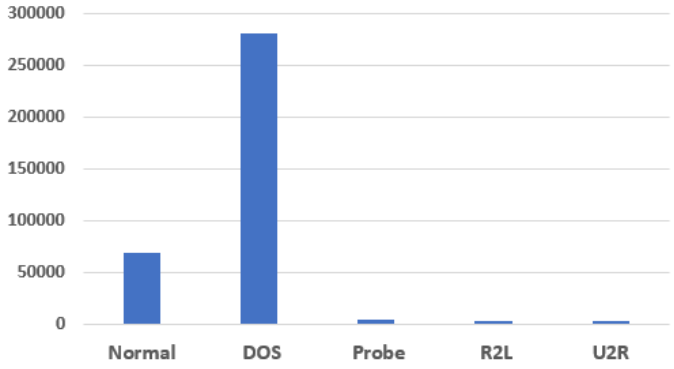

Fig. 2. Imbalanced KDD99 Dataset.

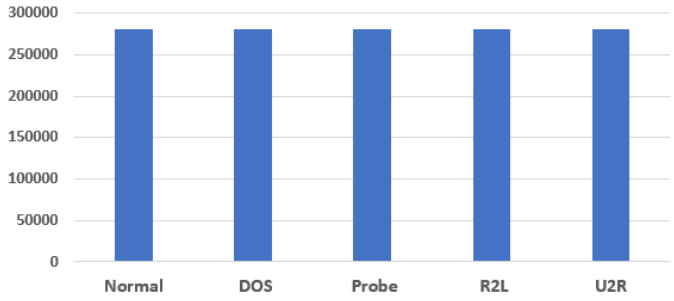

Fig. 3. Balanced KDD99 Dataset.

the first highest major class with a ratio of 36%. The dataset consists of 10 classes, each representing different types of network traffic. The Normal class is the most prevalent, with 93,000 samples, accounting for 36.09% of the total dataset. The Generic class is the second largest, with 58,871 samples, making up 22.84% of the dataset. Other classes such as

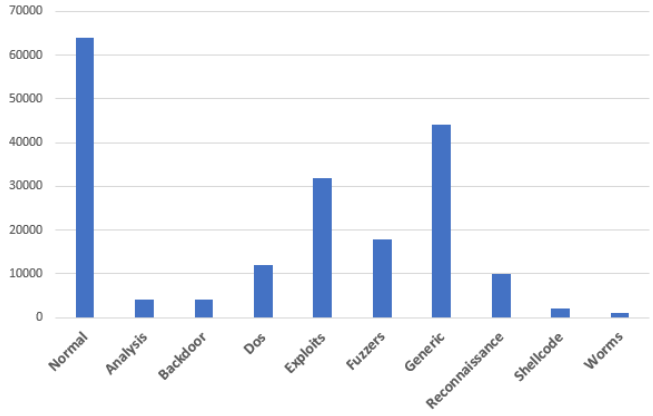

Fig. 4. Imbalanced UNSW_NB15 Dataset.

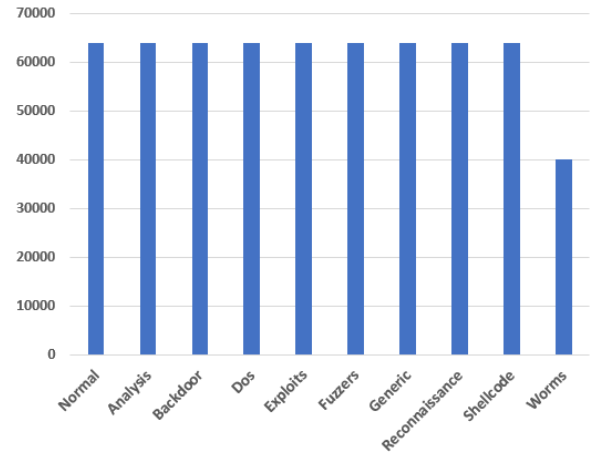

Fig. 5. Balanced UNSW_NB15 Dataset.

Analysis, Backdoor, DoS, Exploits, Fuzzers, Reconnaissance, Shellcode, and Worms contribute to the dataset with varying sample counts and ratios.

The CICIDS2017 multiclass dataset used in this work is completely different from the two previous datasets in having half of the records as normal ones. The highest attack class ratios for DoS Hulk, PortScan and DDoS, are 20%, 14% and 11% respectively The dataset comprises 15 classes, each representing different types of network attacks or benign traffic. The BENIGN class is the most predominant, with 557,646 samples, accounting for 50% of the total dataset. This class represents normal network traffic. Among the attack classes, DoS Hulk has the highest ratio, with 231,073 samples,

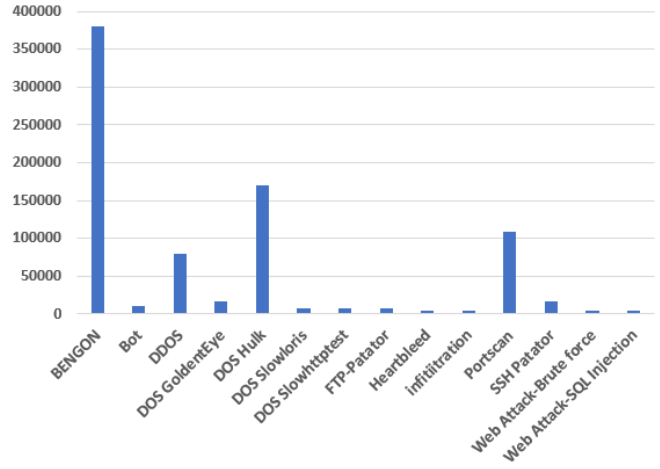

Fig. 6. Imbalanced CICIDS2017 dataset.

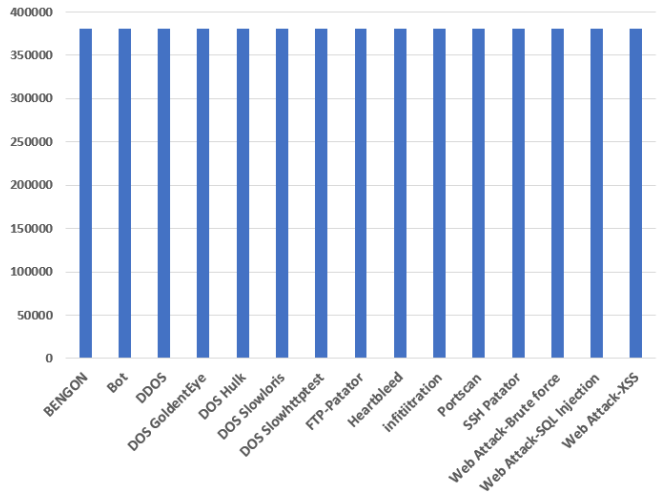

Fig. 7. Balanced CICIDS2017 dataset.

making up 20.71% of the dataset. This indicates a significant presence of DoS Hulk attacks in the dataset. Other notable attack classes include PortScan with 158,930 samples (14.25% of the dataset) and DDoS with 128,027 samples (11.47% of the dataset).

The focus of this study is on three severely imbalanced multiclass datasets: KDD99, UNSW_NB15, and CICIDS2017, which are crucial for ensuring the security of communication networks. To enhance the performance of the ensemble classifier, two key factors are addressed: dataset balancing techniques and appropriate performance metrics. Initially, the dataset is balanced, followed by a decision regarding the importance of positive classes (i.e., attack classes). If positive classes are deemed more important, FN and FP are assessed to determine the appropriate F-beta calculation measure. The Fβ-measure, an extension of the F-measure, incorporates a beta coefficient to adjust the balance between precision and recall. In this study, β value of 1 is used, indicating equal importance of precision and recall.

The SMOTE and Tomek Links approach is employed to balance the KDD99 dataset, combining oversampling of minority classes with removal of majority class instances using Tomek Links. Figures 2 and 3 shows the imbalanced and balanced KDD99 dataset. Similarly, the UNSW_NB15 dataset is balanced using a combination of SVM and SMOTE techniques, with SVM identifying support vectors near minority class instances for synthesizing new instances, as shown in Figures 4 and 5. Finally, the CICIDS2017 dataset is balanced using SMOTE and ENN, where misclassified instances are identified using k-nearest neighbors and eliminated. All attack classes are oversampled to match the number of instances in the majority class, while the number of instances in the normal class is reduced to maintain balance, as shown in Figure 6 and 7.Dataset balancing techniques like SMOTE, Tomek Links, and ENN improved the performance of the classifiers, especially the Extreme Gradient Boosting and Random Forest models. The accuracy of models like Bagging, Multi-layer Perceptron, Logistic Regression, Extreme Gradient Boosting, and Random Forest improved after feature selection using Information Gain and Pearson correlation methods.

TABLE VI
PRECISION METRICS OF MODELS USING KDD99 BALANCED DATASET

MODEL	NORMAL	DOS	PROBE	R2L	U2R
Bagging	100%	100%	100%	99%	43%
MLP	97%	96%	85%	90%	0%
LR	87%	84%	30%	0%	0%
RF	100%	100%	100%	98%	67%
EG Boosting	100%	100%	100%	98%	75%

TABLE VII
RECALL METRICS OF MODELS USING KDD99 BALANCED DATASET

MODEL	NORMAL	DOS	PROBE	R2L	U2R
Bagging	100%	100%	100%	95%	67%
MLP	95%	98%	93%	20%	0%
LR	93%	92%	90%	0%	0%
RF	100%	100%	100%	96%	67%
EG Boosting	100%	100%	100%	98%	67%

TABLE VIII
F1 SCORE METRICS OF MODELS USING KDD99 BALANCED DATASET

MODEL	NORMAL	DOS	PROBE	R2L	U2R
Bagging	100%	100%	100%	97%	52%
MLP	96%	97%	89%	30%	0%
LR	90%	88%	14%	0%	0%
RF	100%	100%	100%	98%	67%
EG Boosting	100%	100%	100%	99%	71%

The results of models classifier using KDD99, UNSW_NB15, and CICIDS2017 datasets are presented and the goal is multiclass classification for balanced datasets. The Tables VI, VII, VIII, IX showa the performance measure of the models used for KDD99 balanced dataset.

The Table X shows the accuracy result of the applied models for using UNSW_NB15 for balanced Dataset. Also, Table XI shows the accuracy result of the applied models for using CICIDS2017 for balanced Dataset.

TABLE IX
ACCURACY METRICS OF MODELS USING KDD99 BALANCED DATASET

	MODEL	ACCURACY
1	Bagging	99.81%
2	MLP	95.19%
3	LR	84.16%
4	RF	99.88%
5	EG Boosting	99.89%

TABLE X
ACCURACY OF MODELS USING UNSW_NB15 BALANCED DATASET

	MODEL	ACCURACY
1	Bagging	98.35%
2	MLP	96.78%
3	LR	97.32%
4	RF	98.61%
5	EG Boosting	98.81%

TABLE XI
ACCURACY OF MODELS USING CICIDS2017 BALANCED DATASET

	MODEL	ACCURACY
1	Bagging	74.47%
2	MLP	72.64%
3	LR	69.73%
4	RF	73.40%
5	EG Boosting	77.46%

Table XI presents results that show that the intrusions are truly difficult to classify with the CICIDS2017 dataset for several reasons. First, they are truly diversified and the CICIDS2017 dataset has a very diverse set of attack classes with different frequencies of samples. Indeed, even though oversampling was used to balance the dataset, the base features of the dataset such as the fact that multiple classes may be present in a sample and nuanced differences in attack behaviors make classification challenging. Second, some models including LR and MLP could not handle these complexities well because of the inadequacy of the models in dealing with such multi-class imbalanced nature and the complex patterns linked to them. They usually yield more accurate results for the dominating classes and do not differentiate too well between localities of different categories, hence yielding low global accuracy.

On the other hand, models such as Extreme Gradient Boosting (EG Boosting) were seen to perform slightly better than the rest through ensemble learning whereby imbalance and higher intricateness were well managed capturing high accuracy compared to the others. Indeed, the characteristic of the used dataset is close to the real world traffic making it challenging to achieve high classification rates on all types of attacks per se. These results sincerely indicate the importance of refining the existing model and advanced data cleansing methods to obtain better accuracy on confusing data sets like CICIDS2017.

The accuracy metrics reveal varying performance levels of different models across three balanced datasets. In the KDD99 dataset, Bagging, Random Forest (RF), and EG Boosting demonstrate exceptionally high accuracies, exceeding 99%, indicating robust performance in intrusion detection. Conversely, in the UNSW_NB15 dataset, all models exhibit high accuracy, with EG Boosting achieving the highest accuracy of 98.81%. However, in the CICIDS2017 dataset, while Bagging and EG Boosting maintain relatively high accuracies, the performance of MLP, LR, and RF models diminishes, suggesting challenges in effectively classifying intrusions within this dataset.

Metrics like precision and recall showed improvement for the proposed meta-ensemble learning model compared to Random Forest and Extreme Gradient Boosting. The results of the classifier Extreme Gradient Boosting, Random Forest, Bagging, Multilayer Perceptron, and Logistic Regression are highlighted for each dataset (KDD99, UNSW_ NB15, and CICIDS2017) in terms of accuracy, precision, recall, and F1 score.

V. CONCLUSION

With the advancements noticed in intrusions and attacks, machine learning-based classification has become a necessity where this study locates itself to increase the performance of intrusion detection systems. In the scope of this work, many binary and multiclass classifiers based on rules, distances and probability approaches have been realized using three widely used semi-structural datasets with different scenarios of imbalanced datasets. The findings related to the most commonly used evaluation metrics that have been applied to evaluate the classifiers, supported by tables and figures throughout the thesis and the results are summed up in the following three sections. Utilizing binary datasets for designing classifiers and unbalanced multiclass datasets for real-world simulation. Feature selection methods such as Information gain, Pearson correlation, and f-test aid in reducing input feature dimensions and improving model efficiency. The results underscore the significance of dataset balancing techniques, particularly in severely imbalanced datasets like KDD99, UNSW_NB15, and CICIDS2017.

Moreover, the study sheds light on the importance of appropriate performance metrics tailored to the specific needs of intrusion detection, considering factors such as false negatives and false positives. By employing techniques like SMOTE, Tomek Links, and ENN, the study demonstrates significant improvements in model performance, particularly in mitigating false negatives.

Overall, this research contributes valuable insights into the development of effective intrusion detection systems, essential for safeguarding communication networks against evolving cyber threats. The findings underscore the potential of machine learning-based approaches in fortifying network security and pave the way for further advancements in the field.

REFERENCES

[1] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing iot network security through deep learning-powered intrusion detection system," *Internet of Things*, vol. 24, p. 100936, 2023.

[2] A. K. Bediya and R. Kumar, "A novel intrusion detection system for internet of things network security," in *Research anthology on convergence of blockchain, internet of things, and security*. IGI Global, 2023, pp. 330–348.
[3] N. O. Aljehane, H. A. Mengash, M. M. Eltahir, F. A. Alotaibi, S. S. Aljameel, A. Yafoz, R. Alsini, and M. Assiri, "Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security," *Alexandria Engineering Journal*, vol. 86, pp. 415–424, 2024.
[4] L. M. Da Silva, I. G. Ferrão, C. Dezan, D. Espes, and K. R. Branco, "Anomaly-based intrusion detection system for in-flight and network security in uav swarm," in *2023 International Conference on Unmanned Aircraft Systems (ICUAS)*. IEEE, 2023, pp. 812–819.
[5] R. Sabitha, S. Gopikrishnan, B. Bejoy, V. Anusuya, and V. Saravanan, "Network based detection of iot attack using ais-ids model," *Wireless Personal Communications*, vol. 128, no. 3, pp. 1543–1566, 2023.
[6] I. Ioannou, P. Nagaradjane, P. Angin, P. Balasubramanian, K. J. Kavitha, P. Murugan, and V. Vassiliou, "Gemlids-miot: A green effective machine learning intrusion detection system based on federated learning for medical iot network security hardening," *Computer Communications*, vol. 218, pp. 209–239, 2024.
[7] J. G. Almaraz-Rivera, J. A. Cantoral-Ceballos, and J. F. Botero, "Enhancing iot network security: Unveiling the power of self-supervised learning against ddos attacks," *Sensors*, vol. 23, no. 21, p. 8701, 2023.
[8] A. A. Putri, C. Agustina, H. Fauzan, M. R. E. Saputra, M. Erdiansyah, and P. S. Wardani, "Network security implementation with snort-based intrusion detection system using windows 10," *JComce-Journal of Computer Science*, vol. 1, no. 1, 2023.
[9] M. G. Haricharan, S. P. Govind, and C. V. Kumar, "An enhanced network security using machine learning and behavioral analysis," in *2023 International Conference for Advancement in Technology (ICONAT)*. IEEE, 2023, pp. 1–5.
[10] O. H. Abdulganiyu, T. A. Tchakoucht, and Y. K. Saheed, "Towards an efficient model for network intrusion detection system (ids): systematic literature review," *Wireless Networks*, vol. 30, no. 1, pp. 453–482, 2024.
[11] G. S. C. Kumar, R. K. Kumar, K. P. V. Kumar, N. R. Sai, and M. Brahmaiah, "Deep residual convolutional neural network: an efficient technique for intrusion detection system," *Expert Systems with Applications*, vol. 238, p. 121912, 2024.
[12] H. Alkahtani and T. H. Aldhyani, "Intrusion detection system to advance internet of things infrastructure-based deep learning algorithms," *Complexity*, vol. 2021, no. 1, p. 5579851, 2021.
[13] N. S. Khudhair, "Competence in cybercrime: A review of existing laws," *Revista Geintec-Gestao Inovacao e Tecnologias*, vol. 11, no. 4, pp. 1950–1969, 2021.
[14] P. L. Indrasiri, E. Lee, V. Rupapara, F. Rustam, and I. Ashraf, "Malicious traffic detection in iot and local networks using stacked ensemble classifier," *Computers, Materials and Continua*, vol. 71, no. 1, pp. 489–515, 2022.
[15] W. A. Alonazi, H. HAMDI, N. A. Azim, and A. Abd El-Aziz, "Sdn architecture for smart homes security with machine learning and deep learning," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 10, 2022.
[16] R. K. Sharma, A. K. Pandey, B. Jayabalan, and P. Naval, "Utilizing machine learning-based intrusion detection technologies for network security," *Proceedings on Engineering*, vol. 6, no. 1, pp. 311–320, 2024.
[17] S. Javanmardi, M. Ghahramani, M. Shojafar, M. Alazab, and A. M. Caruso, "M-rl: A mobility and impersonation-aware ids for ddos udp flooding attacks in iot-fog networks," *Computers & Security*, vol. 140, p. 103778, 2024.
[18] N. Kabilan, V. Ravi, and V. Sowmya, "Unsupervised intrusion detection system for in-vehicle communication networks," *Journal of Safety Science and Resilience*, vol. 5, no. 2, pp. 119–129, 2024.
[19] K. Cengiz, S. Lipsa, R. K. Dash, N. Ivković, and M. Konecki, "A novel intrusion detection system based on artificial neural network and genetic algorithm with a new dimensionality reduction technique for uav communication," *IEEE access*, 2024.
[20] H. Sadia, S. Farhan, Y. U. Haq, R. Sana, T. Mahmood, S. A. O. Bahaj, and A. Rehman, "Intrusion detection system for wireless sensor networks: A machine learning based approach," *IEEE Access*, 2024.
[21] I. Idrissi, M. Azizi, and O. Moussaoui, "A stratified iot deep learning based intrusion detection system," in *2022 2nd international conference on innovative research in applied science, engineering and technology (IRASET)*. IEEE, 2022, pp. 1–8.
[22] N. Dat-Thinh, H. Xuan-Ninh, and L. Kim-Hung, "Midsiot: A multistage intrusion detection system for internet of things," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 9173291, 2022.
[23] A. A. Alsulami, Q. Abu Al-Haija, A. Tayeb, and A. Alqahtani, "An intrusion detection and classification system for iot traffic with improved data engineering," *Applied Sciences*, vol. 12, no. 23, p. 12336, 2022.
[24] I. Ullah and Q. H. Mahmoud, "A technique for generating a botnet dataset for anomalous activity detection in iot networks," in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2020, pp. 134–140.
[25] B. Düzgün, A. Çayır, U. Ünal, and H. Dağ, "Network intrusion detection system by learning jointly from tabular and text-based features," *Expert Systems*, vol. 41, no. 4, p. e13518, 2024.
[26] F. Hang, L. Xie, Z. Zhang, W. Guo, and H. Li, "Research on the application of network security defence in database security services based on deep learning integrated with big data analytics," *International Journal of Intelligent Networks*, vol. 5, pp. 101–109, 2024.
[27] R. Rahim, M. A. Chishti, and M. M. Raheem, "Improving the security of internet of things (iot) using intrusion detection system (ids)," in *2024 21st Learning and Technology Conference (L&T)*. IEEE, 2024, pp. 290–295.
[28] K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "Iot intrusion detection using machine learning with a novel high performing feature selection method," *Applied Sciences*, vol. 12, no. 10, p. 5015, 2022.
[29] K. Roshan, A. Zafar, and S. B. U. Haque, "Untargeted white-box adversarial attack with heuristic defence methods in real-time deep learning based network intrusion detection system," *Computer Communications*, vol. 218, pp. 97–113, 2024.

Abeer Abd Alhameed is a Lecturer at the Departments of Electrical and Biomedical Engineering at the College of Engineering, University of Babylon, Iraq since October 2016. She received her BSc in Electrical Engineering from Al-Mustansiriya University in Baghdad, Iraq, and completed her master's degree in Telecommunication and Networks from Salford University, Manchester, United Kingdom in February 2016 with a distinction degree. She has taught courses in Digital Techniques, Math, and Information Technology and her research interests primarily focus on wireless communication and networks, as well as biomedical engineering. Miss Abeer has several research publications and can be contacted via email: eng.abeer.abd@uobabylon.edu.iq, https://orcid.org/0000-0003-2824-5424, Google Scholar :Abeer Al-Sallami, Research Gate: abeer alsallami, linkedin: Abeer Al-Sallami.

Azhar A. Hadi is a Lecturer at the Department of Electrical Engineering at the College of Engineering, University of Babylon. Received his master's degree in Computer Engineering from the Sharif University of Technology, Tehran, Iran, in 2021. Mr. Azhar research interests include artificial intelligence (AI), deep learning, natural language processing (NLP), and machine learning (ML). He has several research publications in this field. Mr. Azhar can be contacted via email at azhar@uobabylon.edu.iq. His professional profiles and research contributions can be accessed on Google Scholar: Azhar A. Hadi, ResearchGate: Azhar A. Hadi, and LinkedIn: Azhar A. Hadi.

Wasan Hashim Al- Masoody received her Ph.D. degree in Electrical and Computer Engineering from University of Missouri- Columbia, Columbia, Missouri, USA in 2019. While her ME degree was received from the same university in 2018. Before that, she received her M.Sc. degree in Electrical Engineering from the University of Baghdad, Baghdad, Iraq in 2006 and her B.Sc. degree in Electrical Engineering from Al-Mustasiryia University, Baghdad, Iraq in 1994. Currently, she is a faculty member in the Department of Electrical Engineering at the University of Babylon, Babylon. Iraq. Her research interests include wireless communications, convex optimization, and digital signal processing. She can be contacted on email: eng.wasan.hashim.lec@uobabylon.edu.iq.