[1]Shweta Bhardwaj
[2]Seema Rawat
[3]Hima Bindu Maringanti

Network Intrusion Detection System using Hyper Parameter Tuned Weighted XGboost Classifier

Journal of Electrical Systems

Abstract: - Use of Internet of Things is increasing tremendously. With this increase in technologies like smart homes, smart devices and other automation, there is increase in malicious attacks. It is important to handle network security. Network intrusion detection system is vital to protect IoT devices from various malicious attacks. It includes dimensionality reduction, feature selection and classification. The dimensionality reduction is performed using principal component analysis (PCA) and the feature selection is accomplished using Ant Colony Optimization(ACO). Then, the classification is performed with the Extreme Gradient Boost Algorithm (XG-Boost). Benchmarked intrusion detection NSL-KDD dataset is being used and implementation is done on Colaboratory using Python. The system showed 98.2% accuracy, 99.2% precision, 97.1% recall and 98.1% F1-score, which are better than the existing intrusion detection system. The system proves to be robust based on experimental results in terms of evaluation of various performance metrics.

Keywords: Internet of Things, Intrusion detection system, XGBoost, NSL-KDD, ACO, Anomaly Detection.

I. INTRODUCTION

In today's interconnected digital environment, the prevalence of cyber threats poses significant challenges to the security and integrity of information frameworks. As organizations become progressively dependent on digital technology to conduct business and manage sensitive data, the need for robust intrusion detection systems (IDS) increases. It's becoming more and more important. Intrusion detection systems serve as the first line of defence against unauthorized access, malicious activity, and potential breaches, giving organizations the ability to monitor, detect, and react to security incidents in real time.

Over the years, advances in machine learning, artificial intelligence, and cybersecurity technologies have led to significant advances in the development and improvement of intrusion detection systems. These advances have paved the way for the emergence of advanced IDS solutions that can detect and mitigate a wide range of cyber threats, from traditional network intrusions to sophisticated evasive attacks [19-21].

This paper provides a comprehensive overview of recent advances in intrusion detection systems and highlights the various methods, techniques, and technologies used to improve detection accuracy, efficiency, and effectiveness. By surveying current literature and research, we aim to provide insight into the current state of intrusion detection and identify key challenges, trends, and new research directions [22-24].

The IDS for IoT was reviewed in this paper [1, 7]. The study picked articles related to IDS tactics from the literature. As a result, the study created a taxonomy with the goal of categorizing these works. It was carried out in accordance with the validation strategy, IDS placement plan, and security threat. The study also discovered that IoT IDS techniques are still being developed [25-27].

As a result, a wide range of IoT devices and significant attacks have not been addressed by the suggested solutions. Furthermore, it is unclear what placement and detection methods are suitable for Internet of Things devices [28,29]. Therefore, additional research is needed in order to extend in many domains. It must analyze the shortcomings and merits of various placement and detection strategies. It must also improve the range of attack detection and address a variety of IoT technologies. In order to increase security, the study should also concentrate on improving validation schemes and creating a variety of applications, such as autonomic management and alert correlation systems [2, 8].

The development of IoT technology recently has made it possible to create intelligent settings. On the basis of the IoT concept, privacy and security are seen as the two main issues in any smart environment. As a result, this work [3, 9] investigates an overview of the most current IDSs that have been presented with a focus on similar traits, mechanisms, and methodologies. This study also provides a thorough understanding of how IoT engineering, security vulnerabilities, and their relationships to IoT architectural layers are all changing over time. Although this study illustrates prior research on IDS design and implementation for the IoT, it is difficult to suggest an IDS that is efficient, reliable, and robust. Therefore, a number of actions must be made soon to correct this. Future work may examine how to construct hybrid IDS with effective performance, particularly for IoT-based contexts. Additionally, the IDS has not yet been applied to FPGAs, which are programmable hardware

[1] *Corresponding author: Shweta Bhardwaj, sbhardwaj1@amity.edu
[1]Department of Computer Science & Engineering Amity University Uttar Pradesh Noida, India
[2]Department of Information Technology Amity University Uttar Pradesh Noida, India
[3]Department of Computer Science and Applications North Orissa University, Baripada Odisha, India

devices. This makes it easier to adjust surroundings based on IoT. The design must also be suitable for both distributed and centralized placement schemes. It has the ability to recognize a variety of attacks. Additionally, several attack types target IDSs as detection and prevention techniques in the TL (Transportation Layer) of IoT networks.

Additionally, the job of AD (Anomaly Detection) in IDSs is particularly difficult. Robust classifier model is needed with the capacity to recognise a variety of attack kinds. In order to categorise threats occurring in the Internet of Things network, this study [4, 10] addressed the DNN (Deep Neural Network). Three different datasets in a wireless and wired setting are used to evaluate the suggested methodology. Additionally, DNN combined with the GS (Grid Search) method has been utilised to find the best parameter settings for each dataset. The empirical results demonstrate the effectiveness of the suggested DNN-based scheme in terms of false alarm rate, accuracy, recall, and precision. The findings also suggest that different methodologies and datasets be used in AD research. Furthermore, because there is no way to improve the performance of the classifier, the study [5, 6, 11] must concentrate on a few classification problems such biased findings, unbalanced datasets, and so on. Additionally, this work offered the ICVAE DNN (Improved Conditional Variational Auto Encoder) intrusion detection method. This method can learn and investigate the potential sparse demonstrations between network categories and data attributes, making it appropriate for large datasets. However, this study needs to be expanded. The purpose of this study was to investigate effective ways to improve attack identification performance in relation to unidentified and minority attacks. The spatial distribution of the latent variables of the ICVAE must be displayed in this study using the adversarial learning technique. Moreover, the study [12] have not used any feature selection techniques. Our study introduced a novel feature selection technique to select relevant features for classification.

II. RELATED WORK

Recently, network trafficking has increased drastically and various models have been implemented in intrusion detection. Some of them are reviewed in this section. H. Liu and B. Lang (2019), provide an overview of machine learning and deep learning techniques for intrusion detection systems. Various techniques, algorithms, and approaches are in the context of IDS, using both traditional machine learning techniques and deep learning techniques. This study proposes a technique to improve the conditional variational autoencoder and deep neural network performance for intrusion detection categorization. It most likely makes improvements to the methods used now to find intrusions more successfully [5]. This research presents a network intrusion detection technique that combines generative adversarial networks (GANs) and one-dimensional convolutional neural networks (CNNs) with a conditional Wasserstein variational autoencoder. In order to enhance network traffic intrusion detection, it proposes a special approach that combines these techniques [6].

This article gives a general introduction of intrusion detection in the Internet of Things (IoT). It probably talks about different methods of detecting intrusions and issues unique to IoT settings [7]. This paper offers a survey on learning-based network intrusion detection for Internet of Things security. It investigates various machine learning and other learning-based techniques for identifying breaches in Internet of Things networks [8]. This paper gives an overview of IDS (intrusion detection systems) for Internet of Things-based smart settings is given in this study. It probably talks about several intrusion detection techniques designed for IoT-enabled smart settings [9].

This research applies a deep learning approach to the analysis of attack classification in IoT networks. It probably goes over how deep learning methods can be used to efficiently classify attacks in Internet of Things networks [10]. In this paper, machine learning-based intrusion detection systems for Internet of Things applications are covered. It probably investigates how different machine learning techniques can be used to identify intrusions in Internet of Things networks [11].

This paper is a study of traffic accident detection and classification. It proposes a real-time computer vision-based approach for. The system aims to recognize and classify traffic incidents using computer vision technology enabling swift responses and preventive measures. This approach is anticipated to enhance traffic control and uphold safety on roads. The research introduces a data analysis method, for forecasting the performance of high school students done on a case study conducted in Saudi Arabia. Data mining methods are applied in this investigation to identify the elements influencing student educational achievements [13].

Educators can use this data to create customized support strategies and interventions to improve student performance [14]. The article discusses an online learning method based on LSTM networks, known for their ability to model sequential data. These networks are utilized in developing online learning algorithms that can accommodate changing data streams. The study focuses on learning techniques, for intrusion detection systems with an anomaly centric approach presenting a taxonomy of deep learning methods their applications and unresolved research questions [15,16].

Two intrusion detection systems are articulated in this paper. One utilizing deep neural networks and integrated unsupervised feature learning and the other using standard machine learning techniques are presented. This work addresses the benefits and drawbacks of every strategy and sheds light on how well it works [17]. The class imbalance issue in intrusion detection systems is addressed by this research with a Siam-IDS technique that

makes use of Siamese neural networks. It talks about how this network architecture solves the imbalance issue that frequently arises in real-world datasets, helping to increase IDS performance [18].

Such algorithms are important in a variety of applications that require real-time analysis and decision-making, such as online prediction and classification tasks.

III. METHODOLOGY

NSL-KDD dataset was utilised to evaluate the system. The dataset is initially loaded and pre-processed. Direct input of the dataset into the dimensionality reduction is not possible. Due to the possibility that the original dataset may be huge in size and contain some undesirable and useless data. The prediction rate could be impacted by this. As a result, the dataset undergoes pre-processing before dimensionality reduction is applied to the pre-processed data. The data's dimension is decreased via the dimensionality reduction. Principal component analysis was used in this study to achieve dimensionality reduction, removing correlated variables that have no bearing on the decision-making process. It also advocates limiting the amount of features to solve the issue of data over-fitting. The feature selection procedure is carried out after the dimensionality reduction procedure [13,14].

The data is originally generated by the ant colony optimisation, which then examines each position of the data. If the data is relevant, the subsets are gathered; if not, the next piece of data is chosen for evaluation until the subset is gathered. Following the collection of the subset, a decision to end the procedure is made. The subset is returned if the data from the collected subset are the best and most pertinent; otherwise, the pheromones are modified, and the process is repeated until the system has the best subset. Following feature selection, the chosen features are picked at random for training and testing. In this, 80% of the data are used for training and 20% for testing. The categorization process then uses the trained and test findings. The XG-Boost classifier is used in this system to perform the classification. It is a well-known supervised learning technique used for regression and classification on sizable datasets. It employs an incredibly scalable training process that avoids over-fitting issues and a short decision tree that is created incrementally to produce accurate results. After the training of the classification findings, prediction phase is calculated. In either case, the intrusion is detected at the forecast stage. Next, the performance metrics of the proposed system- precision, accuracy, recall and F1-score are measured in order to evaluate its efficacy.

This methodology describes how to evaluate network intrusion detection systems using the NSL-KDD dataset. The NSL-KDD dataset, which is widely used to evaluate intrusion detection systems, is first loaded and preprocessed in order to obtain best performance during evaluation. Data cleaning and normalization are two preprocessing steps that are carried out to prepare the dataset for analysis.

After preprocessing, we utilize dimensionality reduction techniques to reduce the number of features in the dataset. This is essential, especially when working with complicated and large datasets, to manage computational complexity and reduce the likelihood of overfitting. This publication notably mentions principal component analysis (PCA) as the preferred technique for dimensionality reduction.

We look up for factors associated and removing variables that do not contribute to any decision making using PCA, Principal Component Analysis. Feature selection is done after dimensionality reduction. We find the most suitable features from the dataset to attain feature selection that helps in doing further data analysis. ACO, Ant Colony Optimization algorithm is used for feature selection. Repeatedly, we assess a subset of most relevant features for intrusion detection and eliminates less useful features. Post feature selection, dataset is split into a training set and a test set.

Classification model is trained using a training set that comprises 80% of the data; the remaining 20% of the data is comprises for model performance testing. This ensures accurate finding of the model's efficacy in detecting intrusions. XGBoost classifier, a supervised learning algorithm is well known for its accuracy and scalability, is used to for classification. An ensemble of decision trees is iteratively done using XGBoost, with each tree improving over the preceding tree. Overfitting problems are reduced using this method giving an optimum result. The trained XGBoost classifier model is used in the prediction whether attack is normal or intrusion.

System performance is calculated by finding precision, recall, F1 score, and accuracy. These metrics shed light on how well the system detects and categorizes intrusions while reducing false alarms and false negatives.

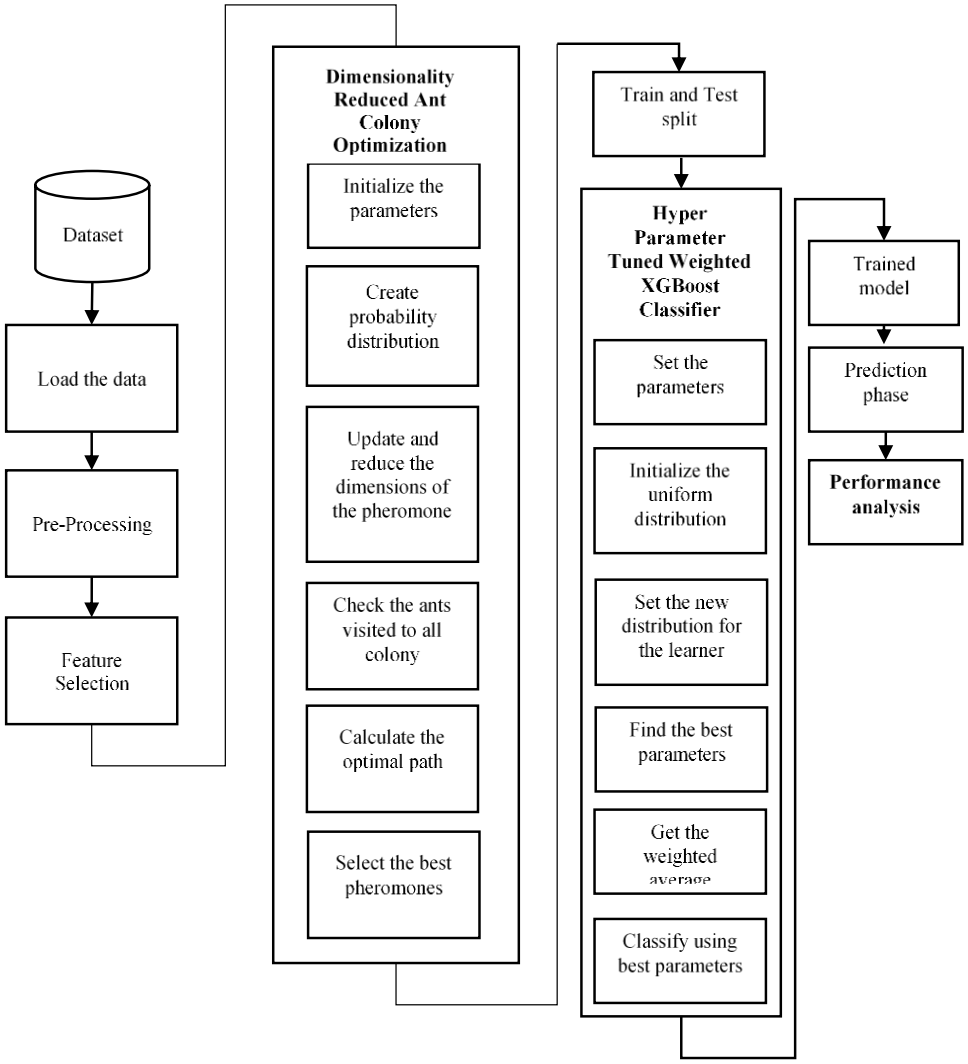

Fig.1. Overall view of the system

Dimensionality Reduced Ant Colony Optimization (DR-ACO)

Dimensionality Reduced Ant Colony Optimization is meta-heuristic stochastic based methodology which utilizes artificial ants for determining resolutions to combinatorial optimization issues. Moreover, the idea behind ACO is to determine the shortest distance from their corresponding nests to the food sources. The ants retain certain chemical substance named pheromone to permit interactions amongst the ants. When an ant moves, it retains a steady pheromone so that it can be followed by other ants. The individual ants travel in a random way. At the same time, when a particular ant finds a pheromone line, it has to make decision whether to follow it or not. When the ant tracks the path, the ant's personal pheromone reinforces the present track. As the pheromone enhances, the chance that the succeeding ant will choose the same path will also enhance. Hence, as the ants traveling in a path increases, the path gains attraction for the succeeding ants. Thus, the ant utilizing the shortest path to a food-source has high chances of returning soon. This study used DR-ACO to select only the relevant features for classification.

Dimensionality Reduced Ant Colony Optimization (DR-ACO) is a state-of-the-art metaheuristic stochastic methodology designed to leverage the power of artificial ants to solve combinatorial optimization problems. DR-ACO is based on the concept of ant behaviour and is inspired by nature's efficient foraging strategies, particularly the ant's ability to find the shortest route from its nest to its food source. Central to the ACO framework is the use of chemicals called pheromones, which facilitate communication and interaction between ants within a colony. Ants create a path for other ants to follow by releasing pheromone. The system makes it possible for groups to make decisions and make it very convenient to identify features using DR-ACO. pheromone trails are being followed by all the ants over the solution space based on the number of features and ant can decide whether or not to follow a pheromone trail. The ant follows the pheromone trail along the path to find the food source and also motivating other ants to follow the pheromone trail. DR-ACO follows most relevant features from the

data set for feature selection and classification by using this efficient model we can do the classification using this efficient feature selection.

Hyper Parameter Tuned Weighted XGBoost Classifier (HP-WXC)

New XGBoost Classifier is an ensemble machine learning (ML) method which is based on decision trees (DT) that uses a gradient-boosting framework. It is a precise and adjustable gradient-boosting machine. It is confirmed that this approach pushes the computational power limits of boosted-tree algorithms. It is designed to improve both model performance and computational speed. This is a useful approach for regression predictor modeling and classification problems. Additionally, there are a wide range of hyper-parameters, which provide a fine-grained control over the model training process.

Machine getting to know has superior considerably with the advent of the XGBoost classifier, particularly in the region of ensemble procedures based totally on decision trees. Its use of a gradient boosting framework, which will increase accuracy and scalability, makes it stand out as a robust device.

This approach is the most desired for computing energy as it has proven to push the computational obstacles of boosted tree algorithms. Large data units may be processed efficiently with the XGBoost classifier on account that it's meticulously advanced to maximise computing pace and decorate model performance. Its adaptability allows it to perform an extensive range of class and regression predictive modeling responsibilities with constant and dependable outcomes.

A wide variety of hyperparameters offered by means of the XGBoost classifier additionally permit users to have best-grained manipulate over the model schooling procedure, permitting the introduction of specific and superior model configurations for certain instances.

The suggested framework was estimated for the expected structure using the NSL KDD benchmark dataset [17]. An improved version of the KDD'99 dataset is called NSL-KDD. This dataset serves as a successful benchmark to assist researchers compare different intrusion detection techniques. Furthermore, both the test and train sets have good records. NSL-KDD datasets are used because they do not accept redundant data in the training set, which could lead to a bias in the classifier's favour of more frequent records. The approach, which has increased detection rates on the frequent records, did not negatively impact learner performance because the introduced testing set has no identical records. There are 22 different kinds of cyberattacks in the NSL-KDD dataset, which are separated into four classes probing attack (PROBE), Denial of Service (DoS), User to Root (U2R) and Root to Local (R2L). The NSL-KDD consists of three nominal values such as User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP).

Features in NSL-KDD dataset

Sr. No.	Feature	Sr. No.	Feature	Sr. No.	Feature
1	Duration	15	Su attempted	29	Same srv rate
2	Protocol type	16	Num root	30	Diff srv rate
3	Service	17	Num file creations	31	Srv diff host rate
4	Flag	18	Num shells	32	Dst host count
5	Source bytes	19	Num access files	33	Dst host srv count
6	Destination bytes	20	Num outbound cmds	34	Dst host same srv rate
7	Land	21	Is host login	35	Dst host diff srv rate
8	Wrong fragment	22	Is guest login	36	Dst host same src port rate
9	Urgent	23	count	37	Dst host srv diff host rate
10	Hot	24	Srv count	38	Dst host serror rate
11	Number failed logins	25	Serror rate	39	Dst host srvserror rate
12	Logged in	26	Srvserror rate	40	Dst host rerror rate
13	Num compromised	27	Rerror rate	41	Dst host srvrerror rate
14	Root shell	28	Srvrerror rate	42	Class label

IV. RESULTS

NSL-KDD contains around 60-80% of information focuses classified as normal network traffic. The remaining 20-40% of the information talks about different attack types. NSL-KDD is divided into diverse categories.

Denial-of-Service (DoS): These attacks point to disturb a system, making it inaccessible to legitimate users.

Probe: These attacks assemble data approximately a framework or arrange vulnerabilities.

User-to-Root (U2R): These attacks point to pick up unauthorized root.

Remote-to-Local (R2L): These attacks permit an unauthorized client to pick up control over a neighbourhood framework.

Following are the attack count in the NSL-KDD dataset with their labels as shown in Figure 2.

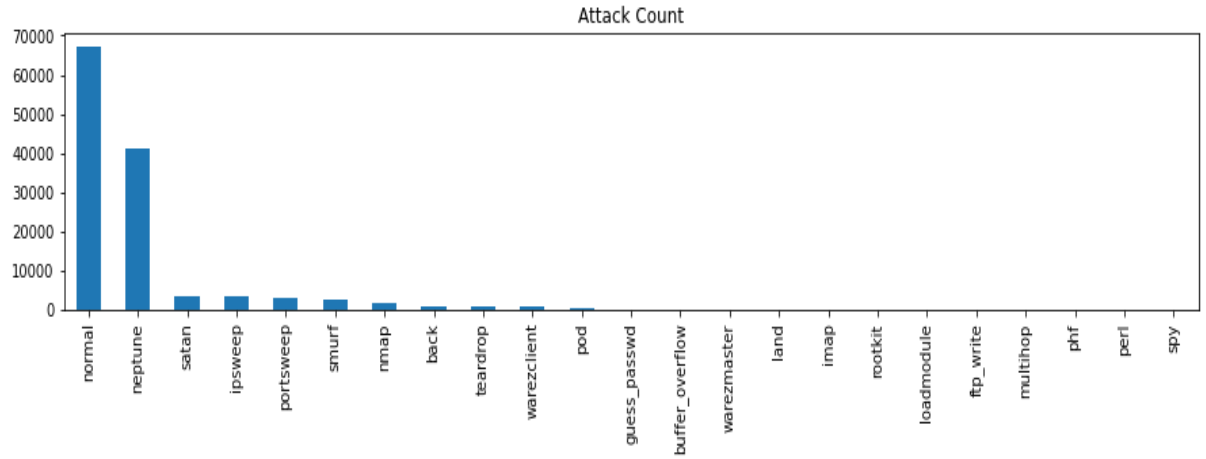

Fig.2. Attack Count

After plotting the attack count graph, separating the labels into Attack and Normal.

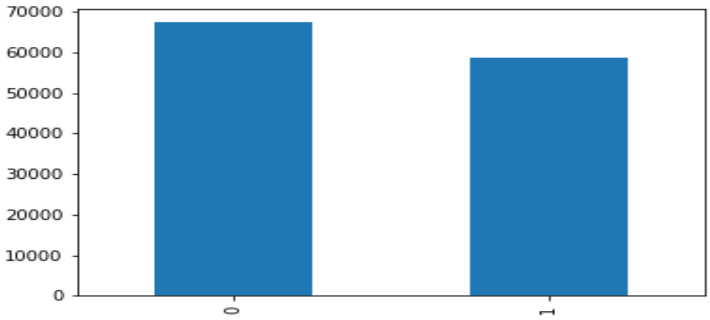

Fig.3. Separating the labels into Attack and Normal

In the above Figure 3, the graph depicts 0 representing Normal traffic and 1 representing Attack.

The confusion matrix stands as the primary metric commonly utilized to assess the effectiveness of an Intrusion Detection System (IDS). From this matrix, numerous metrics can be extracted, encompassing accuracy, precision, detection rate, recall, F-score, false alarm rate (FAR), receiver operating characteristic (ROC) curve, and area under the curve (AUC). [16]. True positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) are the four main components of the confusion matrix depicted in Figure 4. Correct classifications of attack and normal records are written as TP and TN, respectively. Whereas FN depicts an attack record that was mistakenly classified as normal, FP depicts a normal record that was mistakenly classified as an attack.
Confusion matrix is an important tool for evaluating classification models, providing a comprehensive analysis of performance across multiple categories. To provide a comparison of model predictions with actual scores to help clearly understand the model function and any errors. The confusion matrix is organized in rows and columns, with predicted class labels for each column and class score itself for each character. If the expected squares match the actual squares, the correct predictions are represented by the main diagonal of the calculation. Misclassification where the expected class differs from the actual class is represented by rejected items. Generally, the confusion matrix has four main parts. Cases where the model accurately predicts the positive class are known as true positives (TP). True positives are determined by the model's ability to accurately identify 100 examples of a given class as belonging to that class. Cases where the model accurately predicts the negative class are known as true negatives (TN).
For instance, 200 cases out of 250 examples that the model accurately classifies as not belonging to a specific class are counted as true negatives. False Positives (FP) are instances in which the model forecasts the positive class erroneously. For instance, 20 instances that do not fit into a specific class are considered false positives if the model misidentifies them. False Negatives (FN): These are instances in which the model forecasts the negative class inaccurately. False negatives are produced, for instance, when the model mistakenly reports 30 instances as not belonging to a specific class when in fact they do.
The confusion matrix can be used to compute a number of performance indicators that offer information on the model's efficacy once it has been created. The confusion matrix yielded the following important metrics:
Accuracy: The proportion of correctly classified cases relative to the total number of cases
as (TP+TN)/(TP+TN+FP+FN) when calculated.

Precision: The proportion of real positives among all cases the model classifies as positive, in the form of TP/(TP+FP).
Recall rate: The percentage of actual positive cases that the model accurately recognized as true positives, in the form of TP/(TP+FN).
F1 score: A balanced indicator of classifier performance that is derived from a harmonic average of precision and recall as 2*(Precision * Recall)/(Precision Recall) is calculated.
These metrics contribute to a more complete understanding of model performance by considering both the overall accuracy of a model (precision) and the ability to correctly classify observations (recall, accuracy).
In addition to information on model performance, confusion matrices help to identify areas that need modeling. Researchers and experts can identify patterns and trends in data that models may miss by looking at misclassifications (false positives and false negatives) This allows you to increase performance and generalizability through intentional adjustments build on it in your model architecture, feature selection, or training program. Actual and expected classes are represented by basic properties of the confusion matrix.
1)True Positive (TP) - Attack data that has been accurately classified as such.
2)False Positives (FPs): Typical data that is incorrectly classified as an attack.
3)True Negative (TN): Represents normal data with accuracy.
4) False Negative (FN): Data from attacks that were mistakenly classified as normal.

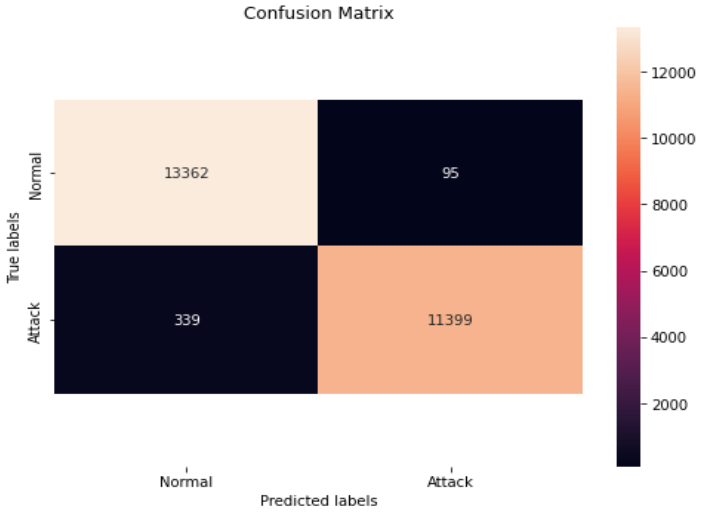

Fig.4. Confusion Matrix

The percentage of attack cases that are mistakenly labeled out of all healthy instances is known as the false positive rate, or FPR. By determining the area under the receiver operating characteristic (ROC) curve, area under the curve (AUC) measures the classifier's overall performance.
The ROC curve plots the true positive rate (TPR), also known as sensitivity, and the false positive rate (FPR). TPR represents the percentage of correctly classified attack instances out of all actual attack instances.
A higher AUC value indicates a better performance of the classifier, as it reflects the model's ability to achieve a high TPR while keeping his FPR low across different classification thresholds.

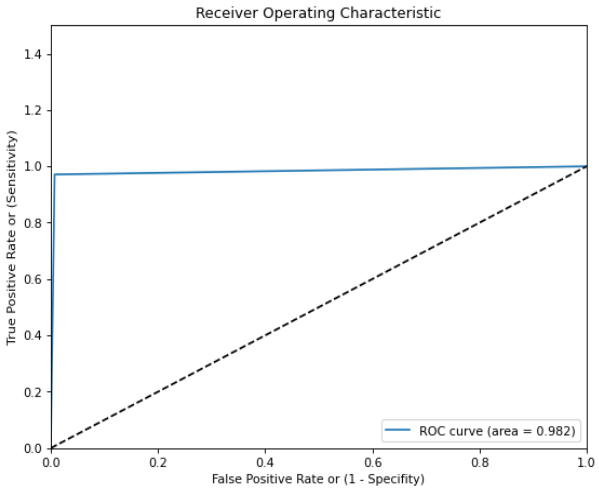

Fig.5. ROC

After finding the confusion matrix and ROC, performance metrics are evaluated like Accuracy, Precision, Recall and F1- Score. The below graph shows how efficient the system is with 98.2% of accuracy, 99.2% of precision, 97.1% of recall and 98.1% F1 score.

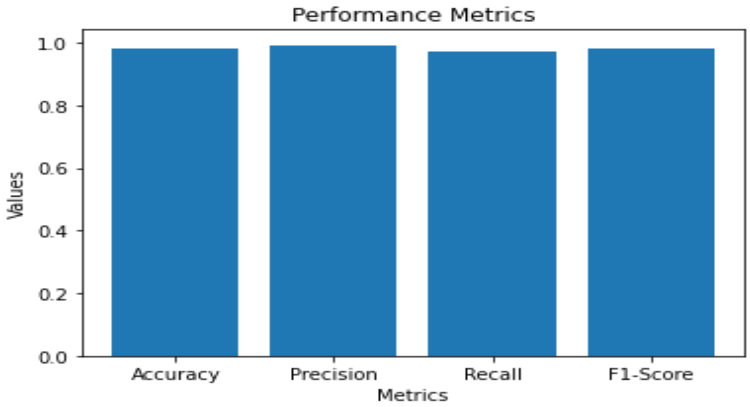

Fig.6. Performance Metrics

The system used the NSL-KDD dataset and performed the pre-processing. The dimensionality reduction is performed efficiently with PCA. The feature selection is enhanced with ACO, and the classification is performed with the XG-Boost algorithm. The performance was estimated based on performance metrics such as, precision, F1-score, recall and accuracy. Also, the efficiency of each system is stated in the performance analysis. Then, a comparative analysis was performed to determine the efficiency and effectiveness of the system.

Further, the comparative analysis with earlier methods concerning the precision, F1-score, accuracy, recall are stated in the following section. The XGBoost-DNN system showed 97.6% accuracy, 97% precision, 97% recall, and 97% F1-score. Then, the LR system showed 87% of accuracy, 87% of precision, recall 87% and 87% of F1-score. The NB system showed 52% of accuracy, 28% of precision, 52% of recall and 36% of F1-score. The SVM system showed 90% of accuracy, precision 90%, recall 90% and F1-score 90%. Therefore, the system showed 98.2% of accuracy, 99.2% of precision, 97.1% of recall and 98.1% F1 score. The system showed improved results than the existing methods. Thus, it proves that the projected system was efficient and effective in intrusion detection. Figure 7 shows the graphical representation of the comparative analysis.

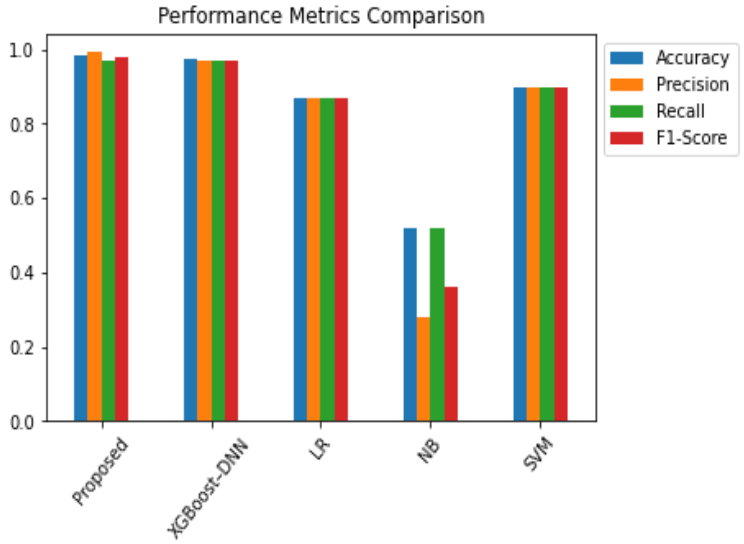

Fig.7. Performance Metrics Comparison

Name of system	Accuracy	Precision	Recall	F-1 Score
XGBoost-DNN	97.6%	97%	97%	97%
LR	87%	87%	87%	87%
NB	52%	28%	52%	36%
SVM	90%	90%	90%	90%
ACO-XGBoost	**98.2%**	**99.2%**	**97.1%**	**98.1%**

V. CONCLUSION

The growth of interconnected systems in an ever-evolving technological environment raises the risk of intrusion and illegal access, necessitating strict safeguards to protect sensitive data. Intrusion detection systems (IDS) have become essential instruments for guaranteeing the security and integrity of digital assets in response to these problems. This paper proposes a new method to improve system security after doing a thorough analysis of IDS. This paper starts with a quick summary of intrusion detection systems (IDS) and then carefully examines the current systems, pointing out their advantages and disadvantages so that better solutions might be developed. The method combines its XG-Boost classifier with ant colony optimization-based feature selection to further improve the intrusion detection. Workflow from dataset detection to preprocessing to dimensionality reduction using principal component analysis and feature selection using ant colony optimization is discussed in detail in the methodology description.

Comparative analysis is also conducted to demonstrate the efficiency and effectiveness of the system. The system performs better than current intrusion detection systems and shows great metrics such as accuracy 98.2%, precision 99.2%, recall 97.1%, F1-score 98.1% and the results show significant improvement. These results demonstrate the effectiveness and efficiency of the strategy to prevent attacks and enhance system security.

VI. FUTURE SCOPE

Looking ahead, there are many possibilities for further growth and development in future research. Enhancing selection processes, using state-of-the-art machine learning tools, including real-time analytics capabilities, and collaborating with cybersecurity experts and industry promoters are some of the possibilities.

First, there is considerable scope for improvement in selection methods to enhance detection and improve evolving counter-systems. Researchers can provide detection systems for efficient and standardized by identifying and prioritizing the most appropriate factors in ensemble-based approaches, swarm intelligence, and genetic algorithms can be considered.

Furthermore, the flexibility and accuracy of detection is expected to increase with the use of state-of-the-art machine learning techniques such as reinforcement learning and deep learning. Deep learning models can automatically identify complex patterns in data, allowing them to better detect attacks and capture details of web traffic.

Similarly, systems can also improve their ability to prevent new threats and vulnerabilities by moving to identification methods based on real-time data from reinforcement learning systems has been modified and refined. Adding anomaly detection methods and real-time object monitoring to an intrusion detection system greatly improves the system response to new threats. Technology can continue to monitor network traffic to identify the suspect.

REFERENCES

[1]. Khraisat, A., Alazab, A. A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecur 4, 18, https://doi.org/10.1186/s42400-021-00077-7, 2021.

[2]. Astha Srivastava, Shashank Gupta, Megha Quamara, Pooja Chaudhary, Vidyadhar Jinnappa Aski. Future IoT-enabled threats and vulnerabilities: State of the art, challenges, and future prospects, 2020.

[3]. Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics* 2020, *9*, 1177. https://doi.org/10.3390/electronics9071177

[4]. Fang Feng, Xin Liu, Binbin Yong, Rui Zhou, Qingguo Zhou. Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device, Ad Hoc Networks, Volume 84, Pages 82-89, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2018.09.014., 2019.

[5]. Yang Y, Zheng K, Wu C. Improving the Classification Effectiveness of Intrusion Detection by Using Improved Conditional Variational AutoEncoder and Deep Neural Network. Sensors (Basel). Jun 2;19(11):2528. doi: 10.3390/s19112528. PMID: 31159512; PMCID: PMC6603523, 2019.

[6]. He, J., Wang, X., Song, Y. et al. Network intrusion detection based on conditional wasserstein variational autoencoder with generative adversarial network and one-dimensional convolutional neural networks. Appl Intell 53, 12416–12436. https://doi.org/10.1007/s10489-022-03995-2, 2023.

[7]. B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," Journal of Network and Computer Applications, vol. 84, pp. 25-37, 2017.

[8]. N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," IEEE Communications Surveys & Tutorials, vol. 21, pp. 2671-2701, 2019.

[9]. M. F. Elrawy, A. I. Awad, and H. F. Hamed, "Intrusion detection systems for IoT-based smart environments: a survey," Journal of Cloud Computing, vol. 7, pp. 1-20, 2018.

[10]. B. A. Tama and K.H. Rhee, "Attack classification analysis of IoT network via deep learning approach," Res. Briefs Inf. Commun. Technol. Evol.(ReBICTE), vol. 3, pp. 1-9, 2017.

[11]. A. Verma and V. Ranga, "Machine learning based intrusion detection systems for IoT applications," Wireless Personal Communications, vol. 111, pp. 2287-2310, 2020.
[12]. Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. J. Sens. Actuator Netw., 12, 29. https://doi.org/10.3390/jsan12020029, 2023.
[13]. Basheer Ahmed, M.I.; Zaghdoud, R.; Ahmed, M.S.; Sendi, R.; Alsharif, S.; Alabdulkarim, J.; Albin Saad, B.A.; Alsabt, R.; Rahman, A.; Krishnasamy, G. A Real-Time Computer Vision Based Approach to Detection and Classification of Traffic Incidents. Big Data Cogn. Comput., 7, 22, 2023.
[14]. Alghamdi, A.S.; Rahman, A. Data Mining Approach to Predict Success of Secondary School Students: A Saudi Arabian Case Study. Educ. Sci., 13, 293, 2023.
[15]. T. Ergen, S.S. Kozat, S. Member, Efficient online learning algorithms based on lstm neural networks, IEEE Trans. Neural Networks Learn. Syst. 29, 3772–3783, 2018.
[16]. Aldweesh, A., Derhab, A., & Emam, A. Z., Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. Knowledge-Based Systems, 189, 2020.
[17]. Rawat S, Srinivasan A, Ravi V, Ghosh U. Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning and deep neural network. *Internet Technology Letters*. 2022; 5:e232.
[18]. Bedi, Punam & Gupta, Neha & Jindal, Vinita. Siam-IDS: Handling class imbalance problem in Intrusion Detection Systems using Siamese Neural Network. Procedia Computer Science. 171. 780-789. 2020.
[19]. Salman Muneer, Umer Farooq, Atifa Athar, Muhammad Ahsan Raza, Taher M. Ghazal, Shadman Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis", Journal of Engineering, vol. 2024, Article ID 3909173, 16 pages, 2024.
[20]. Long, Z., Yan, H., Shen, G. et al. A Transformer-based network intrusion detection approach for cloud security. J Cloud Comp 13, 5, 2024.
[21]. Lu, C.; Cao, Y.; Wang, Z. Research on Intrusion Detection Based on an Enhanced Random Forest Algorithm. *Appl. Sci.*, *14*, 714, 2024.
[22]. Chakrawarti, A., & Shrivastava, S. S. Enhancing Intrusion Detection System using Deep Q-Network Approaches based on Reinforcement Learning. International Journal of Intelligent Systems and Applications in Engineering, 12(12s), 34–45, 2024.
[23]. Ennaji, Sabrine, et al. "i-2NIDS Novel Intelligent Intrusion Detection Approach for a Strong Network Security." IJISP vol.17, no.1 2023: pp.1-17.
[24]. Attou H, Guezzaz A, Benkirane S, et al. Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques. Big Data Mining and Analytics, 6(3): 311-320, 2023.
[25]. Ali, M., Haque, Mu., Durad, M.H. et al. Effective network intrusion detection using stacking-based ensemble approach. Int. J. Inf. Secur. 22, 1781–1798, 2023.
[26]. Talukder, M.A., Islam, M.M., Uddin, M.A. et al. Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. J Big Data 11, 33, 2024.
[27]. Cui, J., Zong, L., Xie, J. et al. A novel multi-module integrated intrusion detection system for high-dimensional imbalanced data. Appl Intell 53, 272–288, 2023.
[28]. Almotairi, Ayoob, Samer Ataweh, Osama A. Khashan, and Nour M. Khafajah. “Enhancing Intrusion Detection in IoT Networks Using Machine Learning-Based Feature Selection and Ensemble Models”, Systems Science & Control Engineering 12, no. 1, 2024.
[29]. H. Y. I. Khalid and N. B. I. Aldabagh, “A Survey on the Latest Intrusion Detection Datasets for Software Defined Networking Environments”, Eng. Technol. Appl. Sci. Res., vol. 14, no. 2, pp. 13190–13200, Apr. 2024.
[30]. https://www.unb.ca/cic/datasets/nsl.html