RESEARCH ARTICLE

SPECIAL ISSUE

International Research Journal on Advanced Science Hub
2582-4376
Vol. 05, Issue 05S
www.rspsciencehub.com

RSP Science Hub

http://dx.doi.org/10.47392/irjash.2023.S072

International Conference on intelligent COMPUting TEchnologies and Research (i-COMPUTER) 2023

An Effective Network Intrusion Detection Model for Coarse-to-Fine Attack Classification of Imbalanced Network Traffic

Y Annie Jerusha [1], S P Syed Ibrahim [2], Vijay Varadharajan [3]

[1] Research Scholar, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nādu, India.
[2] Professor, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nādu, India.
[3] Professor, School of Information and Physical Sciences, The University of Newcastle, Callaghan, Australia.

Email: anniejerusha.y2020@vitstudent.ac.in

Article History

Received: 27 February 2023
Accepted: 20 March 2023

***Keywords**:*

Intrusion Detection Systems (IDS);
Deep Learning (DL);
Generative Adversarial Networks (GAN);
Coarse to Fine-Attack Classification (C-FAC;
CSE-CIC-IDS2018

Abstract

In the present day, cyber security is facing numerous attacks that are causing substantial damage to users. Recent intrusion detection systems are employing advanced methods like deep learning to create effective and efficient intrusion detection systems in order to address these new and intricate attacks. Even the recent benchmark datasets are facing the trouble of detection and prediction of minority attack classes leading the way to missed and false alarms extensively. Hence, these detection systems are biased toward coarse attack classes (majority classes) over fine classes (minority classes). This problem is referred to as Coarse to Fine-Attack Classification (C-FAC). To overcome this challenge and boost the multi-attack classification, a novel approach has been proposed which takes the advantage of ensemble model in phase 1 and Generative Adversarial Networks (GAN) in phase 2. We used classical machine learning and deep learning classification models: Extreme Gradient Boosting (XGBoost), Decision Tress (DT), and Deep Neural Networks (DNN). GAN is cast as an over-sampling method in this model which enhances the classification accuracy of attacks. The effectiveness of our proposed model was evaluated using the two benchmark datasets for intrusions, namely NSL-KDD and CSE-CIC-IDS2018. Based on the experimental results, it was found that our method improved the detection performance and even reduced the false alarm rate of the deep learning network intrusion detection model significantly.

1. Introduction

In the current era of digital technology, computer networks play a vital role in the lives of people. They not only facilitate the sharing of digital information but also offer various services to users. As individuals and organizations rely more heavily on network infrastructures, these networks have become a primary target for cyber-attacks. Such attacks are designed to compromise the privacy, accuracy, and accessibility of online data and services using a variety of network intrusion techniques. Intrusion Detection Systems (IDSs) are security tools that monitor network traffic and systems for suspicious activity or behavior, with the goal of identifying potential threats or attacks. The two types of IDS available are Network-based IDS (NIDS) and Host-based IDS (HIDS). NIDS monitors network traffic and analyzes it for signs of suspicious activity, such as unauthorized access attempts, port scans, and many other attacks. These can be placed at strategic points within a network, to detect attacks as they traverse the network. HIDS monitors individual systems, such as servers or workstations for signs of suspicious activity. They look into system logs, file integrity, and other system-level activities to detect malware infections and other unusual incidents. Our research work is centered on the development of a NIDS. Many Intrusion Detection Systems (IDSs) have been developed to detect such network and system intrusions. To distinguish between legitimate and malicious content, IDSs observe and analyze online activities (Denning). By capturing and scrutinizing online network traffic, NIDSs are capable of identifying any indications of attacks. They even have the benefit of being able to monitor network traffic across multiple devices within a network without requiring additional software on each device. Signature-based NIDSs (S-NIDSs) and Anomaly-based NIDSs (A-NIDSs) are two conventional approaches to developing the NIDSs. Attack signatures are stored by S-NIDSs and utilized to identify attack patterns. The input record will be compared with existing signatures and if found, an alarm will be triggered if matches. However, they are ineffective when it comes to detecting zero-day attacks. A-NIDSs, in contrast, create a behavior profile of the network traffic data they are trained on. Any deviation if noticed from the learned pattern will be identified as a new attack class (Souri and Hosseini). We propose the development of an A-NIDS in this research paper.

The article is structured as follows. Section 2 part provides an overview of intrusion detection, coarse-to-fine-attack class prediction, and related work. Section 3 presents our proposed Coarse to fine-attack classification (C-FAC) algorithm and presents an analysis and experimentation on the benchmark dataset. Finally, Section 4 gives some concluding remarks.

2. Materials and Methods

2.1. Network Intrusion Detection Systems (NIDS)

A NIDS is a critical component of any modern cyber security strategy. NIDS works by monitoring network traffic in real-time and alerting security personnel when it detects suspicious activity. This could include attempts to access unauthorized systems or files, unusual patterns of data transfer, or other indicators of a potential breach. NIDS is particularly useful for detecting and preventing attacks that might otherwise go unnoticed, such as zero-day exploits or stealthy attacks that are designed to evade traditional security measures. In addition to providing early warning of potential security threats, NIDS cans also help to identify vulnerabilities in network systems that need to be addressed. With the ever-increasing number of cyber-attacks on businesses and organizations, deploying an effective NIDS is an essential part of any comprehensive security strategy.

2.2. Coarse to Fine Attack Classification (C-FAC)

The problem of imbalanced attack classes majorly has long been a major obstacle in the realm of machine learning. As a result, intrusion detection also encounters significant difficulties when dealing with network traffic that features highly imbalanced categories. Currently existing intrusion detection models even though showing good performance on coarse attack classification (majority attack classes – attack classes that have more samples in a dataset) do not work well with fine attack classification (minority attack classes – attack classes that have fewer samples in a dataset) (Japkowicz).

First, we provide a concise explanation of the methods and datasets employed to create the C-FAC system. These consist of Deep Neural Networks, Extreme Gradient Boosting, Decision Trees, Generative Adversarial Networks, datasets, and performance evaluation metrics.

2.3. Machine Learning (ML) and Deep Learning in NIDSs

Machine Learning (ML) is a branch of Artificial Intelligence (AI) that enables machines to learn synthetic and closely resemble real data, they effectively expand the minority class potentially increasing the risk of the test data distribution falling outside the range. In such cases, the classifier may not be able to accurately predict this distribution. The primary focus of our C-FAC algorithm is on fine attack classification over coarse attacks using Generative Adversarial Networks (GAN) as an oversampling method.

First, we provide a concise explanation of the methods and datasets employed to create the C-FAC

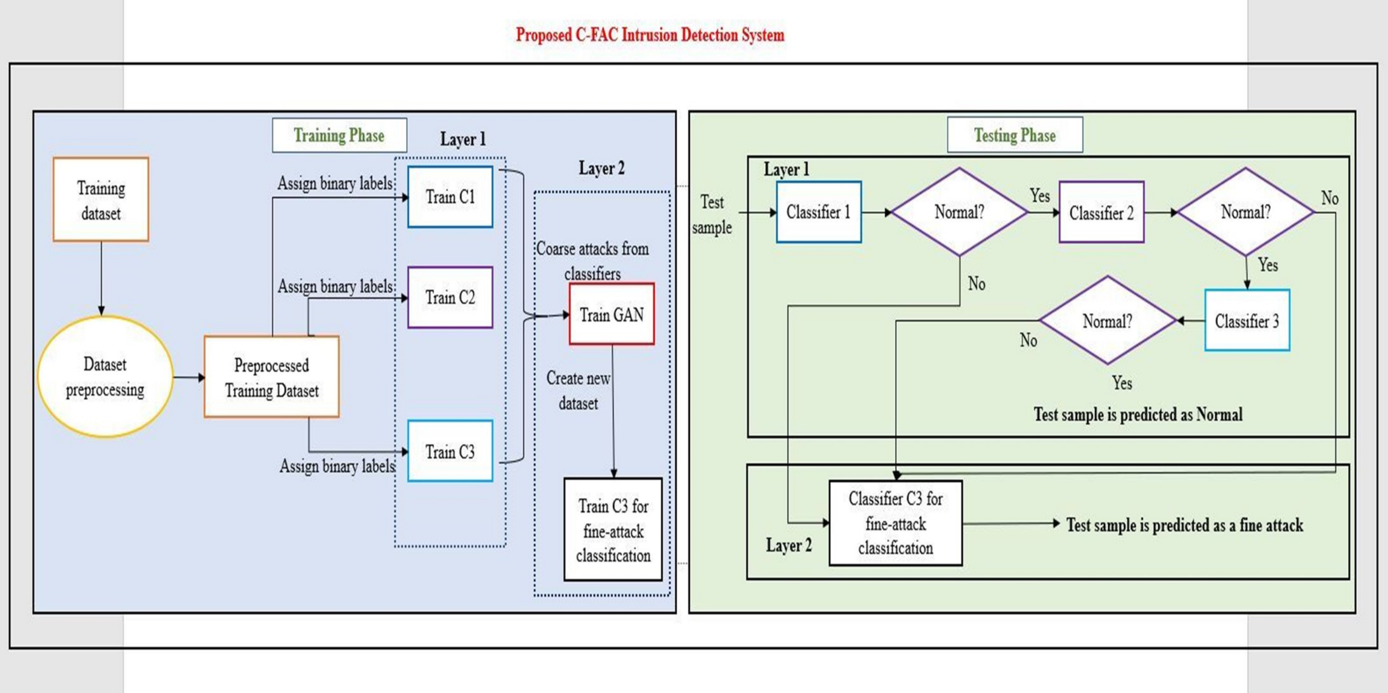

FIGURE 1. **Proposed C-FAC-IDS**

system. These consist of Deep Neural Networks, Extreme Gradient Boosting, Decision Trees, Generative Adversarial Networks, datasets, and performance evaluation metrics.

Machine Learning (ML) and Deep Learning in NIDSs Machine Learning (ML) is a branch of Artificial Intelligence (AI) that enables machines to learn from data and make predictions or decisions without being explicitly programmed. Common ML algorithms include linear regression, logistic regression, decision trees, and support vector machines (SVM) [5]. In contrast, Deep Learning (DL) is a subfield of ML that employs Neural Networks (NN) modeled after the structure of the human brain [6]. Popular DL algorithms include Convolutional Neural Networks (CNN), AutoEncoder (AE), and Recurrent Neural Networks (RNN) [7], [8]. Both ML and DL algorithms are widely used in applications such as image and speech recognition, fraud detection, and many others.

3. Related work

In this section, we will explore several existing NIDS models that have tried fine class classification, and utilized machine learning and deep learning methodologies. To comprehend the coarse-to-fine attack classification, we examine different methods for addressing the issue of class imbalance. Class imbalance arises when the distribution of the data classes in a dataset is uneven, with majority and minority classes termed.

Bedi et al. proposed an IDS called Siam-IDS (Punam, Gupta, and Jindal). They have performed class balancing by using the Siamese method which does not rely on classical class balancing techniques. The proposed work can identify R2L and U2R attacks effectively. It was evaluated against DNN, Convolutional Neural Network (CNN), and it was observed that Siam0IDS has better performance.

Bedi et.al. also proposed an ensemble approach to address the class imbalance issues using an algorithmic method namely I-SiamIDS (Bedi, Gupta, and Jindal). This model, which consists of two layers of ensemble techniques, performed better than its counterparts by achieving significant improvements in accuracy, recall, precision, and F1-score.

JooHwa Lee, and KeeHyun Park has proposed a method to address the class imbalance by utilizing GAN as an unsupervised learning technique that creates new virtual data resembling the original data (Lee and Park). The study also presents a Random Forest (RF) model for identifying detection performance after rectifying data imbalances using GAN. The findings indicate that the proposed work outperformed the models that did not address data imbalances.

Neha Gupta et.al. has suggested LIO-IDS is a NIDS that utilizes two layers to identify different types of intrusions with great precision and minimal computation time (Neha, Jindal, and Bedi). The approach utilized the LSTM classifier in the first layer and incorporated ensemble algorithms and over-sampling methods in the second layer to identify intrusions across various attack categories. Additionally, it employed an enhanced One-vs-One (I-OVO) technique.

Our research work has tried to address the limitation of the coarse-to-fine attack classification method based on previously existing research works. To achieve better results and minimize the misclassification of normal and attacks, we have utilized an ensemble approach in layer 1. In layer 2, we have conducted a fine attack classification.

4. Decision Trees (DT)

Decision trees are a type of ML algorithm that is used for both regression and classification tasks. They are often used in ML because they possess the advantages of being easily understandable and having the ability to work with both categorical and numerical data. Furthermore, they can manage missing data and outliers in the dataset.

Decision trees have the potential to be very useful for creating NIDS due to their ability to rapidly and precisely categorize network traffic. Additionally, decision trees offer a transparent set of guidelines that can be used to comprehend how the NIDS is arriving at its conclusions. This transparency is achieved through Feature Selection, Rule-based classification, Real-time classification, and the production of easily comprehensible results, all of which are strengths of decision trees when applied to NIDS.

5. Extreme Gradient Boosting (XGBoost)

XGBoost is a popular and powerful ML library used for supervised learning problems, particularly for classification and regression tasks. It is a very useful and highly used tool for building NIDSs. In the context of NIDS, XGBoost can be used for two main purposes: Feature Selection and Extraction, and Intrusion detection. It can be particularly useful for NIDS because it can handle large and complex datasets, and can provide accurate predictions even with a relatively small number of features (Liu, Ghosh, and Martin). Additionally, XGBoost can be easily integrated with other ML algorithms and data processing tools, which can further improve the performance of NIDS.

6. Deep Neural Network (DNN)

DNNs are a type of neural network that consists of several layers of interconnected nodes. The layers are densely interconnected, with one node sending input and the other receiving output. The DNNs are typically composed of two layers: input and hidden layers. The input layer receives the input data which can be raw and the hidden layers perform the bulk of the mathematical computation in the network, transforming the input data into a form that can be used to make predictions or classifications. The final layer is the output layer, which produces the final output of the network based on the transformed input. Using backpropagation, which involves iteratively adjusting the weights of the connections between nodes in the network to minimize the difference between the predicted output of the network and the true output, DNNs can learn to perform complex tasks by adjusting the strengths of the connections between nodes during the training process. Their ability to learn complex patterns and relationships in data has made them a popular tool in many areas of ML and Artificial Intelligence (AI).

DNNs have shown great potential in building NIDSs as they are capable of learning complex patterns and relationships between data and detecting subtle and sophisticated attacks (Ring et al.). By using labeled data, these models can be trained to understand the regular patterns of the network and subsequently detect any anomalies that differ from these patterns, which could potentially indicate an intrusion. In classification, DNNs can be used to assign a label to each network connection, indicating whether it is normal or malicious. In anomaly detection, DNNs can detect deviations from normal network behavior, such as unexpected traffic patterns or unusual port usage.

7. Generative Adversarial Network (GAN)

A Generative Adversarial Network (GAN) consists of a pair of neural networks: the Generator and the Discriminator. The generator is fed with any random noise vector and produces synthetic data samples like images, audio, or text, that resemble the ones present in the training data. The discriminator attempts to distinguish between the generated data samples and the real ones from the training data.

GANs have the potential to play a significant role in building NIDSs. The primary function of NIDS is to identify and prevent unauthorized access to a computer network or a system. Once the GAN is trained, it can be used to generate samples that match the learned distribution of normal traffic. Since the GANs are capable of generating synthetic data that is similar to real data, they can identify novel attacks that are not included in traditional NIDS rules and patterns.

These networks can play a significant role in addressing the fine class classification in ML. GANs can be used to generate synthetic examples of minority classes (Tavallaee et al.). Once the GAN is trained, the generated samples can be added to the original dataset to create a balanced dataset to finely classify the classes. By this, the model can be trained to make accurate predictions on both the majority and minority classes, resulting in better overall performance.

8. Proposed C-FAC-IDS

When there is a high imbalance in network traffic, the various types of traffic data look alike, which makes it hard for a classifier to differentiate between them during training. This is especially true for minority attacks that can hide within the large volume of normal traffic and majority attack classes sometimes. In such imbalanced training sets, the majority class samples are essentially useless noise. The C-FAC model is introduced in this article as a two-layered NIDS ensemble approach that can identify and classify intrusions. The initial layer of the model distinguishes between normal and attack categories using binary classification. We have tested many different ML algorithms and DL algorithms and selected DT, XGBoost, and DNN as the classifiers to be used for the model evaluation. To train and test the model for performing binary and fine attack classifications, the datasets NSL-KDD and CSE-CIC-IDS2018 were utilized with binary labels.

The proposed model is illustrated in Figure 1. During the training phase, all three classifiers are taught to distinguish between normal and attack classification (binary classification). The outputs of three classifiers are combined to determine which coarse classes have limited samples and need to be trained using a GAN. The GAN generates samples for these classes to facilitate their detection. After GAN develops the new attack dataset, all three classifiers will be trained on it and the best will be considered. Algorithm 1 outlines the testing process, which involves three stages in layer 1, each with its own classifier. Layer 1 is an ensemble approach and when a test sample passes through it, the first classifier checks whether it is normal or an attack. If it is classified as normal, it moves to the second classifier. If it is an attack, it is flagged as such and goes to layer 2. The process repeats as same for the second and third classifiers, and if the third classifier detects the test sample as normal, it will be considered a final normal classification. Otherwise, it goes to layer 2 for fine classification, which is performed by the third classifier. During the model evaluation, C-FAC is accomplished in layer 2 by identifying the fine classes for both datasets. As all the classifiers are trained with a balanced attack dataset for fine class classification, the model can achieve good performance for C-FAC.

Algorithm 1: Proposed C-FAC Model
Input: Test dataset S
Output: Predict normal or fine-attack

8.1. Layer 1

- For each sample t_i in S
- Predict t_i using classifier1
- If t_i is normal
- send $t_i$to classifier 2
- else to layer 2
- Predict t_i using classifier 2
- if $t_i$is normal
- send $t_i$to classifier 3
- else to layer 2
- Predict t_i using classifier 3
- if $t_i$is normal
- testify $t_i$as normal sample
- else to layer 2 for fine-attack classification

8.2. Datasets

Effective NIDSs rely heavily on good datasets, and the size and quality of the dataset are crucial in determining the accuracy and resilience of the NIDS. For NIDS to be effective, the dataset should encompass a broad range of normal and abnormal network traffic, including both known and unknown attack types. Additionally, the dataset should be representative of the network environment in which the NIDS will be deployed. Therefore, a high-quality dataset is critical for developing effective NIDS as it serves as a foundation for training and evaluating machine learning models. A good dataset should have diverse, accurately labeled, and free of noise and errored samples. By using such, NIDS can be trained to detect and prevent network attacks accurately, which in turn enhances the security of organizations against cyber threats (Gupta, Jindal, and Bedi). In our research work, we have considered NSL-KDD and CSE-CIC-IDS2018 benchmark datasets. NSL-KDD is a well-known dataset in the intrusion detection field and is considered a classic. It is an enhanced version of the KDD99 dataset. While it is not without its shortcomings and may not fully reflect real-world networks, this dataset serves as a valuable reference point for researchers to evaluate various intrusion detection techniques. Each sample in the dataset consists of 41 features and falls into one of the five main classes (Normal and four attack classes) (Abdulhammed et al.).

The CSE-CIC-IDS2018 is a dataset specifically designed for intrusion detection, which was developed by the Canadian Institute of Cyber Security (CIC) in 2018 and hosted on Amazon Web Services (AWS). It is presently the most extensive publicly available intrusion dataset and was developed with the objective of simulating real-world attacks. The dataset represents an upgrade over the CSE-CIC-IDS2017 dataset, and it meets the required standards for attack datasets, as it encompasses different types of well-known attack scenarios. It includes six different attack scenarios and 83 features for each sample and six main classes (Normal and five attack classes).

8.3. Evaluation metrics

To define whether a model is well performed in the field, it has to be evaluated with its relevant metrics to analyze its performance. To do so, a few metrics are drafted for NIDS models. Those metrics will give the particulars concerning the actual and predicted classes. The standard evaluation metrics in deciding the performance of NIDS are Accuracy, Precision, Recall, and F1 score. The conduct of the NIDS model cannot be justified with just a single evaluation metric. Here are a few of the metrics and the terminologies required to define them:

- **True positive (TP):** A true positive in NIDS occurs when the system correctly identifies an attack as an attack.
- **True negative (TN):** A true negative in NIDS occurs when the system correctly identifies normal network traffic as normal.
- **False positive (FP):** A false positive occurs in NIDS when the system incorrectly identifies normal network traffic as an attack.
- **False negative (FN):** A false negative in NIDS occurs when the system fails to identify an attack as an attack.
- **Accuracy:** It is a measure of how many correct predictions were made out of all predictions that were made.

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \quad (1)$$

- Precision is metric that measures the number of correct positive predictions made out of all positive predictions. A high precision rate indicates that the system is generating a low number of false positives.

$$Precision = TP/(TP + FP) \quad (2)$$

Recall also known as sensitivity or true positive rate, is the ratio of the number of correctly identified attacks (true positives) to the total number of attacks present in the network. A high recall value indicates that the NIDS is capable of identifying most of the attacks that occur in the network.

$$Recall = TP/(TP + FN) \quad (3)$$

- F1 score can be defined as the harmonic average of precision and recall. A high value indicates that the IDS is accurately identifying true positives while minimizing false positives.

$$F1Score = 2 * (Precision * Recall)/(Precision + Recall) \quad (4)$$

- False Alarm Rate (FAR) refers to the proportion of times with which an IDS generates false alarms relative to the number of alerts generated. A low false alarm rate is essential for an effective NIDS.

$$False - Alarm\ Rate = ((FP))/((FP + TN)) \quad (5)$$

9. Results and Discussion

9.1. Experimental Evaluation

Our proposed model for intrusion detection is C-FAC. To prepare the data, we first removed the duplicate values, outliers, and standardized numerical values. Then we split the dataset into training and testing datasets. We conduct experiments using both Sklearn and TensorFlow frameworks on the Google Colaboratory platform. The machine learning algorithms run on the CPU, while the deep learning algorithms utilize TPU to accelerate the process.

When testing the model on the NSL-KDD dataset, the dataset was divided into 80 to 20 ratio of training and testing samples. The binary classification had a detection rate of 99.21%, but the fine-attack class classification did not perform well. Specifically, two coarse classes among the attack classes (DoS, Probe, R2L, U2R) were leading to missed detections, namely R2L, and U2R. To improve the fine-attack classification, GAN was used to increase the detection rate and minimize FAR, resulting in an increase from 79.84% to 87.62% as shown in Figure 3. Other techniques such as random over-sampling (81.87%) random under-sampling (81.90%), and SMOTE (82.38%) were also used to evaluate the model's performance and yielded satisfactory results.

The CSE-CIC-IDS2018 dataset is currently being used as a benchmark dataset to evaluate NIDS models. Our evaluation was performed on this dataset using 10% of the total data, with 502,988 samples used for training and 125,748 samples used for testing, which is 80 and 20 in ratio. Although a single classifier did not perform well with binary classification, we were able to increase the detection rate from 58% to 86% using an ensemble approach from our model. We observed fine attack classes such as Brute Force-Web, Brute Force-XSS, SQL Injection, FTP-BruteForce, and DOS attack-SlowHTTPTest. We focused on C-FAC and our proposed model was able to detect most of the fine attack classes in the minority classes with a 98.80% detection rate as shown in Figure 2. For its counterparts, random over-sampling had a detection rate of 81.06%, random under-sampling, and SMOTE 59.37% and 97.73% respectively. Therefore, we can conclude that the proposed C_FAC-IDS is efficient enough of identifying fine intrusions at a good level, making it a strong candidate for an efficient NIDS.

Although we conducted binary classification and numerous other experiments to improve our model prediction ability to specific fine-attack classes, we are only showcasing the predictions and results related to fine-attack-class prediction, which is our main focus. Table 1 contains the experimental data for both datasets.

10. Conclusion

The advancement of Network Intrusion is placing more demand on network intrusion detection. The issue of imbalanced network traffic is causing problems for IDSs, as they struggle to anticipate the behavior of attacks. This poses a significant threat to cybersecurity. In this research paper, we presented a possible way called C-FAC to tackle the problem of fine attack class classification in intrusion detection. This proposed model is a two-layered ensemble approach in which we used XGBoost, DNN, and DT as classifiers at the first layer. The first layer classifies between normal and attacks, using multiple classifiers to increase the likelihood of less false alarm rate. The second layer, however, uses each of the classifiers to categorize the attack samples identifies in the first layer. We evaluated the performance of the proposed work on the NSL-KDD and CSE-CIC-IDS2018 datasets through training and testing. The effectiveness of C-FAC in detecting fine attacks in an imbalanced network environment was evaluated and compared to IDSs developed using various existing class-balancing techniques. The evaluation showed that the proposed model, achieved better Accuracy, Recall, Precision, and F1 Scores compared to the other algorithms. These findings indicate that C-FAC is more effective than its counterparts in detecting fine-class attacks in an imbalanced network environment. In our current research, our main emphasis has been on distinguishing between fine attacks and coarse attacks. However, in our future research, we aim to expand our work by detecting and identifying zero-day attacks with a high level of accuracy in both detection and minimal false alarms.

TABLE 1. **Results compared with Proposed C-FAC and existing models**

Model	NSL-KDD				CSE-CIC-IDS2018			
	Acc	Pre	Recall	F1	Acc	Pre	Recall	F1
XG-Boost+DT+DNN	0.65	0.53	0.59	0.55	0.82	0.63	0.71	0.60
Ensemble+RO	0.81	0.71	0.69	0.69	0.81	0.74	0.73	0.73
Ensemble+RU	0.81	0.72	0.78	0.66	0.59	0.50	0.61	0.54
Ensemble+SMOTE	0.82	0.83	0.81	0.81	0.97	0.73	0.79	0.68
C-FAC model	0.87	0.91	0.88	0.89	0.98	0.87	0.84	0.79

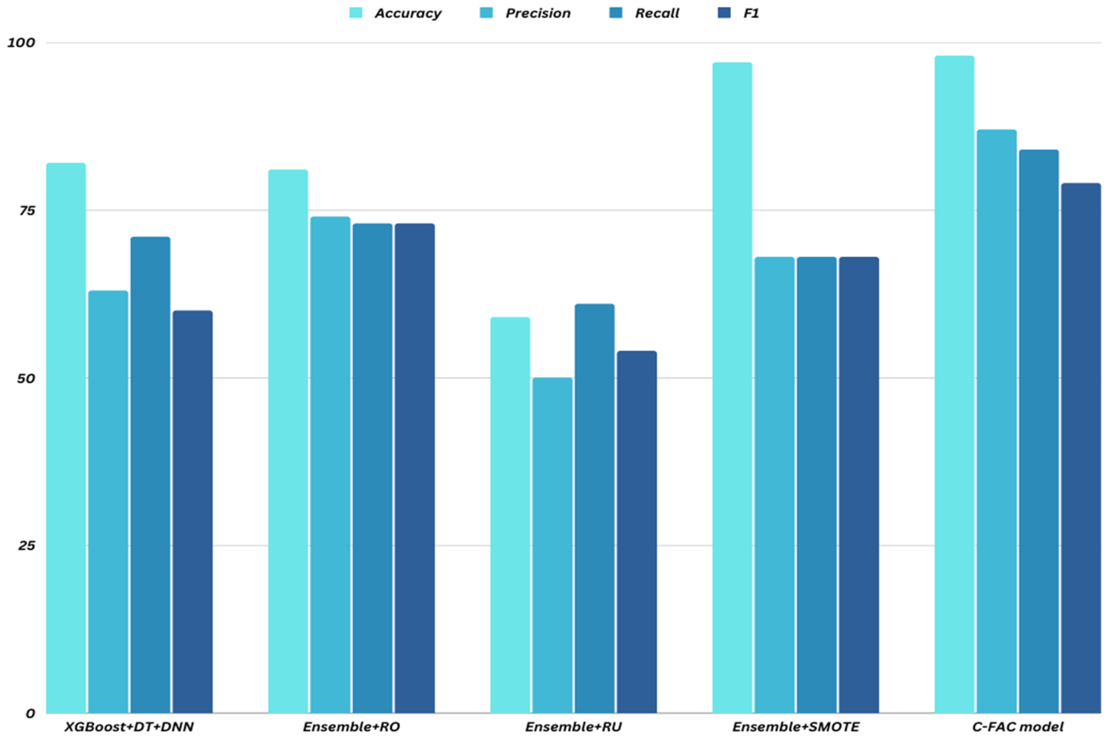

FIGURE 2. **Performance comparison on CSE-CIC-IDS2018 with Proposed C-FAC and existing models**

11. Authors' Note

The authors do not have any conflicts of interest that pertain to the subject matter of this article.

References

Abdulhammed, Razan, et al. "Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic". *IEEE Sensors Letters* 3.1 (2019): 1–4.

Bedi, Punam, Neha Gupta, and Vinita Jindal. "I-SiamIDS: an improved Siam-IDS for handling class imbalance in network-based intrusion detection systems". *Applied Intelligence* 51.2 (2021): 1133–1151.

Denning, D E. "An Intrusion-Detection Model". *IEEE Transactions on Software Engineering* SE-13.2 (1987): 222–232.

Gupta, Neha, Vinita Jindal, and Punam Bedi. "CSE-IDS: Using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems". *Computers & Security* 112 (2022): 102499–102499.

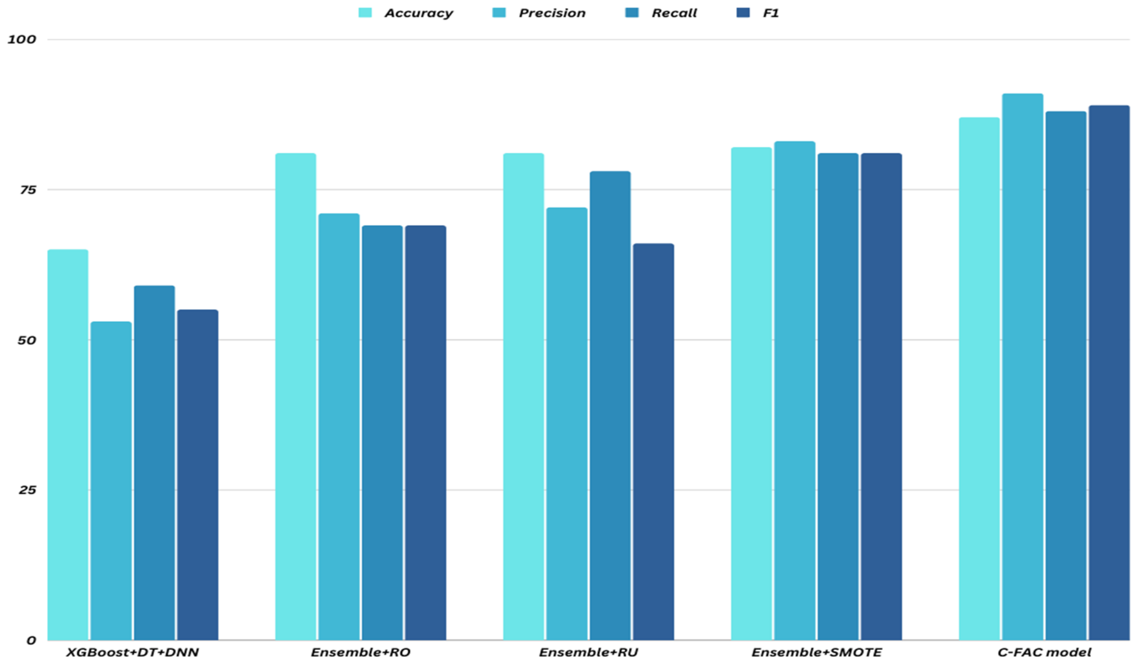

FIGURE 3. Performance comparison on NSL-KDD with Proposed C-FAC and existing models

Japkowicz, N. "The class imbalance problem: Significance and strategies". *Proc. Int. Conf* 56 (2000): 111–117.

Lee, Joohwa and Keehyun Park. "GAN-based imbalanced data intrusion detection system". *Personal and Ubiquitous Computing* 25.1 (2021): 121–128.

Liu, A, J Ghosh, and C E Martin. "'Generative oversampling for mining imbalanced datasets". *Proc. DMIN* (2007): 66–72.

Neha, Gupta, Vinita Jindal, and Punam Bedi. "LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system". *Computer Networks* 192 (2021): 108076–108076.

Punam, Bedi, Neha Gupta, and Vinita Jindal. "Siam-IDS: Handling class imbalance problem in Intrusion Detection Systems using Siamese Neural Network". *Procedia Computer Science* 171 (2020): 780–789.

Ring, Markus, et al. "A survey of network-based intrusion detection data sets". *Computers & Security* 86 (2019): 147–167.

Souri, Alireza and Rahil Hosseini. "A state-of-the-art survey of malware detection approaches using data mining techniques". *Human-centric Computing and Information Sciences* 8.1 (2018): 3–3.

Tavallaee, M, et al. "NSL-KDD dataset". *Retrieved* 9 (2009).

Embargo period: The article has no embargo period.

To cite this Article: , Y Annie Jerusha, S P Syed Ibrahim , and Vijay Varadharajan . "**An Effective Network Intrusion Detection Model for Coarse-to-Fine Attack Classification of Imbalanced Network Traffic**." International Research Journal on Advanced Science Hub 05.05S (2023): 531–540. http://dx.doi.org/10.47392/irjash.2023.S072