Optimizing Class Imbalance and Enhancing Intrusion Detection in SDN Environments using Deep Learning Models

Dr.K.Suresh Babu[1], Dr.M.Sireesha[2], T.G.Ramnadh Babu[3], G.Venkatesh[4], D.Sreenivas[5], and M.Venkatesh[6]

[1,2]Associate Professor, Dept of CSE Narasaraopeta Engineering College(Autonomous) Narasaraopet, India.
[3] Asst.Professor, Dept of CSE Narasaraopeta Engineering College(Autonomous) Narasaraopet, India.
[4,5,6]Student, Dept of CSE Narasaraopeta Engineering College Narasaraopet, India.
sureshkunda546@gmail.com

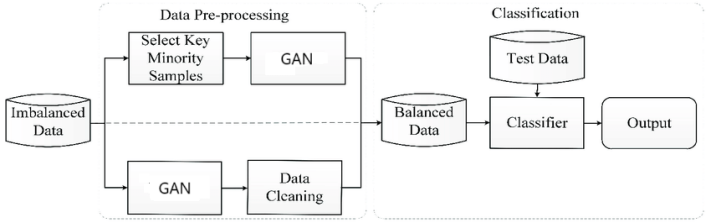
Abstract. This research aim is to addresses the critical issue of class imbalance in intrusion detection systems (IDS) in Software-Defined Networking environments. This paper introduces a novel approach that exploits advanced deep learning techniques to improve minority class attack detection, often missed because they are rare. Balancing the dataset using data synthesis with GAN and SMOTE, this study allows different classifiers to improve their performance. The research explores the effectiveness of multiple deep learning architectures, including MLPs, CNNs, and SNNs,in detecting intrusions. The results show that GAN-based augmentation significantly outperforms traditional methods such as SMOTE, reducing false negatives and increasing overall detection accuracy.The paper also places an emphasis on the preprocessing technique of data that will include mean imputation as well as standardization techniques to enhance the input quality. Results show how the proposed integrated approach is able to improve not only the accuracy of intrusion detection but also the whole security framework in SDN environments.

Keywords: —Software-Defined Networking (SDN), Network Traffic Analysis, Imbalanced Data Handling, Deep Learning Models, Machine Learning models, Minority Class Detection.

1 INTRODUCTION

Class imbalance is a very serious problem in machine learning, particularly in IDS in SDN environments. It is a situation where there are some classes, mostly attack types, that occur much less frequently than the normal traffic, thus creating bias in the models towards the majority class[1]. This would result in low detection rates for minority classes that are very significant in security threat identification. It is important to detect rare events, since they could indeed have extreme implications for network and integrity of data. As a means of addressing class imbalance, the paper focuses on data-level approaches: SMOTE and

GAN[10,15]. Both techniques balance datasets by creating synthetic instances of the under-represented class, which can help the model learn from important data points. The kind of synthetic data that GAN is particularly good at producing mimics reality really well, making the minority classes in the dataset better represented.[10,11] The authors outline the deep models used in the study: Multi-Layer Perceptrons (MLPs), Convolutional Neural Networks (CNNs), and Siamese Neural Networks (SNNs). Each of these models has its benefits: MLP provides a trade-off between complexity and performance; CNN is best suited for spatial hierarchies; SNN enhances detection by similarity learning[12]. It, thus underlines that in determining their efficiency and the possibility of them to be attacked through attacks in a minority class, they are put forward and compared in detail considering some metrics in evaluating those such as accuracy, precision, recall, and F1-score.To summarize, it makes it to introduce well by the actual relevance in conducting a counter approach for balancing class by trying innovative ideas of better detection for intruders with SDN.



2 LITERATURE REVIEW

Recent innovations in SDN have increased flexibility and centralized control but also increased the complexity of cyberattacks, which call for sophisticated Intrusion Detection Systems (IDS) [1]. Machine learning (ML) and deep learning (DL) models are already applied to IDS but class imbalance, where attack instances are hugely underrepresented compared to normal traffic is still a challenge, especially on User-to-Root and Denial of Service attacks, that makes them send many false negatives [5,12]. For this experiment, I used InSDN with deep learning models like Multilayer Perceptron, CNNs, and Siamese Networks[16]. Resampling techniques such as SMOTE are used to overcome the imbalanced set; however noise in high-dimensional data is still an area of concern [1,2,13].GAN is a very effective technique when handling class imbalance since it generates realistic synthetic data, thereby enhancing the representation of minority classes in the dataset [8,9,13].The classifier models like Weighted Random Forest wRF had better classification performance as it assigned a great weight to the minority classes [3,6,14]. Although deep models such as CNNs and SNNs are ideal for big datasets, it was suggested that adversarial training be applied to improve the detection of a minority class [3,8,13]. For better intrusion detection, future work suggests the use of hybrid models combined with complex datasets [4,10].

3 MATERIALS AND METHODS :

3.1 DATASET:

We used InSDN dataset for this research, specified for intrusion detection in the context of software-defined networking environments. The dataset contains 343,889 network flows, thus holding many types of network traffic. It has a class imbalance problem in which DDoS, DoS, and Probe attacks constitute a majority of its data. Those attacks appear more frequently in the dataset than the other classes such as Brute Force Attack (BFA), Web Attacks, and User-to-Root (U2R) attacks, which appear less frequently.

3.2 DATA PRE-PROCESSING:

In the pre-processing data stages of this project all the network identifiers like source IP, destination IP, and flow ID are excluded to avoid over-fitting. This project's data pre-processing includes the handling of missing values and the standardization of numeric data. It utilizes mean imputation for numeric columns and uses the most frequent value for non-numeric columns. The numeric columns are standardized, and after imputation, they get normalized by using StandardScaler applied on the data. Categorical variables are encoded with the help of OneHotEncoder, converting them into the format of numbers and splitting the dataset into features and a target variable at the end[17].

3.3 DISTRIBUTION OF CLASS LABELS FOR TRAINING AND TESTING

It shows the class distribution of an intrusion detection dataset for training and testing. Classes like "Probe," "DDoS," and "Normal" are reasonably well represented, while such rare events as "U2R" and "BOTNET" contain very few samples, showing significant class imbalance. Such high class imbalance requires the use of data level methods such as GAN in order to train the model suitably in an effort to catch all kinds of attacks.

y_train value counts: Label		y_test value counts: Label	
Probe	78503	Probe	19626
DDoS	58823	DDoS	14706
Normal	54739	Normal	13685
DoS	42893	DoS	10723
DDoS	38730	DDoS	9683
BFA	1124	BFA	281
Web-Attack	154	Web-Attack	38
BOTNET	131	BOTNET	33
U2R	14	U2R	3

3.4 HANDLING CLASS IMBALANCE USING DATA-LEVEL METHODS:

Effective class imbalance management in intrusion detection techniques uses methods such as Generative Adversarial Networks that generate synthetic sam-

ples for the underrepresented classes **Fig 1**. Classifier methods enhance the classification performance by giving a greater weight to the minority classes, thereby greatly improving the overall detection rates.

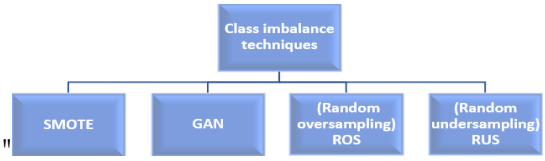


Fig. 1. DATA-LEVEL METHODS

GAN: GAN class imbalance technique uses the support of two networks one is generator and one is discriminator to generate synthetic samples for underrepresented classes within data **Fig 2**. There would be one generator trying to learn how to make realistic data points while another discriminator is there to distinguish between real and synthetic data, thereby balancing the dataset and subsequently the performance of the model [8,10]. The generator gets better at generating synthetic samples over time as the discriminator improves in distinguishing reality from fake. In this adversarial process, high-quality synthetic data develops, mimicking the minority class distribution in the training. WGAN and CGAN are among the latest techniques for addressing class imbalance and enhancing intrusion detection **Fig 3,Fig 4**.

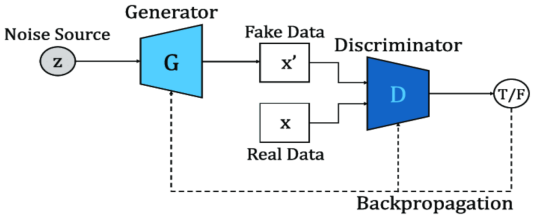


Fig. 2. GAN

3.5 DISTRIBUTION OF CLASS LABELS WITH DATA- LEVEL METHODS:

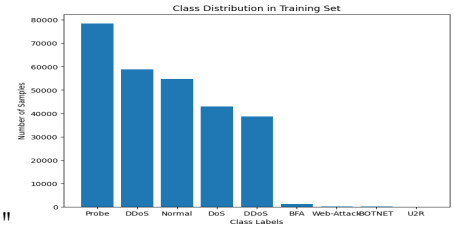


Fig. 3. PRE-BALANCING

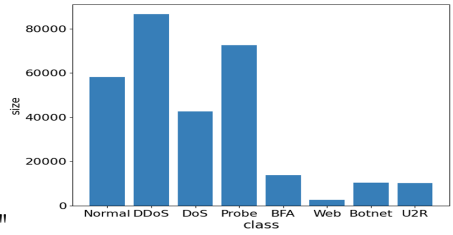


Fig. 4. GAN

4 CLASSIFIER-LEVEL METHODS:

4.1 DEEP LEARNING MODELS:

MLP (Multilayer Perceptron) The MLP model built with 6 hidden layers consists of layers of neuron sizes of (128, 64, 52, 32, 16, 8) and 10 hidden layers size of (512 ,256 ,1024 ,128 ,256, 64 ,128, 32, 16, 8) [Table 2]. The deep neural net will allow the model to learn data patterns at higher levels of abstraction by understanding hierarchical representations. A non-linear activation function can be applied in each layer and therefore this model will generalize well towards different tasks. By back propagation and optimization algorithms, the MLP iteratively changes its weights in order to gain smaller error values. Indeed, such a model is very effective for classification tasks-high accuracy when applied in a scenario where the training set has been large and well-pre-processed with proper tuning, it can be improved even further.

Siamese Neural Networks (SNN) A Siamese Neural Network based Framework for SDN-based intrusion detection utilizes two identical subnetworks that detect malicious activities. This approach develops learning related to normal versus abnormal traffic through comparisons of similarities between input feature pairs. SNN model extracts slight differences in network behaviour by making appropriate use of shared architecture and weights to efficiently differentiate between normal and abnormal traffic **Fig 5**. This framework does well in anomaly detection because it learns distinct attack patterns against networks and is also highly robust against unknown attacks. The model enhances security within the SDN environment using reliable real-time intrusion detection with less false positives.

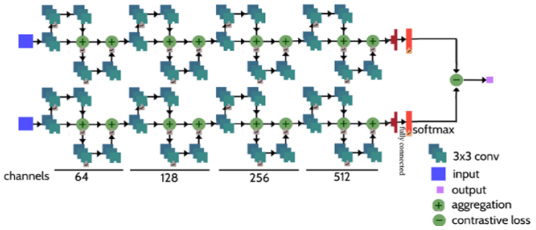


Fig. 5. Architecture of Siamese neural networks framework

Convolutional Neural Network (CNN) A Convolutional Neural Network (CNN) model for SDN intrusion detection utilizes its capability to capture spatial hierarchies within data. Network traffic patterns within the SDN environment can be treated as images or grid-like data, and this means that the CNN will effectively lift local and global features. The model employs multiple convolutional layers for learning elaborate patterns of normal and malicious behaviour in network traffic. This architecture is very effective for intrusion detection as it can learn important features automatically; hence, this is an actual strong tool in identifying anomalies and cyber threats in SDN environments. The size of

the kernel is set at 3 and the activation function is used ReLU (Rectified Linear Unit) in the CNN model.

AUTO ENCODERS Autoencoders are used for intrusion detection in Software-Defined Networking due to the fact that it is possible to extract compressed representations of network traffic data by training on normal traffic. By so doing, autoencoders learn to reconstruct typical patterns, but when there are anomalies or malicious traffic, the reconstruction error is increased, meaning potential intrusions. This model is good for detecting subtle deviations from normal behaviour and classifies sophisticated attacks. Its capacity to process very high dimensionalities coupled with its ability to identify anomalies even in the absence of predefined features makes it an effective method for dynamic SDN scenarios.

4.2 MACHINE LEARNING MODELS

XGBOOST XGBoost is a powerful approach for intrusion detection in Software-Defined Networking systems. XGBoost relies heavily on complex, high-dimensional data that it can manage by boosting decision trees to improve predictive performance. It can deal with very different types of data and missing values; its regularization techniques prevent overfitting. With the greatest possible improvements in accuracy both for more frequent and for less frequent intrusion detection, the gradient boosting framework makes it possible to make very fine-grained model adjustments. Therefore, the efficiency and scalability of XGBoost make it a good candidate for real-time threat and anomaly detection within dynamic SDN environments.

Weighted Random Forest (WRF) A Weighted Random Forest model is an extension of standard Random Forest by the inclusion of sample or class weights [Table 3]. One important problem when it comes to intrusion detection in SDN, is dealing with class imbalances between normal and malicious traffic. Assigning greater weights to classes with fewer instances will have a larger effect on sensitivity for patterns that are rare but would be of great importance for intrusion detection. This makes the detector robust and accurate in identification of threats when there is a class imbalance distribution in SDN environments. The weighted approach gives better performance along with the reduction of false negatives in detecting network anomalies.

5 PROPOSED MODELS

Based on my proposed models for intrusion detection in Software-Defined Networking (SDN) environments, I found that the Weighted Random Forest (WRF) exceeds all other machine learning models used in performance [Table 1]. It has the following advantages: it can handle imbalanced data and offers robust detection. For deep learning, the superior models highlighted are Siamese Neural Networks (SNN) and Convolutional Neural Networks (CNN). SNN performs very well in scenarios where the detection of similarity is vital, while CNN is most

valuable for feature extraction. The third model that performed encouragingly was also Multilayer Perceptron (MLP). Deep learning models, for example, CNN and MLP, are useful for managing huge sets of data since they may process complicated patterns and relationships very well. These models in combination with SDN form an efficient framework for intrusion detection that is able to catch threats in real time.

6 COMPARATIVE ANALYSIS

6.1 MODEL ACCURACY TABLE

The table below presents the accuracy of various classification methods, highlighting their performance in intrusion detection for SDN environments.

Table 1. Accuracy of Proposed Models

Proposed Models	**Accuracy (%)**
MLP 1	99.95
MLP 2	99.90
Siamese Neural Networks	99.91
CNN	99.68
Auto Encoders	96.45
XGBoost	99.70
Random Forest	99.99
Weighted Random Forest	99.99

6.2 TESTING AND TRAINING ACCURACY GRAPHS

The visual testing and training accuracy of the proposed intrusion detection models has shown substantial performance improvements. The visualizations on these models demonstrate the ability of the proposed models to learn patterns from the dataset towards better intrusion detection in an SDN environment. It also provides insight to model convergence and generalization capabilities, as well as effectiveness in intrusion detection, which helps find the optimal trade-off between training accuracy and avoiding overfitting **Fig 6,Fig 7,Fig 8**.

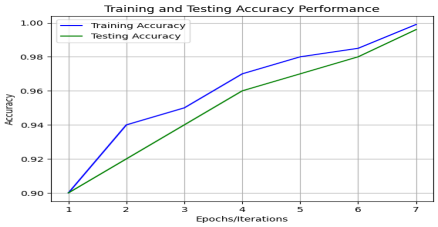


Fig. 6. MLP

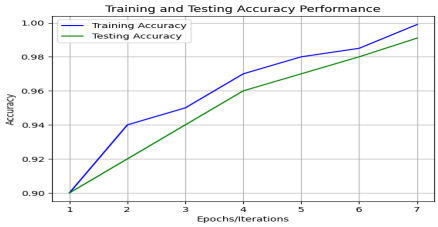


Fig. 7. SNN

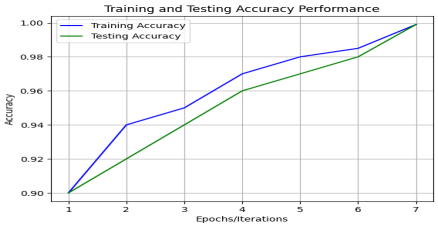


Fig. 8. WRF

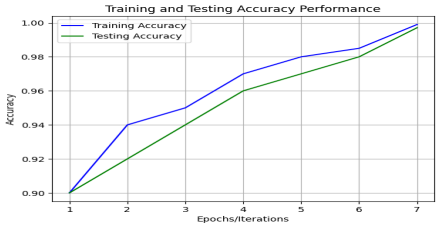


Fig. 9. XGBOOST

6.3 CLASSIFICATION PERFORMANCE OF CLASSIFY-LEVEL METHODS

Classifier-level methods improve the minority-class classification in a dataset by using weighted techniques to enhance detection rates.Various classification performances of the classifier methods are important in case the class imbalance problem is addressed in the context of intrusion detection systems **Fig 10,Fig 11,Fig 12,Fig 13,Fig 14 and Fig 15**.

Accuracy: 99.95%
Classification Report:

	precision	recall	f1-score	support
BFA	0.97	0.99	0.98	260
BOTNET	1.00	1.00	1.00	27
DDoS	1.00	1.00	1.00	14702
DDoS	1.00	1.00	1.00	9747
DoS	1.00	1.00	1.00	10628
Normal	1.00	1.00	1.00	13677
Probe	1.00	1.00	1.00	19695
U2R	0.67	1.00	0.83	4
Web-Attack	0.86	0.95	0.90	38
macro avg	0.94	0.99	0.96	68778
weighted avg	1.00	1.00	1.00	68778

Fig. 10. MLP 1

Accuracy: 99.91%
Classification Report:

	precision	recall	f1-score	support
BFA	0.97	0.99	0.98	260
BOTNET	1.00	1.00	1.00	27
DDoS	1.00	1.00	1.00	14702
DDoS	1.00	1.00	1.00	9747
DoS	1.00	1.00	1.00	10628
Normal	1.00	1.00	1.00	13677
Probe	1.00	1.00	1.00	19695
U2R	0.73	0.76	0.75	4
Web-Attack	0.86	0.95	0.95	38
macro avg	0.89	0.99	0.96	68778
weighted avg	1.00	1.00	1.00	68778

Fig. 11. SNN

Accuracy: 99.68%
Classification Report:

	precision	recall	f1-score	support
BFA	0.97	0.99	0.98	260
BOTNET	1.00	1.00	1.00	27
DDoS	1.00	1.00	1.00	14702
DDoS	1.00	1.00	1.00	9747
DoS	1.00	1.00	1.00	10628
Normal	1.00	1.00	1.00	13677
Probe	1.00	1.00	1.00	19695
U2R	1.00	0.76	0.75	4
Web-Attack	0.89	0.88	0.91	38
macro avg	0.98	0.90	0.91	68778
weighted avg	1.00	1.00	1.00	68778

Fig. 12. CNN

Accuracy: 96.45%
Classification Report:

	precision	recall	f1-score	support
BFA	0.97	0.99	0.98	260
BOTNET	1.00	1.00	1.00	27
DDoS	1.00	1.00	1.00	14702
DDoS	1.00	1.00	1.00	9747
DoS	1.00	1.00	1.00	10628
Normal	1.00	1.00	1.00	13677
Probe	1.00	1.00	1.00	19695
U2R	0.57	0.69	0.73	4
Web-Attack	1.00	0.86	0.85	38
macro avg	0.89	0.90	0.94	68778
weighted avg	1.00	0.95	0.97	68778

Fig. 13. AUTO ENCODERS

Accuracy: 96.70%

Classification Report:

	precision	recall	f1-score	support
BFA	0.99	0.99	0.99	260
BOTNET	1.00	1.00	1.00	27
DDoS	1.00	1.00	0.99	14702
DDoS	1.00	0.99	0.99	9747
DoS	1.00	1.00	1.00	10628
Normal	1.00	1.00	1.00	13677
Probe	1.00	1.00	1.00	19695
U2R	1.00	0.75	0.86	4
Web-Attack	1.00	0.97	0.99	38
macro avg	1.00	0.97	0.98	68778
weighted avg	1.00	1.00	1.00	68778

Fig. 14. XGBOOST

Accuracy: 99.99%

Classification Report:

	precision	recall	f1-score	support
BFA	0.99	1.00	0.99	260
BOTNET	1.00	1.00	1.00	27
DDoS	1.00	1.00	1.00	14702
DDoS	1.00	0.99	0.99	9747
DoS	1.00	1.00	1.00	10628
Normal	1.00	1.00	1.00	13677
Probe	1.00	1.00	1.00	19695
U2R	0.99	0.97	0.99	4
Web-Attack	1.00	0.98	0.99	38
macro avg	0.99	0.97	0.97	68778
weighted avg	1.00	1.00	1.00	68778

Fig. 15. WRF

6.4 HYPERPARAMETERS FOR DEEP LEARNING MODELS:

These are internal variables in a deep or machine learning model that control the way a model is adjusted and refined during training to prevent high errors and refine its predicting abilities. Weights and biases help recognize patterns from the data it has been trained on and apply those same patterns to new, unseen data.The benefit of model parameters is that it allows fine-tuning of algorithms so they might adapt to and even improve on predictions made on training data, thus increasing the accuracy and performance of models.

Table 2. Hyperparameters for Various Models

Model	LR	Batch-size	Epoch	Layers
MLP 1	0.0001 – 0.0002	256 – 512	180	(128, 64, 52, 32, 16, 8)
MLP 2	0.0001 – 0.0002	512 – 1024	200	(512, 256, 1024, 128, 256, 64, 128, 32, 16, 8)
CNN	0.0001 – 0.0002	64 – 256	25	(128, 256, or 512)
Auto encoders	0.0001 – 0.0002	64 – 256	50	(256, 512, 64, 128)
Siamese neural networks framework	0.0001 – 0.0002	32 – 256	200	(64, 128, 64, 128, 512, 512, 256, 8)

6.5 HYPERPARAMETERS FOR MACHINE LEARNING MODELS:

Table 3. Parameters for RF, WRF, and XGBOOST Models

Model	Estimators	Classes	Features	Max Depth	Min Samples in Leaf	Max Split Samples
RF, WRF, XGBOOST	80 – 100	8	52	10	1	2

6.6 CONFUSION MATRIX FOR CLASSIFIER METHODS:

A confusion matrix is one of the most important performance-measuring tools for IDS with class imbalance. Accuracy, precision, recall, and F1-score were used as performance measures in the above study. Significant reductions in false positives along with higher detection rates for minority classes were observed with GAN-based augmentation and WRF **Fig 16,Fig 18,Fig 19 Fig 20 and Fig 21.**

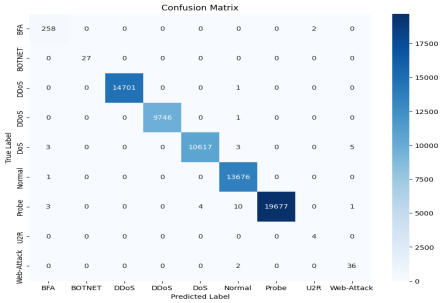


Fig. 16. MLP 1

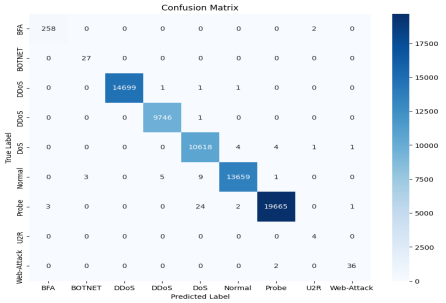


Fig. 17. MLP 2

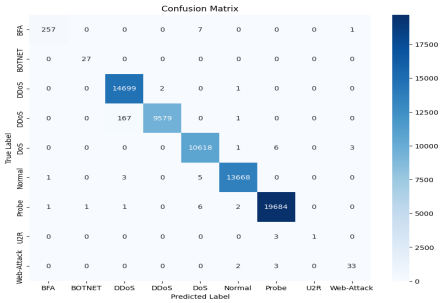


Fig. 18. SNN

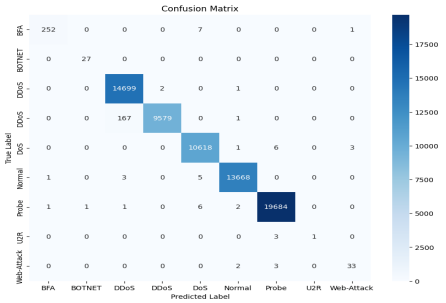


Fig. 19. CNN

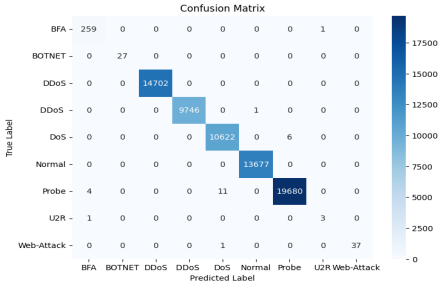


Fig. 20. XGBOOST

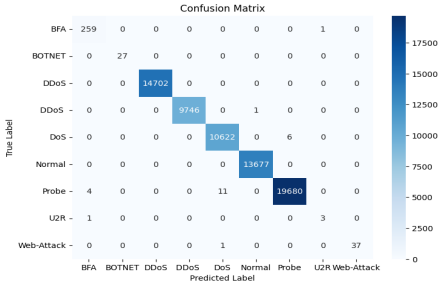


Fig. 21. WRF

7 CONCLUSION AND FUTURE SCOPE:

The minority classes represent very rare but very significant attacks. Such classes detection forms the backbone of SDN intrusion detection. WRF excelled in its task and achieved 99.99% accuracy on imbalanced data. SNN and MLP achieved 99.91% and 99.95%, respectively. CNN depicted one strength, that is, an accuracy of 99.68%. To that effect, intrusion detection improved after employing autoencoders but performed poorly when the minority class was considered at 96.45%. Using generative adversarial networks, synthetic data can be generated to balance class representation or improve detection of rare attacks without causing overfitting.Classifier-level methods such as WRF and XGBoost weight the minority classes very well, but this has a limiting effect on larger datasets. Deep learning models, including CNN, MLP, and SNN work very well with complex data; the CNN model, in this context, had 99.68% accuracy. Future work would thus incorporate enhanced techniques such as ensemble learning, hybrid models, and transfer learning together with real-time analytics and adaptive algorithms to support improvement toward achieving more accuracy and for evolving threats.

References

1. Hassan, H. A., Hemdan, E. E. D., El-Shafai, W., Shokair, M., Abd El-Samie, F. E. (2024). Detection of attacks on software defined networks using machine learning techniques and imbalanced data handling methods. Security and Privacy, 7(2), e350.
2. Yueai, Z., Junjie, C. (2009, April). Application of unbalanced data approach to network intrusion detection. In 2009 First International Workshop on Database Technology and Applications (pp. 140-143). IEEE.
3. Alam, T., Ahmed, C. F., Zahin, S. A., Khan, M. A. H., Islam, M. T. (2019). An effective recursive technique for multi-class classification and regression for imbalanced data. IEEE Access, 7, 127615-127630.
4. Leevy, J. L., Khoshgoftaar, T. M., Peterson, J. M. (2021, August). Mitigating class imbalance for iot network intrusion detection: a survey. In 2021 IEEE Seventh International Conference on Big Data Computing Service and Applications (BigDataService) (pp. 143-148). IEEE.
5. Berbiche, N., El Alami, J. (2024). For Robust DDoS Attack Detection by IDS: Smart Feature Selection and Data Imbalance Management Strategies. Ingénierie des Systèmes d'Information, 29(4).
6. HACILAR, H., Aydin, Z. A. F. E. R., GÜNGÖR, V. Ç. (2024). Network intrusion detection based on machine learning strategies: performance comparisons on imbalanced wired, wireless, and software-defined networking (SDN) network traffics. Turkish Journal of Electrical Engineering and Computer Sciences, 32(4), 623-640.
7. Zhang, G., Wang, X., Li, R., Song, Y., He, J., Lai, J. (2020). Network intrusion detection based on conditional Wasserstein generative adversarial network and cost-sensitive stacked autoencoder. IEEE access, 8, 190431-190447.
8. Rao, Y. N., Suresh Babu, K. (2023). An imbalanced generative adversarial network-based approach for network intrusion detection in an imbalanced dataset. Sensors, 23(1), 550.

9. Babu, K. S., Rao, Y. N. (2023). A study on imbalanced data classification for various applications. Revue d'Intelligence Artificielle, 37(2), 517.
10. Babu, K. S., Rao, Y. N. (2023). MCGAN: modified conditional generative adversarial network (MCGAN) for class imbalance problems in network intrusion detection system. Applied Sciences, 13(4), 2576.
11. Rezvani, S., Wang, X. (2023). A broad review on class imbalance learning techniques. Applied Soft Computing, 143, 110415.
12. Bedi, P., Gupta, N., Jindal, V. (2020). Siam-IDS: Handling class imbalance problem in intrusion detection systems using siamese neural network. Procedia Computer Science, 171, 780-789.
13. Vu, L., Nguyen, Q. U. (2020). Handling imbalanced data in intrusion detection systems using generative adversarial networks. Journal of Research and Development on Information and Communication Technology, 2020(1), 1-13.
14. Chimphlee, S., Chimphlee, W. (2023). Machine learning to improve the performance of anomaly-based network intrusion detection in big data. Indonesian Journal of Electrical Engineering and Computer Science, 30(2), 1106-1119.
15. Gonzalez-Cuautle, D., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Portillo-Portillo, J., Olivares-Mercado, J., ... Sandoval-Orozco, A. L. (2020). Synthetic minority oversampling technique for optimizing classification tasks in botnet and intrusion-detection-system datasets. Applied Sciences, 10(3), 794.
16. Greeshma, B., Sireesha, M., Thirumala Rao, S. N. (2022, February). Detection of arrhythmia using convolutional neural networks. In Proceedings of Second International Conference on Sustainable Expert Systems: ICSES 2021 (pp. 21-30). Singapore: Springer Nature Singapore.
17. Moturi, S., Vemuru, S., Tirumala Rao, S. N., Mallipeddi, S. A. (2023, February). Hybrid Binary Dragonfly Algorithm with Grey Wolf Optimization for Feature Selection. In International Conference On Innovative Computing And Communication (pp. 611-625). Singapore: Springer Nature Singapore.