An Explainable and Optimized Network Intrusion Detection Model using Deep Learning

Haripriya C[1], Prabhudev Jagadeesh M.P[2]
Research Scholar, JSS Academy of Technical Education, Bengaluru, Affiliated to VTU Belagavi, India[1]
Assistant Professor, Global Academy of Technology, Bengaluru, Affiliated to VTU Belagavi, India[1]
Professor, JSS Academy of Technical Education, Bengaluru, Affiliated to VTU Belagavi, India[2]

***Abstract*—In the current age, internet and its usage have become a core part of human existence and with it we have developed technologies that seamlessly integrate with various phases of our day to day activities. The main challenge with most modern-day infrastructure is that the requirements pertaining to security are often an afterthought. Despite growing awareness, current solutions are still unable to completely protect computer networks and internet applications from the ever-evolving threat landscape. In the recent years, deep learning algorithms have proved to be very efficient in detecting network intrusions. However, it is exhausting, time-consuming, and computationally expensive to manually adjust the hyper parameters of deep learning models. Also, it is important to develop models that not only make accurate predictions but also help in understanding how the model is making those predictions. Thus, model explainability helps increase user's trust. The current research gap in the domain of Network Intrusion Detection is the absence of a holistic framework that incorporates both optimization and explainable methods. In this research article, a hybrid approach to hyper parameter optimization using hyperband is proposed. An overall accuracy of 98.58% is achieved by considering all the attack types of the CSE CIC 2018 dataset. The proposed hybrid framework enhances the performance of Network Intrusion Detection by choosing an optimized set of parameters and leverages explainable AI (XAI) methods such as Local Interpretable Model agnostic Explanations (LIME) and SHapely Additive exPlanations (SHAP) to understand model predictions.**

Keywords—Network Intrusion Detection; deep learning; hyper parameter optimization; hyperband; CSE CIC IDS 2018 dataset; XAI methods; LIME; SHAP

I. Introduction

With cyberattacks becoming increasingly prevalent, it is imperative that businesses shift their focus towards cybersecurity. Our lives have transitioned to be internet centric after the pandemic, but cybersecurity problems are also intensifying every day. Researchers are concentrating on creating Deep Learning (DL) based Network Intrusion Detection System (NIDS) to identify zero-day attacks as new varieties of cyberattacks continue to emerge. Outdated attack traffic and no representation of contemporary attack types leads to poor representation of real time network traffic. Also, redundancy, anonymity due to privacy or ethical issues, simulated traffic, lack of traffic diversity, and the absence of an all-inclusive dataset are some issues with most of the existing datasets. Despite numerous attempts, the research community is yet to accomplish the development of systems that can handle threats without human intervention. Malicious cyberattacks create significant security risks, necessitating the development of an innovative, adaptable, and more dependable Intrusion Detection System (IDS). The number of Internet-connected devices is anticipated to reach 50 billion by the end of the decade [1]. Although, techniques for infiltration and security defences have advanced dramatically during the past decade, a significant number of organizations still use outdated cybersecurity solutions.

Considering the above challenges, the primary objective of this research article, is to implement an explainable and optimized network intrusion detection model using DL techniques. The proposed work incorporates both optimization and XAI methods. The main contributions are as follows:

- Implement hyperband algorithm on the proposed DNNHXAI (Deep Neural Network Hypertuned XAI) model to choose optimized parameters.
- Investigate explainability of the proposed model using LIME and SHAP.

II. Literature Survey

Notable numbers of works are proposed in the area of NIDS, Abdulnaser et al. used Apache Spark and DL models on the CSE CIC 2018 dataset. The authors conclude that Spark drastically reduces the training time when compared to DL models [2]. Haripriya et al. performed distributed training of deep auto-encoder including all the attacks of the CSE CIC IDS 2018 dataset. The authors achieved an accuracy of 98.96% by training their proposed model on two worker nodes. [3]. Kanimozhi et al. used Artificial Neural Networks (ANN) and used only the benign and botnet traffic of the CSE CIC 2018 dataset. They used Grid Search CV to perform hyper parameter tuning. However, the authors conclude that their proposed model can be extended to detect the remaining classes of the dataset and usage of higher end frameworks like Tensor Flow to perform hyper tuning optimization [4]. Vimal Gaur implemented Machine Learning (ML) algorithms on CICDDoS2019 dataset to detect Distributed Denial of Service (DDoS) attacks and performed hyper parameter tuning. The author concludes that hyper parameter tuning increases the accuracy by 2.01% [5]. Priya Maidamwar et al. implemented ML algorithms on UNSW-NB15 dataset and used Grid Search CV as their hyper parameter tuning technique. An improvement in accuracy and minimization of False Alarm Rate (FAR) was observed [6].

Amin et al. propose a ML based NIDS model for binary classification on CSE CIC-IDS 2018 dataset. However, they observed that minority classes are misclassified due to class imbalance and suggest researchers to use techniques like Synthetic Minority Oversampling Technique (SMOTE) [7]. Haripriya et al. effectively addressed the class imbalance problem of the CIC CSE IDS2018 dataset by using SMOTE. They used deep autoencoder to classify all the attacks of the dataset [8]. Rambasnet applied and compared various State-of-the-art frameworks on CSE CICIDS2018 dataset. Their findings demonstrate the usefulness of different DL frameworks for detecting network intrusion traffic. An accuracy of 99% was achieved. However, since the class imbalance of the dataset was not addressed, a large number of infiltration samples were misclassified [9].

Anita Shiravani et al. proposed a new method for effectively selecting features using fuzzy numbers. The authors emphasize on the fact that dimensionality reduction plays a major role in pre-processing which in turn improves the system performance [10]. Mohammad Mausam et al. proposed a NIDS framework using Bayesian Optimization (BO) with Gaussian Process (GP). They implemented their proposed method on NSL-KDD dataset and conclude BO-GP outperforms Random Search Optimization [11]. Yoon Teck et al. implemented ML algorithms on CICIDS 2017 dataset and used BO-Tree-structured Parzen Estimator (BO-TPE) as the hyper parameter tuning technique. The authors direct future researchers to apply hyper parameter optimization on DL algorithms to substitute their ML approaches [12].

Abdulatif et al. implemented ML algorithms in Kitsune dataset used in the domain of NIDS. The authors recommend Grid Search optimizer with Tree algorithm for Kitsune dataset [13]. Hyojoon et al. use Proximal Policy Optimization (PPO) algorithm on CICDS2017 and UNSW-NB15 datasets to control the hyper parameters of Deep Neural Network (DNN)-based feature extractor and K-Means cluster module. The authors conclude that feature engineering is crucial in NIDS data pre-processing and direct future researchers to carry out research using diverse datasets [14]. Sara Emadi et al. implement Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN) algorithms on the NSL-KDD dataset. The authors conclude that research in the area of NIDS can further be improved by reducing the training time and using hyper parameter tuning to improve the overall performance [15]. Haripriya et al. carry out a comprehensive study on different benchmark IDS datasets and their impact on network intrusion techniques [16]. The authors insist on the fact that the quality of the dataset plays a vital role in the domain of NIDS.

Zhibo zang et al. carries out an extensive survey on different methods, categorization, research gaps and challenges of XAI in the domain of Cyber security [17]. Pieter Barnard et al. use XGBoost model on the NSL-KDD dataset. The authors use SHAP to explain their proposed model [18]. Zakaria et al. use DNN on NSL-KDD and UNSW-NB15 dataset. The authors conclude their work by using LIME, SHAP and Rule fit methods to improve the interpretability of the proposed model [19]. Shraddha Mane et al. implement DNN on NSL-KDD dataset and use XAI methods to generate explanations [20]. Basim Mahbooba et al. addressed explainability by using Decision Tree (DT) on KDD dataset [21]. Syed wali et al. implements Random Forest (RF) on CIC CSE IDS2018 dataset and used SHAP as an XAI method [22].

Studies from literature reveal that hyper parameter tuning is very important to decide on the best architecture of the DL model. Although researchers have previously worked on optimization algorithms for hyper parameter tuning, there is an increasing need to use advanced optimization algorithms for hyper parameter tuning to speed up the training process. When it comes to optimization, overlooking hyperparameter optimization altogether is the most substantial mistake one can make. Modest adjustments to hyperparameter values can have a significant effect on model's performance. Especially in the domain of network security, the main aim is to speed up the process of intrusion detection and help network administrators to take immediate action before a catastrophic attack on the network occurs. XAI methods can help minimize model bias by outlining the standards for making decisions. Therefore, monitoring the model using XAI methods help in lessening the bias and also unexpected consequences. Previous research works in the field of NIDS reveal that, researchers have either used hyper parameter optimization methods or XAI methods in the field of NIDS. It is observed that none of the researchers used both the methods. This research article leverages both hyper parameter tuning and XAI methods, thus providing hyper optimization along with a comprehensive understanding of model's predictions.

III. Methodology

The proposed framework is divided into two stages. First hyper parameter tuning is done using hyperband. Secondly, XAI methods such as SHAP and LIME are used to interpret the model predictions.

A. Dataset Description and Pre-processing

The proposed work uses the CSE CIC IDS2018 dataset. The main rationale behind choosing the CSE CIC IDS 2018 dataset is, it reflects the current attacks. Unlike the outdated KDD Cup 99 dataset, it also includes a wide range of attacks. It is very essential to choose the dataset that reflects real time network traffic comprising a wide diversity of attacks. The dataset consists of a total of 16,000,000 samples spread over 10 CSV files. The dataset was collected from Amazon Web Services (AWS) S3 bucket [23].

Data type conversion was carried out by converting 64 bit values to 32 bit values. Features containing only one variable were dropped. Also features having infinite and Not a Number (NAN) values were also dropped. Label encoding and one-hot encoding was performed on the different attack types of the dataset. It was noticed that the dataset suffers from class imbalance. It is observed that the number of samples belonging to benign (normal) were more when compared to the attack class. Class imbalance leads to "Accuracy paradox". For instance, while using training data with a very high percentage of benign samples, a model could be trained to predict normal traffic with high accuracy, but it might not be good at detecting attack traffic. Similar observations were made on all the files of the dataset. Thus, to overcome the limitations of the class imbalance, SMOTE was used in the proposed model.

B. Workflow of the Proposed Model

The entire workflow of the proposed framework is shown in Fig. 1. The CSE CIC IDS 2018 dataset is collected from the AWS S3 bucket. To help speed up the training process and improve accuracy, pre-processing is carried. Class imbalance problem of the dataset is addressed using SMOTE [24]. Then the DL model is developed by using DNN. Hyper parameter tuning is carried out using hyperband algorithm and an optimized set of parameters are chosen [25]. The performance of the model is evaluated on the test dataset.

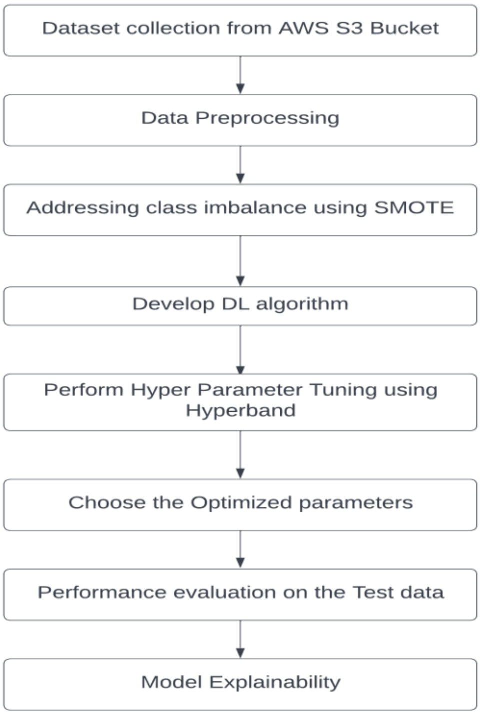

Dataset collection from AWS S3 Bucket
Data Preprocessing
Addressing class imbalance using SMOTE
Develop DL algorithm
Perform Hyper Parameter Tuning using Hyperband
Choose the Optimized parameters
Performance evaluation on the Test data
Model Explainability

Fig. 1. Workflow of the proposed model.

C. Importance of Hyper Parameter Tuning in the Proposed Work

The performance of any ML/DL model depends on the configuration. One major challenge in implementing any ML/DL algorithm is discovering an optimal configuration for the model and the training algorithm. Hyper Parameter Optimization (HPO) is a technique to deal with the challenge of fine-tuning DL hyper parameters. Tuning in an enormous search space is an exhausting process. Data-driven techniques must be employed to address the issues with HPO. Manual processes are ineffective. There are several hyper parameter tuning algorithms namely Random search, Bayesian Optimization (BO) and hyper band. Random search is the least efficient algorithm as it randomly selects parameter combinations from a search space rather than learning from previously tried parameter combinations. BO uses an optimization method that is sequential, and thereby it cannot be used well with parallel resources pair.

Speeding up configuration evaluation is the primary objective of an orthogonal approach to hyper parameter optimization. Hyperband can be considered as an extension of the successive halving approach; the goal of the Hyperband is to regularly apply successive halving to address the trade-off between the number of configurations and resource allocation. Additionally, it can find the ideal combination faster by using successive halving. The primary idea is to fit numerous models for a limited number of epochs and to only continue training the models that perform best on the validation set. Therefore, in comparison to commonly used hyper tuning algorithms like BO, hyperband can dramatically speed up a variety of DL and kernel-based learning tasks. All the above factors motivated us to use hyperband as the hyper parameter tuning technique in the proposed model.

D. Need for Model Explainability in the Proposed Work

Considering the large sizes of NIDS datasets, performance becomes the bottleneck. DL models are incomprehensible, counterintuitive, and challenging for people to understand. All the DL models act like black-box structures. Because DL models are so complicated, interpretability research has taken multiple avenues. Over the years, DL models evolved by improving the performance metrics to handle large data but with increasing complexity came less interpretability. Feature importance methods were used to show how each feature is important to model prediction in general. However, these methods do not give information about individual predictions. Also, which features tend to increase or decrease the prediction is not known. Understanding ML model is referred to as model explainability. There are numerous advantages of integrating XAI methods with DL algorithms. It enables individuals to mitigate the negative impacts of automated decision-making and help in more informed decisions. To identify and protect security vulnerabilities. Integrating algorithms with human values is an essential goal. As an instance, suppose a model is able to determine if the traffic is normal or malicious, the network administrators have to know what parameters the model has considered. This helps to know whether the model contains any bias. It is also essential for network administrators to understand and describe the model's predictions once it has been implemented. Fig. 2 illustrates the importance of XAI methods in the proposed work.

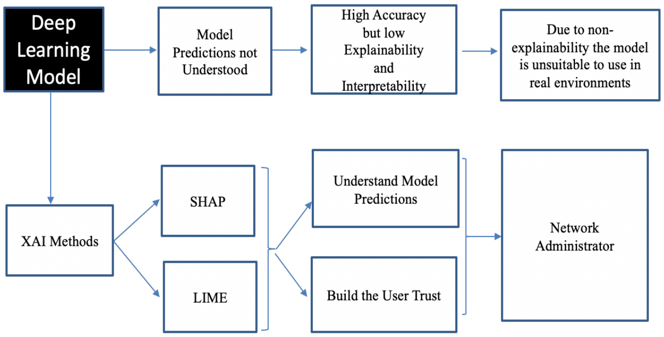

Deep Learning Model
Model Predictions not Understood
High Accuracy but low Explainability and Interpretability
Due to non-explainability the model is unsuitable to use in real environments
XAI Methods
SHAP
LIME
Understand Model Predictions
Build the User Trust
Network Administrator

Fig. 2. Explainable AI methods used in the proposed DNNHXAI model.

IV. Experimental Setup

Table I illustrates the different hyper parameters used while training the proposed DNNHXAI model. The number of hidden units ranged from 2 to 32 with a step value of 3. The number of hidden values ranged from 2 to 10. Different activations such as relu, tanh, sigmoid were used. Relu was the most preferred activation function. The dropout values ranged from 0.0 to 0.1 with a step size of 0.05. An optimized learning rate of 0.001 was chosen. Table II gives the different general parameter values used while training. The batch size was set to 128 with 15 epochs. The loss functions used were binary cross entropy and categorical cross entropy for binary and multi-classification respectively. Adam optimizer was chosen as preferred optimizer as it helps the model to converge faster.

TABLE I. Different Parameters Used for Hyper Parameter Tuning

Sl No	Name of the hyper parameter	Range of values for different hyper parameters	Best hyper parameters given by Hyperband

1	Number of units	Min_value=2, Max_value = 32
		Step=3,
		Default=32
			Units in 0th layer = 29
			Units in 1st layer = 5

2	Number of layers	Min_value =2,
		Max_value = 10
			2

3	Activation	Dense Activation
		Values=relu,tanh, sigmoid
		Default= relu
			relu

4	Dropout	Min_value=0.0,
		Max_value = 0.1
		Default = 0.005,
		Step = 0.05
			0.1

5	Learning Rate	Values = 1e -2,1e -3,1e -4	0.001

TABLE II. Gives the Different General Parameter Values used while Training

Sl.No	Parameter	Value
1	Batch size	128
2	Number of epochs	15
3	Loss function	Binary Cross entropy Categorical Cross entropy
4	Optimizer	Adam

All the experiments were carried out using Google Colab which is a cloud-based environment. To speed up the training process, Graphical Processing Units (GPU) was chosen as the runtime option. The train – test split was set to 75% and 25 % respectively.

V. Results and Discussion

An accuracy of 96.67% was achieved without hyper parameter tuning. With usage of hyperband (see Fig. 3) as the hyper parameter tuning technique, the accuracy peaked to 98.58%.

SHAP and LIME methods are used to explain the predictions of the proposed model [26] [27]. Fig. 4 gives the waterfall plot. It shows how a positive SHAP value positively impacts the prediction. On the contrary, a negative SHAP Value has a negative impact on the prediction. The magnitude helps us understand how strong the impact is. It also illustrates the feature importance of SHAP analysis by using the summary plot by considering the CSV file containing Distributed Denial of Service (DDOS) attack. The chosen CSV file contains two classes benign (normal traffic) and DDOS (attack traffic). The Class label is encoded as ‘0’ and ‘1’ for Benign and DDOS attack respectively. As per the result, min packet length is the highest ranking feature.

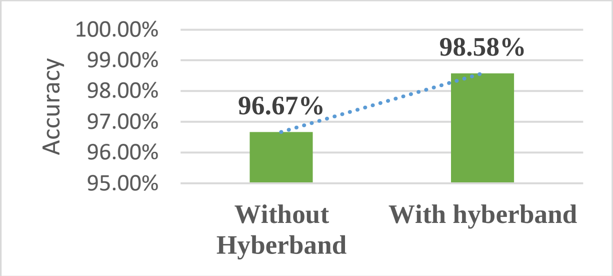


Fig. 3. Difference in accuracy with and without hyperband optimization.

Fig. 5 illustrates how LIME can be used to understand local predictions given by the model by considering the Comma Separated Values (CSV) file containing DDOS attack in the CSE CIC IDS 2018 dataset. The features shaded in blue indicate positive influence on the output. Conversely, the features shaded in orange indicate negative influence on the output. Similar experiments were conducted on the different attacks of the dataset. The key difference between SHAP and LIME is how they provide explanations. SHAP uses a game-theoretic approach to provide global explanations. Conversely, LIME is model specific that provides local interpretable explanations. In this research work, an attempt was made to investigate model interpretability using SHAP and LIME. However, it is observed that LIME explanations are not robust because of its instability. For each prediction, a new explanatory is generated by the LIME algorithm. Thus, small variations in the data lead to different interpretations. In contrast, SHAP helps in providing global explanations, therefore explaining the overall model’s behavior across all the instances. Finally, we conclude that SHAP performs better than LIME.

Table III gives the comparative analysis of the proposed work with other latest works exiting in the literature. It is observed that researchers have either used Optimization or Explainability but not both. Also, outdated datasets like NSL-KDD that do not reflect current attacks are still being used. Conventional hyper parameter tuning techniques like Grid Search CV are no longer suitable as it is time-exhaustive and computationally expensive, especially if it involves a high dimensional search space. Although, Random Search CV is better than Grid search CV, a lot of variance is observed because of its randomness. Research works [3][4][5][10][11] use different optimization methods for hyper parameter tuning. Research works [17][18][19][20][21][28] use different XAI methods. Table III clearly illustrates that none of the previous works in the field of NIDS incorporated a hybrid model leveraging both hyper-parameter optimization and explainability. Comparison was based on the usage of optimization, XAI method and accuracy as the performance metric. In this research article, a hybrid approach incorporating both optimization and explainability is implemented. Advanced Optimization algorithms such as a hyperband helps in finding the hyper parameters faster with improved accuracy. Explainable methods such as LIME and SHAP help in gaining greater insights on the data by understanding model predictions and thus increasing user's trust in the model.

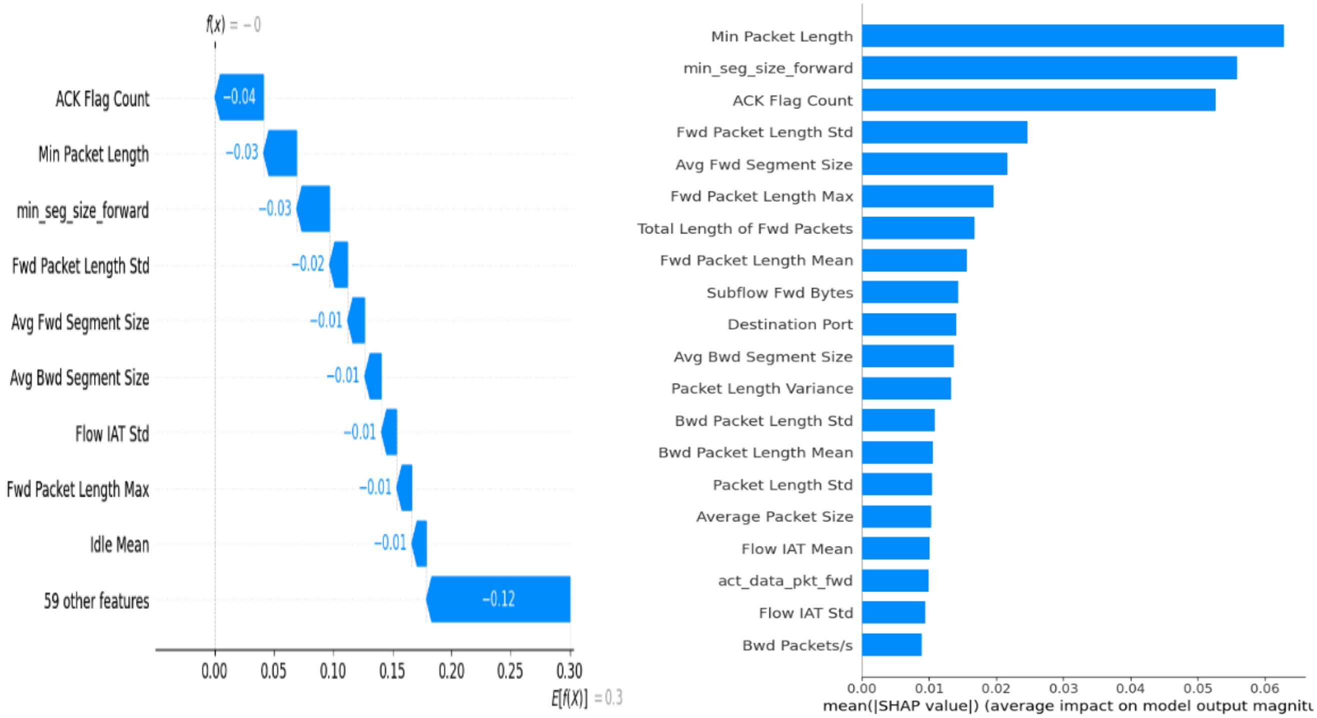
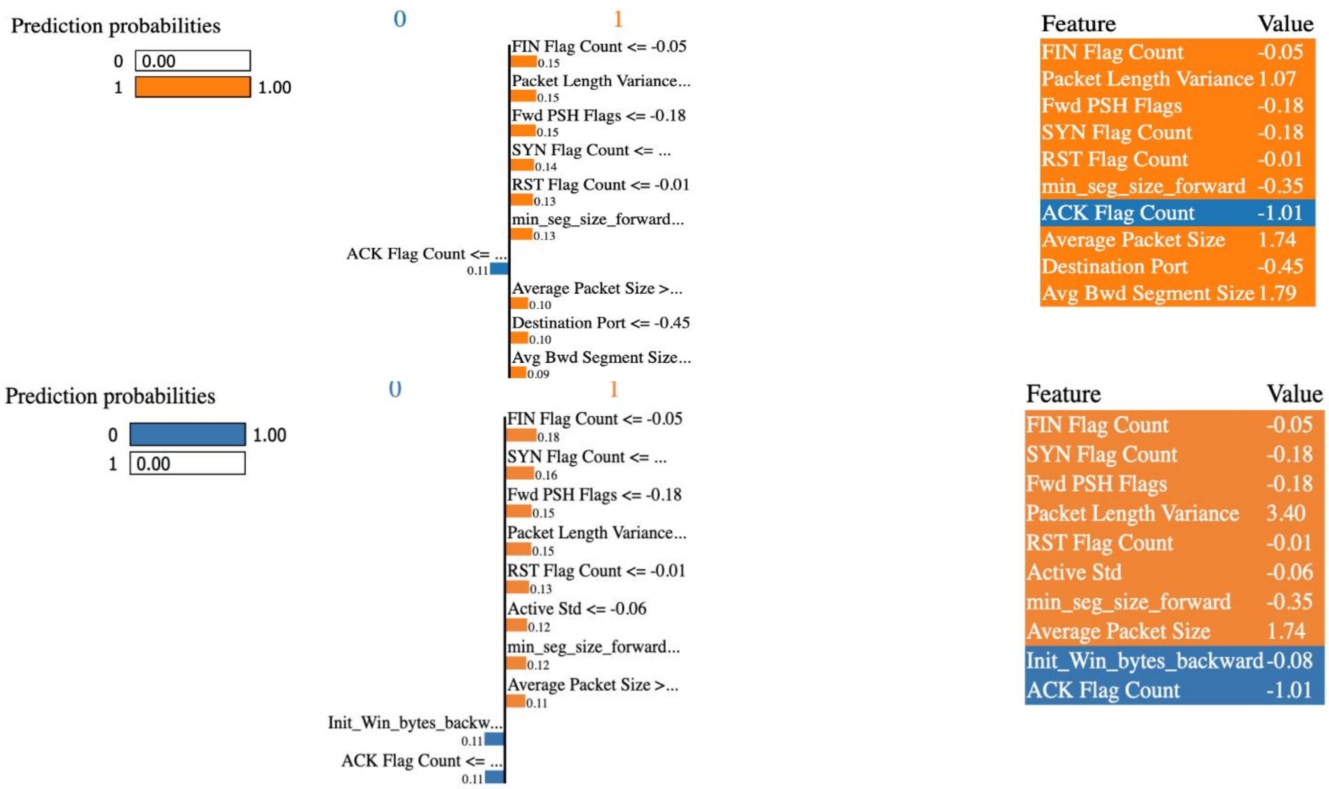


Fig. 4. SHAP explanations using summary and waterfall plot.



Feature	Value
FIN Flag Count	-0.05
Packet Length Variance	1.07
Fwd PSH Flags	-0.18
SYN Flag Count	-0.18
RST Flag Count	-0.01
min_seg_size_forward	-0.35
ACK Flag Count	-1.01
Average Packet Size	1.74
Destination Port	-0.45
Avg Bwd Segment Size	1.79

Feature	Value
FIN Flag Count	-0.05
SYN Flag Count	-0.18
Fwd PSH Flags	-0.18
Packet Length Variance	3.40
RST Flag Count	-0.01
Active Std	-0.06
min_seg_size_forward	-0.35
Average Packet Size	1.74
Init_Win_bytes_backward	-0.08
ACK Flag Count	-1.01

Fig. 5. LIME local explanations.

TABLE III. COMPARATIVE ANALYSIS OF THE PROPOSED WORK

Sl.No	Authors	Algorithm used	Dataset Used	Optimization method	XAI method	Accuracy
1	Kanimozhi et al. [3], 2019	ANN	CSECIC IDS 2018	Grid Search CV	-	99.97%
2	Vimal Gaur et al. [4], 2022	ML algorithms	CICDDoS2019	NA	-	98.78%
3	Priya R Maidamwar et al. [5] , 2022	RF and MLP	UNSW NB15	Grid Search CV	-	99.34%
4	Mohammad Mausam et al. [10], 2022	DNN	KDDTest+ KDDTest21	BO-GP BO-GP	-	82.95% 54.99%
5	Yoon Teck et al. [11], 2022	ML algorithms	CICIDS 2017	BO-TPE	-	98%
7	Pieter Barnard et al. [17], 2022	XGBoost, autoencoder	NSL -KDD	-	SHAP	93.28%
8	Zakaria et al. [18], 2022	DNN	NSL-KDD and UNSW-NB15	-	LIME, SHAPE, and Rule Fit	88%
9	Shraddha Mane et al. [19], 2021	DNN	KDD test+	-	SHAP, LIME, and BRCG	82.4%
10	Basim Mahabooba [20], 2021	DT	KDD	-	Self-explainable	NA
11	Syed Wali et al. [21] , 2021	Stacked RF	CICIDS	-	SHAP	98.5% 100%
12	Deepak Kumar et al. [28], 2022	RF, KNN	NSL KDD99	-	SHAP, LIME	99.4%
13	**Proposed Work**	**DNNHXAI**	**CSECICIDS 2018**	**Hyperband**	**SHAP, LIME**	**98.58%**

VI. CONCLUSION

With the advancement in technology, the number of cyberattacks is increasing exponentially. Although, DL models prove to be efficiently detect intrusions, its complexity has increased tremendously at the price of massive computational overhead. It is exhausting, time-consuming, and computationally expensive to manually adjust the hyper parameters of DL models. In this research paper, hyperband an advanced hyper parameter tuning algorithm is applied on the proposed DNNHXAI model. It is observed that the configuration of model hyper parameters has a significant impact on its prediction accuracy. Although DL models today are able to achieve very good accuracies, there is an increasing need to enhance the user's trust by using XAI methods. First, the algorithm should have the best performing parameter configured and XAI methods should be used to deduce the contributing factors. Particularly, in the domain of cybersecurity, an attacker can largely exploit a vulnerability within few seconds. To address the above stated challenges, an attempt is made to not only configure the best parameters but also to understand the model predictions in an efficient manner. A single model that can detect a variety of attacks is proposed. It is efficient to quickly differentiate between normal and attack traffic. The proposed model overcomes the problems encountered in traditional DL algorithms w.r.t hyper parameter optimization and explainability. Instance by instance explanation is done with both LIME and SHAP. The main outcome of combining hyper parameter tuning with XAI techniques is to enable network administrator to take appropriate action based on the certainty of a detected attack. Considering all the files of the dataset, an overall accuracy of 96.67% and 98.56% is achieved without and with hyper parameter tuning respectively. The framework implements efficient pre-processing techniques, addresses class imbalance, uses the latest benchmark IDS dataset that reflects recent attacks, implements advanced hyper parameter tuning techniques and leverages XAI methods to understand model's predictions. Promising results were achieved and an improvement in model's performance is observed when hyper parameter tuning is used. XAI methods are used to increase the explainability of model's predictions. As a future work, researchers are advised to leverage transfer learning techniques on the latest datasets in the domain of NIDS. Also, additional XAI methods can be used on different DL algorithms to explain model's predictions more efficiently.

REFERENCES

[1] Singh, Satyanand. (2021). Environmental Energy Harvesting Techniques to Power Standalone IoT-Equipped Sensor and Its Application in 5G Communication. Emerging Science Journal. 4. 116-126. 10.28991/esj-2021-SP1-08.

[2] Hagar, Abdulnaser & Gawali, Dr.Bharti. (2022). Apache Spark and Deep Learning Models for High-Performance Network Intrusion Detection Using CSE-CIC-IDS2018. *Computational Intelligence and Neuroscience*. 2022. 1-11. 10.1155/2022/3131153.

[3] Haripriya C and Prabhudev Jagadeesh M. P, "Distributed Training of Deep Autoencoder for Network Intrusion Detection" *International Journal of Advanced Computer Science and Applications* (IJACSA), 14(6), 2023. http://dx.doi.org/10.14569/IJACSA.2023.0140633.

[4] Kanimozhi, V. & Jacob, Prem. (2019). Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 cloud computing. ICT Express. 5. 10.1016/j.icte.2019.03.003.

[5] Vimal Gaur, Dr. Rajneesh Kumar (2022). HPDDoS: A HyperParameter Model for Detection of Multiclass DDoS Attacks. *Vol. 71 No. 3s2 (2022): Special Issue on Mathematics Theory and its Contribution in Robotics and Computer Engineering.*

[6] Maidamwar, P. R., Bartere, M. M., & Lokulwar, P. P. (2022). Classification of Hybrid Intrusion Detection System Using Supervised Machine Learning with Hyper-Parameter Optimization. *Journal of Algebraic Statistics*, 13(3), 1532-1550.

[7] Amin Lama, Dr. Preeti Savant (2022). Network-Based Intrusion Detection Systems Using Machine Learning Algorithms. *International Journal of Engineering Applied Sciences and Technology*, 2022 Vol. 6, Issue 11, ISSN No. 2455-2143, Pages 145-155.

[8] Haripriya C, Prabhudev Jagadeesh M. P (2022). An Efficient Autoencoder Based Deep Learning Technique to Detect Network

Intrusions. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, 13(7), 13A7P, 1-9. http://TUENGR.COM/V13/13A7P.pdf DOI: 10.14456/ITJEMAST.2022.142.

[9] Basnet, Ram & Shash, Riad & Johnson, Clayton & Walgren, Lucas & Doleck, Tenzin. (2019). Towards Detecting and Classifying Network Intrusion Traffic Using Deep Learning Frameworks. 10.22667/JISIS.2019.11.30.001.

[10] Shiravani, A., Sadreddini, M.H. & Nahook, H.N. (2023) Network intrusion detection using data dimensions reduction techniques. *J Big Data 10*, 27. https://doi.org/10.1186/s40537-023-00697-5.

[11] Masum, Mohammad & Shahriar, Hossain & Haddad, Hisham & Hossain Faruk, Md Jobair & Valero, Maria & Khan, Md & Rahman, Mohammad & Adnan, Muhaiminul & Cuzzocrea, Alfredo. (2022). Bayesian Hyperparameter Optimization for Deep Neural Network-Based Network Intrusion Detection..

[12] Yoon-Teck Bau, Tey Yee Yang Brandon. (2022) Machine Learning Approaches to Intrusion Detection System Using BO-TPE. Atlantis Highlights in Computer Sciences. *Proceedings of the International Conference on Computer, Information Technology and Intelligent Computing* (CITIC 2022).

[13] Alabdulatif, & Rizvi, Sajjad. (2023). Network intrusion detection system using an optimized machine learning algorithm. Mehran University Research Journal of Engineering and Technology.42.153.10.22581/ muet1982.2301.14.

[14] Han, H.; Kim, H.; Kim, Y. An Efficient Hyperparameter Control Method for a Network Intrusion Detection System Based on Proximal Policy Optimization. Symmetry 2022, 14, 161. https://doi.org/10.3390/ sym14010161.

[15] Al-Emadi, Sara & Al-Mohannadi, Aisha & Al-Senaid, Felwa. (2019). Using Deep Learning Techniques for Network Intrusion Detection. 10.1109/ICIoT48696.2020.9089524.

[16] Haripriya C, Prabhudev Jagadeesh M. P. "A Review of Benchmark Datasets and its Impact on Network Intrusion Detection Techniques," 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, 2022, pp. 1-6, doi: 10.1109/CCIP57447.2022.10058660.

[17] Zhang, Zhibo & Al Hamadi, Hussam & Damiani, Ernesto & Yeun, Chan & Taher, Dr. Fatma. (2022). Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. 10.48550/arXiv.2208.14937.

[18] Barnard, Pieter & Marchetti, Nicola & Silva, Luiz. (2022). Robust Network Intrusion Detection Through Explainable Artificial Intelligence (XAI). IEEE Networking Letters. 4. 1-1. 10.1109/LNET.2022.3186589.

[19] Z. A. E. Houda, B. Brik and L. Khoukhi, "“Why Should I Trust Your IDS?”: An Explainable Deep Learning Framework for Intrusion Detection Systems in Internet of Things Networks," in IEEE Open Journal of the Communications Society, vol. 3, pp. 1164-1176, 2022, doi: 10.1109/OJCOMS.2022.3188750.

[20] S. Mane and D. Rao, “Explaining Network Intrusion Detection System Using Explainable AI Framework.” arXiv, Mar. 12, 2021. doi: 10.48550/arXiv.2103.07110.

[21] B. Mahbooba, M. Timilsina, R. Sahal, and M. Serrano, “Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model,” *Complexity*, vol. 2021, p. e6634811, Jan. 2021, doi: 10.1155/2021/6634811.

[22] Wali, syed & Khan, Irfan. (2021). Explainable AI and Random Forest Based Reliable Intrusion Detection system. 10.36227/techrxiv.17169080.v1.

[23] A Realistic Cyber Defense Dataset (CSE-CIC-IDS2018) was accessed on 01.01.2023 from https://registry.opendata.aws/cse-cic-ids2018.

[24] Chawla, Nitesh & Bowyer, Kevin & Hall, Lawrence & Kegelmeyer, W. (2002). SMOTE: Synthetic Minority Over-Sampling Technique. J. Artif. Intell. Res. (JAIR). 16. 321-357. 10.1613/jair.953.

[25] Li Lisha, Jamieson Kevin, DeSalvo Giulia, Rostamizadeh Afshin, and Talwalkar Ameet. 2017. Hyperband: A novel bandit-based approach to hyperparameter optimization. J. Mach. Learn. Res. 18, 1 (2017), 6765–6816.

[26] Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. Advances in neural information processing systems, 30.

[27] Ribeiro, Marco & Singh, Sameer & Guestrin, Carlos. (2016). “Why Should I Trust You?”: Explaining the Predictions of Any Classifier. 97-101. 10.18653/v1/N16-3020.

[28] Deepak Kumar Sharma, Jahanavi Mishra, Aeshit Singh, Raghav Govil, Gautam Srivastava, Jerry Chun-Wei Lin, (2022) *Explainable Artificial Intelligence for Cybersecurity, Computers and Electrical Engineering*, Volume103,108356,ISSN 00457906, https ://doi.org/10.1016/j.compele ceng.2022.108356.