IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

DeepDefender: High-Precision Network Threat Classification Using Adversarial-Resistant Neural Networks

Gaurav Sarraf
Independent Researcher
sarrafgsarraf@gmail.com

Abstract: *Deep learning is a recent technology that is applicable in different areas in the contemporary world. The applications that identify potential adversarial attacks and prevent them are utilized in order to offer effective solutions associated with the broad spectrum of computer security with the assistance of deep learning (DL) models. With the ever-growing adversarial deep learning, accessibility to the deep learning model can vary in the number of levels, and in this case, the attackers can conduct a series of attacks to reach the intended goal. Concurrently, the DL models and algorithms are quite susceptible to numerous cybersecurity attacks. The research details a potential approach to classifying and predicting network threats using an ANN model trained on the CICIDS 2017 dataset. To evaluate the efficacy of the stratified data-splitting artificial neural network (ANN) model, key performance indicators were recall (REC), accuracy (ACC), precision (PRE), and F1-score (F1). The results show that the model is robust and trustworthy in detecting and classifying different types of cyberattacks, with a 99.7% ACC rate, a 99.9% PRE rate, a 99.9% REC rate, and an F1 of 99.9%. These results show that deep learning systems based on ANNs have the ability to improve network security.*

Keywords: Cyber Security, Threat Classification, Intrusion Detection, Network Security, Artificial Intelligence, Artificial Neural Networks

I. INTRODUCTION

The resilience of adversarial attacks has been of greater interest in the modern world and has received more attention in addition to new ways of constructing them and superior defense mechanisms [1]. In the recent past, cyberattacks have taken a new form particularly those that are related to systems where sensitive information is stored or processed. Critical national infrastructures are of great concern due to the reliance that they attach to their systems regarding significant information or service provision. The environment of the sphere of cybersecurity is constantly changing, and online communication plays the primary role in adversarial attacks, and more ingenious and sophisticated methods are implemented on the traditional vectors [2].

The cost of cybercrime is estimated at trillions of dollars annually across the globe. Traditional cybersecurity tools, such as rule-based detection tools, are not as dynamic as the present-day cyberattack, thus are more likely to result in security breaches [3][4]. The rule-based detection systems database system signature is a manual system that should be updated by human specialists on a periodic basis and fine-tuned [5][6]. This makes the conventional detection systems inefficient to handle high volumes of data in real-time because the primary cause is slow training and adaptation. This has contributed to the need to have more intelligent and adaptable ways of countering these malevolent activities prior to their having a significant impact [7][8].

ML and DL have the ability to adapt to new instances of attack and learn past occurrences, implying that they are powerful approaches to being proactive in identifying threats [9]. The cyber threat detection system, which is based on ML and DL, offers adequate and timely detection of threats. First, the system gathers, processes and pre-processes network traffic data and retrieves useful information about the packets e.g. packet size, arrival times between packets and protocol information [10][11]. The data undergoes the steps of data preparation multiple times to make it believable

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

before it is used to train the models. Assuming the application of ML and DL models, anomalies can be recognized on the pre-processed data. ML and DL models can enhance cybersecurity protection with the constant addition of new data. The current cybersecurity issues can be addressed using this scalable and flexible approach.

Motivation and Contribution

The proposed research project is informed by the growing frequency, complexity, and advancement of computer attacks on modern networks, posing serious threats to data integrity and confidentiality, and the stability of critical infrastructure. Conventional intrusion detection systems have a hard time with large volumes of multidimensional network traffic, which means that they can hardly detect the new and varied forms of attacks. The proposed research designed to create a network intrusion forecasting and categorization model capable of identifying both familiar and unfamiliar attacks on the basis of advanced ML and DL tools. The model must be robust, precise and flexible. The rationale of the study is to enhance network security, reduce false positives, and provide a tool that provides accurate results of preventing threats in timely and high-risk contexts. There are several critical contributions that this study has brought about as discussed below:

- Implemented a comprehensive data preparation process for the CICIDS 2017 dataset, including handling missing values, noise removal, and normalization.
- Proposed and mathematically detailed a dedicated ANN model designed for complex intrusion detection tasks.
- PCA-based feature selection and Random Oversampling to optimize both dataset dimensionality and class balance before model training.
- Using a battery of evaluation measures, including ACC, PRE, REC, and F1, allowed for a thorough and impartial assessment of the model's effectiveness.

A. Organization of the Paper

The following is the paper's outline: In Section II, literature review on network threat classification and prediction. Section III explains the dataset, the preparation procedures, and how the model is put into action. Section IV presents the findings from the experiments as well as a comparison analysis. Section V closes the study by analyzing major points, addressing consequences, and proposing ideas for additional research.

II. LITERATURE REVIEW

A thorough review and analysis of significant research studies on Network Threat Prediction and Classification was carried out to guide and strengthen the development of this study.

Mishra (2021) The classification of regular and problematic traffic was accomplished using a SVM learning algorithm. The goal of conducting network traffic analysis was to identify and block any potentially harmful data transfers. The applications utilized were A tree architecture for the network, an emulator for minijets used for network design, an OS for hosting the emulator, VMware Fusion for creating virtual environments, and Ubuntu Linux. To access the network traffic captured in an existing cap file, Wireshark was utilized. With a 99% success rate, the SVM classifier outperformed the others [12].

Sivamani, Sahay and Gamal (2020) provide a novel method for improving the main classification network in order to detect harmful inputs. An adversary familiar with the victim classifier would have a very hard time penetrating the detection system due to the presence of many observer networks. Attain an ACC of 97.5% on the CIFAR-10dataset and 99.5% on the MNIST dataset by implementing the Fast Gradient Sign Attack in a semi-white box configuration. By all accounts, the optimal outcome reveals a false positive rate of about 0.12% [13].

Joloudari et al. (2020) APT-attacks on the NSL-KDD dataset can be detected and categorized in real-time using ML approaches such as C5.0 DT, Bayesian networks, and DL. This leads to ACC values of 95.64% for the C5.0 DT, 88.37% for the Bayesian network, and 98.85% for the 6-layer DL model. Also, the 6-layer DL model had an FPR of 1.13, the Bayesian network model had an FPR of 10.47, and the C5.0 decision tree model had an FPR of 2.56, the essential threshold [14].

Ahmad et al. (2020) suggested an IDS that uses a DNN. The DL-based system keeps an eye on both legitimate and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

fraudulent traffic. Accuracy levels of up to 99.78% are achieved when it sorts and separates harmful traffic. Employed in experiments and compared to earlier methods reveals promising outcomes [15].

Dawoud et al. (2020) explore the possibility of using DL for anomaly detection by contrasting autoencoders, which are non-probabilistic algorithms, with constrained Boltzmann machines, which are models built on generative energy. This paper focuses on unsupervised DL algorithms and seeks to give a full evaluation of various approaches. The simulated trials show a detection ACC of around 99% when compared to similar work [16].

Kumar et al. (2019) developed a technique to identify potential dangers by analyzing darknet data to train Machine Learning classifiers. An approach based on concept drift detector and supervised machine learning was suggested in this research. The findings demonstrate that classifiers have an ACC of over 99% when it comes to identifying both old and new threats and can easily differentiate between malicious and benign communications [17].

A significant knowledge vacuum remains regarding the scalability, generalizability, and real-time adaptability of these systems in ever-changing network settings, even though numerous deep learning and machine learning models have attained remarkable ACC rates for intrusion detection and adversarial input classification. Most studies such as those summarized in Table I focus on static datasets (e.g., NSL-KDD, MNIST, CIFAR-10) or simulated traffic, limiting their applicability to evolving threat landscapes and heterogeneous network infrastructures. Furthermore, while ensemble and hybrid models show promise, few works address cross-domain validation, concept drift, or integration with live monitoring systems. Research in the future needs to fill these gaps by creating adaptable frameworks that can withstand adversarial evasion, zero-day attacks, and real-time deployment on various platforms

Table 1: Comparative Summary of Machine Learning and Deep Learning Techniques for Network Threat Detection

Author	Proposed Work	Data	Results	Limitations & Future Work
Mishra (2021)	Used SVM to classify normal vs. abnormal traffic. Conducted static and dynamic malware analysis.	Wireshark; network designed using Mininet emulator and VMware Fusion; Ubuntu Linux OS with tree topology.	SVM achieved 99% ACC in classifying malicious traffic.	Limited to SVM; future work could explore ensemble models and real-time traffic adaptation.
Sivamani, Sahay & Gamal (2020)	Detect adversarial inputs using multiple binary observer networks	MNIST and CIFAR-10 datasets;	Detection ACC: 99.5% (MNIST), 97.5% (CIFAR-10); false positives: 0.12%	Tested only on image datasets; applicability to network traffic can be explored
Joloudari et al. (2020)	Analysis of the NSL-KDD dataset for APT-attack detection using C5.0, Bayesian networks, and 6-layer deep learning	NSL-KDD dataset.	ACC: 95.64% (C5.0), 88.37% (Bayesian), 98.85% (DL); FPR: 2.56, 10.47, 1.13	Dataset limitations; real-time detection efficiency not evaluated
Ahmad et al. (2020)	Detecting harmful and valid traffic using DNN in IDS	Network traffic from authentic and non-authentic sources.	ACC: 99.78%	Need to address evolving threats; overfitting prevention methods can be enhanced
Dawoud et al. (2020)	Anomaly detection using unsupervised deep learning (RBM & Autoencoders)	Simulated network traffic datasets	Detection ACC ≈ 99%	Tested on simulation data; real-world deployment can be studied
Kumar et al. (2019)	Threat identification using ML classifiers on	Darknet traffic datasets	ACC > 99%	Focused on darknet traffic; scalability to large

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

	darknet traffic, including concept drift detection			networks needs assessment

III. RESEARCH METHODOLOGY

The methodology involved using the CICIDS 2017 dataset, which was preprocessed by handling missing values, noise removal, and min–max normalization. The next step in reducing dimensionality while keeping critical information was data balancing, which followed feature selection by principal component analysis (PCA). A 70:30 split was used to divide the additional data into training and testing sets in order to maintain the class distribution. In the end, a model trained on an ANN was put into action, and its ACC, PRE, REC, and F1 among other important metrics were computed using a confusion matrix to guarantee a thorough evaluation of the model's classification abilities. Figure. 1. shows the Proposed flowchart for Network Threat Prediction and Classification are shown below:

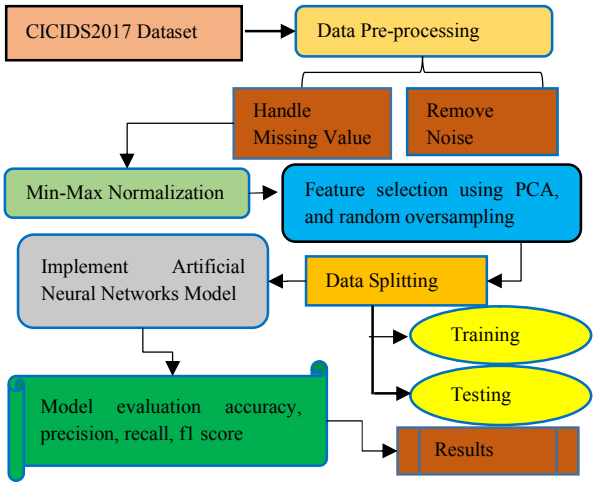

Fig. 1. Proposed Flowchart for Network Threat Prediction and Classification

Each component of the suggested methodology is detailed in the section that follows.

A. Data Collection

This analysis makes use of the CICIDS 2017dataset. Including the label information, there are 85 aspects and approximately 2.8 million data points. BruteForceFile TransferProtocol, BruteForce SecureShell, DDoS, Heartbleed, WebAttack, Infiltration, Botnet, and DistributedDebugging are just a few of the many attacks that have been implemented. The following are examples of data visualizations that were employed to analyses the distribution of attacks, feature correlations, etc. bar plots and heatmaps:

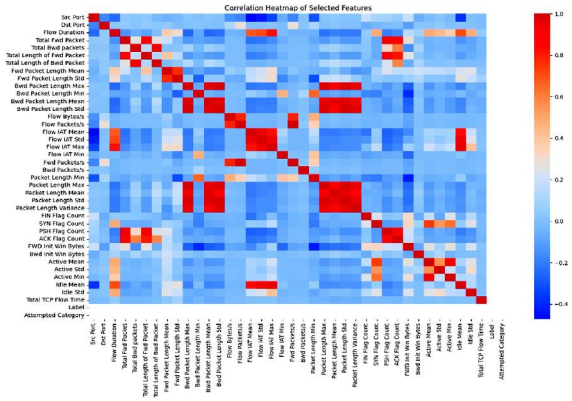

Fig. 2. Feature Correlation Analysis

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

Figure 2 visualizes the correlations among chosen attributes in the network traffic dataset. The color gradient signifies the degree of linear correlations between features; a diagonal line of deep red squares indicates perfect self-correlation, while blue denotes negative correlation and red positive correlation. Features that are important for feature selection and dimensionality reduction, like packet length, flow time, and header flags, exhibit different levels of interdependence. This analysis is essential for identifying redundant or highly correlated variables that may impact model performance or introduce bias.

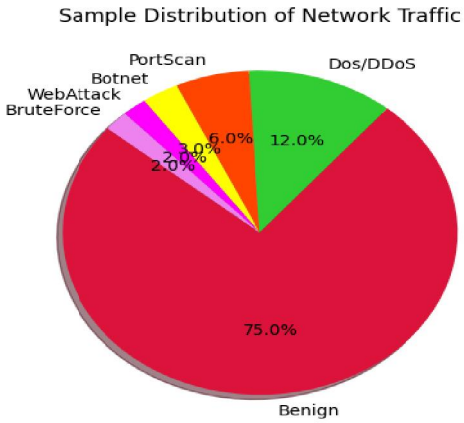

Fig. 3.Pie chart for Class distribution

Figure 3 shows the class distribution of network traffic, where Benign traffic dominates at 75%, followed by DoS/DDoS (12%), PortScan (6%), and smaller shares of BruteForce, WebAttack, and Botnet. This imbalance underscores the importance of meticulous model tuning to ensure accurate detection across all classes.

B. Data Pre-Processing

Data preparation was based on the CICIDS 2017, and it included concatenation, cleaning, and feature engineering. The pre-processing procedures covered the treatment of missing data, removal of noise, and normalization. The most important pre-processing processes are as follows:

- **Handle missing value:** Missing data handling missing data involves the methods of dealing with the lack of item or case data during data integration, which can be incomplete datasets or differences in the way items are labelled.
- **Remove Noise:** A noise reduction is described as any filtering operation on an image that helps smooth the image but avoids blurring areas of contrast boundaries, which is typically accomplished by a median filtering or an edge and detail preservation algorithm.

C. Min-Max Normalization

Feature normalization was carried out using the min-max technique, bringing them to a range of 0 to 1. This was done to make the classifiers better and make the outliers less of an impact. Normalization was accomplished out in the mathematical formula shown in Equation (1):

$$X' = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

X is the starting point for the feature, X' is its normalized value, X_{min} is its minimum value, and X_{max} is its maximum value.

D. Feature Selection Using PCA

The two-step procedure for feature selection using PCA is as follows: first, the original features are transformed using PCA to generate new uncorrelated components; second, the features are chosen according to their contribution to the most significant principal components, which are typically identified by their loadings. By sorting features according to their variance-heavy principal component contributions, this approach can minimize dimensionality without losing any

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

useful information for the model.

E. Random Oversampling (RO)

A rudimentary approach to rebalancing the class distribution in an imbalanced dataset is provided by random oversampling (RO). Considering the importance of RO in rebalancing datasets to enhance performance without causing overfitting, it incorporates instances randomly from the minority group into the training set. The proposed framework also takes into consideration big, imbalanced datasets. As shown in Figure 4, the RO process.

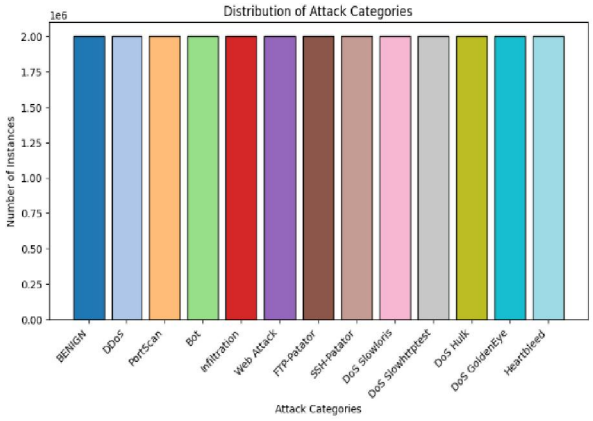

Fig. 4. Balanced Distribution of CICIDS2017 Dataset by Attack Category

Figure 4 presents the balanced distribution of attack categories within the CICIDS2017 dataset. The x-axis lists a wide variety of forms of attack and the Y-axis is used to measure the number of attacks per category, with the highest number being 2 million. All bars have an equal or similar height, and it is about 1.75 million cases, which shows that there is a consistent representation of all types of attacks. It is an essential aspect of machine learning because it provides more robust models in training since it reduces class imbalance and provides equal evaluation of various threat categories.

F. Data Splitting

A stratified split of 70:30 was used to divide the dataset into two parts one for training and one for testing. This methodology made sure that the two samples had the same representation of classes as the original sample.

G. Proposed Artificial Neural Networks (ANN) Model

ANNs are a sort of computer model that seeks to replicate the way the human brain analyzes information in order to identify hidden patterns and connections. A network of interconnected neurones called an input, hidden, and output layer makes up an ANN. The neurons react to the inputs as weighted connections and activation functions and thus, the network learns through the various algorithms like backpropagation. ANNs are founded on the human body and they are generally used in such activities as classification, pattern recognition, and also acquisition of data through experience via synapses as shown by Equation (2).

$$y_k = \varphi(u_k + b_k)u_k = \sum_{j=0}^{m} w_{kj}x_j \qquad (2)$$

A bias that influences an input of the activation function φ is denoted by b_k, and w_{kj} is the synaptic weight of input x_jTo k. A multilayer perceptron's strength lies in its hidden neurons, which are highly connected to one another through synapses. This allows the network to recognize patterns, which is essential for solving difficult issues. Iterative algorithms are able to train biases and weights using an error function that is defined for the n-th iteration on neuron i as Equation (3):

$$e_i = d_i(n) - y_i(n) \qquad (3)$$

Where the neuron's output is denoted by y and d is the desired output. For an O-sized output layer, this error function

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

can be refined as an error energy function in Equations (4 and 5):

$$E_{avg} = \frac{1}{N}\sum_{n=1}^{N} E(n) \quad (4)$$

$$E(n) = \frac{1}{2}\sum_{i=1}^{o} e_i^2(n) \quad (5)$$

The size of the dataset is denoted as N. To achieve maximum efficiency, optimization involves minimizing the error energy function as it propagates backwards through the network, layer by layer.

H. Evaluation Metrics

The suggested design was tested with various performance indicators to determine its efficacy. A Confusion Matrix was constructed to represent the overall number of accurate and wrong guesses for every class, providing a summary of the categorization outcomes. This matrix was used to produce the values of TP, FP, TN, and FN, which stand for True Negatives. Following the presentation and formulation in Equations (6) to (9) of these values, important performance measures like REC, ACC, PRE, and F1-score were computed:

$$Accuracy = \frac{TP+TN}{TP+Fp+TN+FN} \quad (6)$$

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

$$F1-score = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (9)$$

The ACC is the proportion of input samples that yield accurate predictions as a percentage of the entire sample size. As a percentage of the total numb of positive occurrences, the proportion of successfully predicted positive cases shows the quantity of genuine positives recognized by the model. The REC metric compares the number of TP to the number of accurately predicted positives, indicating how well the model detects positive cases. In cases of class imbalance, the F1 a balanced metric ranging from 0 to 1 is particularly helpful because it is the harmonic mean of REC and PRE.

IV. RESULTS AND DISCUSSION

An NVIDIA RTX 3090 GPU with 24 GB of video RAM and an Intel Core i9-11900 K CPU (3.5 GHz, 8 cores, 16 threads) were the components used in the desktop PC that was subjected to the trials. With an eye towards system analysis and design, the OS in question was Ubuntu 20.04 LTS. Table II provides a summary of the outcomes of training and testing the proposed model using important performance measures on the CICIDS 2017dataset. The model's 99.7% ACC rate shows that it consistently produces trustworthy predictions across the dataset. The ANN model consistently identifies threats with remarkable consistency, with PRE, REC, and F1 all recorded at 99.9%. It does this while minimizing FP and FN. The findings indicate the effectiveness and strength of the model in dealing with complex intrusion detection problems with close to perfection classification.

Table 2: Results of the proposed model for Network Threat Classification

Performance Matrix	Artificial Neural Networks (ANN) Model
Accuracy	99.7
Precision	99.9
Recall	99.9
F1-score	99.9

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 2, Issue 1, May 2022
Impact Factor: 6.252

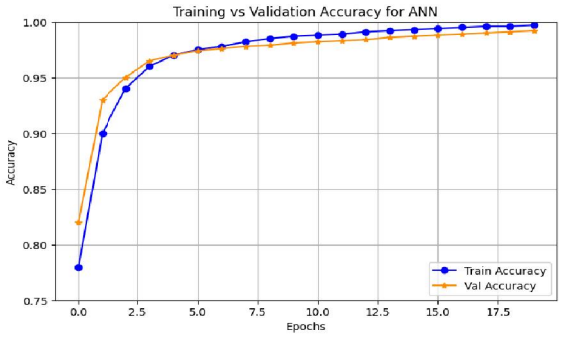

Fig. 5. Training and Validation Accuracy Curve for the ANN Model

Figure 5 displays the ACC of the model over multiple training and validation epochs. A consistent increase is observed in both the training and validation ACC (blue and orange lines, respectively), with the former showing quick progress in the early epochs and the latter showing a slow stabilization as they approach 1.0. When the training and validation curves are so closely aligned, it means the model is learning well without excessive overfitting and has achieved high ACC on both datasets by the time training is complete.

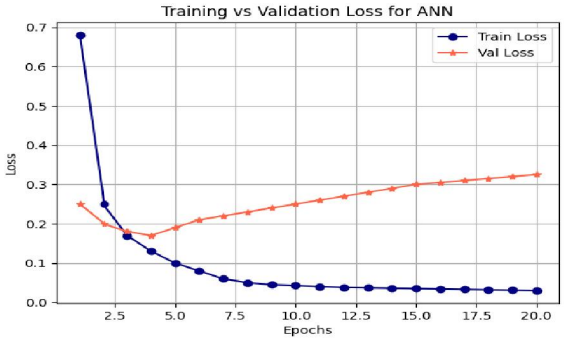

Fig. 6. Training and Validation Loss Curve for the ANN Model

A neural network's Train Loss (blue line) and Val Loss (orange line) throughout training epochs are shown in Figure 6, which clearly indicates overfitting. Initially, both losses decrease sharply; however, around epoch 3, the Val Loss reaches its minimum point (approximately 0.12) and begins to steadily increase, rising to over 0.3 by the final epoch.

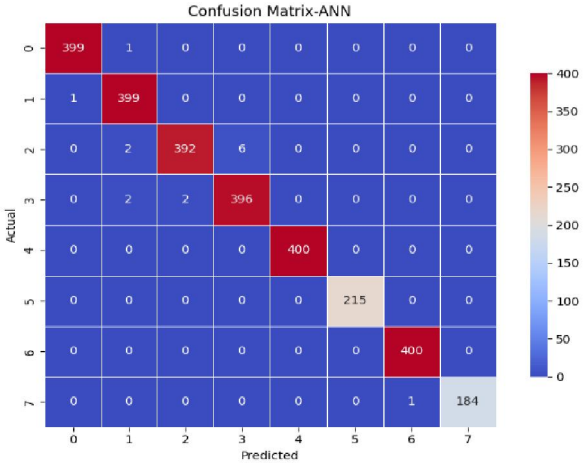

Fig. 7. Confusion Matrix for the ANN Model

In contrast, the Train Loss continues its descent to a value near zero, showing the model is becoming exceptionally

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

good at minimizing loss on the training data. This growing divergence, where training performance improves while performance on the unseen validation data deteriorates, is the classic signature of a model that has learned the training data's noise or specific examples too well, resulting in poor generalization.

Figure 7 shows the ANN model's confusion matrix, which shows how well it classified eight different classes (0–7). The matrix highlights strong diagonal dominance, indicating high ACC in correctly predicting each class, with perfect classification for classes 0, 1, 3, 4, and 6. Minor misclassifications are observed for class 2 (6 instances predicted as class 3) and class 7 (1 instance predicted as class 6), suggesting minimal confusion. The color gradient from blue (low values) to deep red (high values) visually reinforces the model's PRE, with the darkest cells aligned along the diagonal, confirming the ANN's robust predictive capability.

A. Comparative analysis

The efficacy of the ANN model is evaluated by comparing its ACC with other models that are currently available, as shown in Table III. The SVM was able to give an ACC of 90.1%, DNN improved on the ACC of the SVM with 96.4, LR again improved on ACC of the DNN with 96.6 indicating high reliability. ANN had the highest ACC (99.7%) and almost perfect PRE, REC, and F1 (99.9%), which proves that it is superior and strong in Network Threat Prediction and Classification tasks.

Table 3: Comparison of different ML and dl models for network threat classification on cicids 2017 dataset

Model	Accuracy	Precision	Recall	F1-score
SVM[18]	90.1	-	92.6	78.6
DNN[19]	96.4	96.2	96.5	-
LR[20]	96.6	97	99	98
ANN	99.7	99.9	99.9	99.9

The proposed ANN-based model has a huge advantage in predicting and classifying threats to the network with a high level of ACC. The DL structure enables the model to acquire complex patterns and relationships between high-dimensional network traffic data, which can be utilized effectively to detect and classify a large range of cyberattacks. The model has a superior PRE, REC and F1 besides high ACC, meaning that it is a reliable model insofar as minimizing FP and FN are concerned. The above strengths render the ANN model very robust and applicable in real-life network security applications that offer a potent instrument for detecting threats in time and in an accurate manner.

V. CONCLUSION AND FUTURE STUDY

The rapid digitization and multiplication of the internet-connected devices not only transformed everyday lives but also created a vast and highly dangerous attack surface to the cybercriminals that continuously grows more complicated and malevolent as a part of the cybersecurity environment. Deep machine learning has demonstrated good performance in classification of network traffic. According to the outcome of the experiment, the comparative analysis of different ML and DL models on the CICIDS 2017dataset in the network threat prediction and classification showed that traditional models such as SVM have a moderate rate of 90.1, and DL models showed a higher performance, with a rate of 96.4 and 96.6, respectively, with DNN and LR. All other models produced lower results than the proposed ANN model, which had the highest ACC of 99.7% meaning that it had a better ability to pick the complex pattern and relationship in the network traffic data. This demonstrates how perfect DNNs are for powerful network security applications, especially ANN, for reliably identifying and categorizing various cyberattacks. The ever-changing threat of cyberattacks necessitates a multi-DL strategy for improving earlier threat forecasts by discovering trends in past data over a long track.

REFERENCES

[1] J. X. Morris, E. Lifland, J. Y. Yoo, J. Grigsby, D. Jin, and Y. Qi, "TextAttack: A Framework for Adversarial Attacks, Data Augmentation, and Adversarial Training in NLP," in *EMNLP 2020 - Conference on Empirical Methods in Natural Language Processing, Proceedings of Systems Demonstrations*, 2020. doi:

10.18653/v1/2020.emnlp-demos.16.

[2] D. C. Le, N. Zincir-Heywood, and M. I. Heywood, "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning," *IEEE Trans. Netw. Serv. Manag.*, vol. 17, no. 1, pp. 30–44, Mar. 2020, doi: 10.1109/TNSM.2020.2967721.

[3] G. Sarraf, "Behavioral Analytics for Continuous Insider Threat Detection in Zero-Trust Architectures," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 596–602, 2021.

[4] I. Ghafir *et al.*, "Detection of advanced persistent threat using machine-learning correlation analysis," *Futur. Gener. Comput. Syst.*, vol. 89, pp. 349–359, Dec. 2018, doi: 10.1016/j.future.2018.06.055.

[5] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System," *IEEE Access*, vol. 8, pp. 83965–83973, 2020, doi: 10.1109/ACCESS.2020.2992249.

[6] K.-D. Lu, G.-Q. Zeng, X. Luo, J. Weng, W. Luo, and Y. Wu, "Evolutionary Deep Belief Network for Cyber-Attack Detection in Industrial Automation and Control System," *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7618–7627, Nov. 2021, doi: 10.1109/TII.2021.3053304.

[7] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems," *J. Inf. Secur. Appl.*, vol. 58, p. 102717, May 2021, doi: 10.1016/j.jisa.2020.102717.

[8] K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," in *2020 International Conference on Cyber Warfare and Security (ICCWS)*, IEEE, Oct. 2020, pp. 1–6. doi: 10.1109/ICCWS48432.2020.9292388.

[9] S. B. V. Naga, K. C. Sunkara, S. Thangavel, and R. Sundaram, "Secure and Scalable Data Replication Strategies in Distributed Storage Networks," *Int. J. AI, BigData, Comput. Manag. Stud.*, vol. 2, no. 2, pp. 18–27, 2021, doi: 10.63282/3050-9416.IJAIBDCMS-V2I2P103.

[10] E. Sheybani and G. Javidi, "Seminars in Proactive Artificial Intelligence for Cybersecurity (SPAIC)," *IMCIC 2019 - 10th Int. Multi-Conference Complexity, Informatics Cybern. Proc.*, vol. 17, no. 1, 2019.

[11] V. M. L. G. Nerella, "Architecting secure, automated multi-cloud database platforms strategies for scalable compliance," *Int. J. Intell. Syst. Appl. Eng.*, vol. 9, no. 1, pp. 128–138, 2021.

[12] S. Mishra, "Network Traffic Analysis Using Machine Learning Techniques in IoT Networks," *Int. J. Softw. Innov.*, vol. 9, no. 4, pp. 107–123, 2021, doi: 10.4018/IJSI.289172.

[13] K. S. Sivamani, R. Sahay, and A. El Gamal, "Non-Intrusive Detection of Adversarial Deep Learning Attacks via Observer Networks," *IEEE Lett. Comput. Soc.*, vol. 3, no. 1, pp. 25–28, Jan. 2020, doi: 10.1109/LOCS.2020.2990897.

[14] J. Hassannataj Joloudari, M. Haderbadi, A. Mashmool, M. Ghasemigol, S. S. Band, and A. Mosavi, "Early Detection of the Advanced Persistent Threat Attack Using Performance Analysis of Deep Learning," *IEEE Access*, vol. 8, pp. 186125–186137, 2020, doi: 10.1109/ACCESS.2020.3029202.

[15] S. Ahmad, F. Arif, Z. Zabeehullah, and N. Iltaf, "Novel Approach Using Deep Learning for Intrusion Detection and Classification of the Network Traffic," in *2020 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/CIVEMSA48639.2020.9132744.

[16] A. Dawoud, O. A. Sianaki, S. Shahristani, and C. Raun, "Internet of Things Intrusion Detection: A Deep Learning Approach," in *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, IEEE, Dec. 2020, pp. 1516–1522. doi: 10.1109/SSCI47803.2020.9308293.

[17] S. Kumar, H. Vranken, J. van Dijk, and T. Hamalainen, "Deep in the Dark: A Novel Threat Detection System using Darknet Traffic," in *2019 IEEE International Conference on Big Data (Big Data)*, IEEE, Dec. 2019, pp. 4273–4279. doi: 10.1109/BigData47090.2019.9006374.

[18] J. Lee, J. Kim, I. Kim, and K. Han, "Cyber Threat Detection Based on Artificial Neural Networks Using Event Profiles," *IEEE Access*, vol. 7, pp. 165607–165626, 2019, doi: 10.1109/ACCESS.2019.2953095.

[19] K. Atefi, H. Hashim, and T. Khodadadi, "A Hybrid Anomaly Classification with Deep Learning (DL) and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 2, Issue 1, May 2022 Impact Factor: 6.252

Binary Algorithms (BA) as Optimizer in the Intrusion Detection System (IDS)," in *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*, IEEE, Feb. 2020, pp. 29–34. doi: 10.1109/CSPA48992.2020.9068725.

[20] P. Jairu, "A Supervised Machine Learning Approach to Network Intrusion Detection on CICIDS-2017 Dataset," St. Cloud State University, 2021.