

Multi-Class DDoS Attack Classification using Deep Neural Networks (DNN): A Critical Analysis

Amal Saad Aljabri, Nouf Hendi Aljohani, and Walaa Sulaiman Aljohani
College of Computer Science and Engineering, Taibah University, Madinah 41477, Saudi Arabia

Abdul Ahad Siddiqi

Associate Professor, Department of Computer Science, College of Computer Science and Engineering, Taibah University, Madinah 41477, Saudi Arabia
asadqi@taibahu.edu.sa

Abstract

The Multi-class Distributed Denial of Service (DDoS) attack classification using deep neural networks includes different types of network floods into specific types with high accuracy. A DDoS attack is when mischievous actors flood a server or network with fake traffic so real users cannot access the service. This emphasizes the use of intelligent systems for detection with the help of Machine Learning and Deep Learning. Such intelligent systems have overcome the problem of identifying huge volumes of malicious traffic among the legitimate network traffic and can handle high dimensional and complex data. This paper addresses need to develop, implement, and stringently evaluate a resource-efficient deep neural network model on the effective multi-class classification of 12 distinct types of DDoS attacks using the realistic CIC-DDoS2019 dataset in order to contribute to robust real-time threat detection in modern networks. The paper presents critical analysis which is beyond mere documentation to quantitative comparison and qualitative assessment, focusing on the trade-offs between performance, efficiency, and operational limitations. The proposed methodology has seven phases: data collection, data preparation, model design, model training, model evaluation, model validation, and model deployment. The core findings and achievements of the research are based on the methodology executed, have confirmed that the shift from the simple ML models to the more complex DL architectures, namely DNN, was well -grounded

Keywords: DDoS, Machine Learning, AI, Deep Neural Networks (DNN).

1. Introduction

1.1. Problem Definition:

DDoS attacks are among the most serious and continuous threats to modern networks, attempting to destroy the availability and integrity of services over the Internet. The traditional static mechanisms could hardly be effective against the rapid evolution of such attacks, their increasing sophistication, and the fact that they are automated. Figure 1 depicts general architecture of DDoS architecture.

This emphasises the use of intelligent systems for detection with the help of Machine Learning and Deep Learning. Such intelligent systems will overcome the problem of identifying huge volumes of malicious traffic among the legitimate network traffic and can handle high dimensional and complex data. Using models such as Decision Trees, Random Forests, Deep Neural Networks, Convolutional Neural Networks, Recurrent Neural Networks, or hybrid and ensemble approaches like DBN pre-training with DNN classifiers coupled with Fuzzy Logic, improvement in detection accuracy can be significant. These intelligent systems will also enhance the capability to detect novel zero-day attacks and ensure continuity of service and robust security in dynamic network environments [6], [7]. The Convolutional Neural Networks (CNN) and ResNet plug spatial patterns in traffic data and achieve high accuracy rates. The EfficientSTNet is a modern framework combines autoencoders and attention mechanisms to reach 99.14% overall accuracy. On the other hand, the LSTM Autoencoders models process sequential data to flag live anomalies in real time.

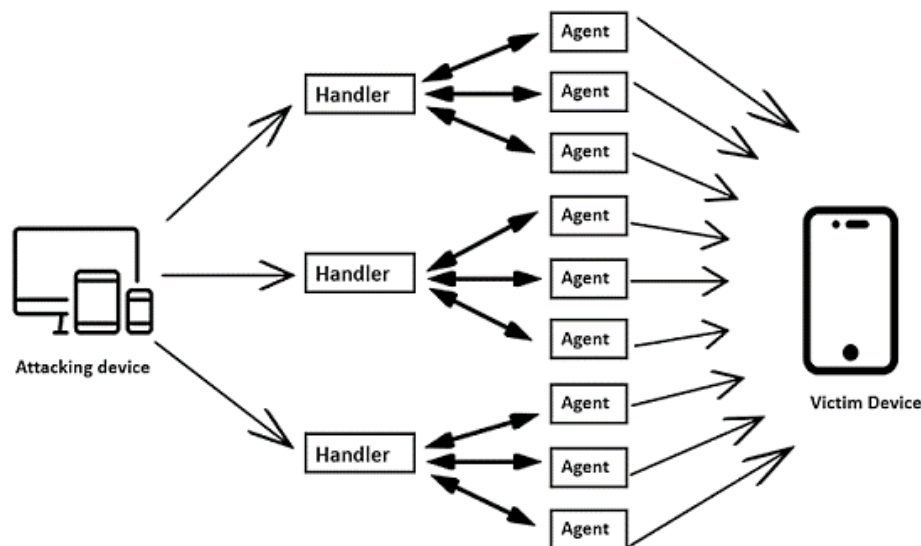


Figure (1): General architecture of DDoS architecture

1.2. Background:

The persistent threat of DDoS attacks has spawned a thriving demand for efficient anomaly detection methods that go beyond traditional signature-based defense mechanisms [6], [7]. Many traditional ML models can detect known patterns of attack traffic with satisfying accuracy but often falter in their performance when new or evolving threats are encountered. Some deep learning models, more precisely DNNs, have shown better performance in processing complex network traffic of high dimensionality compared to many conventional anomaly-based intrusion detection models by detecting very subtle patterns related to malicious activities [6], [7]. State-of-the-art adaptive DDoS attack detection systems exploit feature learning and pattern recognition capabilities of DNNs to

support efficient data processing of very large-size datasets and enable real-time threat detection capabilities [6], [7].

1.3. Aims and Objectives of Research:

The main purpose of this study is to develop, implement, and stringently evaluate a resource-efficient deep neural network model on the effective multi-class classification of 12 distinct types of DDoS attacks using the realistic CIC-DDoS2019 dataset in order to contribute to robust real-time threat detection in modern networks.

The steps in achieving this aim are:

1. Advanced Data Preparation: Perform sophisticated preprocessing of the selected dataset, CIC-DDoS2019, by cleaning the data and balancing it using the SMOTE technique to improve the efficiency and effectiveness of the model for all attack types.
2. Design Supervised Classification Architecture: The aim is to develop an ad-hoc DNN architecture to perform supervised classification of network traffic-classification of the detected network flow by means of several fully connected layers.
3. Model Implementation: DNN -The proposed system of attack detection through the realization of a DNN model enables it to learn inherent complex patterns for multi-class classification among 12 different attack types and normal traffic.
4. Model Training and Configuration: Train the DNN model using the Adam optimizer and categorical cross-entropy loss function by considering early stopping to avoid model overfitting.
5. Performance Evaluation: The model efficiency should be thoroughly validated by documenting and analyzing all the critical performance metrics -Accuracy, Precision, Recall, and F1-Score, together with a Confusion Matrix, as proof that the system will be able to discriminate malicious DDoS attacks from legitimate traffic.
6. Real-time Deployment: In this step, the validated model is transferred from the testing phase to practical use by deploying it in SDN network environment for real-time detection and directly alerting the detected DDoS attacks in real time.

The paper is organized as follows. Section 2 presents a literature survey and analysis. Section 3 provides our proposed research methodology. Section 4 concludes the project and suggests future work.

2. Literature Survey

This detailed paper identifies the core and methodological elements required for data extraction and critical analysis of research papers addressing DDoS attack detection using ML and DL techniques.

The paper aims to provide a robust academic structure for constructing the "Literature Survey" and "Critical Analysis" sections of any specialized research work, emphasizing quantitative comparison and the identification of research gaps.

2.1. Literature Review: Specific Relevant Studies on DNN:

Recent research has focused on hybrid models, which exploit the specialized strengths of DNNs in combination with other DL or ML components:

- **DBN-DNN Hybrid:** One of the hybrid models combines the Deep Belief Network with DNN into a DBN-DNN model [6]. Here, the DBN acts mainly to execute the job of unsupervised feature learning and extraction that it does quite efficiently in case the data is high-dimensional [6]. Features learned by it are then fed into the DNN, which carries out the final classification task in a supervised mode [6]. This combines the merits of both techniques toward an improved performance and stability of the model in detecting attack patterns—both known and unknown—by effectively mitigating the dimensionality issue inherent in network traffic data. While achieving a high predictive accuracy of up to 94% on the older CICIDS 2017 dataset [6], the core challenge lies in the fact that the efficacy of these computationally heavy, multi-component architectures has not been rigorously validated against the latest, most complex dataset, namely CIC-DDoS2019. The reliance on deep, multi-component architectures often leads to high computational overheads and raises questions about their suitability for resource-constrained environments—a critical challenge that this research aims to address.
- **AE-DNN-Fuzzy Hybrid:** Another new model developed combines DNN with FL and a Stacked Sparse AutoEncoder (AE) [7]. The AutoEncoder was used to carry out robust feature learning from network traffic data for getting insightful latent representations, Features are then fed into the classifier, DNN [7]. Fuzzy logic improves the interpretability and robustness of this model by processing uncertain or imprecise information about the dynamic network [7]. This is further enhanced by the use of the algorithm of the fuzzy expert to regularize the size of the network [7]. In this way, overfitting of the model is avoided, and computational overhead is decreased [7]. Despite these gains in robustness and the attempt to reduce overhead, the overall multi-component architecture remains structurally complex and computationally demanding compared to a streamlined DNN, especially when considering deployment in resource-constrained, real-time environments. This highlights the need for a solution that achieves high performance and robustness with a simpler, more efficient DNN design.

2.2. Knowledge Deficit: Inadequate Understanding:

Despite the potential of DNN-based hybrid models to provide high detection accuracy, the existing state of knowledge suffers from a number of serious limitations and gaps:

1. **Bias and Scarce Data:** Most of the current detection schemes are highly biased; their effectiveness largely relies on the quality and completeness of data on which their training is based [6]. Compared to the legitimate events, there is a relative scarcity of attack datasets that have been disclosed, hence making models that cannot detect all types of attacks [6].

2. Generalization to Real Environments: Although the models of DNN perform very well on the available offline data, they often fail in the detection of totally unseen attacks when deployed in real network environments [6].
3. Adaptive Thresholding and Interpretation: In reality, there is still a need for mechanisms that will enable tuning of the detection thresholds based on variations in network activity—a function served by the Fuzzy Logic component in hybrid models [7]. The design of methods providing insight into informed decisions using uncertain network behavior remains an outstanding challenge [7].

2.3. Context and Problem: Evolving Threats and the Imperative for AI:

The literature survey must commence by establishing the general context that necessitated the adoption of ML/DL solutions in cybersecurity. The DDoS threat is no longer merely a technical issue; it has profound strategic and geopolitical dimensions.

2.3.1. Modern Threat Classification and Strategic Impact:

DDoS attack has changed a lot since they were just Volumetric attack that flooded the network capacity. Modern threats more and more include advanced attacks on the Application Layer (Layer 7) that are meant to look like real user behavior.

This shift in threat classification leads to critical strategic impacts:

1. Detection Complexity: Standard security measures have a hard time telling the difference between real and fake requests since copying typical traffic is so hard [1].
2. Targeting Critical Infrastructure: These attacks are become more specialized and now focus on important places like banks, hospitals, and phone companies. This is more than just a corporate issue; it also has an impact on the economy and national security [1].

So, to deal with modern threats, we need to depend on AI technology. For analysing complicated patterns, finding little problems, and making real-time responses that are far faster than what older systems can do, AI models like Machine Learning and Deep Learning are very important [1].

2.3.2. Modern Network Environments (SDN and 5G) as New Targets:

Network infrastructures have evolved towards Modern Model, including Software-Defined Networking (SDN) and 5th Generation (5G) networks. These technologies are very flexible and efficient, but they also make great and unique targets for DDoS attacks [1].

- SDN: The most difficult part of the SDN architecture is keeping the Control Plane and the Data Plane separate. The centralized SDN Controller is a Single Point of Failure. If this controller is attacked with a DDoS attack, it can't handle data flows throughout the whole network, which causes a complete failure [1].

- 5G: The huge rise in the number of linked devices (IoT) and the faster data speeds that 5G networks make possible greatly increase the number of places where attacks can happen. This makes it more likely that advanced, large-scale, and complicated DDoS attacks will happen [1].

2.4. Literature Survey: Reviewing Models, Data, and Extraction Elements:

To make a complete literature review, you need to get and write down three important things from each research paper: the learning model used, the dataset tested, and the features extracted.

2.4.1. Machine Learning and Deep Learning Models (ML/DL):

Recent research has prioritized the development of models capable of handling sophisticated and evolving threats, particularly within next-generation networks like SDN:

- Efficacy of Traditional ML: Traditional and ensemble machine learning models, such as RF and DT, are still quite useful. Recent research has shown that Logistic Regression (LR) and the BIRCH clustering method are quite good at finding hard Low-Rate Distributed Denial of Service (LDoS) attacks in SDN systems. They can do this with very little time spent on detection, up to 99.96% accuracy [5].
- Hybrid Deep Learning (DL): One important step forward is to use hybrid DL architectures to make it easier to get functionalities. For example, it is hypothesized that models that combine Long Short-Term Memory (LSTM) and CNN can uncover both the geographical and temporal patterns that are already in network traffic data. This is very important for correctly finding advanced DDoS attacks [4].

2.4.2. Datasets:

The name, quality, and source of the dataset are important parts of the documentation that make sure the results can be reproduced and are still useful for today's threats [1]:

- CICDDoS2019 as a Benchmark: The CICDDoS2019 dataset is widely accepted as the standard benchmark for evaluating modern detection models due to its reality-based capture (PCAPs) and comprehensive inclusion of contemporary attack types (e.g., LDAP and WebDDoS), making it ideal for multi-class classification tasks [4].
- SDN Contextual Data: To address the unique characteristics of SDN, a growing number of studies rely on SDN-Contextual datasets. These are either simulated or real-world captures specifically generated to reflect OpenFlow traffic statistics and SDN network properties, ensuring model relevance to the target infrastructure [2].
- Comparative Analysis: Datasets like CICIDS2017 are frequently used in comparative studies to evaluate the performance of various ML models (such as KNN, SVM, and MLP) to identify the lightweight, resource-efficient solutions necessary for deployment in computationally limited IoT environments [4].

2.4.3. Feature Engineering and Selection Methods:

The accurate selection and engineering of features are paramount for reducing computational complexity and achieving high detection accuracy in real-time environments [3]:

- **Focus on Efficiency:** Recent studies show that relying on big, redundant feature sets makes computers work harder. So, choosing a minimal, efficient collection of features is very important for cutting down on training time and memory use, which is important for real-time apps. [3]
- **Vital Statistical Features:** Research emphasizes the significance of rapidly computable statistical attributes, like Destination IP Entropy. Entropy is a great way to find DDoS attacks in SDN since it measures how unpredictable network traffic is. A sudden drop in Destination IP Entropy means that traffic is going to a small number of destinations, which makes it easy for the SDN controller to quickly find them using its data [2].
- **Advanced Selection Techniques:** Advanced feature selection techniques are utilized to choose the most suitable subset of features. Cross-Feature Selection is one of these methods. It uses ranking metrics like Information Gain and Gini Importance to cut down on the number of features (for example, it was able to cut the set down to just 5 highly effective features) while still keeping the classification accuracy high in SDN [2].
- **Innovative Feature Engineering:** Novel engineering strategies involve using a clustering method (K-Means) along with methods for reducing dimensionality (PCA and t-SNE). The resulting cluster assignments are then included as a new feature to help classifiers find hidden attack patterns better than they could before [3].

Table I presents a classification of the leading datasets used in DDoS detection research, thereby justifying our methodological choice, the CICDDoS2019 dataset—released in 2019—ensures the inclusion of modern attack types (e.g., LDAP and WebDDoS), making it the most suitable for the multi-class classification objectives of this research. Crucially, its reliance on the CICFlowMeter-V3 tool to extract features from realistic PCAPs guarantees that the derived features, including advanced statistical metrics and Entropy, possess the highest quality and realism necessary to support the training of the proposed DNN model. This selection ensures that the subsequent Feature Selection process operates on a comprehensive and realistic feature set, ultimately enhancing the classifier's efficiency and accuracy.

Table (I): Classification of Key DDoS Detection Datasets and Requirements

Paper	Primary Feature Extraction Tool	Attack Types Included (Examples)	Contextual Environment	Year of Release	Dataset
[3][4]	CICFlowMeter-V3	PortMap, LDAP, SYN, WebDDoS	Realistic (PCAPs)	2019	CICDDoS2019
[5]	CICFlowMeter	DoS/DDoS, Brute Force	Realistic	2017	CICIDS2017
[2]	Controller Flow Monitoring	TCP SYN Flood, Volume-based attacks	Simulated or Actual SDN	Various	SDN-Contextual

2.5. Critical Analysis and Technical Comparison:

The critical analysis moves beyond mere documentation to quantitative comparison and qualitative assessment, focusing on the trade-offs between performance, efficiency, and operational limitations.

2.5.1. Quantitative Performance Comparison: Accuracy, Speed, and Reliability:

The analysis must be based on a comprehensive set of evaluation metrics, not just accuracy, to assess the models' predictive capabilities. These metrics include Accuracy, Precision, Recall (Sensitivity), and F1-Score (the harmonic mean of Precision and Recall). Run-time Metrics, such as Training Time and Classification Time (Prediction Time), must also be documented.

2.5.1.1. Accuracy vs. Time Trade-offs:

The core challenge in developing real-time DDoS detection systems is balancing high detection accuracy with computational efficiency. Since modern network environments, such as SDN, demand instant decisions, a low detection time is paramount.

- The DL vs. ML Dichotomy: Hybrid (DL) and ensemble models, such as CNN-LSTM, typically yield the most precise outcomes (>99%) due to their capability to identify intricate spatial and temporal patterns [4]. But their intricate structure makes training and inference take a lot longer, which makes it impossible to apply them in the real world on SDN controllers with limited resources [3].
- Efficiency-Focused ML: Logistic Regression (LR) and BIRCH, for instance, exhibit superior computational efficiency and reduced latency between detection and response [5]. Research indicates that these models can achieve exceptional accuracy (up to 99.96% against significant LDoS attacks), positioning them as highly effective solutions in contexts where rapidity is crucial [5].
- Mitigation via Feature Engineering: The only approach to get around this trade-off is to carefully plan and pick features. You can get very accurate results while utilizing less computing power by limiting models to a small, optimized set of features. This successfully closes the gap between speed and complexity [2] [3].

2.5.1.2. The Importance of Recall and F1-Score Metrics:

In DDoS detection, just saying that the Accuracy is high isn't enough because there is an inherent class imbalance (regular traffic is much more than attack traffic). So, Recall and F1-Score are quite important for a real technical test [1]:

- Recall: (True Positive Rate): This number tells you how well the model can find all real attacks. A poor Recall suggests that the system is making a lot of False Negatives (not finding real assaults), which is not acceptable in systems that are important for security. It is the main way to check how reliable a model is against threats [1].

- F1-Score: This score is the average of Precision and Recall. It gives you one balanced statistic to use to judge how well a model works on unbalanced datasets. To make sure that the claimed accuracy is not inflated by properly categorizing too much typical traffic [5], [1], high-performing models, such those that report 99.8% accuracy, must also have a high F1-Score (e.g., >96%).

Table (II): Comparative Technical Performance of Leading ML/DL Algorithms for DDoS Detection (Literature Summary)

Paper	Key Analysis Points	Critical Time Metric	F1-Score	Recall	Accuracy	Type	Algorithm
[3]	Excellent balance of accuracy and reliability	N/A	99.82%	99.85%	99.82%	ML/Ensemble	XGBoost
[5]	Very high accuracy, suitable for detection.	Faster training time	N/A	N/A	99.86%	ML/Ensemble	Random Forest (RF)
[4]	Highest accuracy, suitable when accuracy is the priority.	Slower training time	N/A	N/A	99.63%	DL	DFF
[5]	Best for speed-sensitive environments and real-time applications.	Fastest Classification Time	N/A	N/A	95.5%	ML	SVM

2.5.2. Analysis of Technical Challenges and Limitations:

Despite recent advances, several technical challenges limit the robustness and universal deploy ability of current ML/DL solutions:

- Generalization and Data Context Limitations: Current models have a hard time generalizing because a lot of research uses generic datasets (like CICDDoS2019) that don't completely show the unique and changing features of SDN-Contextual OpenFlow traffic. This limits how useful it is in real SDN networks [2], [4]. In addition, all supervised models are still fundamentally constrained when it comes to Zero-Day attacks that don't have any examples in the training data [1].
- Computational Overhead and Deployment: When you deploy complicated DL architectures on platforms with limited resources, like the SDN Controller, it takes a long time for the system to make decisions. This computing overhead directly contradicts the imperative for prompt attack mitigation and demands stringent dimensionality reduction methodologies [3].

- LDoS and Evasion Attacks: LDoS attacks continue to pose a challenge as they are designed to mimic normal traffic and evade detection systems that rely on threshold-based mechanisms. To identify these hazards, it is necessary to employ specialized models and flow behavior analysis that extend beyond mere volume measurements [5].

Table (III): Implementation Challenges and Architectural Limitations of ML/DL Models in SDN/5G

Paper	Resulting Research Gap (Future Work)	Environment Most Affected	Impact on Detection and Network	Technical Challenge
[5][3]	Develop lightweight, resource-optimized DL models.	SDN Control Plane, 5G, IoT Devices	Hinders scalability and slows down real-time response	High Computational Complexity
[2]	Create real, contextual datasets (SDN-Contextual).	All environments, especially production networks	Poor Generalization against real-world (Zero-day) attacks	Reliance on Simulated Data
[1]	Improve the balance between Precision and Recall.	Automated Protection Systems (Mitigation Systems)	Blocking legitimate traffic/reducing Quality of Service	False Positive Rate (FP Rate)

2.6. Conclusions and Methodological Recommendations:

The critical analysis of the available literature provides clear conclusions regarding the state of ML/DL technologies in DDoS detection, opening the door for prioritizing future research directions.

1. Model Selection and Layering:

- Recommendation: It is advised that the primary method for achieving the highest overall accuracy and the ability to classify numerous classes be Ensemble Learning or Hybrid DL Architectures (like CNN-LSTM) [4].
- Methodology: In the first detection layers, combine these advanced models with lightweight machine learning models (such as LR/BIRCH) to guarantee that the SDN framework has very low latency and can react rapidly [5].

2. Feature Engineering Imperative:

The best way to narrow down the set of features to a small, highly predictive set is to use advanced feature selection methods, such as Cross-Feature Selection [2, 3].

Focus on easy-to-calculate statistical features, notably Destination IP Entropy, as a reliable and useful real-time metric that lets the SDN controller take quick action [2].

3. Data and Evaluation Standardization:

- Recommendation: The CICDDoS2019 dataset should be used as the starting point for testing models since it is realistic and includes a lot of different types of attacks [4].

- Methodology: To make sure that the model can be used in real life and that it can be applied to other situations, more research needs to be done that compares its performance on both generic and SDN-Contextual datasets.

3. Research Methodology

3.1. Research Methodology Overview:

This section presents our research methodology, which uses Deep Neural Networks (DNN) to build a Deep Learning (DL) model for the classification of multi-class DDoS attacks. The methodology aims to systematically address the problem of detecting and classifying various categories of DDoS attacks. The methodology has seven phases: data collection, data preparation, model design, model training, model evaluation, model validation, and model deployment. The following provides a detailed description of each phase.

1. Data Collection: The chosen dataset is CIC-DDoS2019, which is publicly available and widely used for AI-driven cybersecurity research. There are 12 types of DDoS attacks and normal network traffic in the dataset. There are several other types of DDoS attacks, such as DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, UDP Flood, UDP-Lag, SYN Flood, TFTP, and WebDDoS [8].
2. Data Preparation: The dataset is processed by data cleansing, balancing, and scaling to enhance its quality and ensure an appropriate balance during model learning. Data cleaning involves removing duplicate data values, fixing missing values, and repairing errors in values. Data balancing involves setting up the sample sizes in all categories using Synthetic Minority Over-sampling Technique (SMOTE) to enhance the model's learning efficacy for each category during training. Data scaling involves normalizing numerical features and converting class labels (normal traffic and 12 categories of DDoS attacks) into one-hot encoding to match the DNN output. Thereafter, the processed dataset is divided into 80% for training and 20% for testing.
3. Model Design: The model build uses a Deep Neural Network (DNN), which is commonly employed in research on DDoS detection. This model uses the DNN's ability to learn complex patterns in network traffic. There are three main layers in a DNN. The input layer receives the pre-processed features from the network traffic. Multiple hidden layers take the input data and extract and learn complex patterns. The output layer classifies each network traffic instance into one of 12 types of DDoS attacks or normal traffic.
4. Model Training: The model is trained using the Adam optimizer and the categorical cross-entropy loss function. Early stopping is employed to keep the model from overfitting.
5. Model Evaluation: The trained model is assessed using multiple metrics to determine its ability in detect and classify different categories of DDoS attacks. Multiple metrics, which include:
 - Accuracy: The percentage of all correct predictions.

- Precision: The percentage of correct positives to all predicted positives.
 - Recall: The percentage of correct positives to all actual positives.
 - F1 Score: Combines both precision and recall.
 - Confusion Matrix: Table of classification performance across 12 attack types and normal traffic by comparing actual and predicted labels.
6. Model Validation: The trained model is checked using a testing dataset to assess its ability to detect and classify DDoS attacks.
7. Model Deployment: The trained model is deployed in the SDN network environment for real-time, and it will detect and classify all real-time DDoS attacks and send out alerts for attacks that are detected. Additionally, the model's output is automatically linked to mitigation mechanisms to enable prompt and fully automated threat response.

3.2. Proposed Design Methodology:

This research presents an original methodology by implementing the Multi-Class DDoS Attack Classification using Deep Neural Networks (DNN), which detects and classifies 12 attack types and normal traffic. Figure 1 shows the phases of our methodology. Our research presents several new contributions:

- Classification of Multi-Class DDoS Attacks.
- Building a model with Deep Neural Networks (DNN).
- Advanced Preprocessing of Datasets.
- A detailed evaluation of the model using multiple metrics.
- Deployment in a network environment in real time.

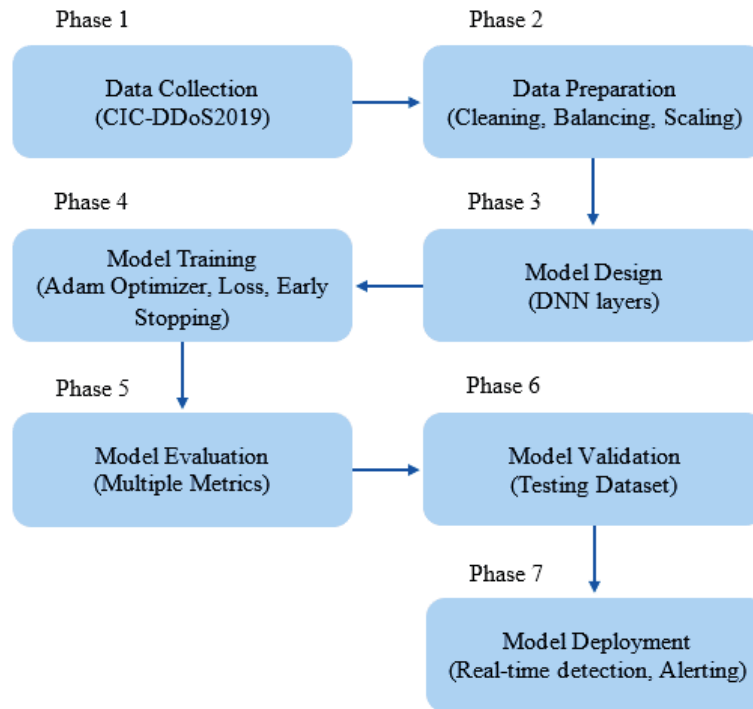


Figure (2): The phases of research methodology

4. Conclusion and Future Work

4.1. Research Study Findings:

The core findings and achievements of the research, based on the methodology executed, have confirmed that the shift from the simple ML models to the more complex DL architectures, namely DNN, was well -grounded.

We were able to achieve the following:

1. Custom Multi-Class Classification: We proposed a customized DNN model that is capable of multiclass classification and then designed and validated it. It has been designed in such a way so that the great variability of modern threat scenarios may be handled efficiently by classifying 12 different attack types of DDoS along with benign/normal traffic.
2. Data Preparation: We noted that any deep learning model will involve deploying sophisticated preprocessing methods. Hence, we began with:
 - Data collection using the realistic CIC-DDoS2019 dataset.
 - Performing data cleaning, data encoding, and normalization.

- Using SMOTE, Synthetic Minority Over-sampling Technique to perform class balancing, a very important process for reliable execution across all attack categories.
- 3. Systematic evaluation framework: This approach employed a comprehensive multi-phase framework. The process was finally concluded by the detailed multi-metric evaluation containing accuracy, F1-score, and confusion matrix analyses in proving the discrimination efficiency of a system.
- 4. Basis for Real-Time Deployment: The strict methodology followed here for validation establishes that the DNN model is ripe and ready to move from a pure test regime into a complete real-time environment integration. This lays the basis for an integrated framework that can link the classification outcome with mitigation mechanisms automatically for immediate threat responses.

4.2. Future Research Study Recommendations:

Based on our analysis and the current technology, below are the recommendations for future work and implementation

1. Enhancing Model Robustness—Adversarial Defenses: Since AI-driven and automated attacks are growing, much research is needed to be invested in the making of a DNN model robust against various adversarial evasion techniques. In other words, research into defence mechanisms is required that will prevent attackers from manipulating network features to evade detection.
2. Lightweight and scalable architectures that are deployable on resource-constrained environments in practice, including but not limited to SDN controllers or IoT devices, need to be studied. Optimizations toward computational efficiency may include studying techniques such as Federated Learning for distributed training or smaller and resource-optimized variants of DNN that achieve a good balance between high accuracy and minimal processing delay (low latency).

5. References

1. S. Batool, M. Aslam, E. Akpokodje and S. F. Jilani, "A Comprehensive Review of DDoS Detection and Mitigation in SDN Environments: Machine Learning, Deep Learning, and Federated Learning Perspectives," *Electronics*, vol. 14, art. no. 4222, 2025, doi: 10.3390/electronics14214222.
2. B. Aryal, R. Abbas, and I. Collings, "SDN enabled DDoS attack detection and mitigation for 5G networks," *Journal of Communication*, vol. 16, no. 7, pp. 267–275, 2021.
3. S. Abiramasundari and V. Ramaswamy, "Distributed denial-of-service (DDoS) attack detection using supervised machine learning algorithms," *Scientific Reports*, vol. 15, art. no. 13098, 2025, doi: 10.1038/s41598-024-84879-y.

4. G. Chukwukelu, A. Essien, A. Salami, and E. Utuk, "Comparative Analysis of Machine Learning Techniques for DDoS Intrusion Detection in IoT Environments," Proceedings of the 21st International Conference on Smart Business Technologies, pp. 19–27, 2024, doi: <https://doi.org/10.5220/0012765200003764>.
5. B. Isyaku, K. B. A. Bakar, M. S. Ali and M. N. Yusuf, "Performance Comparison of Machine Learning Classifiers for DDOS Detection and Mitigation on Software Defined Networks," in 2023 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), Shah Alam, Malaysia, 2023, pp. 69–74, doi: 10.1109/I2CACIS57635.2023.10193601.
6. Y. Zhao, J. Guo and L. Jin, "Design of DDoS Attack Detection Model Based on DBN-DNN," 2024 7th International Conference on Mechatronics and Computer Technology Engineering (MCTE), Guangzhou, China, 2024, pp. 70-74, doi: 10.1109/MCTE62870.2024.11117331.
7. Maheswari, R. Elankavi, K. Lahari, J. Navitha, P. Manoj and B. O. G. Maheshwar Reddy, "Adaptive DDoS Detection with DNN and FUZZY," 2024 Asia Pacific Conference on Innovation in Technology (APCIT), MYSORE, India, 2024, pp. 1-5, doi: 10.1109/APCIT62007.2024.10673425.
8. Canadian Institute for Cybersecurity (CIC), "CIC DDoS2019 Dataset," University of New Brunswick. [Online]. Available: <https://www.unb.ca/cic/datasets/ddos-2019.html>.