CHAPTER 3

PROPOSED METHODOLOGY

3.1 Introduction

Developing a complexity-aware intelligent intrusion detection system with an improved feature engineering technique is the main goal of this thesis in order to identify Distributed Denial of Service (DDoS) assaults. For anomaly detection, a methodological framework is created using machine learning as well as deep learning models, feature selection strategies and data pretreatment approaches (Malik, M. and Dutta, M., et al, 2023). The suggested intelligent intrusion detection model's dependability and effectiveness in reducing DDoS attacks would be guaranteed by a proper and sufficient assessment of its performance under various circumstances.

As previously discussed, significant gaps exist in protecting the digital landscape from DDoS attacks. This thesis proposes an intelligent IDS tailored for detecting Single Vector DDoS Flooding attacks, multiple DDoS Flooding attacks, and multiple DDoS attacks. The methodologies underlying these approaches have been explained in preceding chapters. This chapter outlines the proposed research design, which encompasses appropriate data collection, various algorithms and techniques used for Feature Selection, and meticulous evaluation to achieve the objective of accurately detecting DDoS attacks. Additionally, various computational intelligence techniques are employed to optimize the feature extraction and selection process, complemented by the application of Machine and DL algorithms.

3.2 Steps Involved in the Proposed Methodology

Based on the observations from the previous chapter, the major objective of the thesis is formulated. Designing a complexity-aware intelligent intrusion detection system based on computational intelligence, attention-enabled ML, and DL models is the goal of the proposed research. This will help mitigate various DDoS attacks, such as single vector DDoS flooding, multi vector DDoS flooding, and multiple DDoS attacks. A workstation equipped with a 256 GB Nvidia Titan Board with16 GB of RAM and an i9 CPU was used to execute the whole experiment. The research has proposed with four stages. Each step is explained as follows. An overview of the methodology proposed is displayed in Figure 3.1.

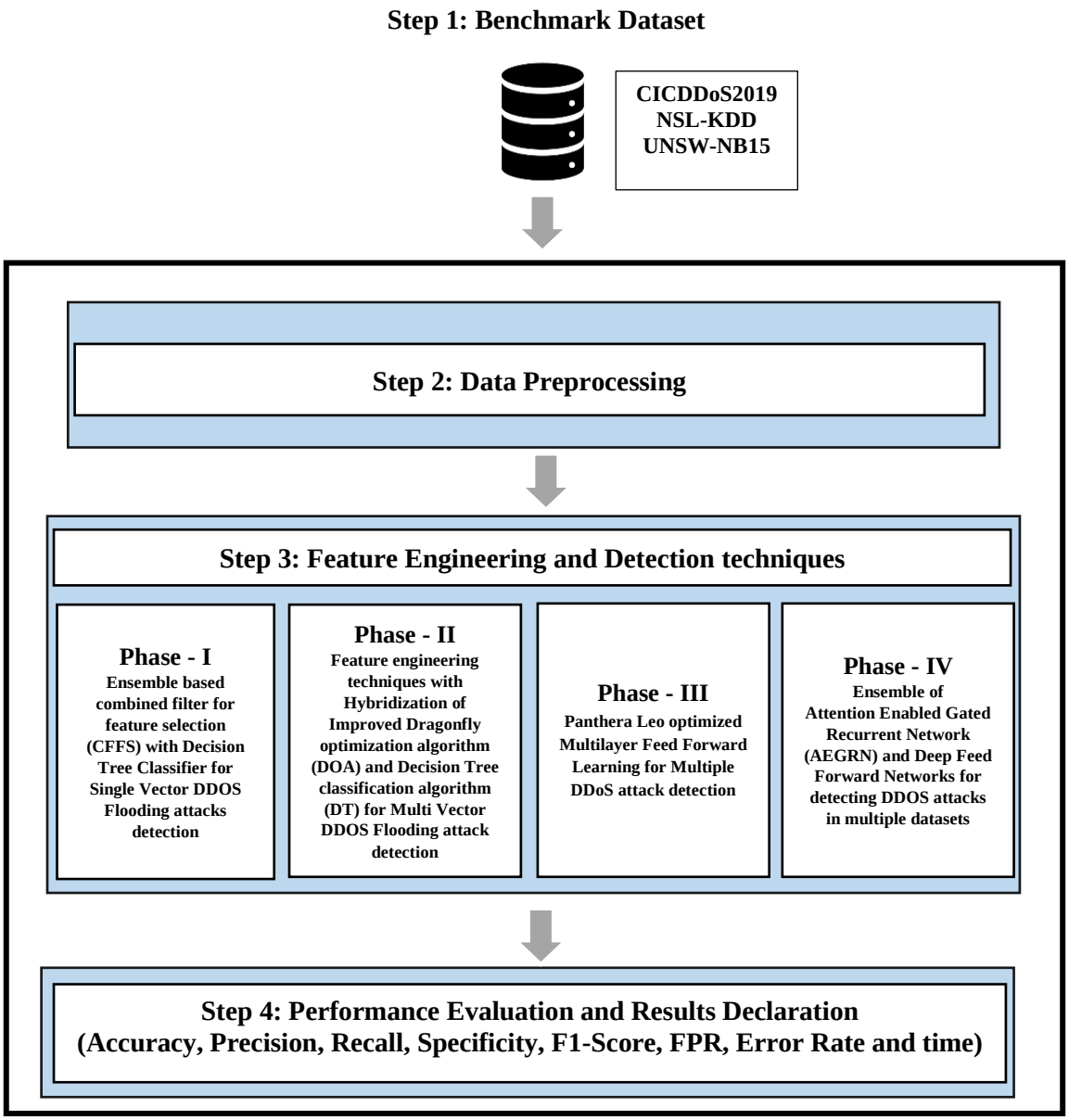

Figure 3.1: Overview of the Proposed Research Methodology

This four-step process is used in the overall study design to effectively identify DDoS assaults. Finding the right dataset to verify the suggested model is the initial step. In second step preparation of the data, which includes managing null values, standardizing the data and removing missing values are involved. The accuracy and resilience of the detection process are improved in step three when the suggested feature engineering and detection approaches are used to identify DDoS assaults. The fourth step is confirming the findings, comparing them with the current models, and assessing the performance using a variety of indicators. The results will show how well the suggested methodology detects DDoS assaults in the digital landscape, providing improved detection accuracy and reliability.

Step 1: Data collection

In order to identify DDoS assaults, the first step is to gather datasets. The following is a list of the datasets utilized in this study to assess the suggested methodologies,

(i) CICDDoS2019

(ii) UNSW-NB15

(iii) NSLKDD

(i) CICDDoS2019

The Canadian Institute for Cybersecurity (https://www.unb.ca/cic/datasets/ddos-2019.html) provided the dataset that was utilized as a case study in this article. Universities, business, and independent researchers utilize the CICDDoS2019 dataset worldwide as a labelled standard. The benign and current frequent DDoS assaults in CICDoS2019 closely mirror actual data. Additionally, "it contains the outcomes of the network traffic analysis performed using CICFlowMeter-V3 with flows labelled according to the time stamp, source and destination IP addresses, source and destination ports, protocols, and attacks (CSV files)". The CICDDoS2019 dataset comprises a total of 294,627 records. Of these, 172,647 records (58.6%) are classified as attack traffic, while 121,980 records (41.4%) are classified as normal traffic (Khalid, S., Khalil, T. and Nasreen, S., 2014).

(ii) UNSW-NB15

The UNSW-NB15 dataset, a a recent addition to the public domain, is also used for testing. There are 49 features and one class attribute in the dataset with the training and test sets. There are 175,341 events in the training set of which 119,341 are attack traffic and 56,000 are ordinary traffic. The test set comprises 82,332 cases, of which 37,000 are instances of regular traffic and 45,332 are instances of attack traffic. As a result, the dataset now has 257,673 entries in total. Cross-fold validation employs just the training set, whereas hold-out validation employs both the test and training sets (https://research.unsw.edu.au/projects/unsw-nb15-dataset).

(iii) NSLKDD

The NSL-KDD dataset is also used for validating the classifier. The class attribute is the first of 41 attributes in the dataset. This study employs the use of the KDDTrain+

(training) as well as KDDTest+ (testing) sets from the NSL-KDD dataset. Of the 25,192 instances in the KDDTrain+ collection, 11,743 are of normal traffic and 13,499 are of attack traffic. Of the 22,544 occurrences in the KDDTest+ collection, 9,711 are assaults and 12,833 are regular traffic. This results in 47736 records overall in the NSL-KDD dataset. Each dataset is subjected to independent cross-fold and hold-out validation of classifiers. In order to prevent arbitrary sampling from the whole NSL-KDD dataset, these sets were chosen (https://www.unb.ca/cic/datasets/nsl.html).

Step 2: Data Preprocessing

When preparing the data for analysis, significant filtration and normalization are required. In particular, the operations connected with the elimination of duplicates, missing values treatment by imputation or deletion, and feature selection are implied by the term filtration. Scaling changes the values of all the variables in the doubles so that, none of the features dominates the other because of variation in their scales. This is often done by normalizing the numbers and brings the mean either by standardizing the data to 0 and the standard deviation to 1 them between 0 and 1. Such steps provide a solid groundwork for performing dependable analyses and models conducive to generating sound understanding of threats and protection in cyber environments.

Step 3: Proposed Feature Engineering and Detection Techniques

This research builds on feature engineering approaches by using complex algorithms and superior techniques. One major improvement is the implementation of the Ensemble-Based CFFS that combines different filter techniques for better selection of features to boost the detection rate of single-vector DDoS attacks. The research also employs bio-inspired feature selection technique such as the IDOA to enhance the detection rate and minimize computational complexity. Another one of the more sophisticated techniques applied is the so-called Panthera Leo Optimization or PLO, which mimics lion hunting and applies it to the DDoS attack multivector structure for the purpose of feature selection and tuning of parameters. Also, feature learning using deep learning models, including AEGRN, is performed to automatically extract high-level features and enhance the detection performance across multiple datasets. These enhancements are verified on CICDDoS2019, NSL-KDD+, and UNSW datasets.

It should be mentioned that there are several advantages of fully automatically selected features over handcrafted features are quite numerous. Features chosen by using the filters like the Ensemble-Based Combined Filter for Feature Selection (CFFS), Improved Dragonfly Optimization Algorithm (IDOA) and Panthera Leo Optimization (PLO) are the most appropriate and rational way to select the features. This automation helps to select only significant and most informative features and reduce the human factor in feature selection indispensable in the hand-made approach. Moreover, the automatically selected features also improve computational performance by cutting down the time for training and prediction by minimizing the set of features. This efficiency is highly desirable when dealing with big data and intricate attack behaviors as was illustrated in the experimented trials with CICDDoS2019 and UNSW-NB15 datasets. In addition, the high reliability and stability of automatically selected features enhance the applicability of the models and their performance on various datasets and attacks. On the other hand, while hand crafted features can be intuitive and easy to come up with owing to the domain expertise, then often they are not easily scalable and are time consuming to design and to ensure they are valid. The application of feature selection in this research enhances the model efficiency and validity in complex and dynamic cyber security circumstances.

The following are four important findings of this research work on detecting DDoS attacks using different advanced techniques. Contribution 1 is a Feature Engineering with Ensemble-based Combined Filter for Feature Selection (CFFS) in link with a Decision Tree Classifier for identification of single vector DDoS flooding attacks. Contribution 2 introduces a strategic framework with feature engineering techniques through the hybridization of the Improved Dragonfly Optimization Algorithm (IDOA) and Classification Algorithm (DT) for identifying several DDoS flooding assaults. Contribution 3 presents an Intelligent IDS utilizing Panthera Leo Optimization, extensively evaluating its efficacy. Contribution 4 develops an Intelligent IDS incorporating Attention-Enabled Gated Recurrent Networks, achieving high accuracy across multiple datasets. Each contribution is rigorously assessed using standard metrics. These advancements enhance DDoS attack detection while justifying the need for a complexity-aware Intelligent IDS to address challenges like computational efficiency and adaptability to evolving attack patterns.

Step 4: Performance Evaluation

In each of the three contribution chapters, the performance assessment is conducted using the following measuring measures. Each of these metrics is a conventional way to access the performance for categorization in the cybersecurity area (Saranya T et al, 2020). The fundamental words that are utilized to define the performance measures are,

(i) False Positive (FP)

(ii) True Positive (TP)

(iii) False Negative (FN)

(iv) True Negative (TN)

The definitions of each term are given below:

(i) **False Positive (FP):** The count of items that are mistakenly classified as positive but are really negative, meaning that an ingredient with the label "benign" is instead classed as "malicious."

(ii) **True Positive (TP):** The proportion of items is accurately identified as positive, meaning that they are labeled "malicious" and solely classed as such.

(iii) **False Negative (FN):** components that are mistakenly categorized as negative but are really beneficial; for example, an element with the label "malicious" is classed as "benign."

(iv) **True Negative (TN):** The quantity of components that are accurately identified as negative, meaning that they are only classed as "benign" when their identity is "benign".

The performance indicators used in this access for evaluating the proposed frameworks are given below:

(i) Accuracy: It is the measure of accurate classification made to the total count of predictions made.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (3.1)$$

(ii) Recall: The ratio of accurately categorized negatives to the total of accurate predictions and incorrectly classified negatives is known by another name, the true positive rate.

$$Recall = \frac{\text{TP}}{\text{TP+FN}} \qquad (3.2)$$

(iii) Specificity: It is the measure that judges how good a model is on the aspect of predicting true negatives of each of the classes available.

$$Specificity = \frac{TN}{TN+FP} \qquad (3.3)$$

(iv) Precision: It is the ratio of all correctly categorized predicted to all positively classed predictions.

$$Precision = \frac{TN}{TP+FP} \qquad (3.4)$$

(v) F1-Score: Its definition is the harmonic mean of precision and recall.

$$F1 - Score = \frac{Precison*Recall}{Precision+Recall} * 2 \qquad (3.5)$$

(vi) FPR: It is the ratio of the total number of real negative instances to the number of false positives, or inaccurate positive forecasts.

$$False\ Positive\ Rate = \frac{FP}{FP+TN} \qquad (3.6)$$

(vii) Error Rate: It is computed as the proportion of inaccurate predictions both false positives and false negatives to all forecasts.

$$Error\ Rate = \frac{FP+FN}{FP+FN+TP+TN} \qquad (3.7)$$

3.3 Research Design

The overall research design of the thesis is represented in Figure 3.2

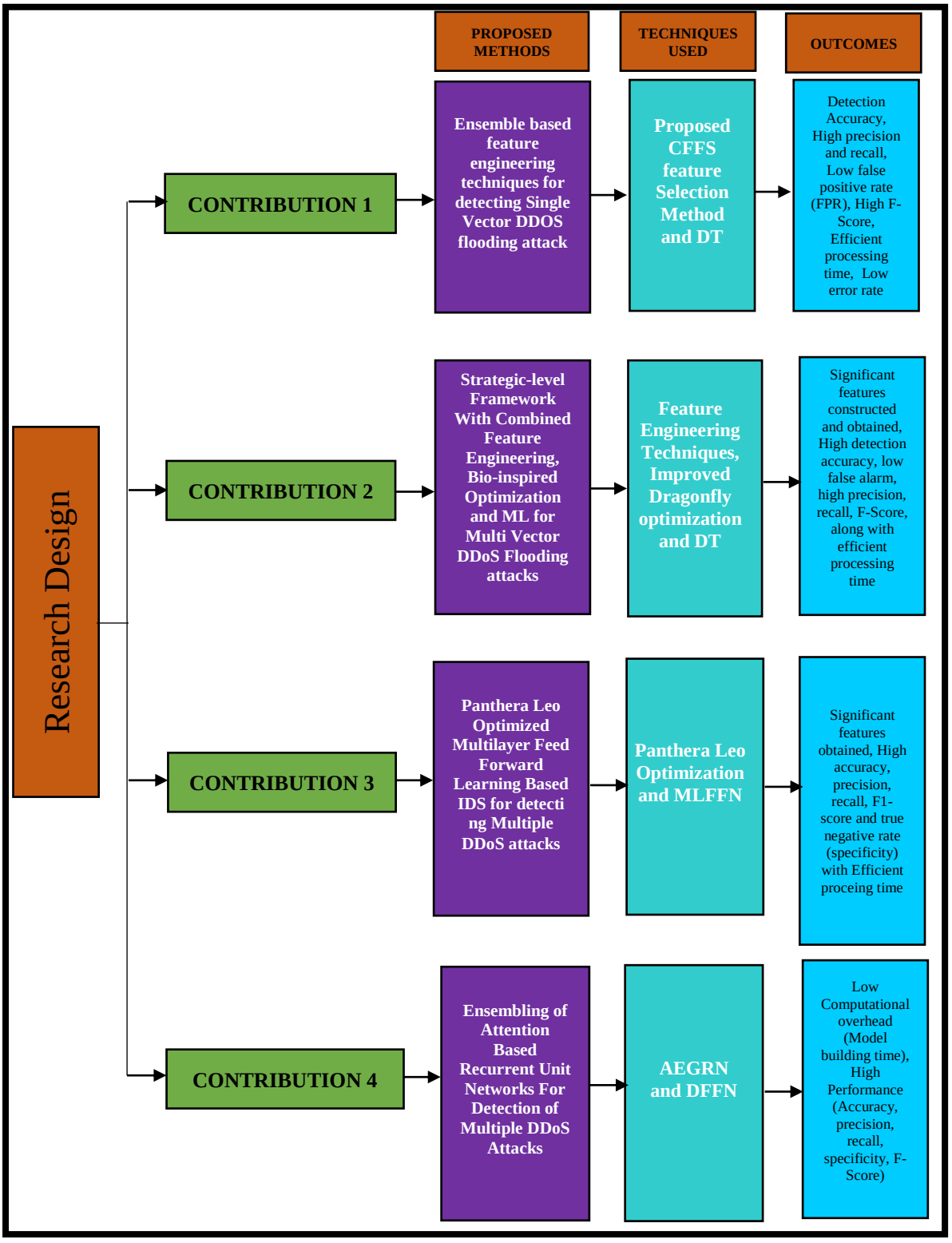

Figure 3.2 Overall Research Design

All the four contributions are explained in detail in the coming chapters.

3.4 Chapter Summary

The suggested study design, which addressed the detection of DDoS attacks, was briefly covered in this chapter. The importance of identifying attacks is underscored, with effective attack handling methods proposed to fulfill the thesis objectives. The research is organized into four distinct contributions, each aimed at enhancing feature selection and detection techniques. The subsequent chapters will delve into detailed steps, including the experimental setup and the outcomes obtained, offering a comprehensive understanding of the research methodology employed.