

# Automated and Explainable Denial of Service Analysis for AI-Driven Intrusion Detection Systems

Paul Badu Yakubu<sup>a</sup>, Lester Santana<sup>a</sup>, Mohamed Rahouti<sup>a,\*</sup>, Yufeng Xin<sup>1</sup>, Abdellah Chehri<sup>c</sup>, Mohammed Aledhari<sup>d</sup>

<sup>a</sup>*Computer and Information Science Department, Fordham University, New York, NY, USA*

<sup>b</sup>*RENCI, University of North Carolina at Chapel Hill, Chapel Hill, NC, USA*

<sup>c</sup>*Department of Mathematics and Computer Science, Royal Military College of Canada, Kingston, ON, Canada*

<sup>d</sup>*Data Science Department, University of North Texas, Denton, TX, USA*

## Abstract

With the increasing frequency and sophistication of Distributed Denial of Service (DDoS) attacks, it has become critical to develop more efficient and interpretable detection methods. Traditional detection systems often struggle with scalability and transparency, hindering real-time response and understanding of attack vectors. This paper presents an automated framework for detecting and interpreting DDoS attacks using machine learning (ML). The proposed method leverages the Tree-based Pipeline Optimization Tool (TPOT) to automate the selection and optimization of ML models and features, reducing the need for manual experimentation. SHapley Additive exPlanations (SHAP) is incorporated to enhance model interpretability, providing detailed insights into the contribution of individual features to the detection process. By combining TPOT's automated pipeline selection with SHAP's interpretability, this approach improves the accuracy and transparency of DDoS detection. Experimental results demonstrate that key features such as mean backward packet length and minimum forward packet header length are critical in detecting DDoS attacks, offering a scalable and explainable cybersecurity solution.

**Keywords:** Denial of Service, Feature Selection, Machine Learning, Explainability, Interpretability

## 1. Introduction

Denial-of-Service (DoS) attacks are among the most persistent and significant threats to the availability and reliability of online services Owusu et al. (2025a). By overwhelming systems with excessive traffic, these attacks can incapacitate critical infrastructure, leaving legitimate users unable to access vital resources. Given the widespread reliance on network services, the impact of such attacks can be severe, ranging from financial losses to compromised user trust. As the sophistication and frequency of DoS and Distributed Denial-of-Service (DDoS) attacks continue to evolve, the development of robust detection and mitigation mechanisms remains a top priority for cybersecurity professionals Li et al. (2023).

The complexity of modern DDoS attacks lies in their ability to mimic legitimate traffic patterns, making it increasingly difficult for traditional rule-based systems to detect them. This challenge has led to the widespread adoption of machine learning(ML)-based approaches, which can analyze vast amounts of network traffic data and identify subtle anomalies indicative of an attack Garcia-Teodoro et al. (2004); Jones and Sielken (2005). However, while ML models offer improved detection capabilities, they come with their own set of challenges,

such as the need for high-dimensional feature spaces, which can lead to increased computational overhead and potential overfitting Al-Shareeda et al. (2023).

To address these challenges, feature selection and dimensionality reduction techniques are often employed to balance the trade-offs between accuracy and computational efficiency Shukla et al. (2024). These methods enable the identification of the most informative features—such as packet size, flow duration, and backward packet lengths—while minimizing noise and redundant data Malik et al. (2023); Guyon and Elisseeff (2003). Recent advancements in explainable AI have further enhanced the interpretability of these models, providing insights into how individual features contribute to the model's decisions and enabling more transparent cybersecurity frameworks Lundberg and Lee (2017a); Kalutharage et al. (2023).

In this context, the proposed work leverages both automated ML tools and explainability techniques to build a robust DDoS detection framework. By combining the Tree-based Pipeline Optimization Tool (TPOT) for automating the selection and optimization of ML pipelines with SHapley Additive exPlanations (SHAP) for interpretability, this approach aims to improve both the accuracy and transparency of DDoS detection systems Olson et al. (2016); Lundberg and Lee (2017a). Figure 1 presents the automated DoS detection pipeline, which begins with raw network traffic data collection, followed by preprocessing and feature engineering steps. TPOT is utilized to automatically select the most suitable ML model, and SHAP is applied for explainability, providing insights into the model's decision-

\*Corresponding author: Abdellah Chehri (chehri@rmc.ca)

Email addresses: pbaduyakubu@fordham.edu (Paul Badu Yakubu), lsantanacarmona@fordham.edu (Lester Santana), mrahouti@fordham.edu (Mohamed Rahouti), yxin@renci.org (Yufeng Xin), chehri@rmc.ca (Abdellah Chehri), Mohammed.Aledhari@unt.edu (Mohammed Aledhari)

making process. This integration of automated pipeline optimization and interpretability not only enhances detection accuracy but also ensures that the system’s decisions can be understood and trusted. As DDoS attacks become increasingly sophisticated, the use of such automated and interpretable solutions is essential to staying ahead of emerging threats.

The main contributions of this paper are summarized as follows:

- Leverages TPOT to automate the selection and optimization of ML models, significantly enhancing the robustness and accuracy of DoS attack detection by systematically identifying high-performing pipelines and optimal feature sets. This automation not only reduces the need for manual experimentation but also leads to more consistent and reproducible detection outcomes.
- Integrates SHAP to provide detailed interpretability of the ML model, offering insights into the contribution of individual features to the model’s predictions, enhancing transparency in cybersecurity applications.
- Proposes a framework demonstrating superior accuracy and effectiveness in detecting DoS attacks by employing advanced feature selection and dimensionality reduction techniques. Owing to its automated and model-agnostic design, the methodology is inherently flexible and can be extended to other cybersecurity threat detection tasks beyond DoS.

The rest of this paper is organized as follows. Section 2 provides an overview of the background and related work, discussing traditional and ML-based approaches for DoS detection. Section 3 presents the research problem and goals, detailing the specific challenges addressed in this study. In Section 4, the methodology is described, outlining the integration of TPOT and SHAP for automated model selection and feature importance analysis. The results of the experimental evaluation are presented and analyzed in Section 5. Section 6 highlights the key lessons learned from this study and outlines future research directions. Finally, Section 7 concludes the paper and suggests directions for future research.

## 2. Background and Related Work

DoS and DDoS attacks represent some of the most significant threats to the availability and reliability of online services. These attacks flood targeted systems with an overwhelming amount of malicious traffic, rendering them inaccessible to legitimate users. Effective detection and mitigation of DoS and DDoS attacks are crucial for maintaining the integrity of networked systems. The dynamic and complex nature of these attacks, coupled with the increasing sophistication of attack methodologies, necessitates advanced detection mechanisms that can adapt in real-time Fenil and Mohan Kumar (2020).

### 2.1. Traditional Methods for DoS and DDoS Detection

Traditional methods for detecting DoS and DDoS attacks often rely on predefined signatures or anomaly-based detection techniques. Signature-based methods, while effective against known attacks, struggle to identify novel or evolving threats Yang et al. (2022). Anomaly-based techniques, on the other hand, monitor network traffic for deviations from established patterns but can suffer from high false positive rates Jones and Sielken (2005).

### 2.2. ML Approaches

In recent years, ML has emerged as a powerful tool for detecting DoS and DDoS attacks, with numerous studies proposing tailored solutions leveraging supervised learning techniques. For example, Deepa et al. Deepa et al. (2018) introduced a hybrid detection system combining Support Vector Machines (SVM) with feature selection techniques to reduce false positives in DDoS detection. Their system achieved improved accuracy by selecting critical traffic features before classification, though it required extensive manual tuning.

Similarly, Zhang and Zhou Zhang and Zhou (2008) utilized k-Nearest Neighbors (k-NN) with wavelet-based preprocessing to capture temporal patterns in packet-level data. While their method demonstrated high accuracy for specific attack types, it lacked generalization to newer, low-rate DDoS variants. Chen et al. Chen et al. (2006) explored decision tree learning for attack classification, emphasizing the interpretability and transparency of the resulting models. However, their approach did not incorporate feature selection or optimization, limiting its scalability to large datasets.

Other studies such as Gupta et al. Gupta et al. (2018) developed a comprehensive ML-based DDoS mitigation framework for UAV networks using software-defined networking (SDN). Their system integrated multiple classifiers—Random Forests, Logistic Regression, Decision Trees, and XGBoost—into an ensemble, significantly improving traffic rerouting and attack mitigation performance. This framework highlighted the advantages of ensemble learning in capturing diverse traffic characteristics but required careful coordination between components. Another approach was proposed by Yang et al. Yang et al. (2014), who combined entropy analysis with ensemble classifiers to detect low-rate DDoS attacks. By monitoring statistical shifts in traffic entropy, their method could identify stealthy attacks that evade conventional detection; however, its reliance on entropy thresholds reduced adaptability to dynamically evolving threats.

Further advances have introduced increasingly sophisticated ML strategies tailored for DoS and DDoS detection in diverse network environments. Zhao et al. Zhao et al. (2023) emphasized the importance of feature engineering to improve detection performance, especially in the context of evolving attack behaviors. Santana et al. Santana et al. (2024) further explored explainability techniques to highlight feature importance and enhance trust in ML-based DoS detectors. For resource-constrained settings such as the Internet of Medical Things (IoMT), Clark et al. Clark et al. (2024) presented a

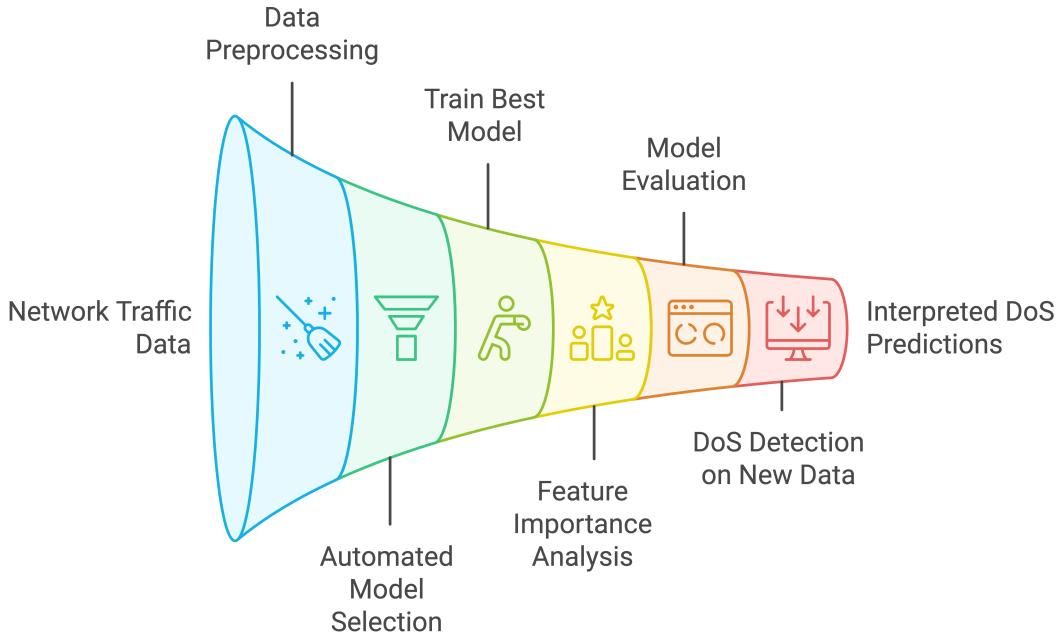


Figure 1: Automated DoS detection pipeline.

lightweight detection framework optimized for edge devices, while Hafid et al. Hafid et al. (2025) proposed a cost-aware and interpretable ML system tailored for IoMT-based intrusion detection. To improve data efficiency, Alfatemi et al. Alfatemi et al. (2025) introduced ProtoMAML, a hybrid meta-learning framework that combines Prototypical Networks with MAML for effective DDoS detection under limited training data. Owusu et al. Owusu et al. (2025b) proposed a robust detection framework using combinatorial fusion and generative AI, and their subsequent work Owusu et al. (2024) explored online DDoS detection using adaptive sampling and change point detection. Finally, Al-Zewairi et al. Al-Zewairi et al. developed a multi-stage intrusion detection system leveraging enhanced Zero Trust principles to detect unknown and emerging threats in both IoT and traditional network environments. These contributions collectively reflect the ongoing shift toward adaptive, interpretable, and resource-efficient ML-based intrusion detection systems.

In summary, while traditional ML approaches have demonstrated efficacy in DDoS detection, they often involve manual pipeline construction and lack interpretability. These limitations motivate the need for automated and explainable detection frameworks, such as the one proposed in this work, which leverages TPOT for pipeline optimization and SHAP for feature-level interpretability.

### 2.3. Feature Selection and Dimensionality Reduction

Feature selection is a critical step in enhancing the performance of ML models for DoS detection. High-dimensional feature spaces provide detailed insights into network behavior but also introduce challenges such as increased computational complexity and the risk of overfitting. Techniques such as Prin-

cipal Component Analysis (PCA) and other dimensionality reduction methods transform features into a lower-dimensional space while preserving essential information Guyon and Elisseeff (2003). Recent studies have highlighted the effectiveness of feature engineering and selection in detecting DDoS attacks in the context of IoT, where high-dimensional data often leads to inefficiencies. Malik et al. Malik et al. (2023) demonstrated that a comprehensive feature engineering approach significantly improves detection accuracy by reducing irrelevant features while maintaining critical information. Furthermore, Abu Bakar et al. Abu Bakar et al. (2023) proposed an intelligent agent-based detection system that combines automatic feature extraction and selection, leading to enhanced performance in identifying DDoS attacks with minimal manual intervention.

The importance of distinguishing between feature selection and feature extraction has also been discussed by Ngo et al. Ngo et al. (2024), who compared the two methods in the context of intrusion detection. Their findings showed that while feature selection helps in retaining the most important features, feature extraction, such as PCA, is effective in reducing feature dimensions, resulting in improved model performance without compromising accuracy. Additionally, Kemp et al. Kemp et al. (2023) applied feature reduction to effectively detect application-layer DoS attacks, emphasizing that dimensionality reduction techniques can minimize computational overhead, making real-time detection feasible even in resource-constrained environments.

### 2.4. Interpretability and Explainability in ML Models

As ML models become more complex, understanding their decision-making processes becomes increasingly challenging. This has led to a growing focus on interpretability and explain-

ability in ML. Methods such as SHAP provide interpretable insights into feature contributions and model predictions. SHAP values help quantify the impact of each feature on the model’s output, offering a clearer understanding of how predictions are made Lundberg and Lee (2017a). Kalutharage et al. Kalutharage et al. (2023) explored an explainable AI (XAI) approach to identify DDoS attacks in IoT networks, using explainable methods to provide insights into the decision-making of deep learning models, which is critical for gaining trust in automated systems.

The importance of explainability is further underscored by Sharma et al. Sharma et al. (2024), who introduced an XAI-based deep learning approach for intrusion detection in IoT networks, highlighting that explainability not only improves trust but also aids in identifying potential model biases. Alzu’bi et al. Alzu’bi et al. (2024) similarly leveraged deep transfer learning with XAI techniques for classifying DDoS attacks, allowing for detailed analysis of feature importance and enhancing the interpretability of otherwise black-box models. Moreover, Arreche et al. Arreche et al. (2024) evaluated several black-box XAI frameworks for network intrusion detection, emphasizing the need for effective XAI tools that can elucidate the underlying reasoning of complex ML models.

The review by Nwakanma et al. Nwakanma et al. (2023) on the application of XAI in connected vehicles and other intelligent systems underscores the growing trend towards integrating interpretability into cybersecurity solutions. By making models more transparent, stakeholders are better equipped to understand the risks associated with false positives or negatives. The analysis provided by Al-Shareeda et al. Al-Shareeda et al. (2023) further confirms the necessity of explainable models in the domain of DDoS detection, where complex attack patterns necessitate clear explanations of model decisions to ensure reliability and effectiveness in practical applications.

### 2.5. Uniqueness of This Paper

This paper uniquely integrates the TPOT and SHAP to automate model selection and enhance interpretability for DoS/DDoS attack detection. Unlike existing studies that often rely on manual feature selection or traditional ML approaches, this work automates the pipeline selection, thus reducing experimental overhead while optimizing detection accuracy and efficiency. Additionally, the incorporation of SHAP provides detailed insights into feature contributions, addressing the “black box” nature of many ML models in cybersecurity. This combination of automation and interpretability significantly enhances both the effectiveness and trustworthiness of DDoS detection systems.

## 3. Research Problem and Goals

The detection and mitigation of DoS and DDoS attacks remain a significant challenge in ensuring the availability and reliability of networked systems Mirkovic and Reiher (2004); Garcia-Teodoro et al. (2004); Li et al. (2020). These attacks generate a high volume of malicious traffic, which overwhelms

---

**Algorithm 1** Automated DoS detection and feature engineering using TPOT and SHAP.

---

```

1: Input: Network traffic dataset  $D = \{(X_{train}, y_{train}), (X_{test}, y_{test})\}$ 
2: Output: Trained model  $M$  with selected features and interpretability analysis
3: procedure FEATURE SELECTION AND MODEL TRAINING WITH TPOT
4:   // Step 1: Configure TPOT for automated pipeline optimization
5:   Initialize TPOT with generations  $g$ , population size  $p$ , and scoring metric  $s$ 
6:   Set TPOT configuration to include feature selection methods
7:   // Step 2: Train and optimize the pipeline
8:   Fit TPOT on training data  $(X_{train}, y_{train})$ 
9:   Extract the best pipeline  $P_{best}$  from TPOT
10:  // Step 3: Evaluate the optimized model
11:  Evaluate  $P_{best}$  on test data  $(X_{test}, y_{test})$ 
12:  Save the trained model  $M$  for further analysis
13: procedure FEATURE IMPORTANCE ANALYSIS WITH SHAP
14:   // Step 4: Compute SHAP values for the best model
15:   Calculate SHAP values for features in  $P_{best}$  using the test data
16:   Rank features based on their SHAP importance values
17:   // Step 5: Visualize and interpret feature importance
18:   Generate SHAP summary plots for visual interpretation
19:   Analyze the impact of top-ranked features on the model’s predictions
20: procedure DoS DETECTION
21:   Input: New network traffic data  $X_{new}$ 
22:   // Step 6: Predict using the trained model
23:   Apply the trained model  $M$  to predict labels for  $X_{new}$ 
24:   Output the predicted labels  $\hat{y}_{new}$ 
25: return Trained model  $M$ , SHAP analysis results, and predictions  $\hat{y}_{new}$ 

```

---

targeted systems, rendering them inaccessible to legitimate users. The complexity of detecting DDoS attacks lies in the high-dimensional nature of network traffic data, the need for real-time analysis, and the evolving tactics of attackers, which require adaptive and robust detection mechanisms Singh and Kumar (2018); Li et al. (2018). Traditional approaches, such as signature-based and anomaly-based detection, face limitations, including the inability to effectively recognize novel and sophisticated attack patterns, high false positive rates, and the challenges associated with manual feature selection Jones and Sielken (2005); Yang et al. (2014).

To address these challenges, this study aims to enhance DDoS detection by automating the selection of ML models and optimizing feature selection using TPOT. By automating these processes, the study seeks to reduce the manual experimentation required to identify effective models and feature sets, thereby improving scalability and efficiency Olson et al.

(2016). Furthermore, the lack of interpretability in ML models for DDoS detection has been a critical barrier to their deployment, as stakeholders need to understand and trust the model’s decisions. To address this issue, SHAP is utilized to provide transparency into the model’s decision-making process, highlighting the contribution of individual features and improving trustworthiness Lundberg and Lee (2017a).

This research focuses on creating an automated and interpretable framework for DDoS detection that not only optimizes model selection and feature importance but also enhances transparency, making it a practical solution for real-world network security applications. The ultimate goal is to streamline the development of ML models for DDoS detection while ensuring their effectiveness, scalability, and transparency, thereby contributing valuable insights into the deployment of AI-driven cybersecurity solutions.

#### 4. Methodology

Algorithm 1 outlines our comprehensive approach to DoS detection by integrating automated ML and interpretability techniques. It begins with configuring and utilizing the TPOT to automatically select the optimal feature subset and ML pipeline, ensuring enhanced accuracy and efficiency. Once the best pipeline is identified, the model’s feature importance is further analyzed using SHAP, which ranks features based on their contribution to the model’s predictions, providing critical insights into the model’s decision-making process. The final model, equipped with optimized features and interpretability, is then employed to predict DoS attacks on new network traffic data, offering a robust and transparent solution for AI-driven cybersecurity.

In this study, as discussed above, we leverage the TPOT alongside SHAP to enhance feature selection, model performance, and interpretability in ML models for detecting DoS attacks. TPOT automates the design of the ML pipeline, optimizing feature selection and hyperparameters, thereby identifying the best-performing model configurations. By streamlining the process of discovering optimal model architectures and settings, TPOT improves the accuracy and efficiency of DoS detection models. Complementing TPOT, SHAP provides detailed, interpretable insights into the contributions of individual features and the rationale behind model predictions. The integration of TPOT’s automated optimization and SHAP’s interpretability facilitates a comprehensive understanding of model behavior, making it possible to not only achieve high performance in detecting DoS attacks but also to understand the underlying factors influencing model decisions. This combination enhances both the performance and transparency of ML models in intrusion detection applications Olson et al. (2016).

##### 4.1. Dataset

The Lycos-IDS2017 dataset Sharafaldin et al. (2018) we used in this paper is a comprehensive network traffic dataset that includes various types of network attacks, including DDoS. The

Feature	Info
Decision tuple	ID, src/dest IP, src/dst port, protocol
Time	Timestamp, duration
Fwd pkts	Total, len (total, max, min, std, min)
Bwd pkts	Total, len (total, max, min, std, min)
IAT	Mean, std, max, min
Fwd IAT	Total, mean, std, max, min
Bwd IAT	Total, mean, std, max, min
Fwd flags	Push, URG
Flags	Bwd (Push, URG), Count
Pkts len/size	Pkts (min, std, max, mean, var), size (avg)
Pkt loss	Down/up ratio
Flags count	FIN/SYN/RST/PSH/ACK/URG/CWE/ECE
Fwd pkt header	Len, avg (Seg size, bytes/bulk, bulk rate)
Bwd pkt header	Len, avg (Seg size, bytes/bulk, bulk rate)
Subflow	Fwd/bwd (pkts, Bytes)
Init win Bytes	Fwd, Bwd
Active/idle	Mean, max, std, min
Other labels	Inbound, Similar HTTP

Table 1: Flow features and statistics in the Lycos-IDS2017 dataset Sharafaldin et al. (2018).

dataset was preprocessed to handle missing values, encode categorical variables, and normalize continuous features. We focus on a subset of features most relevant to DDoS detection, as identified by the TPOT optimization process Sharafaldin et al. (2018).

Key attributes of the dataset listed in Table 1 include `flag_rst` (Reset flag in TCP headers), `pk_len_std` (standard deviation of packet lengths), `fwd_subflow_bytes_mean` (average byte size of forward subflows), `flow_duration` (total duration of network flows), `bwd_pkt_len_mean` (average size of backward packets), and `bwd_pkt_len_tot` (total length of backward packets). These features provide an in-depth view of network behaviors, supporting our analysis effectively.

##### 4.2. Automated Model Selection through TPOT

TPOT is a framework that automates the design and optimization of ML pipelines through genetic programming. It systematically explores various combinations of preprocessing techniques, feature selection methods, and ML algorithms to identify the most effective pipeline for a given dataset. In this work, we outline the methodology for employing TPOT in the automated selection of models and features specifically for DoS detection (Algorithm 2). TPOT can be configured to include feature selection operators within the optimization process by incorporating desired feature selection methods. The TPOT pipeline is then fitted to the training data, during which TPOT iteratively evaluates and optimizes different pipelines that encompass feature selection steps. Upon completion of the opti-

mization process, the best-performing pipeline is extracted, encapsulating the optimal feature selection techniques and associated parameters Olson et al. (2016).

TPOT optimizes a pipeline  $P$  by solving:

$$P^* = \arg \max_{P \in \mathcal{P}} \text{Accuracy}(P(D_{\text{train}})),$$

where  $P^*$  is the optimal pipeline,  $P$  is the set of all possible pipelines, and  $D_{\text{train}}$  is the training dataset. The pipeline consists of a sequence of data preprocessing steps, feature selection, and model selection.

---

**Algorithm 2** Automated model selection using TPOT.

---

**Require:** Training dataset  $(X_{\text{train}}, y_{\text{train}})$ , generations  $g = 2$ , population size  $p = 30$ , scoring metric  $s = \text{'accuracy'}$ , configuration  $c = \text{'TPOT light'}$

**Ensure:** Optimized ML pipeline  $\mathcal{P}_{\text{best}}$

- 1: **Initialize** TPOT with parameters  $(g, p, s, c)$
  - 2: **Start timer** to measure total runtime
  - 3: **Fit** TPOT on  $(X_{\text{train}}, y_{\text{train}})$  to evolve pipelines
  - 4: **Obtain** best pipeline  $\mathcal{P}_{\text{best}}$
  - 5: **Evaluate** accuracy of  $\mathcal{P}_{\text{best}}$  on test data  $(X_{\text{test}}, y_{\text{test}})$
  - 6: **Print** accuracy and total runtime
  - 7: **Export**  $\mathcal{P}_{\text{best}}$  to a Python file
- 

In our work, we use TPOT to automate selecting the best ML pipeline using genetic programming. The key parameters we set for the TPOTClassifier are ‘generations=2’, ‘population\_size=30’, and ‘scoring=accuracy’, which means the algorithm will evolve the model over 2 generations with a population size of 30 pipelines per generation, optimizing for accuracy. The ‘config\_dict=TPOT light’ indicates a simplified configuration to speed up the process. The timer measures the total runtime for the optimization process, and the ‘tpot.fit(X\_train, y\_train)’ command trains the model on the training data. After fitting, the model’s accuracy on the testing data and the total time taken for the process are printed. Finally, the best model pipeline discovered by TPOT is exported to a Python file.

The output shows that after two generations, the TPOT algorithm identified the best pipeline as a DecisionTreeClassifier with specific parameters: ‘criterion=entropy’, ‘max\_depth=10’, ‘min\_samples\_leaf=2’, and ‘min\_samples\_split=7’. The best internal cross-validation score achieved was approximately 0.9992, and the best accuracy score on the test data was 0.9991, indicating an excellent model performance. The process took 11 minutes and 22 seconds, demonstrating TPOT’s efficiency in automating the model selection and optimization process while achieving high accuracy. This is particularly useful for leveraging ML without extensive manual experimentation and tuning of models.

#### 4.3. Intelligent TPOT Pipeline-based Feature Importance Extraction

Next, we extract the important features from the best pipeline in the TPOT file. Our focus was on the features with an

Rank	Feature	Importance
1	bwd_pkt_len_mean	0.620557
2	fwd_pkt_hdr_len_min	0.117785
3	flag_fin	0.0803743
4	fwd_iat_min	0.0378663
5	pkt_len_var	0.0349627
6	fwd_iat_mean	0.0317716
7	fwd_tcp_init_win_bytes	0.0131679
8	fwd_flag_psh	0.00993987
9	down_up_ratio	0.00961987
10	fwd_pkt_cnt	0.00924045
11	bwd_tcp_init_win_bytes	0.00877884
12	active_min	0.00588071
13	bwd_iat_min	0.00492238
14	bwd_iat_mean	0.00411989
15	fwd_pkt_hdr_len_tot	0.00354573
16	bwd_pkt_per_s	0.00197074
17	iat_std	0.00171884
18	flag_rst	0.00107015
19	fwd_pkt_len_mean	0.000886202
20	bwd_iat_std	0.000457246
21	fwd_iat_max	0.00043774
22	fwd_pkt_len_max	0.000408617
23	flag_SYN	0.000408114
24	pkt_per_s	0.000110606

Table 2: Feature importance in descending order.

importance score greater than zero because these features contribute meaningfully to the model’s predictions, whereas features with an importance score of zero have no influence and can be disregarded. By filtering out non-influential features, we reduce the complexity of the model without compromising its performance, which is crucial for enhancing interpretability and avoiding overfitting. The results of this process are shown in Table 2, which depicts the feature importances in descending order. The most important feature is bwd\_pkt\_len\_mean with an importance score of 0.620557, followed by fwd\_pkt\_hdr\_len\_min at 0.117785, and flag\_fin at 0.0803743. The table lists 24 features with non-zero importance scores, indicating their relevance to the Decision Tree model’s performance. This provides insights into which features contribute most significantly to the model’s decision-making process, helping to better understand and interpret the model’s predictions. The detailed ranking of features allows for further analysis and potential feature selection for future modeling efforts.

In the context of detecting DDoS attacks, bwd\_pkt\_len\_mean (Mean Backward Packet Length) is identified as the most significant feature, with an importance score of 0.620557. This feature represents the average size of packets transmitted from the target server back to the client, which may be an attacker in the case of a DDoS scenario. During a DDoS attack, attackers typically inundate the target with numerous small and repetitive requests. Consequently, the

server responds with a large number of uniform, small packets, resulting in a consistent mean backward packet length. The predictability and uniformity of the backward traffic generated in response to such attacks render `bwd_pkt_len_mean` a critical indicator for identifying malicious activities. The prominence of this feature, compared to others, underscores the strong correlation between consistent response packet sizes and the occurrence of a DDoS attack.

The second most significant feature in detecting DDoS attacks is `fwd_pkt_hdr_len_min` (Minimum Forward Packet Header Length), with an importance score of 0.117785. This feature measures the smallest header size in the forward packets sent from the attacker to the server. DDoS attacks, particularly volumetric ones, often involve minimal headers to maximize the number of packets sent within a short timeframe. Attackers utilize minimal packet headers to evade detection while consuming minimal bandwidth, thereby overwhelming the target. The consistency in the small header sizes of these forwarded packets makes `fwd_pkt_hdr_len_min` an effective indicator of DDoS traffic, as normal network traffic typically exhibits more variability in packet header lengths.

In addition to the aforementioned features, `flag_fin` and `fwd_iat_min` are ranked third and fourth, respectively, in terms of their importance. `flag_fin` (importance score: 0.0803743) represents the presence of the TCP FIN flag, which indicates the termination of a connection. Abnormal patterns in the use of this flag may suggest malicious attempts to establish and abruptly terminate numerous connections, which is a common behavior in DDoS attacks such as SYN floods or TCP-based attacks. Similarly, `fwd_iat_min` (importance score: 0.0378663), which measures the minimum inter-arrival time of forward packets, is crucial for distinguishing attack traffic from legitimate user behavior. DDoS attacks typically involve rapid bursts of packets with very short intervals between them, whereas normal traffic is characterized by more sporadic packet transmissions. This distinction makes `fwd_iat_min` a valuable feature in identifying high-frequency attacks.

Other features, such as ‘`pkt_len_var`’ (Packet Length Variance) and ‘`fwd_iat_mean`’ (Mean Forward Inter-Arrival Time), also play a significant role. The ‘`pkt_len_var`’ (0.0349627) captures the variability in packet lengths, which tends to be lower in DDoS traffic due to the repetitive nature of attack packets. In contrast, normal traffic is more likely to show a higher variance in packet lengths, making this feature useful for distinguishing between attack and legitimate traffic. Similarly, ‘`fwd_iat_mean`’ (0.0317716) measures the average time between forward packets and can help identify anomalies in packet timing, such as the consistent rapid-fire requests seen during DDoS attacks. These features, although lower in rank, still contribute significantly to identifying patterns specific to DDoS attacks by analyzing the consistency and timing characteristics of network traffic.

#### 4.4. Utilizing SHAP for Feature Importance Analysis Across Different Classes

SHAP values are a method used to explain the output of any ML model by employing a game-theoretic approach that mea-

sures each feature’s contribution to the final outcome. In ML, each feature is assigned an importance value representing its contribution to the model’s output. SHAP values illustrate how each feature affects each final prediction, the relative significance of each feature, and the model’s reliance on feature interactions. Features with positive SHAP values have a positive impact on the prediction, while those with negative values exert a negative influence. The magnitude of these values indicates the strength of each feature’s effect.

Interpreting the model’s decision-making process is crucial for understanding how and why certain predictions are made. In this study, SHAP was used to provide insights into the contributions of individual features to the model’s predictions. SHAP values are derived from cooperative game theory, specifically the concept of Shapley values, which allocate credit for a cooperative game’s outcome to individual players (in this case, features) Lundberg and Lee (2017b).

For a given feature  $i$  in an instance  $x$ , the SHAP value  $\phi_i$  is computed as:

$$\phi_i = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|! (|F| - |S| - 1)!}{|F|!} [f(S \cup \{i\}) - f(S)]$$

Where:

- $F$  is the set of all features,
- $S$  is a subset of features excluding  $i$ ,
- $f(S)$  is the model’s prediction based only on features in  $S$ .

This equation essentially calculates the marginal contribution of each feature to the prediction, averaged over all possible feature combinations.

In our final stage, we extract and display the feature importances from the best pipeline identified by TPOT and compare them with the important features obtained in the previous step. First, the final pipeline model is retrieved using `tpot.fitted_pipeline_`, and the column names of the input data are assigned to `feature_names`. If the final model in the pipeline is a `DecisionTreeClassifier`, the feature importances are extracted, and a dictionary is created pairing each feature name with its corresponding importance. Features with zero importance are filtered out, and the remaining features are sorted by importance in descending order. The sorted features are then formatted into a pandas DataFrame, including a ranked index, and printed in a markdown table format.

Figure 2 shows the SHAP additive values of the important features across all six labels, where the contribution of each feature to the final prediction can be computed independently and then summed up.

The top-ranked feature, `bwd_pkt_len_mean` (Mean Backward Packet Length), is critical because it measures the average length of packets sent from the target server back to the source. During a DDoS attack, the server typically responds to an overwhelming number of small, repetitive requests from multiple sources. These requests are often minimal in nature,

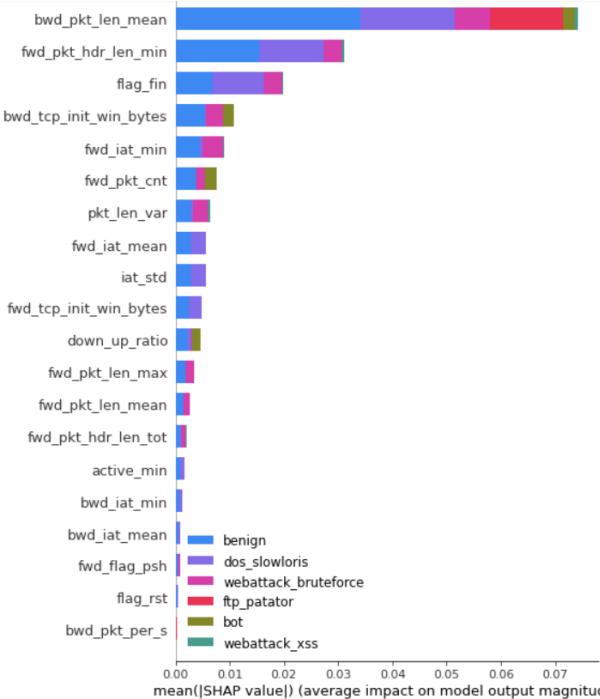


Figure 2: A summary plot showing important features for all classes

such as HTTP GET requests, which demand a simple acknowledgement or small response. Consequently, the size of the packets sent back (backward packets) tends to be consistent and relatively small. The mean backward packet length thus reveals an important signature: the more consistent and shorter the backward packets are, the more likely it is that the server is under attack. In normal traffic conditions, the size of backward packets would vary considerably based on the nature of the requests, such as loading complex pages or responding to various types of queries. A consistent pattern of small backward packet lengths can indicate the presence of a DDoS attack, where the server is constantly bombarded with repetitive requests, leading to a uniform response size Singh and Kumar (2018); Das et al. (2019); Amini et al. (2015).

Similarly, ‘fwd\_pkt\_hdr\_len\_min’ (Minimum Forward Packet Header Length) provides vital insights into the nature of the traffic sent to the server, specifically by measuring the smallest header size in the packets sent from the attackers to the target. In many DDoS attacks, especially volumetric ones, the attacker’s goal is to send as many packets as possible in the shortest time frame to overwhelm the server’s resources. These attack packets often have minimal headers, containing just enough information to be processed but not enough to carry substantial or meaningful data. This results in a consistently small forward packet header size during the attack. In contrast, legitimate traffic typically has varying header sizes depending on the type of communication, as different requests and services require different amounts of header information. Therefore, a persistently low minimum packet header length can signal that a DDoS attack is underway, characterized by an unusually high volume of small, repetitive packets designed

to strain the target’s resources. Together, ‘bwd\_pkt\_len\_mean’ and ‘fwd\_pkt\_hdr\_len\_min’ serve as critical indicators, helping to distinguish between normal network activity and the abnormal traffic patterns seen during DDoS attacks Kumar and Jain (2019); Li et al. (2018).

Traffic Label	Label	Train set	Test set
benign	0	83163	194140
bot	1	18	40
dos_slowloris	2	1045	2406
ftp_patator	3	579	1344
webattack_bruteforce	4	434	926
webattack_xss	5	36	121

Table 3: Ntetworking flow label distribution in train and test sets.

## 5. Performance Evaluation and Feature Impact Analysis

	benign	bot	dos_s..	ftp_p..	web..b..	web..x..
benign	194089	1	7	9	9	4
bot	4	39	0	0	0	0
dos_s..	36	0	2397	0	0	0
ftp_p..	0	0	0	1335	0	0
web..b..	11	0	2	0	917	117
web..x..	0	0	0	0	0	0

Table 4: Confusion matrix.

In the evaluation of our model’s performance, the confusion matrix in Table 4 provides a detailed breakdown of correct and incorrect predictions. The matrix shows that the model accurately detects most benign traffic, with very few false positives. However, the small number of misclassifications in other attack types highlights potential areas for improvement, particularly in identifying web-based attacks such as XSS (Cross-Site Scripting) and FTP-based attacks. We calculated the false positive rate (FPR) and false negative rate (FNR) to gain further insights. For example, the FPR for benign traffic was 0.002%, indicating the model’s robustness in detecting legitimate traffic. Meanwhile, the FNR for webattack\_xss was relatively high at 3.7%, suggesting a need for model refinement in handling specific attack vectors.

In addition to the AUC-ROC, we used a Precision-Recall Curve (PRC) to assess the model’s performance, particularly due to the imbalanced nature of the dataset where true negatives (benign traffic) dominate. The PRC provides a better understanding of the model’s ability to correctly identify attacks. As depicted in Figure 2, the model achieves a high precision across most attack categories, reflecting its strong capability to minimize false positives. However, the recall for the webattack\_xss category was lower, indicating that while the model rarely misclassifies benign traffic as malicious, it could occasionally fail to detect specific attack patterns.

### 5.1. Feature Groups and Descriptions

To better understand the behavior of different input variables in the context of DoS attack detection, we grouped the extracted

features into several logical categories based on their functional characteristics. This breakdown provides insight into which types of features are more indicative of attack patterns versus those that tend to resemble benign traffic. Below, we describe each feature group along with an analysis of its potential relevance and limitations in identifying DoS traffic.

### 5.1.1. Flow duration and packet lengths

Table 5: Flow duration and packet length features.

Feature Name	Description
<i>flow_duration</i>	Total duration of the network flow
<i>pkt_len_max</i>	Maximum packet length in the flow
<i>pkt_len_min</i>	Minimum packet length in the flow
<i>pkt_len_mean</i>	Mean (average) packet length
<i>pkt_len_var</i>	Variance in packet lengths

Table 5 highlights the flow duration and packet length features, which measure the overall duration of network flows and various packet length statistics. While these metrics are generally informative, they may not exhibit significant changes during a DoS attack, which typically involves a high volume of short, repetitive requests rather than substantial variations in flow durations or packet lengths.

### 5.1.2. Throughput metrics

Table 6: Throughput metrics features.

Feature Name	Description
<i>bytes_per_s</i>	Number of bytes transmitted per second
<i>pkt_per_s</i>	Number of packets transmitted per second
<i>fwd_pkt_per_s</i>	Number of forward packets transmitted per second

Table 6 lists the throughput metrics features, which represent the network throughput in terms of bytes and packets per second. In the context of DoS attacks, particularly volumetric attacks, these throughput metrics may not serve as effective differentiators, as attack traffic can closely mimic normal high-volume traffic patterns.

### 5.1.3. Forward and backward packet lengths

Table 7 lists the forward and backward packet length features which represent detailed statistics of packet lengths and counts in both forward and backward directions. Similar to previous packet length metrics, these features may not exhibit distinctive patterns that differentiate DoS traffic from legitimate traffic, particularly when the attack traffic is designed to closely resemble normal traffic.

### 5.1.4. Inter-arrival times (IAT) and activity periods

Table 8 reveals the IAT and activity/idle period features, which represent various aspects of timing between packets, as well as periods of activity and idleness. While these inter-arrival time (IAT) and activity metrics can be informative in certain contexts, they may not effectively capture the rapid and

Table 7: Forward and backward packet length features.

Feature Name	Description
<b>Forward Packet Features</b>	
<i>fwd_pkt_len_tot</i>	Total length of forward packets
<i>fwd_pkt_len_max</i>	Maximum length of forward packets
<i>fwd_pkt_len_min</i>	Minimum length of forward packets
<i>fwd_pkt_len_std</i>	Standard deviation of forward packet lengths
<i>fwd_pkt_hdr_len_tot</i>	Total header length of forward packets
<i>fwd_non_empty_pkt_cnt</i>	Count of non-empty forward packets
<b>Backward Packet Features</b>	
<i>bwd_pkt_cnt</i>	Total number of backward packets
<i>bwd_pkt_len_tot</i>	Total length of backward packets
<i>bwd_pkt_len_max</i>	Maximum length of backward packets
<i>bwd_pkt_len_min</i>	Minimum length of backward packets
<i>bwd_pkt_hdr_len_tot</i>	Total header length of backward packets
<i>bwd_pkt_hdr_len_min</i>	Minimum header length of backward packets
<i>bwd_non_empty_pkt_cnt</i>	Count of non-empty backward packets

Table 8: IAT and activity/idle period features.

Feature Name	Description
<b>IAT Features</b>	
<i>iat_min</i>	Minimum inter-arrival time between any two packets
<i>fwd_iat_tot</i>	Total inter-arrival time for forward packets
<i>fwd_iat_std</i>	Standard deviation of forward packet IAT
<i>bwd_iat_max</i>	Maximum inter-arrival time for backward packets
<i>bwd_iat_mean</i>	Mean inter-arrival time for backward packets
<i>bwd_iat_std</i>	Standard deviation of backward packet IAT
<b>Activity and idle period features</b>	
<i>active_max</i>	Maximum duration of active periods
<i>active_mean</i>	Mean duration of active periods
<i>active_std</i>	Standard deviation of active durations
<i>idle_max</i>	Maximum duration of idle periods
<i>idle_min</i>	Minimum duration of idle periods
<i>idle_mean</i>	Mean duration of idle periods
<i>idle_std</i>	Standard deviation of idle durations

overwhelming characteristics of DoS attacks, particularly as attack traffic may not exhibit clear timing patterns that distinguish it from normal traffic, especially in sophisticated scenarios.

### 5.1.5. TCP/IP flags

Table 9: TCP/IP flag features (i.e., flag indicators).

Feature Name	Description
<i>flag_ack</i>	Presence of the ACK (Acknowledgment) flag
<i>flag_psh</i>	Presence of the PSH (Push) flag
<i>bwd_flag_psh</i>	Presence of the PSH flag in backward packets
<i>flag_cwr</i>	CWR (Congestion Window Reduced) flag
<i>flag_ece</i>	ECE (Explicit Congestion Notification Echo) flag

Table 9 highlights the TCP/IP flag features, which represent the counts of specific TCP/IP flags in network traffic. While analyzing these flags can occasionally help detect DoS attacks, these particular flags may not be as indicative as others, such as SYN or RST flags, in identifying malicious activity.

### 5.1.6. Bulk transfer metrics

Table 10 lists the bulk transfer features, which represent average metrics related to bulk data transfers in both forward and

Table 10: Bulk transfer features.

Feature Name	Description
<b>Forward bulk transfer metrics</b>	
<i>fwd_bulk_bytes_mean</i>	Mean nbr. of bytes in forward bulk transfers
<i>fwd_bulk_pkt_mean</i>	Mean nbr. of packets in forward bulk transfers
<i>fwd_bulk_rate_mean</i>	Mean rate of forward bulk data transfer
<b>Backward bulk transfer metrics</b>	
<i>bwd_bulk_bytes_mean</i>	Mean nbr. of bytes in backward bulk transfers
<i>bwd_bulk_pkt_mean</i>	Mean nbr. of packets in backward bulk transfers
<i>bwd_bulk_rate_mean</i>	Mean rate of backward bulk data transfer

backward directions. These metrics may not be significantly impacted by DoS attacks, which typically focus on overwhelming the target with numerous small requests rather than large bulk data transfers.

#### 5.1.7. Subflow metrics

Table 11: Subflow features.

Feature Name	Description
<b>Forward subflow metric</b>	
<i>fwd_subflow_bytes_mean</i>	Mean nbr. of bytes per forward subflow
<b>Backward subflow metrics</b>	
<i>bwd_subflow_bytes_mean</i>	Mean nbr. of bytes per backward subflow
<i>bwd_subflow_pkt_mean</i>	Mean nbr. of packets per backward subflow

Table 11 summarizes the subflow features, which represent the average metrics of subflows in both forward and backward directions. Similar to bulk transfer metrics, these subflow metrics may not exhibit significant changes during DoS attacks.

The common thread among these features is that they measure aspects of network traffic that may not exhibit significant deviations during DoS attacks, especially if the attack traffic is designed to closely mimic legitimate traffic. DoS attacks typically focus on overwhelming the target with high volumes of traffic or specific types of requests (such as SYN floods), rather than altering packet sizes, flow durations, or bulk transfer patterns. Therefore, features that directly capture the volume, frequency, and abnormal flags (like SYN or RST) tend to be more indicative of DoS attacks.

The importance of specific features in detecting DoS attacks on a network lies in their ability to capture the abnormal traffic patterns and behaviors characteristic of such attacks. The most significant feature, ‘bwd\_pkt\_len\_mean’, which refers to the mean length of packets traveling from the server to the client, is crucial as DoS attacks often generate large volumes of traffic that can alter the typical packet size distribution. Similarly, ‘fwd\_pkt\_hdr\_len\_min’ and ‘fwd\_iat\_min’, which measure the minimum header length of forward packets and the minimum inter-arrival time between forward packets, respectively, help identify unusual spikes in traffic and rapid packet exchanges that are typical in flood-based attacks. The presence of flags such as ‘flag\_fin’, ‘flag\_psh’, and ‘fwd\_flag\_psh’ is vital as these TCP flags can indicate connection termination or push functions, which can be exploited during DoS attacks to disrupt normal communication.

Furthermore, ‘pkt\_len\_var’, indicating packet length variance, helps in detecting inconsistencies in packet sizes, another hallmark of a network under attack. Metrics like ‘fwd\_tcp\_init\_win\_bytes’ and ‘bwd\_tcp\_init\_win\_bytes’, representing the initial TCP window sizes, can reveal congestion or unusual usage patterns, as attackers may attempt to manipulate these windows to overwhelm the network. Features such as ‘active\_min’ and ‘bwd\_iat\_mean’ provide insights into the duration and timing of connections, with irregular values pointing to potential attacks. The inclusion of throughput-related features like ‘bwd\_pkt\_per\_s’ and ‘pkt\_s’ is also significant, as DoS attacks typically involve high packet rates intended to saturate the network bandwidth. These features provide a comprehensive view of the network’s operational metrics, enabling the detection of deviations from normal behavior that signal the presence of DoS attacks.

## 6. Learned Lessons and Future Directions

Throughout the development and evaluation of this work, several critical lessons were learned regarding the effective use of automated ML tools and explainable AI in the detection of DoS/DDoS attacks. One of the key insights gained was the value of leveraging automated ML frameworks, such as TPOT, to streamline the model selection and feature optimization processes. Automating these processes reduced the need for manual experimentation, resulting in significant time savings and ensuring that optimal hyperparameters and feature sets were systematically identified. However, it was also evident that the model’s success heavily depended on careful feature engineering, as not all features contributed equally to the final prediction outcomes.

The automated model selection process using TPOT identified a DecisionTreeClassifier as the most effective model for DDoS detection, optimizing for both accuracy and computational efficiency. The SHAP analysis revealed that *bwd\_pkt\_len\_mean*, *fwd\_pkt\_hdr\_len\_min*, and *flag\_fin* are the most important features contributing to the model’s predictions. The selection of these features is justified by their ability to capture critical aspects of network traffic that are indicative of DDoS attacks. For example, abnormal patterns in packet lengths and TCP flags are well-known indicators of various types of DDoS attacks, such as volumetric attacks and protocol-based attacks. The high SHAP values associated with these features confirm their importance in the detection process.

Another lesson learned involved the integration of SHAP to improve the interpretability of ML models. By providing insights into the contributions of individual features to the model’s predictions, SHAP not only addressed the “black box” nature of complex models but also allowed for greater trust and transparency in the decision-making process. This transparency is crucial for cybersecurity applications, where the ability to explain and justify model predictions can be essential for operational decisions. Nonetheless, the interpretability provided by SHAP can be computationally intensive, especially for larger

datasets, which may limit its applicability in real-time scenarios without further optimization.

Further, the interpretability provided by SHAP allows network administrators to understand the decision-making process of the model, making it easier to trust and deploy in real-world environments. This is particularly important in operational security settings, where the ability to explain why a certain traffic flow was flagged as malicious is crucial for incident response and mitigation.

From the experimental results, it also became apparent that certain features, such as packet length statistics and TCP flags, are particularly influential in detecting DDoS attacks, whereas metrics related to bulk data transfers and subflow measurements were less significant. This finding suggests that future efforts should focus on enhancing feature selection mechanisms to further refine the detection models and potentially improve their efficiency by excluding less relevant features.

Moving forward, several research directions could further enhance the effectiveness and applicability of the proposed methodology. One potential avenue is the integration of real-time SHAP optimization methods to reduce computational overhead and enable the deployment of explainable AI in time-sensitive environments. Developing lightweight interpretability mechanisms that can provide near real-time explanations without compromising accuracy would be invaluable for practical implementations in cybersecurity.

Another promising research direction is to explore the use of deep learning models in conjunction with TPOT to assess whether more sophisticated models, such as Convolutional Neural Networks (CNNs) or Long Short-Term Memory (LSTM) networks, could provide improved detection performance. Such models could be trained to detect more complex patterns in network traffic, potentially improving the accuracy of DDoS detection systems even in the face of evolving attack strategies.

Moreover, expanding the scope of this research to include other types of cyber threats, such as ransomware or Advanced Persistent Threats (APTs), would provide a more comprehensive cybersecurity solution. The adaptability of TPOT to different attack types and the potential for incorporating ensemble learning techniques could yield a more generalized model capable of addressing a wide range of threats in diverse environments.

## 7. Conclusion

In this study, we presented a novel approach for detecting Distributed Denial of Service (DDoS) attacks by leveraging the Tree-based Pipeline Optimization Tool (TPOT) for automated machine learning (ML) and SHapley Additive exPlanations (SHAP) for model interpretability. The integration of TPOT significantly streamlined the model selection and feature optimization processes, while SHAP provided essential insights into the contributions of individual features, thereby addressing the challenge of model transparency. Our experimental results demonstrated that features such as mean backward packet

length and minimum forward packet header length were critical for effective detection, while others, such as bulk transfer metrics, contributed less to the model's predictive performance.

The proposed framework not only enhances detection accuracy but also ensures that the decision-making process remains interpretable and trustworthy—an essential requirement in cybersecurity applications. Future research will focus on optimizing the scalability and efficiency of the interpretability mechanism, as well as extending the applicability of the framework to detect a broader range of cyber threats, further contributing to robust and transparent network security solutions.

## Author Contributions

**Paul Badu Yakubu:** Conceptualization, Investigation, Software, Methodology, Data curation, Writing – original draft; **Lester Santana:** Investigation, Validation, Formal analysis, Visualization; **Mohamed Rahouti:** Supervision, Project administration, Writing – review & editing, Funding acquisition; **Yufeng Xin:** Validation, Visualization; **Abdellah Chehri:** Methodology, Validation, Writing – review & editing; Funding acquisition; Mohammed Aledhari: Validation, Visualization.

## Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

## Conflicts of Interest

The authors declare no conflicts of interest.

## funding information

Funding Agency: Natural Sciences and Engineering Research Council of Canada (Grant Number: RGPIN-2022-3256).

## References

- Abu Bakar, R., Huang, X., Javed, M.S., Hussain, S., Majeed, M.F., 2023. An intelligent agent-based detection system for ddos attacks using automatic feature extraction and selection. Sensors 23, 3333.
- Al-Shareeda, M.A., Manickam, S., Saare, M.A., 2023. Ddos attacks detection using machine learning and deep learning techniques: Analysis and comparison. Bulletin of Electrical Engineering and Informatics 12, 930–939.
- Al-Zewairi, M., Almajali, S., Ayyash, M., Rahouti, M., Martinez, F., Quadar, N., . Multi-stage enhanced zero trust intrusion detection system for unknown attack detection in internet of things and traditional networks. ACM Transactions on Privacy and Security .

- Alfatemi, A., Rahouti, M., Bhuiyan, Z.A., Solyman, A., Aledhari, M., 2025. Protomaml: A hybrid meta-learning approach integrating prototypical networks for data-efficient ddos attack detection, in: 2025 International Wireless Communications and Mobile Computing (IWCMC), IEEE. pp. 1144–1149.
- Alzu’bi, A., Albashayreh, A., Abuarqoub, A., Alfawair, M.A., 2024. Explainable ai-based ddos attacks classification using deep transfer learning. *Computers, Materials and Continua* 80, 3785–3802.
- Amini, R., Jahanshahi, M., Mortazavi, R., Amini, A., 2015. Feature-based detection of ddos attacks. *International Journal of Communication Networks and Information Security* 7, 154–162.
- Arreche, O., Guntur, T.R., Roberts, J.W., Abdallah, M., 2024. E-xai: Evaluating black-box explainable ai frameworks for network intrusion detection. *IEEE Access* .
- Chen, K.C., et al., 2006. Decision tree learning. *Machine Learning* 19, 273–297.
- Clark, T., Rahouti, M., Xiong, K., 2024. Machine learning-based detection for cyber attacks in internet of medical things devices, in: 2024 IEEE MIT Undergraduate Research Technology Conference (URTC), IEEE. pp. 1–5.
- Das, M., Roy, A., Das, A., 2019. Packet-based anomaly detection of ddos attacks using knn and svm. *Journal of Network and Computer Applications* 147, 102–111.
- Deepa, P., et al., 2018. Enhanced intrusion detection using machine learning-based hybrid approaches for dos attacks. *Journal of Computer Networks and Communications* 2018, 1–9.
- Fenil, E., Mohan Kumar, P., 2020. Survey on ddos defense mechanisms. *Concurrency and Computation: Practice and Experience* 32, e5114.
- Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., Vazquez, E., 2004. Anomaly-based network intrusion detection: Techniques, systems and challenges, in: *Computers & Security*, Elsevier. pp. 18–28.
- Gupta, B.B., et al., 2018. Machine learning-based ddos mitigation for uav networks utilizing software-defined networks. *Journal of Network and Computer Applications* 100, 111–120.
- Guyon, I., Elisseeff, A., 2003. An introduction to variable and feature selection. *Journal of Machine Learning Research* 3, 1157–1182.
- Hafid, A., Rahouti, M., Aledhari, M., 2025. Optimizing intrusion detection in iomt networks through interpretable and cost-aware machine learning. *Mathematics* 13, 1574.
- Jones, A., Sielken, R., 2005. A comparison of signature-based and anomaly-based intrusion detection systems, in: *Computers & Security*, Elsevier. pp. 24–28.
- Kalutharage, C.S., Liu, X., Chrysoulas, C., Pitropakis, N., Papadopoulos, P., 2023. Explainable ai-based ddos attack identification method for iot networks. *Computers* 12, 32.
- Kemp, C., Calvert, C., Khoshgoftaar, T.M., Leevy, J.L., 2023. An approach to application-layer dos detection. *Journal of Big Data* 10, 22.
- Kumar, P., Jain, R., 2019. A comprehensive survey of ddos attack detection mechanisms using machine learning. *Computer Communications* 134, 1–18.
- Li, Q., Huang, H., Li, R., Lv, J., Yuan, Z., Ma, L., Han, Y., Jiang, Y., 2023. A comprehensive survey on ddos defense systems: New trends and challenges. *Computer Networks* , 109895.
- Li, X., Li, Y., He, M., Qi, M., 2018. Ddos attack detection based on packet behavior at the network layer. *IEEE Access* 6, 73258–73267.
- Li, Y., Sun, T., Liu, X., Zhao, J., 2020. Recent advances in network intrusion detection: A review. *Computers & Security* 92, 101733.
- Lundberg, S.M., Lee, S.I., 2017a. A unified approach to interpreting model predictions, in: *Advances in Neural Information Processing Systems*, pp. 4765–4774.
- Lundberg, S.M., Lee, S.I., 2017b. A unified approach to interpreting model predictions, in: Guyon, I., Luxburg, U.V., Bengio, S., Wallach, H., Fergus, R., Vishwanathan, S., Garnett, R. (Eds.), *Advances in Neural Information Processing Systems* 30. Curran Associates, Inc., pp. 4765–4774.
- Malik, M., Dutta, M., et al., 2023. Feature engineering and machine learning framework for ddos attack detection in the standardized internet of things. *IEEE Internet of Things Journal* 10, 8658–8669.
- Mirkovic, J., Reiher, P., 2004. Ddos defense mechanisms: A survey. *Proceedings of the IEEE* 94, 180–197.
- Ngo, V.D., Vuong, T.C., Van Luong, T., Tran, H., 2024. Machine learning-based intrusion detection: feature selection versus feature extraction. *Cluster Computing* 27, 2365–2379.
- Nwakanma, C.I., Ahakonye, L.A.C., Njoku, J.N., Odirichukwu, J.C., Okolie, S.A., Uzondu, C., Ndubuisi Nweke, C.C., Kim, D.S., 2023. Explainable artificial intelligence (xai) for intrusion detection and mitigation in intelligent connected vehicles: A review. *Applied Sciences* 13, 1252.
- Olson, R.S., Bartley, N., Urbanowicz, R.J., Moore, J.H., 2016. Evaluation of a tree-based pipeline optimization tool for automating data science, in: *Proceedings of the Genetic and Evolutionary Computation Conference 2016*, ACM, New York, NY, USA. pp. 485–492. doi:10.1145/2908812.2908918.

Owusu, E., Mapkar, M., Rahouti, M., Hsu, D.F., Schweikert, C., Verma, D.C., 2025a. Unified multimodel fusion for precision defense against evasive denial-of-service attacks, in: Assurance and Security for AI-enabled Systems 2025, SPIE. pp. 42–53.

Owusu, E., Mapkar, M., Rahouti, M., Verma, D.C., 2025b. Robust intrusion detection with combinatorial fusion and generative artificial intelligence. Computer 58, 46–57.

Owusu, E., Rahouti, M., Jagathee Saperumal, S.K., Xiong, K., Xin, Y., Lu, L., Hsu, D.F., 2024. Online network dos/ddos detection: sampling, change point detection, and machine learning methods. IEEE Communications Surveys & Tutorials .

Santana, L., Yakubu, P.B., Owusu, E., Rahouti, M., Chehri, A., Xiong, K., Xin, Y., 2024. Exploring feature importance and explainability towards enhanced ml-based dos detection in ai systems, in: 2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall), IEEE. pp. 1–5.

Sharafaldin, I., Habibi Lashkari, A., Ghorbani, A.A., 2018. La-beled dataset for intrusion detection system (ids) in cyber se-curity: The ids-2017 dataset.

Sharma, B., Sharma, L., Lal, C., Roy, S., 2024. Explainable artificial intelligence for intrusion detection in iot networks: A deep learning based approach. Expert Systems with Ap-plications 238, 121751.

Shukla, P., Krishna, C.R., Patil, N.V., 2024. Iot traffic-based ddos attacks detection mechanisms: A comprehensive re-view. The Journal of Supercomputing 80, 9986–10043.

Singh, S.B., Kumar, K.K., 2018. Trends in validation of ddos research. Procedia Computer Science 125, 747–753.

Yang, J., et al., 2014. Entropy-based approach for ddos attack detection in software-defined networks. Computer Networks 75, 63–71.

Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y., Han, H., 2022. A systematic literature review of methods and datasets for anomaly-based network intrusion detection. Computers & Security 116, 102675.

Zhang, Y., Zhou, X., 2008. Detection of dos attacks based on wavelet analysis and k-nearest neighbor classifier, in: Computer and Information Technology, 2008. CIT 2008. 8th IEEE International Conference on, IEEE. pp. 429–433.

Zhao, S., Santana, L., Owusu, E., Rahouti, M., Xiong, K., Xin, Y., 2023. Enhancing ml-based dos attack detection with fea-ture engineering: Ieee cns 23 poster, in: 2023 IEEE Con-ference on Communications and Network Security (CNS), IEEE. pp. 1–2.