Detection of Application-Layer Dos Attacks in IoT Devices Using Feature Selection and Machine Learning Models

Mustabeen Aziz[1], Muhammad Usman Sana[2]*, Tayybah Kiren[3]*, Tahmina Ehsan[1], Alvena Ehsan[1], Fateha Minahil[1]
[1]Department of Information Technology, University of Gujrat, Pakistan
[2]Department of Software Engineering, University of Gujrat, Pakistan
[3]Department of Computer Science (RCET), University of Engineering and Technology Lahore, Pakistan
*** Correspondence:** m.usman@uog.edu.pk, tayybah@uet.edu.pk

Citation | Aziz. M, Sana. M. U, Kiren. T, Ehsan. T, Ehsan. A, Minahil. F, "Detection of Application-Layer Dos Attacks in IoT Devices Using Feature Selection and Machine Learning Models", IJIST, Special Issue pp 197-207, March 2025
Received | Feb 21, 2025 **Revised |** March 05, 2025 **Accepted |** March 11, 2025 **Published |** March 14, 2025.

With technological advancements, innovations like the Internet of Things (IoT) have become widespread, connecting more devices to the Internet. However, as the number of connected devices increases, cyber-attacks—especially Distributed Denial of Service (DDoS) attacks—are also becoming more frequent. This research explores these cyber threats, focusing on DDoS attacks, and proposes strategies to protect IoT devices. It specifically aims to detect DDoS attacks in IoT devices using feature selection methods and machine learning algorithms. The study targets attack detection at the application layer of IoT devices by analyzing a relevant dataset. By applying feature selection techniques and machine learning models, we strive to enhance the accuracy and efficiency of DDoS detection, ultimately improving IoT security.

Keywords: Distributed Denial of Service (DDoS), Cybersecurity, Internet of Things, Feature Selection.

Introduction:

In recent years, millions of IoT devices have been connected for communication, relying on the Internet to transmit data between devices. These include sensors, smart devices, actuators, and RFID devices. However, IoT devices face cybersecurity challenges, particularly cyber-attacks. As the number of connected devices grows, different types of attacks emerge, including Distributed Denial of Service (DDoS) attacks.

ADDoS attack does not steal information but floods the server with excessive traffic, slowing it down. This study focuses on detecting exploitation- and reflection-based DDoS attacks using reduced features [1]. The main goal of a DDoS attack is to overwhelm a targeted website or server with high traffic from multiple sources, rendering it inaccessible. These attacks are particularly harmful because they originate from numerous locations, making them difficult to mitigate [2].

Application-layer DDoS attacks, such as HTTP request-based attacks, are especially dangerous because they require relatively few attacking connections to disrupt a website. Their traffic closely resembles normal traffic, making detection challenging [3]. In APDDoS attacks, attackers send numerous packets to the target server, causing congestion and slowing it down. To launch this attack, each participating system first establishes a TCP connection with the victim's server, requiring a valid IP address [4].

Research Contributions:

- This study focuses on detecting DDoS attacks at the application layer of IoT devices, as shown in Figure 1.
- It employs the Extra Tree feature selection method to identify relevant features for detecting DDoS attacks.
- Hyperparameter tuning and k-fold cross-validation are applied to enhance model robustness and prevent overfitting.
- Machine learning models and feature selection techniques are used to improve IoT security and enhance DDoS attack detection.

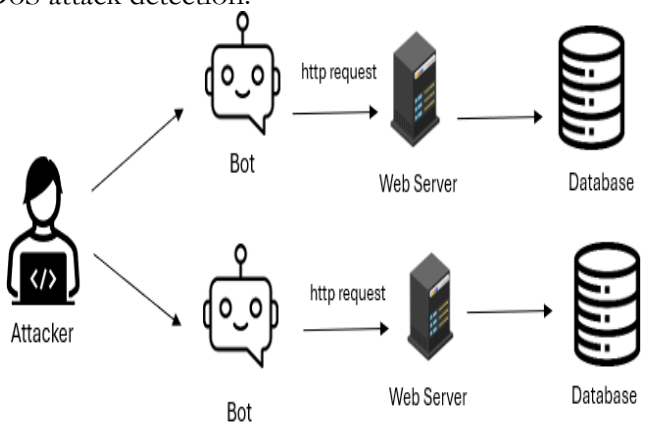

Figure. 1. Application-layer DOS attack

DDoS attacks are categorized into two types:

- **Network Layer DDoS Attacks** – These aim to generate high volumes of traffic to overwhelm the target.
- **Application Layer DDoS Attacks** – These mimic legitimate behavior while using low bandwidth, making them harder to detect and mitigate [5].

DDoS attacks can harm networks in various ways. Most application-layer DDoS (APDDoS) attacks exploit protocols such as HTTPS, HTTP page flood, DNS query flood, and HTTP bandwidth utilization [6].

- **Exploitation attacks** include SYN flood, UDP lag, and UDP flood.

- **Reflection-based attacks** involve SNMP, MSSQL, LDAP, SSDP, DNS, and NETBIOS.

The objective of this paper is to detect DDoS attacks at the application layer of IoT devices. The research contributions include:

- Detecting DDoS attacks using a feature selection method.
- Applying machine learning algorithms for detection.
- Comparing different ML models to improve DDoS attack detection at the application layer.

Denial of Service Attack:

A DDoS attack targets IoT devices by overwhelming them with excessive traffic. Hackers exploit these devices to access resources and disrupt normal operations [7]. In this attack, multiple devices send numerous requests to a server, which treats them as legitimate and responds to each one. As the server receives more requests than it can handle, it slows down. The goal of a DDoS attack is not to steal information but to degrade server performance.

There are three main types of DDoS attacks [8]:

- Protocol-Based Attacks – Exploit network protocols to overwhelm resources.
- Application Layer Attacks – Target specific applications, mimicking legitimate traffic.
- Volume-Based Attacks – Flood the network with massive amounts of traffic.

When multiple computers send requests to a single server beyond its capacity, the server cannot differentiate IP addresses, leading to incorrect responses and further congestion.

Research Focus:

- This study focuses on detecting DoS attacks at the application layer in the IoT environment.
- The Extra Tree feature selection method is used to identify key features for detecting DDoS attacks.
- The dataset includes relevant features of application-layer attacks for accurate detection.
- Hyperparameter tuning and k-fold cross-validation are applied to enhance model robustness and prevent overfitting.
- Machine learning models and feature selection techniques are used to strengthen IoT security and improve DDoS attack detection.

Novelty of the Study:

This research emphasizes application-layer DDoS attacks, which closely resemble normal traffic and are harder to detect than traditional network-layer attacks. By using an application-layer DDoS dataset, this approach provides a practical solution for the early detection of APDDoS attacks in IoT networks.

Objectives of the Study:

Key Objectives of This Study:

- Detect **application-layer DDoS attacks** in IoT devices using machine learning techniques.
- Improve detection accuracy and efficiency by applying Extra Tree feature selection, which reduces dataset dimensionality while preserving essential features.
- Evaluate and compare the performance of Decision Tree, Naïve Bayes, and Logistic Regression classifiers using key metrics such as accuracy, precision, recall, and F1-score.
- Enhance IoT security by identifying the most effective machine learning model for real-time detection and practical deployment in IoT environments.

Literature Review:

In [9], the attacker targets an IP address and sends requests to a server via the Internet. This type of attack is called a reflection attack, where the response size is larger than the request size. DDoS detection methods fall into three categories:

- **Supervised learning** – Uses labeled data for classification.
- **Unsupervised learning** – Works with unlabeled data to identify patterns.
- **Hybrid learning** – Combines both approaches to distinguish DDoS attacks from normal traffic.

A hybrid machine learning method is used for DDoS detection, working in three phases:

- DBSCAN algorithm clusters benign and DDoS network flows.
- Clusters are partitioned and analyzed using statistical measures.
- The CICIDS dataset is used for training, while the CICDDoS2019 dataset is used for testing.
- DBSCAN is used for unsupervised learning, while classification algorithms are applied for supervised learning.

In [10], DDoS attacks are recognized as a major threat to cloud computing, IoT, and 5G networks. While many researchers have studied DoS attacks, they often use outdated datasets that lack modern threats. This study employs an SDN-based (Software-Defined Network) architecture to detect DDoS attacks at the transport and application layers using deep learning (DL) and machine learning (ML) algorithms.

- **Transport layer attacks**: UDP flood, TCP-SYN flood.
- **Application layer attacks:** High- and low-volume HTTP-based attacks.

The study uses machine learning models such as Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN), along with deep learning techniques like Multilayer Perceptron (MLP), Convolutional Neural Network (CNN), and Gated Recurrent Unit (GRU).

- The CICDDoS2017 and CICDDoS2019 datasets are used.
- Achieved 98% accuracy for application-layer attacks and 95% accuracy for transport-layer attacks.

In [11], the study highlights DDoS attacks as a major challenge to internet security. These attacks target the transport, application, and network layers using various protocols such as ICMP, HTTP, TCP, and UDP.

- A DDoS taxonomy is proposed to categorize different attack types.
- The CICDDoS2019 dataset is used to provide a feature set for detecting various DDoS attacks.
- Machine learning techniques used: Random Forest, Logistic Regression, Naïve Bayes, and ID3 algorithms.
- The study focuses on detecting SYN, DNS, MSSQL, UDP-Lag, and LDAP attacks.
- In [12], the study addresses IoT security by applying machine learning (ML) and artificial intelligence (AI) techniques.
- IoT devices rely on sensors and communicate via wired and wireless networks.
- The study applies AI-based intrusion detection and ML-based classification to detect anomalies in IoT systems.
- Neural networks are used to train the system to identify invalid traffic.
- Focuses on differences between IoT systems and traditional systems.
- Uses the KDD Cup 1999 dataset, which contains IoT and cybersecurity data.
- In [13], a review of ensemble learning techniques is conducted, comparing different feature selection methods for DDoS detection.
- Evaluates True Positive Rate (TPR), False Positive Rate (FPR), False Negative Rate (FNR), and accuracy.
- Highlights challenges in existing models, such as high false rates and low detection rates.
- Compares traditional ML models with ensemble learning techniques:
- Stacking-based, Bagging-based, and Boosting-based approaches.

- Traditional ML methods include Naïve Bayes (NB), K-Nearest Neighbors (KNN), and Decision Tree (DT).
- Focuses on intrusion detection in smart grids to distinguish malicious activities from normal activities.

In [14], various feature selection methods are analyzed for detecting DDoS attacks, including:

- Chi-Square, ANOVA, Extra Tree, and Mutual Information methods.
- Machine learning algorithms Random Forest (RF) and Decision Tree (DT) are applied.
- The Extra Tree feature selection method is used to extract the most relevant features for detecting different DDoS attack types.

Table 1. Comparison of Published Results

Ref	Problem	Methodology	Accuracy%	Features	Dataset
[9]	Detecting unprecedented DDoS attacks	Hybrid ML-based method	99%	All Features	CICIDS2017 CICDDOS2019
[10]	SDN-based architecture to Detect DDOS attacks at the Application and Transport Layer	ML and DL algorithms	99%	All features	CICDDOS2019
[11]	Real-time detection of different taxonomies of DDOS	To propose a taxonomy of DDOS for application later		Generate dataset	CICDDOS2019
[12]	To secure the IOT system	AI-based intrusion detection and classification in IOT networks using machine learning.	97.77%	All features	KDD Cup 1999
[13]	Intrusion detection in smart grids	Use ensemble learning and ML techniques for intrusion detection	93.4% 97.4%	All features	CICDDOS2019
[14]	Feature selection for detection of DDOS	Feature selection techniques and ML classifiers	82% 61%	Top Ten Features	CICDDOS2019
[15]	Detect DDOS Attack	Extra Tree-Random Forest model is used for detection of DDOS Attack	99%	99%	CICDDOS2019

Feature Selection and DDoS Detection:

In this study, the top 10 features are selected to detect DDoS attacks. The accuracy of detection is analyzed using three feature selection methods:

- Chi-Square

- Extra Tree
- Mutual Information

The performance of these feature selection techniques is evaluated using two machine learning classifiers:

- Decision Tree (DT)
- Random Forest (RF)

Study in [15]

In [15], the author applies the ET-RF model to the CICDDoS2019 dataset for DDoS attack detection. The study is divided into two scenarios:

1. Performance Evaluation of ML Algorithms
   - Different machine learning models, including K-Nearest Neighbors (KNN), Decision Tree (DT), and Random Forest (RF), are compared.
   - The Random Forest (RF) classifier, combined with the ET-RF feature selection method, achieves the highest accuracy.
2. Detection of Different DDoS Attack Types
   - Various DDoS attack types are analyzed independently to improve detection precision.

Methodology:

Research Methodology:

First, we identified the research question, focusing on cybersecurity—specifically, the detection of DDoS attacks in IoT devices**.**

Literature Selection:

To gather relevant studies, we searched platforms like Google Scholar and ResearchGate using keywords such as:

- "Cybersecurity"
- "IoT"
- "Machine Learning"

During this process, we encountered several recurring papers. After filtering, we selected 50 studies most relevant to our topic.

Data Collection & Analysis:

As we reviewed these papers, we identified common challenges and gaps in the field. We then analyzed data from these studies to understand the current research landscape on DDoS attacks in IoT environments. This helped us pinpoint a research gap and refine our focus.

Experimentation:

For experimentation, we applied an Application-Layer DDoS attack dataset. After pre-processing, including handling missing or null values, we used the Extra Trees feature selection technique to identify the most relevant features, as shown in Figure 2**.**

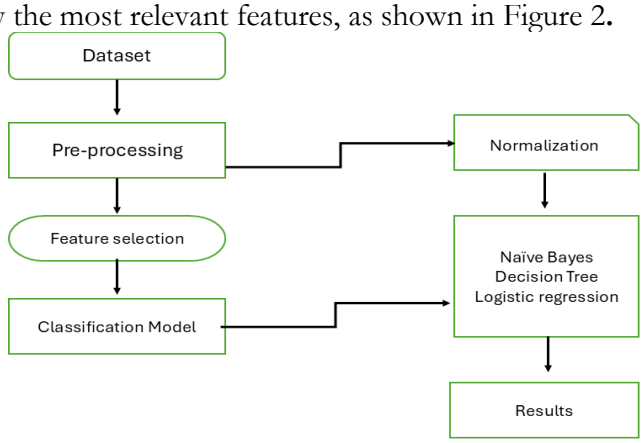

Figure 2. Methodology

Next, we utilized three machine learning classifiers—Naïve Bayes (NB), Decision Tree (DT), and Logistic Regression (LR)—to evaluate the performance of the selected features.

To ensure a fair comparison, we:

- Tuned hyper-parameters for each classifier to optimize accuracy.
- Applied k-fold cross-validation to enhance model robustness and prevent overfitting.

Finally, we compared the performance metrics of NB, DT, and LR. The results, presented in Figure 3, provide a clear assessment of their effectiveness in detecting DDoS attacks.

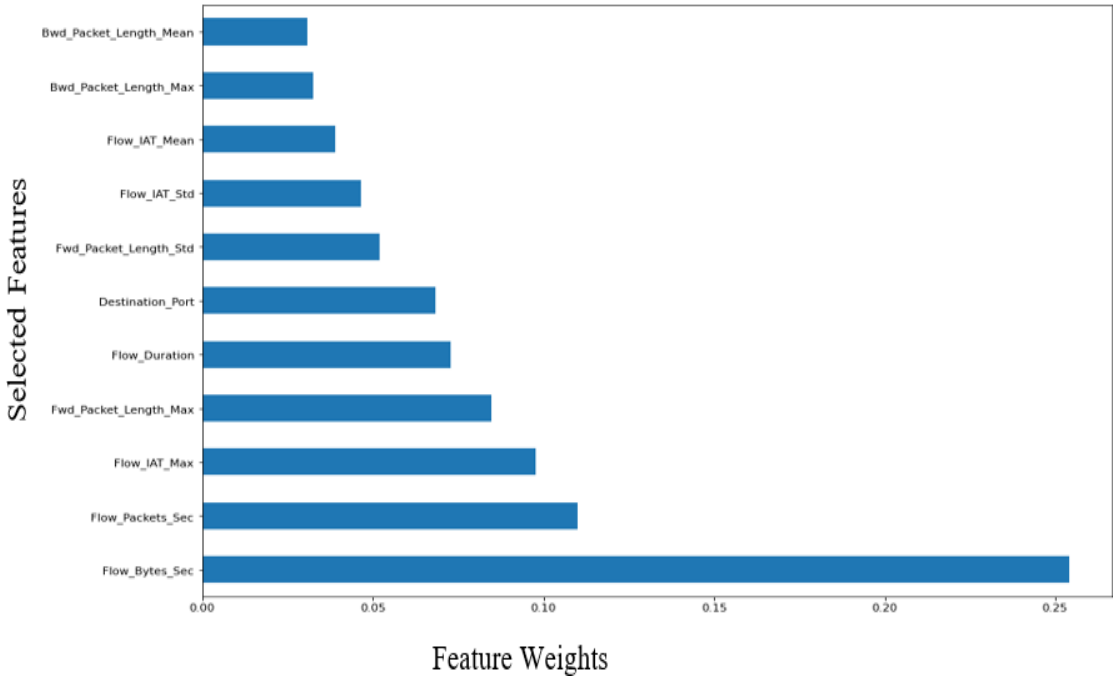

Figure 3. Extra Tree Feature selection

Decision Tree:

The Decision Tree (DT) algorithm is a supervised learning method used for classification. It follows a hierarchical structure to make decisions by partitioning data into subsets based on input values.

DT operates in a tree-like structure, where:

- **Branches** represent feature labels.
- **Leaves** represent class labels.
- **Decisions** are made at each branch, leading to target values at the leaves.

This structured approach helps in effectively classifying data [16].

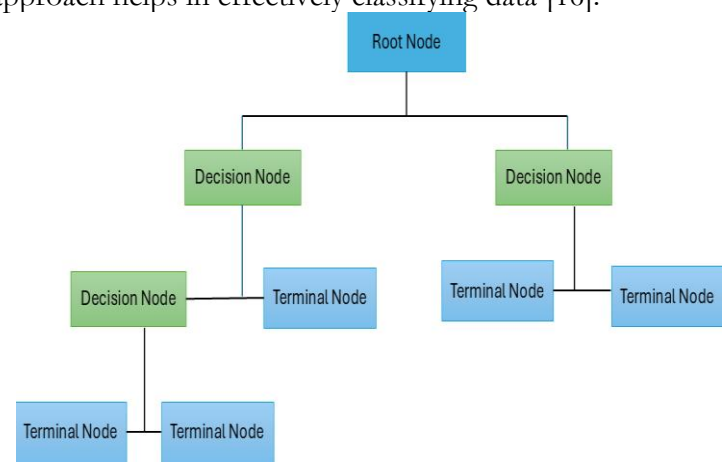

Figure. 4 Decision Tree Learning Architecture

Naive Bayes:

Naïve Bayes is a set of probabilistic algorithms based on Bayes' Theorem, commonly used for classification tasks. The term "Naïve" refers to the assumption that all features in the dataset are independent, though this is rarely true in real-world scenarios.

Despite this simplification, Naïve Bayes classifiers often deliver strong performance, especially in text classification tasks such as:

- **Sentiment analysis**
- **Spam detection**
- **Document categorization**

These characteristics make Naïve Bayes a widely used and effective classification technique [17].

$$P(A/B) = \frac{P(B/A).P(A)}{P(B)} \quad (1)$$

Logistic Regression:

Logistic Regression is a widely used machine learning approach for binary classification tasks. Despite its name, it is a classification model, not a regression one.

The primary goal of Logistic Regression is to estimate the probability that a given input belongs to a specific category. It does this by applying the sigmoid function, which maps predictions to values between 0 and 1, making it ideal for yes/no or true/false classification problems.

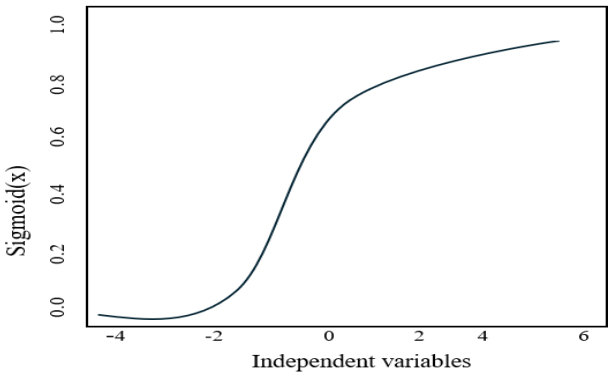

Figure 5 Logistic Regression

Result and Discussion:

The results presented in Table 2 highlight the performance of three machine learning classifiers—Decision Tree (DT), Naïve Bayes (NB), and Logistic Regression (LR)—based on key evaluation metrics. These results demonstrate the effectiveness of different algorithms in detecting application-layer DDoS attacks targeting IoT devices.

The models were evaluated using multiple metrics, including accuracy, precision, recall, F1-score, and cross-validation accuracy. Among these, the Decision Tree (DT) outperformed the other classifiers, achieving an accuracy of 99%. It also demonstrated high precision (98%), recall (99%), and F1-score (98%), making it a highly effective model for distinguishing between legitimate and malicious traffic.

Furthermore, the high recall value indicates that the Decision Tree is capable of detecting the majority of attack instances, making it a reliable choice for real-time security applications in IoT environments.

Table 2: Performance Results of Proposed Machine Learning Models for Detection of DDoS

Algorithm	Accuracy	Precision	Recall	F1-Score	Cv-Accuracy
Decision tree	99%	98	999	98	98.9
Naïve Bayes	94%	99	92	92	94.1
Logistic regression	89%	88	87	87	88

The Naïve Bayes (NB) classifier achieved a notable accuracy of 94%, with an exceptionally high precision of 99%. However, its recall was slightly lower at 92%, indicating that while the model is highly confident in its positive classifications, it may misclassify some attack instances as benign, leading to false negatives. Despite this, its cross-validation accuracy of 94.1% demonstrates consistent performance across different data splits, making it a reliable and generalizable model.

Among the three classifiers, Logistic Regression (LR) was the least effective. While it remains a viable option, its lower recall suggests that it may fail to detect all attack instances, which is critical in cybersecurity applications. However, its high precision indicates that when it does classify an instance as an attack, it is highly likely to be correct.

The bar chart in Figure 6 visually compares the accuracy of the three classification models: Decision Tree, Naïve Bayes, and Logistic Regression. The Decision Tree exhibits the highest accuracy, followed by Naïve Bayes, while Logistic Regression ranks the lowest. This visualization effectively highlights the performance differences among the models, aiding in the selection of the most suitable classifier for detecting application-layer DDoS attacks in IoT environments.

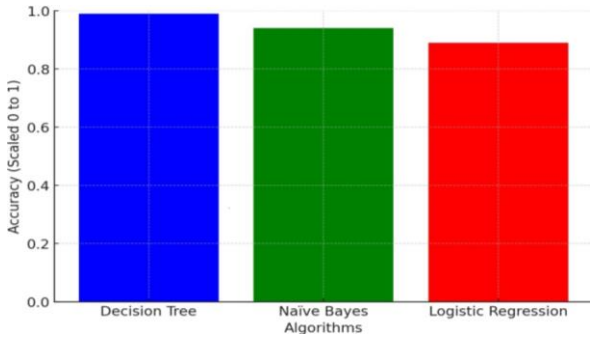

Figure 6. ML Classifier Comparison

Overall, the results indicate that Decision Trees are the most effective models for detecting application-layer DoS attacks in IoT environments, owing to their high accuracy and recall. Naïve Bayes also performs well, particularly in terms of precision, making it useful in scenarios where minimizing false positives is a priority. Logistic Regression, while still useful, is not the best choice when high recall is essential for detecting all attack instances.

The bar chart in Figure 6 visually compares the performance of the proposed machine learning models, clearly highlighting the Decision Tree as the most effective classifier.

Discussion:

This study demonstrates the effectiveness of machine learning-based approaches in detecting application-layer Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) environments. By leveraging the Extra Tree feature selection method, the proposed framework successfully reduces dataset dimensionality while preserving the most relevant features, enhancing both model accuracy and computational efficiency.

A comparative evaluation of three machine learning classifiers—Decision Tree, Naïve Bayes, and Logistic Regression—highlights the superior performance of the Decision Tree model, which achieved the highest accuracy (99%), precision (98%), recall (99%), and F1-score (98%). This confirms its effectiveness in distinguishing normal and attack traffic, making it a reliable choice for real-time DDoS detection in IoT networks.

The Naïve Bayes classifier also performed well, attaining 94% accuracy and a precision score of 99%. However, its lower recall (92%) suggests it may misclassify some attack instances as benign, leading to false negatives. This trade-off makes Naïve Bayes suitable for applications where minimizing false positives is critical, but less ideal for comprehensive attack detection. Logistic Regression, while achieving 89% accuracy, performed less effectively due to its lower recall and F1 score. This makes it a weaker option for highly imbalanced datasets or scenarios

requiring high recall, though its simplicity and interpretability may still be valuable in specific IoT applications.

Future Directions:

The results emphasize the importance of selecting appropriate machine learning models and feature selection techniques to improve the detection of sophisticated DDoS attacks that mimic legitimate traffic. The Extra Tree feature selection method effectively enhances classification accuracy by identifying key distinguishing features.

However, certain limitations remain, including the need for further optimization of classifiers for real-time deployment in large-scale IoT networks. Future research could explore:

- Advanced deep learning models**,** hybrid algorithms, or ensemble learning techniques to improve detection rates and reduce false positives**.**
- Expanding the dataset scope to include dynamic, real-time data for improved practical applicability in diverse IoT environments.

Conclusion:

Securing IoT Devices Against DDoS Attacks Using Machine Learning:

IoT devices play a crucial role in data collection and communication but remain vulnerable to cyber threats, particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. As the number of IoT devices grows, these threats become more severe.

To address this challenge, we explored DDoS attack detection at the application layer using Extra Tree feature selection and machine learning (ML) models. The results showed that the Decision Tree classifier achieved the highest accuracy (99%), outperforming Naïve Bayes (94%) and Logistic Regression (89%). This demonstrates the effectiveness of ML-based feature selection in strengthening IoT security against DDoS attacks.

Future research could focus on:

- **Advanced deep learning techniques** for improved accuracy and robustness.
- Real-time detection systems to enhance practical applications in IoT security.
- Hybrid models combine multiple algorithms for **stronger and more adaptive defense mechanisms** against evolving cyber threats.

Future Work:

Although, this approach works well. There are ways to make it better. One improvement could be making the system faster so it can handle large data easily. Another idea is to use advanced machine and deep learning algorithms to make results more accurate. Future research can also focus on testing this method in real-world situations to see how well it works.

Acknowledgment: Sincere gratitude is expressed to Dr. Muhammad Usman Sana for invaluable guidance and support throughout this research, which greatly contributed to the completion of this paper.

Author's Contribution: Mustabeen Aziz led the research and experiments. Muhammad Usman Sana and Tayybah Kiren supervised and reviewed the work. Alvena Ehsan, Tahmina Ehsan, and Fateha Minahil contributed to data analysis, literature review, and manuscript preparation.

Conflict of Interest: The authors declare no conflict of interest regarding this publication.

References:

[1] D. Kshirsagar and S. Kumar, "A feature reduction based reflected and exploited DDoS attacks detection system," *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 1, pp. 393–405, Jan. 2022, doi: 10.1007/S12652-021-02907-5/METRICS.

[2] H. B. and M. F. D. Mohammed Sharif, "Detection of Application-Layer DDoS Attacks Produced by Various Freely Accessible Toolkits Using Machine Learning," *IEEE Access*, vol. 11, pp. 51810–51819, 2023, doi: 10.1109/ACCESS.2023.3280122.

[3] A. Praseed and P. S. Thilagam, "Modelling Behavioural Dynamics for Asymmetric Application Layer DDoS Detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 617–626, 2021, doi: 10.1109/TIFS.2020.3017928.

[4] D. M. S. and M. F. H. Beitollahi, "Application Layer DDoS Attack Detection Using Cuckoo Search Algorithm-Trained Radial Basis Function," *IEEE Access*, vol. 10, pp. 63844–63854, 2022, doi: 10.1109/ACCESS.2022.3182818.

[5] C. Benzaid, M. Boukhalfa, and T. Taleb, "Robust Self-Protection Against Application-Layer (D)DoS Attacks in SDN Environment," *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2020-May, May 2020, doi: 10.1109/WCNC45663.2020.9120472.

[6] A. Munshi, N. A. Alqarni, and N. Abdullah Almalki, "DDOS Attack on IOT Devices," *ICCAIS 2020 - 3rd Int. Conf. Comput. Appl. Inf. Secur.*, Mar. 2020, doi: 10.1109/ICCAIS48893.2020.9096818.

[7] M. Odusami, S. Misra, O. Abayomi-Alli, A. Abayomi-Alli, and L. Fernandez-Sanz, "A survey and meta-analysis of application-layer distributed denial-of-service attack," *Int. J. Commun. Syst.*, vol. 33, no. 18, p. e4603, Dec. 2020, doi: 10.1002/DAC.4603.

[8] V. Gaur and R. Kumar, "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices," *Arab. J. Sci. Eng.*, vol. 47, no. 2, pp. 1353–1374, Feb. 2022, doi: 10.1007/S13369-021-05947-3/METRICS.

[9] S. Z. & S. M. Mohammad Najafimehr, "A hybrid machine learning approach for detecting unprecedented DDoS attacks," *J. Supercomput.*, vol. 78, pp. 8106–8136, 2022, doi: https://doi.org/10.1007/s11227-021-04253-x.

[10] C. V.-R. and J. A. P.-D. N. M. Yungaicela-Naula, "SDN-Based Architecture for Transport and Application Layer DDoS Attack Detection by Using Machine and Deep Learning," *IEEE Access*, vol. 9, pp. 108495–108512, 2021, doi: 10.1109/ACCESS.2021.3101650.

[11] I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," *Proc. - Int. Carnahan Conf. Secur. Technol.*, vol. 2019-October, Oct. 2019, doi: 10.1109/CCST.2019.8888419.

[12] M. T. Mahmood, S. R. A. Ahmed, and M. R. A. Ahmed, "Using Machine Learning to Secure IOT Systems," *4th Int. Symp. Multidiscip. Stud. Innov. Technol. ISMSIT 2020 - Proc.*, Oct. 2020, doi: 10.1109/ISMSIT50672.2020.9254304.

[13] T. T. Khoei, G. Aissou, W. C. Hu, and N. Kaabouch, "Ensemble Learning Methods for Anomaly Intrusion Detection System in Smart Grid," *IEEE Int. Conf. Electro Inf. Technol.*, vol. 2021-May, pp. 129–135, May 2021, doi: 10.1109/EIT51626.2021.9491891.

[14] V. Gaur and R. Kumar, "FSMDAD: Feature Selection Method for DDoS Attack Detection," *Proc. Int. Conf. Electron. Renew. Syst. ICEARS 2022*, pp. 939–944, 2022, doi: 10.1109/ICEARS53579.2022.9752308.

[15] V. Gaur and R. Kumar, "ET-RF based Model for Detection of Distributed Denial of Service Attacks," *Int. Conf. Sustain. Comput. Data Commun. Syst. ICSCDS 2022 - Proc.*, pp. 1205–1212, 2022, doi: 10.1109/ICSCDS53736.2022.9760938.

[16] K. C. Amir Mosavi, Pinar Ozturk, "Flood Prediction Using Machine Learning Models: Literature Review," *Water*, vol. 10, no. 11, p. 1536, 2018, doi: https://doi.org/10.3390/w10111536.

[17] T. R. Mohamed El Kourdi, Amine Bensaid, "Automatic Arabic document categorization based on the Naïve Bayes algorithm," *Proc. Work. Comput. Approaches to Arab. Script-based Lang. (Semitic '04). Assoc. Comput. Linguist. USA*, pp. 51–58, 2004, [Online]. Available: https://dl.acm.org/doi/10.5555/1621804.1621819