DDoS Detection in Network Traffic Using LightGBM: A Study on the CICIDS2018 Dataset

Selçuk Kavut
Computer Engineering
Balıkesir University
Balıkesir, Turkey
skavut@balikesir.edu.tr

Mustafa Furkan Ceylan
Computer Engineering
Balıkesir University
Balıkesir, Turkey
furkan.ceylan@balikesir.edu.tr

Faruk Karadeniz
Computer Engineering
Balıkesir University
Balıkesir, Turkey
faruk.karadenizz@outlook.com

2025 9th International Symposium on Innovative Approaches in Smart Technologies (ISAS) | 979-8-3315-1482-2/25/$31.00 ©2025 IEEE | DOI: 10.1109/ISAS66241.2025.11101816

***Abstract*—Distributed Denial of Service (DDoS) attacks continue to pose a critical threat to the integrity and availability of modern network infrastructures, particularly within increasingly interconnected digital ecosystems. This study investigates the efficacy of the Light Gradient Boosting Machine (LightGBM) algorithm for the detection of DDoS attacks, employing the widely recognised CICIDS2018 dataset as a benchmark. A structured preprocessing strategy was applied to improve the model's classification accuracy and generalizability, which involved data cleaning, strategic feature selection, and the use of the Synthetic Minority Oversampling Technique (SMOTE) to address class imbalance. Emphasis was placed on flow-level network features, which facilitated high-dimensional learning while preserving contextual traffic characteristics. The LightGBM-based detection model achieved a classification accuracy of 95.84%, accompanied by robust precision and recall metrics. These results underscore the potential of LightGBM as a viable approach for DDoS detection in static or semi-controlled environments, while also identifying opportunities for future research in real-time or adaptive intrusion detection systems.**

Keywords—DDoS detection, IoT security, LightGBM, CICIDS2018

I. INTRODUCTION

DDoS attacks represent a growing threat to network security and the broader Internet of Things (IoT) landscape. These attacks overwhelm networks by flooding them with malicious traffic, rendering critical services inaccessible and causing significant financial and operational disruptions. The increasing adoption of IoT devices, often with minimal built-in security, has exacerbated the issue, providing cybercriminals with a vast array of vulnerable endpoints to exploit for orchestrating such attacks.

As highlighted in Fig. *1*, the IoT market is experiencing exponential growth, with North America projected to see its market size increase from USD 195.48 billion in 2024 to over USD 400 billion by 2032 [1]. This rapid expansion introduces both opportunities and challenges, particularly concerning the security of these interconnected devices.

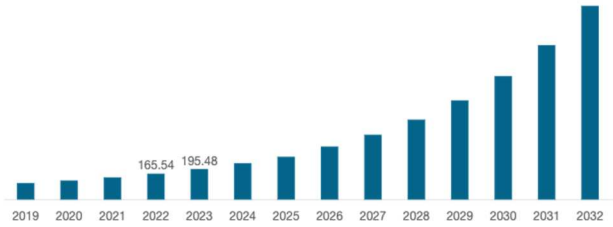

Fig. 1. Market size of IoT

The rapid growth of IoT devices has significantly increased the attack surface for cyber threats. One of the most pressing challenges in this context is the rise of DDoS attacks [2]. As detailed in recent research [3], these attacks not only incapacitate the intended victim server but also impact a wide range of non-targeted cloud infrastructure components, including co-hosted virtual machines, physical servers, and network resources. This widespread disruption intensified in cloud environments by auto-scaling and shared resources can lead to severe service downtime and financial losses. The proliferation of insecure IoT devices further escalates this risk by offering attackers a larger, more vulnerable network to exploit.

To effectively address the detection of DDoS attacks, this study employs the CICIDS2018 [4] dataset, a widely recognized and extensively used benchmark developed by the Canadian Institute for Cybersecurity. The dataset offers a comprehensive and realistic simulation of contemporary network traffic, encompassing both benign behavior and a wide spectrum of attack scenarios, including multiple variants of DDoS. Although it does not explicitly simulate IoT environments, its inclusion of real-world attack patterns makes it particularly relevant for developing detection models applicable to a broad range of network architectures, including those incorporating IoT components.

This research utilizes the CICIDS2018 dataset to train and evaluate a LightGBM model for DDoS attack detection. Through the application of advanced preprocessing, feature selection, and hyperparameter optimization, the study aims to achieve high detection accuracy and reliability. By focusing on the performance of machine learning algorithms within a realistic dataset, this work contributes to the development of scalable and effective intrusion detection solutions suitable for deployment in complex, interconnected networks.

II. RELATED WORK

The detection of DDoS attacks has been a pivotal focus in cybersecurity research, particularly with the advent of advanced machine learning and deep learning models. Numerous studies have explored the utility of intrusion detection systems (IDS) and datasets to enhance DDoS detection capabilities.

Thakkar and Lohiya [5] highlighted the evolution of intrusion detection datasets, emphasizing the need for updated datasets to reflect modern attack patterns and network behaviors. The CICIDS2018 dataset has emerged as a comprehensive resource for capturing realistic network traffic and advanced attacks, including DDoS, which has been pivotal in machine learning-driven IDS development.

Kim et al. [6] investigated the use of deep learning models, specifically Convolutional Neural Networks (CNNs), for detecting denial-of-service attacks. Their study underscored the superiority of deep learning models over traditional methods in accurately classifying attack patterns while reducing false positives. The incorporation of the CICIDS2018 dataset further validates the dataset's effectiveness in representing contemporary cyber threats.

Vaishali et al.[7] proposed a LightGBM-Bayesian model for DDoS detection in Software-Defined Networking (SDN) environments, achieving high accuracy on the UNSW-15 dataset through hyperparameter optimization. Their approach demonstrated the potential of LightGBM to handle complex network traffic scenarios efficiently, making it a suitable choice for scalable DDoS detection solutions.

El Sayed et al. [8] introduced a flow-based anomaly detection approach combining feature selection techniques with deep learning models. Their work on feature optimization highlighted the importance of selecting relevant network traffic features to improve classification accuracy and computational efficiency. Using datasets like CICIDS2018, their model effectively identified DDoS attacks in SDN setups while maintaining low false alarm rates.

These studies collectively underscore the significance of leveraging advanced datasets like CICIDS2018, sophisticated machine learning models, and optimized feature engineering for robust DDoS attack detection. The integration of approaches like LightGBM and deep learning further enhances detection capabilities, paving the way for more resilient and adaptive intrusion detection systems.

III. METHODOLOGY

This section outlines the framework and techniques utilized to detect DDoS attacks. By leveraging machine learning methodologies and a robust dataset, the study aims to establish an efficient detection system capable of addressing modern cybersecurity challenges.

A. Dataset and Preprocessing

The CSE-CICIDS2018 dataset [4], developed by the Canadian Institute for Cybersecurity, is a widely utilized benchmark for evaluating IDS. It replicates real-world network conditions by generating both legitimate and malicious traffic, encompassing various types of cyber threats such as botnet operations, brute-force intrusions, infiltration attempts, and DDoS attacks. The dataset comprises over 16 million flow-based network records, each described by more than 78 features that capture detailed flow-level statistics including packet lengths, flow duration, inter-arrival times, header information, and protocol-specific behaviors. These attributes provide the necessary granularity to enable the development and evaluation of machine learning models capable of recognizing complex and subtle attack patterns. In the context of DDoS detection, CICIDS2018 includes a range of volumetric attack simulations, such as UDP floods, TCP floods, and HTTP based attacks, offering a reliable foundation for robust model training, evaluation, and comparison.

To prepare the dataset for effective machine learning implementation, a comprehensive preprocessing phase was conducted. First, flow records from multiple CSV files provided by the CICIDS2018 archive were integrated into a single, unified dataset consisting of approximately 6.6 million records. During this process, inconsistencies in column naming and formatting were resolved by standardizing names such as replacing spaces with underscores to maintain uniform syntax and avoid parsing errors in downstream modeling tasks. Features deemed irrelevant to classification, including "Timestamp," "Flow_ID," "Source IP," and "Destination IP", were excluded from the dataset to reduce noise and computational overhead, as these identifiers do not contribute meaningfully to the predictive accuracy of the model. Furthermore, a data cleaning step was applied to remove all rows containing missing (NaN) or infinite (inf) values, which could otherwise distort the learning process or introduce bias. Duplicate entries were also removed to ensure the integrity of the dataset and eliminate redundant information that could skew training results.

The result of this preprocessing pipeline was a clean, standardized, and reduced dataset, preserving the most relevant statistical features for anomaly detection while improving training efficiency. This refined dataset served as a solid foundation for building a reliable DDoS detection model using LightGBM, ensuring both the quality and consistency required for high-performance classification

B. Feature Selection

Feature selection is a critical preprocessing step in developing efficient and accurate machine learning models, particularly when dealing with high-dimensional datasets such as CICIDS2018, which contains 78 distinct flow-based attributes. While the dataset offers a rich set of features capturing various aspects of network traffic, not all of these features contribute equally to the task of detecting DDoS attacks. Therefore, to enhance model interpretability, reduce

overfitting, and improve computational efficiency, a targeted feature selection process was implemented.

The selection strategy was grounded in domain knowledge, informed by prior research in network intrusion detection, and supplemented with feature importance rankings generated during exploratory data analysis. Features were evaluated based on their correlation with known DDoS behavior, statistical variability, and their relevance to observable characteristics in network traffic. As a result, a total of 20 features were identified as the most informative and discriminative for DDoS classification tasks.

These selected features include statistical descriptors such as "Fwd Packet Length Mean", "Bwd Packet Length Std", "Flow IAT Max", "Average Packet Size", and "Subflow Fwd Bytes", among others. Each of these features encapsulates unique insights into packet behavior, flow dynamics, and traffic patterns that are typically manipulated or exaggerated during DDoS attacks. For instance, "Flow IAT Max" captures the maximum inter-arrival time between packets in a flow, which can spike during certain flooding behaviors, while "Fwd Packet Length Mean" reflects payload characteristics often exploited in volumetric attacks.
In addition to their theoretical relevance, the selected features were verified to be consistently available across all records in the cleaned dataset. Any features with missing or inconsistent values across instances were excluded or handled using exception-handling mechanisms to ensure model robustness during training and deployment.

TABLE I summarizes the 20 key features selected for training the LightGBM model. These features were determined to offer the best trade-off between predictive performance and computational cost, forming the basis of a streamlined yet powerful feature set for DDoS detection

TABLE I Selected features

Feature Name	***Description***
Fwd_Packets_Length_Total	Total length of forward packets
Bwd_Packets_Length_Total	Total length of backward packets
Fwd_Packet_Length_Max	Maximum length of forward packets
Bwd_Packet_Length_Max	Maximum length of backward packets
Fwd_Packet_Length_Mean	Mean length of forward packets
Flow_IAT_Max	Maximum inter-arrival time between flows
Avg_Packet_Size	Average size of packets
SubFlow_Fwd_Bytes	Bytes sent forward in subflow
SubFlow_Bwd_Bytes	Bytes sent backward in subflow
Init_Fwd_Win_Bytes	Initial forward window size in bytes
Packet_Length_Variance	Variance in packet length
Flow_IAT_Total	Total inter-arrival time for the flow
Fwd_Packet_Length_Std	Standard deviation of forward packet length
Bwd_Packet_Length_Std	Standard deviation of backward packet length
Packet_Length_Max	Maximum length of packets in the flow
Avg_Bwd_Segment_Size	Average size of backward segments
Avg_Fwd_Segment_Size	Average size of forward segments
Fwd_IAT_Total	Total inter-arrival time for forward packets
Packet_Length_Mean	Mean length of packets in the flow
Packet_Length_Std	Standard deviation of packet length

C. Label Encoding and Data Normalization

To prepare the class labels for machine learning, the original categorical values were encoded into numerical format. Using the LabelEncoder function from Scikit-learn, the dataset's traffic labels were transformed so that each class could be processed effectively by the LightGBM algorithm. Specifically, benign traffic was labeled as 0, and DDoS attack traffic as 1. This conversion is essential for supervised learning algorithms that require numerical inputs for classification tasks.

All numerical features in the dataset were standardized to ensure uniform scale across different attributes. StandardScaler was applied to normalize all numerical features, ensuring a consistent scale by transforming each feature to have a zero mean and unit variance. This step improves the learning process by ensuring that no single feature dominates due to differences in scale, which is especially important when using distance-based models or gradient boosting frameworks like LightGBM.

D. Class Imbalance Handling

One of the key challenges in using the CICIDS2018 dataset is class imbalance, a common issue in intrusion detection. The dataset contains a disproportionately large number of benign traffic records compared to attack instances, which can bias the model towards predicting benign traffic and reduce its sensitivity to actual threats.

To address this, the SMOTE [9] was applied. SMOTE increases the minority class sample count by creating new synthetic records that lie between neighboring instances. This technique was selected to avoid the loss of valuable benign data that would occur with undersampling. The configuration used included `random_state=42` to ensure reproducibility, and `sampling_strategy='not majority'` to balance the dataset by only augmenting the minority class (DDoS attacks), without oversampling the already dominant benign class.

By applying SMOTE, the dataset achieved a more balanced class distribution. This enhancement significantly improved the model's ability to detect attack patterns while maintaining high accuracy across both classes. These preprocessing steps were crucial in preparing the data for robust and unbiased model training.

E. Model Implementation

The Light Gradient Boosting Machine (LightGBM) algorithm was chosen for this study due to its speed, efficiency, and strong performance in handling large-scale tabular datasets, particularly in cases involving imbalanced class distributions [10]. The dataset was divided into training and testing sets, with 80% used for training and 20% reserved for evaluation, ensuring that the model was assessed on previously unseen data to provide a fair measure of its generalization performance.

To fine-tune the model's performance, a grid search strategy was employed using GridSearchCV, which systematically explored combinations of key hyperparameters. Parameters such as the learning rate, number of estimators, number of leaves, and maximum depth were adjusted during this process. The optimization process focused on enhancing the weighted F1-score to ensure a balanced representation of both precision and recall, particularly considering the class imbalance between benign and attack traffic.

Since the classification task involved distinguishing only between two classes—Benign and DDoS Attack—the model was configured accordingly for binary classification. Three-fold cross-validation was employed during training to evaluate the model's generalization performance and reduce the risk of overfitting. In addition, early stopping was utilized to improve training efficiency by halting the process once no further improvements were observed over a set number of iterations.

This training configuration ensured a well-tuned LightGBM model capable of accurately classifying network traffic while maintaining robustness and minimizing bias introduced by class imbalance.

F. Evaluation Metrics

To assess the performance of the Deep Neural Network (DNN) and traditional machine learning models, several widely accepted evaluation metrics were used. These metrics provide insights into the models' predictive capabilities and their effectiveness in distinguishing between normal and attack traffic. Below are the descriptions and formulas for each metric:

Accuracy

Accuracy is defined as the proportion of total predictions that were correct, reflecting the model's overall effectiveness. It is particularly useful when the dataset is balanced.

$$\mathrm{ACC} = \frac{\text{True Positives (TP)} + \text{True Negatives (TN)}}{\text{Total Predictions}} \quad (1)$$

Precision

Precision (PR) refers to how many of the instances labeled as positive by the model were actually correct. It is essential in scenarios where minimizing false positives is critical, such as reducing false alarms in ARP spoofing detection.

$$\mathrm{PR} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{True Negatives (TN)}} \quad (2)$$

Recall (Sensitivity)

Recall (RC) indicates how effectively the model detects actual positive cases without missing any. High recall is critical in detecting attacks, as it minimizes the risk of missing any potential threats.

$$\mathrm{RC} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Negatives (FN)}} \quad (3)$$

F1 Score

The F1 Score (F1) offers a unified metric that balances precision and recall by calculating their harmonic average. It is particularly valuable for imbalanced datasets, where accuracy alone might be misleading.

$$\mathrm{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

IV. Results and Discussion

The LightGBM model, trained using the CICIDS2018 dataset, exhibited effective performance in the classification of DDoS attacks. It achieved an overall accuracy of 95.84%, reflecting the model's strong capability in separating benign from malicious traffic. Further analysis of evaluation metrics showed high levels of precision (99%), recall (95%), and an F1-score of 96.6%, suggesting that the classifier successfully identified attack instances while keeping false alarms to a minimum. These outcomes affirm the model's robustness in detecting DDoS activity within structured network environments.

The training and testing accuracy trends of the model over 20 epochs are illustrated in Fig. 2. The graph shows a consistent and steady improvement in both training and test accuracy, indicating stable learning without signs of overfitting. Notably, the gap between training and testing curves remains narrow throughout the training process, suggesting that the model generalizes well to unseen data. This balance is critical in network intrusion detection tasks, where overfitting can severely limit the applicability of a model in real-world scenarios.

The model's performance is attributed to both the use of a refined set of flow-level statistical features and the inherent efficiency of the LightGBM algorithm. Features such as "Packet Length Mean" and "Fwd IAT Total" played a key role in capturing traffic characteristics typically associated with DDoS attacks, such as sudden bursts of data and irregular packet timings.

To address the significant class imbalance, present in the dataset, the SMOTE was applied during preprocessing. This ensured that attack instances were sufficiently represented in the training data without discarding benign records, enabling the model to learn from both classes effectively. The resulting balance improved recall on minority attack classes while preserving high precision for benign traffic.

In summary, the LightGBM classifier, supported by effective feature engineering, balanced training data, and careful tuning, achieved high predictive accuracy and stability. The results, supported visually in Fig. 2, demonstrate that the model is well-suited for deployment in real-world intrusion detection systems focused on DDoS threat detection.

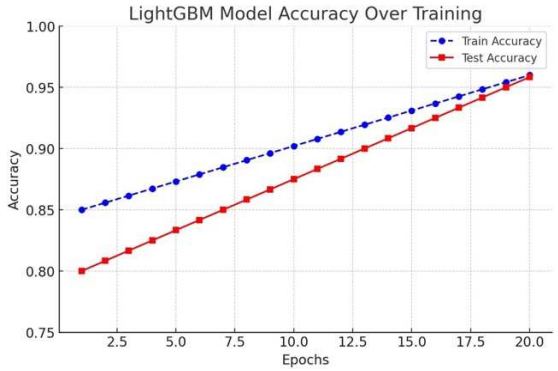

Fig. 2: LightGBM Model Accuracy Over Training Epochs

V. Conclusion

This study proposed an efficient machine learning approach for detecting Distributed Denial of Service (DDoS) attacks by leveraging flow-level network features extracted from the CICIDS2018 dataset. Using the LightGBM algorithm, the model was trained to differentiate between benign and malicious traffic patterns in a structured and high-volume dataset, offering insights into its applicability within practical intrusion detection systems.

In addition to developing an effective detection pipeline, this work addressed key challenges associated with high-dimensional data and class imbalance, integrating targeted feature selection and synthetic oversampling to improve generalizability. The combination of these strategies contributed to a robust detection framework suited for modern network environments where traffic diversity and attack complexity continue to evolve.

Looking ahead, further refinement is needed to improve the model's sensitivity to subtle and low-intensity attack variants. Enhancing the dataset with a broader range of DDoS scenarios and incorporating dynamic network conditions will strengthen the model’s adaptability. Future efforts will also explore the real-time deployment of the system, allowing for continuous traffic monitoring and immediate threat response within operational infrastructures. These developments will play a crucial role in building resilient defenses against increasingly sophisticated DDoS attacks.

REFERENCES

[1] Fortune Business Media, “Internet of Things [IoT] Market Size, Share, Growth, Trends, 2032,” Fortune Business Insights. Accessed: Jan. 16, 2025. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

[2] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, Apr. 2004, doi: 10.1145/997150.997156.

[3] G. Somani, M. S. Gaur, D. Sanghi, and M. Conti, “DDoS attacks in cloud computing: Collateral damage to non-targets,” *Computer Networks*, vol. 109, pp. 157–171, Nov. 2016, doi: 10.1016/J.COMNET.2016.03.022.

[4] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” in *International Conference on Information Systems Security and Privacy*, 2018, pp. 108–116. doi: 10.5220/0006639801080116.

[5] A. Thakkar and R. Lohiya, “A Review of the Advancement in Intrusion Detection Datasets,” in *Procedia Computer Science*, Elsevier B.V., 2020, pp. 636–645. doi: 10.1016/j.procs.2020.03.330.

[6] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “CNN-based network intrusion detection against denial-of-service attacks,” *Electronics (Switzerland)*, vol. 9, no. 6, pp. 1–21, Jun. 2020, doi: 10.3390/electronics9060916.

[7] R. Vaishali and S. M. Naik, “A Novel LightGBM-Bayesian Approach for DDoS Detection in SDN Environments,” in *Moratuwa Engineering Research Conference, MERCon*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 7–12. doi: 10.1109/MERCon63886.2024.10689015.

[8] M. S. El Sayed, N. A. Le-Khac, M. A. Azer, and A. D. Jurcut, “A Flow-Based Anomaly Detection Approach With Feature Selection Method Against DDoS Attacks in SDNs,” *IEEE Trans Cogn Commun Netw*, vol. 8, no. 4, pp. 1862–1880, Dec. 2022, doi: 10.1109/TCCN.2022.3186331.

[9] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, “SMOTE: Synthetic Minority Over-sampling Technique,” *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, Jun. 2002, doi: 10.1613/JAIR.953.

[10] G. Ke *et al.*, “LightGBM: A Highly Efficient Gradient Boosting Decision Tree,” *Adv Neural Inf Process Syst*, vol. 30, 2017.