IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

FMDADM: A FEATURE-DRIVEN MULTI-LAYER FRAMEWORK FOR DDOS ATTACK DETECTION AND MITIGATION IN STATEFUL SDN-ENABLED IOT NETWORKS

[1]Archana,[2]Arpita, [3]Bhavani,[4]Pallavi, [5]Sneha T

[1-4]Students, [5]Assistant Professor

[1-5]Computer Science & Engineering,

[1-5]Sharnbasva University,Kalaburagi,Karnataka,India

Abstract: Distributed Denial of Service (DDoS) attacks represent one of the most significant security threats to Internet of Things (IoT) networks, causing service disruption, resource exhaustion, and degradation of network performance. This study presents FMDADM, a multi-layer DDoS attack detection and mitigation framework based on machine learning for stateful SDN-inspired IoT environments. The proposed framework utilizes flow-based network traffic features extracted from the DrDoS_DNS dataset and applies preprocessing, normalization, and feature selection using SelectKBest with mutual information. Ten highly relevant traffic attributes are selected to improve classification efficiency and reduce computational complexity. Multiple machine learning algorithms, including Decision Tree, Random Forest, Logistic Regression, Support Vector Machine, and Naive Bayes, are trained and evaluated to identify malicious traffic patterns. A layered detection strategy combines rapid filtering and detailed verification to enhance reliability and accuracy. The framework also incorporates stateful traffic analysis and real-time monitoring through a Flask-based dashboard. Experimental results demonstrate effective attack detection, reduced false alarms, improved response capability, and enhanced security for IoT networks.

Index Terms – DDoS Detection, Internet of Things (IoT), Machine Learning, Random Forest, Decision Tree, Stateful Analysis, Network Security, Traffic Classification, SDN-Inspired Mitigation, DrDoS_DNS Dataset.

I. INTRODUCTION

The rapid expansion of digital technologies and interconnected communication systems has transformed the way information is generated, processed, and exchanged across modern environments. The Internet of Things (IoT) has emerged as a key component of this transformation by enabling smart devices, sensors, and embedded systems to communicate and operate autonomously. IoT applications are now widely deployed in smart homes, healthcare systems, industrial automation, transportation networks, agriculture, and environmental monitoring. These connected infrastructures improve operational efficiency, support real-time decision making, and provide enhanced user experiences through continuous data exchange. However, the increasing number of internet-connected devices has also introduced significant security challenges that threaten the reliability, availability, and integrity of network services.As IoT networks continue to grow in scale and complexity, they become attractive targets for cyber attackers seeking to exploit vulnerabilities in connected devices and communication channels. Many IoT devices possess limited computational resources and often operate with insufficient security mechanisms, making them vulnerable to a variety of cyber threats.

Among these threats, Distributed Denial of Service (DDoS) attacks have become one of the most serious concerns due to their ability to overwhelm network resources and disrupt critical services. In a DDoS attack, a large number of compromised devices simultaneously generate malicious traffic toward a target system, resulting in bandwidth exhaustion, service degradation, increased latency, and potential system failure. The emergence of IoT-based botnets has further amplified the scale and impact of such attacks, emphasizing the need for effective detection and mitigation solutions.Traditional security approaches primarily rely on signature-based detection methods and predefined rules to identify malicious activities. Although these techniques can detect known attack patterns, they often struggle to adapt to evolving threats and previously unseen traffic behaviors. Machine learning has emerged as a promising solution because of its ability to learn complex traffic patterns and automatically distinguish malicious activities from legitimate network communications. This capability makes machine learning particularly suitable for dynamic and heterogeneous IoT environments.This study presents FMDADM, a Multi-Layer DDoS Attack Detection and Mitigation Framework Using Machine Learning for Stateful SDN-Based IoT Networks. The proposed framework utilizes the DrDoS_DNS dataset, feature selection techniques, multiple machine learning classifiers, layered detection mechanisms, and SDN-inspired mitigation strategies to improve attack identification and response capabilities. Furthermore, a Flask-based monitoring platform enables real-time traffic analysis, prediction, and visualization. The framework aims to enhance network security, reduce false alarms, and strengthen the resilience of IoT infrastructures against increasingly sophisticated DDoS attacks.

II. Related Works

Article[1] "Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on IoT Networks Using Machine Learning Algorithms" by Zaed Mahdi, Nada Abdalhussien, Naba Mahmood, and Rana Zaki in 2024: This study proposed a real-time machine learning framework for detecting DDoS attacks in IoT environments. The authors utilized recent IoT traffic datasets containing both legitimate and malicious network flows. Feature engineering techniques were applied to improve classification performance. Multiple machine learning models were evaluated using standard metrics. The framework achieved high detection accuracy while maintaining low latency. Experimental results demonstrated effective identification of attack traffic. The proposed system enhanced network resilience against evolving cyber threats.

Article[2] "A Machine Learning Approach for DDoS Detection on IoT Devices" by Alireza Seifousadati, Saeid Ghasemshirazi, and Mohammad Fathian in 2021: This paper investigated machine learning techniques for identifying DDoS attacks targeting IoT devices. The CICDDoS2019 dataset was utilized for experimentation and analysis. Various classification algorithms were trained and evaluated using flow-based features. Ensemble methods demonstrated superior performance compared to conventional approaches. The study emphasized the importance of feature selection in improving model efficiency. Experimental results showed high detection accuracy and reliability. The framework effectively differentiated malicious and normal traffic. The research supported the adoption of intelligent security solutions in IoT environments.

Article[3] "Machine Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance" by Mohammed Alduailij, Abdullah Alshammari, and Fahad Alharbi in 2022: The authors proposed a feature selection methodology that combines mutual information with Random Forest feature importance. The approach focused on reducing feature redundancy and computational complexity. Network traffic attributes were ranked according to their significance. Machine learning classifiers were trained using the optimized feature subset. Experimental evaluations demonstrated improved accuracy and detection efficiency. The framework successfully identified attack traffic across multiple scenarios.

Article[4] "DDoS Attack Detection Techniques in IoT Networks: A Survey" by Amir Pakmehr, Abdulrahman Alhaidari, and Mansour Al-Rakhami in 2024: This survey examined recent DDoS detection techniques designed for IoT networks. Detection methods were categorized into signature-based, anomaly-based, machine learning, and deep learning approaches. The authors analyzed strengths and weaknesses of existing solutions. Various public datasets and evaluation metrics were reviewed. Scalability and resource limitations were identified as major challenges. The study emphasized the increasing importance of intelligent detection frameworks. Future research opportunities were discussed in detail. The survey provides valuable insights for researchers in IoT security.

Article[5] "Machine Learning-Driven DDoS Attack Detection in VANET Cloud Infrastructure" by Harsh Setia, Nitin Kumar, and Sandeep Kumar in 2024: This work presented a machine learning framework for detecting DDoS attacks in vehicular cloud environments. The proposed architecture analyzed traffic flow characteristics and communication patterns. Multiple classification algorithms were evaluated and compared. Experimental results demonstrated strong detection capability under dynamic conditions. The framework achieved high classification accuracy and low false positive rates. Real-time monitoring enhanced attack response efficiency.

Article[6] "DDoS Attacks Detection Based on Machine Learning and Deep Learning Techniques" by Mehdi Ebrahim Manaa, Suad Alasadi, and Hussein Al-Khamees in 2024: This research compared machine learning and deep learning methods for DDoS attack detection. Multiple cybersecurity datasets were utilized during experimentation. Accuracy, precision, recall, and F1-score were used for evaluation. Deep learning models effectively identified unknown attack patterns. Traditional machine learning algorithms provided faster prediction times. The study highlighted trade-offs between complexity and performance.

Article[7] "Systematic Literature Review of IoT Botnet DDoS Attacks and Detection Systems" by Murat Gelgi, Yong Guan, Sandeep Arunachala, and Nicola Dragoni in 2024: This systematic review analyzed recent research related to IoT botnet-driven DDoS attacks. The authors categorized existing detection systems into several major groups. Signature-based, anomaly-based, machine learning, and deep learning techniques were evaluated. Challenges associated with scalability and deployment were discussed. The review identified significant research gaps in large-scale IoT environments. Existing mitigation strategies were also examined comprehensively. Future directions for intelligent defense mechanisms were proposed. The paper serves as a strong foundation for cybersecurity researchers.

Article[8] "Artificial Intelligence Techniques for IoT-Based DDoS Attack Detection: A Review" by Bharat Bala, Vikas Sharma, and Rajesh Kumar in 2024: This review focused on artificial intelligence techniques used for DDoS attack detection in IoT systems. Various machine learning and deep learning algorithms were analyzed. The authors discussed dataset quality and feature engineering challenges. Performance metrics used in previous studies were compared. The review highlighted the importance of model optimization. Existing limitations and practical deployment issues were identified.

Article[9] "Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System" by Shubham Sharma, Priyanshu Verma, and Ankit Gupta in 2024: This study introduced a real-time cyberattack detection framework for IoT networks. Machine learning techniques were integrated with continuous traffic monitoring. The system analyzed communication patterns to identify malicious activities. Real-time prediction improved attack response capability. Experimental evaluations showed high detection accuracy. False alarm rates were significantly reduced through feature optimization.

Article[10] "A Comparative Analysis of Machine Learning Models for DDoS Detection in IoT Networks" by Sushil Shakya and Robert Abbas in 2024: The authors conducted a comparative analysis of multiple machine learning algorithms. Models including XGBoost, Naive Bayes, K-Nearest Neighbors, and SGD were evaluated. Standard performance metrics were used for comparison. Each classifier exhibited different strengths under varying conditions. The study identified models suitable for real-time deployment. Experimental results confirmed the effectiveness of intelligent detection systems.

Article[11] "An Efficient DDoS Attack Detection in Software Defined Networks Using Multi-Feature Selection and Ensemble Learning" by Anand V. Kachavimath, Prashant Patil, and Shivanand Totad in 2025:
This research proposed an SDN-based DDoS detection framework utilizing ensemble learning techniques. Advanced feature selection methods improved traffic classification performance. The framework analyzed network flow statistics within centralized SDN environments. Experimental results demonstrated high detection accuracy. Ensemble learning reduced false positives and enhanced reliability. The system supported efficient monitoring of large-scale networks.

Article[12] "Enhancing Machine Learning-Based DDoS Detection Through Adaptive Hyperparameter Optimization" by Shuai Chen, Yifan Wang, and Xiaolong Zhang in 2025: This paper presented an adaptive hyperparameter optimization strategy for DDoS detection models. Machine learning classifiers were trained using modern cybersecurity datasets. Grid search and optimization techniques improved model performance. Detection accuracy increased while computational cost was reduced. The framework effectively handled complex attack patterns. Experimental results outperformed conventional parameter tuning methods. The proposed approach supported scalable deployment in real-world environments.

III. PROBLEM STETEMENT

The rapid growth of Internet of Things (IoT) networks has increased exposure to cyber threats, particularly Distributed Denial of Service (DDoS) attacks that can disrupt services by overwhelming network resources with malicious traffic. Existing detection methods often rely on static rules and signature-based approaches, which are ineffective against evolving and previously unseen attack patterns. Additionally, the heterogeneous nature of IoT devices, limited computational resources, and continuously changing traffic behavior make accurate attack detection more challenging. High false alarm rates, delayed response mechanisms, and the lack of integrated mitigation strategies further weaken network security.

IV. OBJECTIVES

The primary objective of this study is to develop an intelligent framework named FMDADM for detecting and mitigating Distributed Denial of Service (DDoS) attacks in stateful SDN-based IoT networks. The study aims to utilize the DrDoS_DNS dataset obtained from Kaggle for training and evaluating machine learning models. Another objective is to preprocess network traffic data and select the most informative features using SelectKBest with Mutual Information. The framework evaluates multiple algorithms including Decision Tree, Random Forest, Logistic Regression, Support Vector Machine (SVM), and Naive Bayes to identify the most effective classifier. Additionally, the project seeks to provide real-time prediction, monitoring, visualization, and attack management through a Flask-based web application.

V. METHODOLOGY

1)Data Collection: The data collection stage forms the foundation of the proposed FMDADM framework. The DrDoS_DNS dataset obtained from Kaggle is used as the primary source of network traffic records for analysis and model development. The dataset contains both benign traffic and Distributed Denial of Service (DDoS) attack traffic generated under realistic network conditions. Various flow-based attributes such as packet counts, packet lengths, traffic rates, and timing information are included in the dataset.

2) Data Preprocessing: Data preprocessing is performed to improve the quality and consistency of the collected dataset before machine learning analysis. Missing values and invalid entries are identified and removed to avoid errors during training. Infinite values are replaced with valid numerical values to ensure computational stability. The target labels are converted into binary classes representing normal and attack traffic. Furthermore, StandardScaler is applied to normalize feature values, ensuring that all attributes contribute equally to the learning process and improving overall model performance.

3) Feature Extraction: Feature extraction is carried out to identify the most informative traffic characteristics required for DDoS attack detection. The SelectKBest technique combined with Mutual Information is employed to evaluate the relevance of each feature with respect to the target class. From the available traffic attributes, the ten most significant features are selected based on their importance scores. These features include packet statistics, traffic rates, and inter-arrival time measurements. Reducing the feature space helps minimize computational complexity while preserving essential information required for accurate classification.

4) Model Selection:Model selection involves choosing suitable machine learning algorithms capable of effectively identifying DDoS attacks. Multiple classification models are considered to compare their detection capabilities under identical conditions. The selected algorithms include Decision Tree, Random Forest, Logistic Regression, Support Vector Machine (SVM), and Naive Bayes. Each algorithm offers unique advantages in terms of accuracy, speed, interpretability, and robustness.

5) Model Training: During the training phase, the processed dataset is divided into training and testing subsets using an 80:20 ratio. The selected machine learning algorithms are trained using the optimized feature set obtained from feature extraction. Each model learns patterns associated with normal and malicious network behavior from historical traffic records. The training process enables the classifiers to establish decision boundaries for accurate prediction. Trained models are stored and prepared for future classification tasks and real-time deployment within the framework.

6) Model Evaluation: Model evaluation is performed to assess the effectiveness of each classifier in detecting DDoS attacks. Accuracy is used as the primary performance metric to measure the percentage of correctly classified samples. In addition, a confusion matrix is generated to analyze True Positives, True Negatives, False Positives, and False Negatives. Performance comparison charts are created to visualize the results of different algorithms.

7) Integration with Flask: The final stage integrates the trained machine learning model into a Flask-based web application for practical deployment and monitoring. The saved classifier, feature list, and preprocessing components are loaded into the application environment. Users can provide traffic feature values through an interactive interface and obtain instant predictions. The application displays whether the traffic is normal or malicious and provides real-time monitoring support. Dashboard components, prediction logs, and visualization tools enhance usability and enable continuous observation of network security conditions.

VI. SYSTEM ARCHITECTURE

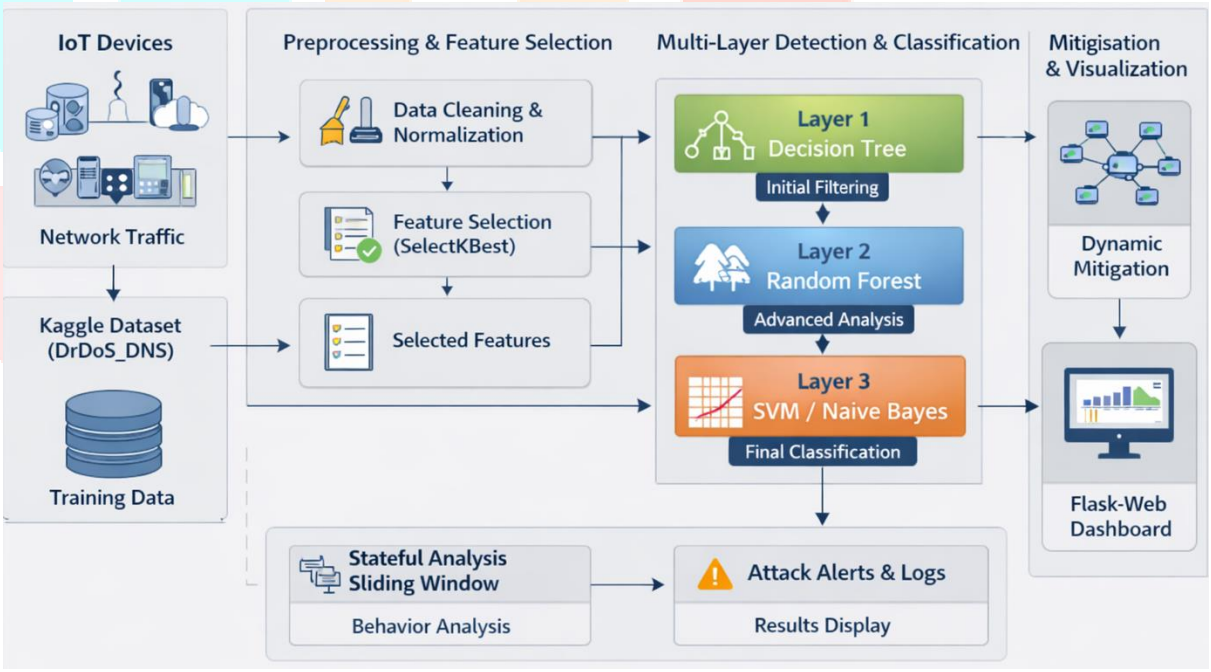

Fig 1: System Architecture of the Proposed FMDADM Framework for Multi-Layer DDoS Attack Detection and Mitigation in Stateful SDN-Based IoT Networks

The proposed FMDADM architecture provides a structured framework for detecting and mitigating Distributed Denial of Service (DDoS) attacks in IoT networks using machine learning techniques. Initially, network traffic generated by IoT devices is collected and represented using flow-based features obtained from the Kaggle DrDoS_DNS dataset. The collected data undergoes preprocessing, where cleaning and normalization operations remove inconsistencies and prepare the dataset for analysis. Feature selection is then performed using SelectKBest to identify the most relevant traffic attributes and reduce computational complexity. The selected features are processed through a multi-layer detection mechanism. In the first layer, a Decision Tree classifier performs rapid filtering of incoming traffic and identifies suspicious flows. The second layer utilizes a Random Forest classifier to conduct advanced traffic analysis and validation. The third layer employs Support Vector Machine and Naive Bayes classifiers for final traffic classification. A stateful analysis module using a sliding window continuously monitors traffic behavior and supports attack

identification. Based on classification results, dynamic mitigation actions are simulated, while a Flask-based dashboard provides real-time visualization, alerts, logs, and monitoring capabilities.

VII. Experimental Setup

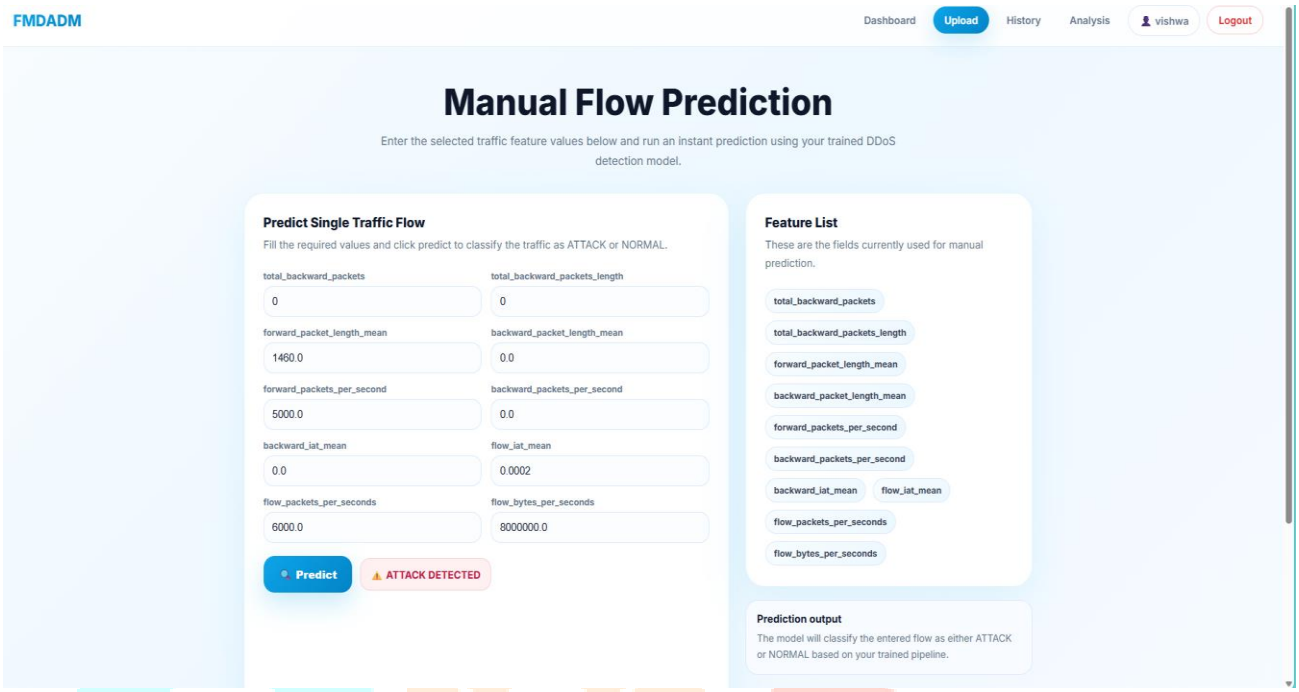

Fig. 2: Manual Flow Prediction Interface of the Proposed FMDADM Framework

The manual flow prediction interface enables users to enter selected network traffic feature values and perform real-time DDoS attack classification using the trained machine learning model. The system analyzes the provided traffic parameters and instantly predicts whether the traffic is normal or malicious, displaying the results through an interactive and user-friendly dashboard.

VIII. Conclusion and Future Works

In this research, FMDADM was developed as a multi-layer machine learning framework for detecting and mitigating Distributed Denial of Service attacks in stateful SDN-based IoT networks. The framework utilized the DrDoS_DNS dataset, feature selection techniques, multiple classifiers, and a Flask-based monitoring platform to improve attack identification and response capability. Experimental evaluation demonstrated effective traffic classification, reduced false alarms, and enhanced network security. Future work will focus on integrating deep learning models, larger and more diverse datasets, real SDN controllers, adaptive mitigation strategies, encrypted traffic analysis, and cloud deployment to further improve scalability, robustness, and practical applicability for future real-world implementations.

References

[1] Z. Mahdi, N. Abdalhussien, N. Mahmood, and R. Zaki, “Detection of Real-Time Distributed Denial-of-Service (DDoS) Attacks on IoT Networks Using Machine Learning Algorithms,” 2024.
[2] A. Seifousadati, S. Ghasemshirazi, and M. Fathian, “A Machine Learning Approach for DDoS Detection on IoT Devices,” 2021.
[3] M. Alduailij, A. Alshammari, and F. Alharbi, “Machine Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance,” 2022.
[4] A. Pakmehr, A. Alhaidari, and M. Al-Rakhami, “DDoS Attack Detection Techniques in IoT Networks: A Survey,” 2024.
[5] H. Setia, N. Kumar, and S. Kumar, “Machine Learning-Driven DDoS Attack Detection in VANET Cloud Infrastructure,” 2024.
[6] M. E. Manaa, S. Alasadi, and H. Al-Khamees, “DDoS Attacks Detection Based on Machine Learning and Deep Learning Techniques,” 2024.

[7] M. Gelgi, Y. Guan, S. Arunachala, and N. Dragoni, “Systematic Literature Review of IoT Botnet DDoS Attacks and Detection Systems,” 2024.
[8] B. Bala, V. Sharma, and R. Kumar, “Artificial Intelligence Techniques for IoT-Based DDoS Attack Detection: A Review,” 2024.
[9] S. Sharma, P. Verma, and A. Gupta, “Machine Learning Enabled Novel Real-Time IoT Targeted DoS/DDoS Cyber Attack Detection System,” 2024.
[10] S. Shakya and R. Abbas, “A Comparative Analysis of Machine Learning Models for DDoS Detection in IoT Networks,” 2024.
[11] A. V. Kachavimath, P. Patil, and S. Totad, “An Efficient DDoS Attack Detection in Software Defined Networks Using Multi-Feature Selection and Ensemble Learning,” 2025.
[12] S. Chen, Y. Wang, and X. Zhang, “Enhancing Machine Learning-Based DDoS Detection Through Adaptive Hyperparameter Optimization,” 2025.