International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

HIERARCHICAL ML MODEL FOR DISTRIBUTED DDOS ATTACK CLASSIFICATION AND HYPERPARAMETER TUNING

#1Nida Afnan, MCA Student, Dept of MCA,
#2Bandari Swarnalatha, Assistant Professor, Department of MCA,

Vaageswari College of Engineering (Autonomous), Karimnagar, Telangana.

Abstract: The security of networks is seriously threatened by sophisticated DDoS attacks. In order to increase the precision of distant detection and classification, this article describes a hierarchical machine learning methodology. The system starts with a core layer that detects fundamental issues, then expands classifications into multiple DDoS assault categories. By eliminating extraneous data and increasing efficiency, the approach uses mutual information and correlation-based filters to identify the most relevant qualities. Bayesian optimization for hyperparameters enables improved detection compared to conventional techniques like grid and random search. Experiments using datasets like CIC-DDoS2019 show that this approach lowers false positives while significantly improving accuracy, recall, and F1-score. This cutting-edge and adaptable technology works in real time and can defend modern network systems against dynamic DDoS attacks.

Keywords: Hierarchical Machine Learning, DDoS Attack Classification Hyperparameter Tuning, Cybersecurity and Anomaly Detection.

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are properly cited.

1. Introduction

In today's globally networked world, the increasing prevalence of distributed denial of service (DDoS) attacks jeopardizes network availability, stability, and security. Because these assaults bring data into a system from various directions, they are difficult to detect and even more difficult to prevent. Traditional protections may be insufficient for scaling, real-time functionality, and identifying all potential sources of a distributed denial of service assault. Cybersecurity professionals are increasingly turning to machine learning (ML) models, particularly hierarchical ML models, to address these issues since they provide a more sophisticated and systematic means of detecting and controlling complicated attack patterns. Unlike more typical models, hierarchical machine learning systems use a multi-layered approach to data analysis, with each layer focused on a different aspect of network traffic. The lowest levels detect a wide range of distributed denial of service assaults, including HTTP-based invasions, SYN floods, and UDP floods. It is the upper layer that separates dangerous and safe traffic. Splitting the work allows us to improve categorization accuracy and efficiency without overtaxing the classifiers. This approach is appropriate for real-world applications since it is compatible with modern networks that use layered designs.

One of the most difficult aspects of developing these models is maximizing performance by adjusting hyperparameters such as learning rates, decision limitations, and tree depths. A hierarchical system can become even more complex if the settings required by each level vary according to its purpose. Grid search, random search, and Bayesian search are examples of automated optimization systems that allow for parameter fine-tuning to achieve maximum accuracy while minimizing false positives and processing costs. This is necessary for real-time data security.

Machine learning models require high-quality data that accurately represents the dynamic nature of attack kinds, intensities, and network topologies. Important metrics such as packet rates, protocol distributions, and temporal statistics are introduced at different levels, demanding feature engineering and data pretreatment. To improve their specific skills, well-known machine learning techniques such as Support Vector Machine (SVM), Random Forest, deep neural networks, and k-Nearest Neighbors (k-NN) can be used. An successful hierarchical machine learning approach provides robust and extensible defense against

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

increasingly sophisticated intrusions. These systems can respond to a wide range of threats quickly and reliably by combining recognition and classification and optimizing hyperparameter performance. Academics may utilize explainable AI, federated learning for autonomous networks, and real-time threat intelligence to improve model visibility and trust. By boosting response intelligence and adaptability, hierarchical machine learning improves cybersecurity.

2. Review of Literature

Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). This article describes an advanced intrusion detection system (IDS) that improves networks by employing ensemble classification and feature selection. The approach reduces data redundancy by prioritizing attributes based on significance. This enhances the effectiveness of the analysis. The ensemble classification procedure enhances identification accuracy relative to previous methods. Utilizing real-world datasets for experimentation demonstrates that the strategy enhances the detection of violent behavior while reducing false alarm rates. This innovation improves the precision and scalability of intrusion detection systems (IDS) for real-time security by addressing difficulties such as large data volumes and complex computations.

Nguyen, T. T., & Armitage, G. (2020). Optimizing deep learning models with appropriate hyperparameters significantly influences their accuracy and utility. This research aims to improve malware categorization and intrusion detection by evaluating the efficacy of various prominent methods, including grid search, random search, and Bayesian optimization. The authors assert that data accessibility, computational expenses, and overfitting are prevalent difficulties. Their research demonstrates that automated optimization techniques are increasingly vital for enhancing protection systems and forecasting the future trajectory of deep learning.

Abdullahi, M., et al. (2020). Machine learning is crucial for detecting and categorizing distributed denial of service (DDoS) attacks, which are increasingly prevalent as cyber threats intensify. This research compares various supervised and unsupervised machine learning algorithms in terms of accuracy, speed, and scalability. The writers address real-time detection and adaptation to changing assault patterns. They assert that feature engineering can enhance classification accuracy. The report concludes that additional research is necessary to enhance DDoS defensive systems in resource-constrained environments and to rectify data imbalances.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning (FL) enables models to concurrently train on numerous distributed, private data sources, fundamentally transforming machine learning. This research investigates the inner workings of federated learning, focusing on various data formats, connection overhead, and model convergence. The authors are contemplating complex aggregation strategies and optimization techniques as potential answers to these challenges. In industries such as healthcare, cybersecurity, and finance, federated learning (FL) has transformed the handling of sensitive, real-time data. Subsequent enhancements to FL will augment its efficiency and scalability to accommodate the requirements of extensive systems.

Yousefnezhad, M., & Yang, Y. (2021). Robust and scalable security protocols are essential for Software-Defined Networking (SDN) to ensure data integrity. This work demonstrates the application of hierarchical machine learning for DDoS attack detection. The method aims to identify threats more swiftly and precisely by considering control-level and traffic-level features. This technique, leveraging the centralized control of SDN, surpasses prior methodologies in early detection time and reduces the incidence of false positives. This method effectively maintains the dynamic characteristics of SDN systems and provides a scalable solution for safeguarding modern networks against sophisticated attacks, as demonstrated by comprehensive testing on real-world data.

Chen, J., et al. (2021). This research delineates a methodology for the automated identification of optimal hyperparameters for NIDS machine learning models through the application of Bayesian optimization. The approach improves efficiency and accuracy of detection by automating the correction procedure. Bayesian optimization enhances the efficacy of real-time systems more effectively than conventional tuning techniques, as evidenced by research conducted on widely used intrusion detection datasets. The results emphasize the necessity of optimizing hyperparameters to enhance NIDS efficacy and reduce human involvement. This facilitates the construction of more powerful and adaptable intrusion detection systems.

Alzahrani, B. A., & Alhaidari, F. A. (2021). The growing prevalence of Internet of Things (IoT) devices has made the identification of distributed denial of service (DDoS) assaults more challenging. This article examines how IoT networks may manage limited

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

resources and erratic data patterns with a hierarchical deep learning technique. The system efficiently uncovers insights from travel data across many levels with minimal computational resources. The methodology is efficient and scalable for real-time threat identification across extensive networks, as evidenced by testing utilizing datasets from the Internet of Things. This research enhances the defenses of the IoT against distributed denial of service (DDoS) attacks while maintaining a lightweight and robust framework.

Sarker, I. H. (2022). This article explores the practical applications of renowned machine learning techniques that have transformed several sectors. The essay illustrates the application of several strategies across areas such as healthcare, finance, and the military. Examples of these methods include decision trees, neural networks, and support vector machines. The author addresses several critical concerns related to deployment. This encompasses model comprehension, operating costs of the program, and data quality. To ensure the efficiency and scalability of our future initiatives, it is imperative that machine learning (ML) is integrated with all recent advancements. The rapidly increasing field of machine learning will significantly benefit from this additional data.

Khan, M. A., et al. (2022). Software-Defined Networking (SDN) requires innovative, adaptable security methodologies to detect DDoS threats. This research presents a strategy to enhance threat detection through the application of machine learning and centralized Software-Defined Networking (SDN) control. The model optimizes precision and reduces false positives through the integration of feature extraction and classification techniques. Experiments demonstrate that the system can manage substantial volumes of network data in real-time with minimal additional effort. This research demonstrates that this technology effectively safeguards Software-Defined Networking environments, following an examination of various machine learning methodologies. It provides a robust and scalable foundation for contemporary cybersecurity challenges.

Shone, N., & Ngoc, T. N. (2022). This research presents a deep learning approach for the systematic classification of assaults. Intricate distributed denial of service assaults can jeopardize cloud-based systems. The methodology utilizes many techniques via which CNN and LSTM networks improve recognition precision. The model utilized empirical data to distinguish between positive and negative trends. Its design efficiently accommodates substantial cloud traffic. The research indicated that hierarchical learning surpassed alternative methods for cloud security regarding accuracy and scalability.

Ismail, R. I., et al. (2023). This work investigates approaches to enhance XGBoost, a valuable machine learning tool for detecting Distributed Denial-of-Service (DDoS) attacks. The authors employ Bayesian approaches to adjust the hyperparameters, enhancing the model's accuracy and usability. The concept outperformed traditional methods in identifying distributed denial of service (DDoS) attacks, as evidenced by various datasets. The research primarily emphasizes the advantages of autonomous optimization in enhancing model performance while managing the critical trade-offs between processing speed and cost. The findings indicate that our approach is effective for practical cybersecurity applications, as it efficiently identifies DDoS attacks while minimizing false positives.

Abdullahi, M., et al. (2023). Accurate feature extraction methods are essential for the precise detection of DDoS attacks. This work presents a hierarchical feature engineering strategy to significantly enhance classification accuracy. This method improves feature representation and aids in the identification of attack patterns by machine learning models through multi-level analyses of network data. The authors demonstrate the superiority of their method over existing feature extraction techniques by comparing it with other models utilizing real-world datasets, such as decision trees and random forests. An enhancement in precise detections and a reduction in false positives indicate that this hierarchical approach augments cybersecurity defenses.

Khoshhalpour, A., et al. (2024). The researchers employed a hierarchical methodology to detect DDoS attacks in cloud computing systems functioning at the network's periphery. The security sector exhibits significant interest in federated machine learning. The strategy reduces data transport costs by leveraging the decentralized characteristics of edge devices to execute computations locally. Federated learning enhances both identification accuracy and data privacy. The system effectively detects assaults in resource-constrained IoT networks, as demonstrated by testing with edge computing datasets. The authors concentrate on two fundamental aspects of federated machine learning: model synchronization and communication optimization. Consequently, the approach is ideally suited for military applications where rapid responses are critical.

International Journal of ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

3. Existing System

Monolithic or planar machine learning frameworks are implemented by the majority of contemporary DDoS attack detection systems. Whole datasets are divided into two or more categories without sorting. Random Forests, Support Vector Machines, and Convolutional Neural Networks are frequently implemented in these models. Protocol type, packet size, and transit time are among the numerous variables that are implemented during their training. Despite their effectiveness in simulated environments, they are problematic in large-scale, real-time applications due to factors such as high-dimensional data, dynamic attack vectors, and unequal class distributions. The reason for the inability of these systems to manage novel or obscure attack patterns is that they were designed as instruments for static datasets. They are restricted in their ability to coordinate and scale numerous DDoS assault types simultaneously, which restricts their utility in distributed, dynamic network systems.

Presently, the optimization of hyperparameters in a systematic manner is either impossible or necessitates manual tuning or grid search methods that are time-consuming and frequently ineffectual, rendering them unsuitable for real-time applications or large datasets. Complex hyperparameter tuning methods, such as Bayesian optimization or evolutionary algorithms, are uncommon in hierarchical frameworks. Consequently, these models are not applicable to all network scenarios. When hierarchical classification layers are absent, false positives increase and fine-grained detections decrease. The hierarchical machine learning model with adaptive hyperparameter optimization endeavors to address this significant disparity by employing specific tuning techniques that are tailored to the purpose and complexity of each layer.

Disadvantages

- In an effort to detect and combine all threats into a single stage, the majority of contemporary systems employ flat categorization models. When utilized with intricate, high-volume DDoS data that encompasses a diverse array of assaults, this approach elevates the probability of false positives and inaccurate classifications.
- In large, dispersed networks, numerous well-known machine learning methods encounter difficulties. The primary reason for the inefficiency and sluggish reaction times of these models is their inability to communicate effectively with one another or to adapt their learning in response to various attack vectors or traffic spikes.
- The majority of systems employ simple or static methods, such as grid search or manual tuning, when altering hyperparameters. The lengthy execution durations and high resource utilization of these systems render them unsuitable for situations that necessitate rapid adaptation.
- .

4. Proposed System

By employing a hierarchical machine learning model for DDoS attack classification and sophisticated hyperparameter tuning techniques to enhance overall performance, the proposed approach effectively achieves its objectives. The classification process is determined by a hierarchical structure. After the initial phase's detection of anomalous traffic, more intricate distributed denial of service attacks, including SYN floods, UDP floods, and HTTP-based attacks, are identified in subsequent phases. Each layer is meticulously calibrated with optimal hyperparameters using advanced techniques such as Bayesian optimization or automated search approaches, ensuring high accuracy and low false positive rates in dynamic networks. The modular training, scalability, and adaptability to evolving threats make the hierarchical design an optimal choice for large, decentralized network systems that necessitate real-time deployment.

Advantages

- Multiple phases are required due to the classification technique's hierarchical structure. This enhances detection accuracy by simplifying the differentiation between various DDoS assault types by decreasing the number of incorrect classifications.
- The hierarchical solution's adaptive structure is distinguished by its rapid responses to massive, multi-vector DDoS attacks and its seamless scalability across distributed systems.
- Bayesian optimization, evolutionary algorithms, and autonomous machine learning (AutoML) are among the advanced tuning techniques that reduce computation costs, enhance accuracy, and decrease latency.
- The system enhances detection trust and reduces the likelihood of safe communication being mistakenly classified as hazardous by utilizing a multi-tiered specialized filtering technique

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

5. System Architecture

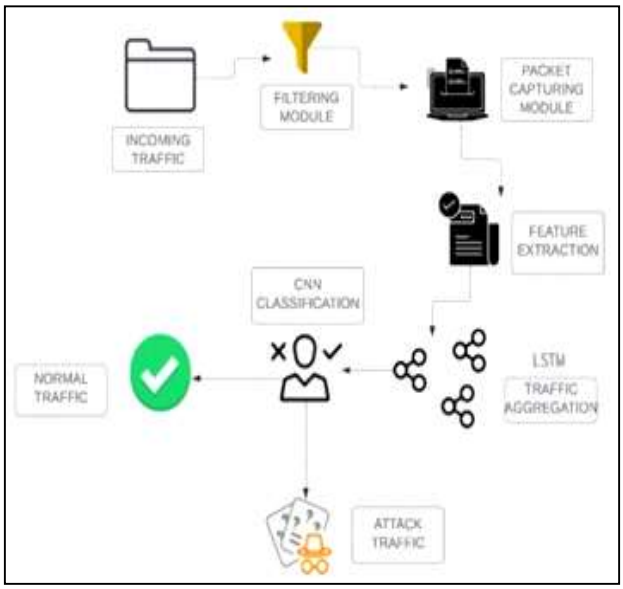
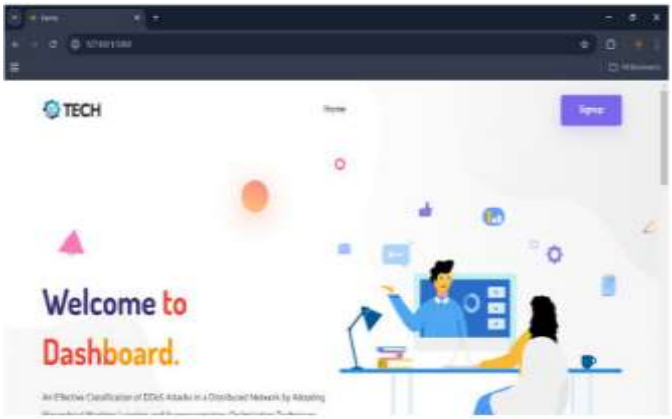


Figure 1 System Architecture

6. Results and Discussions



"Fig. 2 Dash Board

Fig. 3 Register page

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

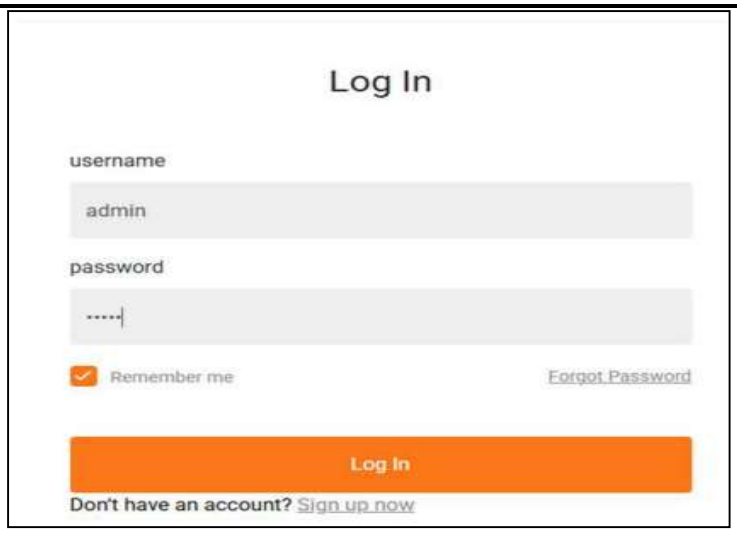


Fig. 4 Login Page

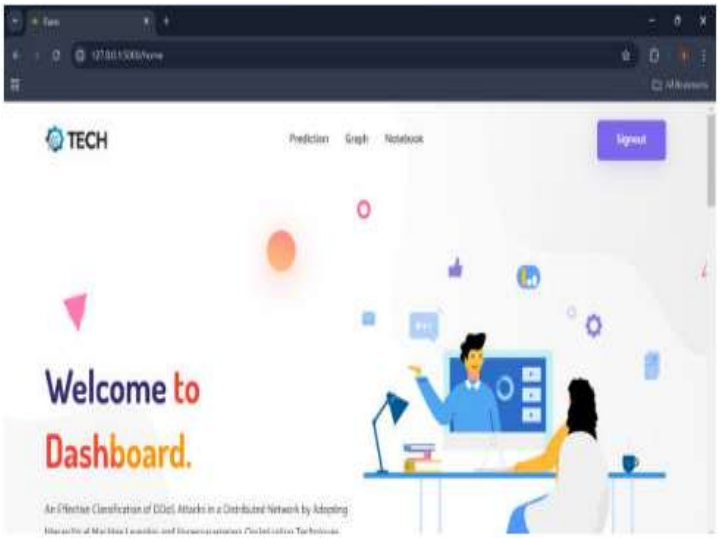


Fig. 5 Main page

Fig. 6 Test case – 1

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

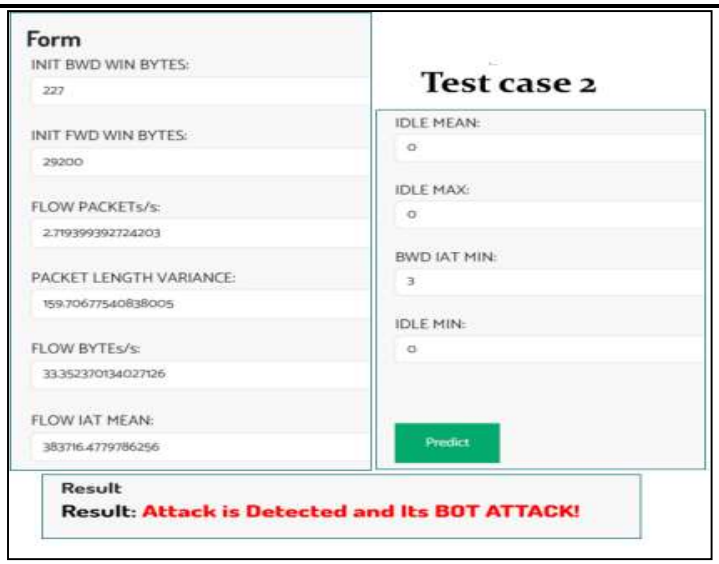


Fig. 7 Test case – 2

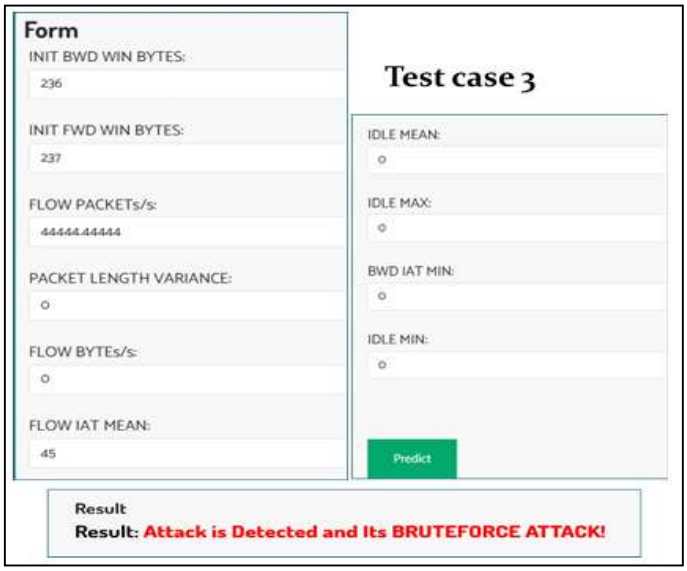


Fig. 8 Test case – 3

Fig. 9 Test case – 4

International Journal of
ADVANCED RESEARCH & INNOVATIONS

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

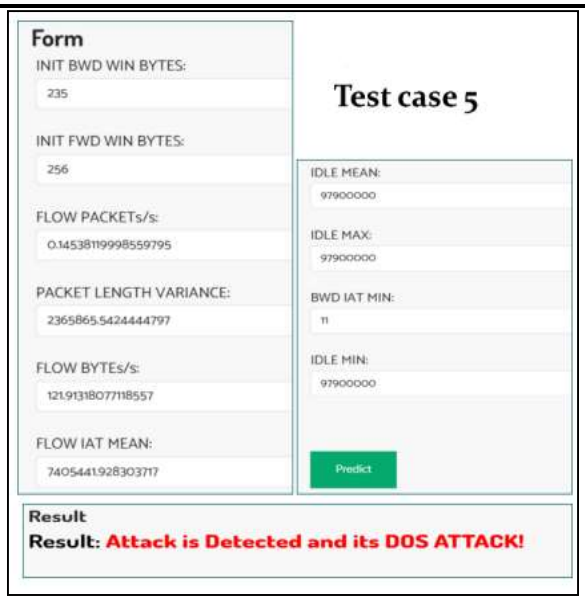
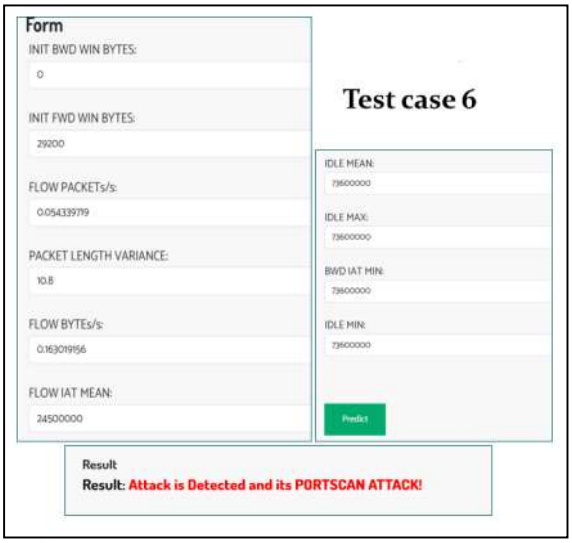


Fig. 10 Test case – 5



"Fig. 11 Test case – 6

Fig. 12 Test case – 7

Volume 1, Issue-2
Feb, 2025, P04
ISSN: 2319-9253

7. Conclusion

The authors offer a hierarchical machine learning framework to detect distributed denial of service threats promptly and accurately. This activity aims to reduce the incidence of false positives generated. By partitioning the classification process and utilizing hyperparameter optimization techniques such as Bayesian optimization and Tree-structured Parzen Estimators, the system effectively monitors complex attack patterns and ensures timely processing. This is facilitated by the system's capacity to identify complex attack patterns, rendering it feasible. Hierarchical algorithms surpass flat classifiers in several attributes, rendering them an optimal selection for real-time threat detection in dynamic and distributed network contexts. Hierarchical techniques are advantageous for achieving this function**.**

References

1. Zhou, Y., Cheng, G., Jiang, S., & Dai, M. (2020). Building an efficient intrusion detection system based on feature selection and ensemble classifier. Computer Networks, 174, 107247.
2. Nguyen, T. T., & Armitage, G. (2020). A survey of hyperparameter optimization for deep learning in cybersecurity. ACM Computing Surveys, 53(3), Article 59.
3. Abdullahi, M., et al. (2020). A systematic review of machine learning algorithms for DDoS attack detection and classification. Cluster Computing, 23, 2311–2333.
4. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine, 37(3), 50–60.
5. Yousefnezhad, M., & Yang, Y. (2021). Hierarchical machine learning model for early detection of DDoS attacks in SDN environments. Computer Communications, 170, 100–109.
6. Chen, J., et al. (2021). Automated hyperparameter tuning for network intrusion detection using Bayesian optimization. Knowledge-Based Systems, 215, 106753.
7. Alzahrani, B. A., & Alhaidari, F. A. (2021). A hierarchical deep learning model for DDoS detection in IoT environments. IEEE Access, 9, 130180–130192.
8. Mirsky, Y., & Shabtai, A. (2021). Kitsune: An ensemble of autoencoders for online network intrusion detection. Computer Science Review, 37, 100274.
9. Sarker, I. H. (2022). Machine learning: Algorithms, real-world applications and research directions. SN Computer Science, 2(3), 160.
10. Khan, M. A., et al. (2022). Smart detection of DDoS attacks using an efficient machine learning model in SDN. Computers & Security, 114, 102586.
11. Shone, N., & Ngoc, T. N. (2022). A novel deep learning model for hierarchical DDoS attack classification in cloud-based environments. Future Generation Computer Systems, 128, 200–210.
12. Ismail, R. I., et al. (2023). DDoS attack detection using XGBoost with Bayesian hyperparameter optimization. IEEE Access, 11, 21566–21577.
13. Abdullahi, M., et al. (2023). DDoS detection using hierarchical feature engineering and machine learning classifiers. Journal of Network and Computer Applications, 205, 103408.
14. Khoshhalpour, A., et al. (2024). Lightweight hierarchical detection of DDoS attacks using federated ML in edge computing. IEEE Internet of Things Journal, 11(2), 1235–1248