Journals Pub

International Journal of
Broadband Cellular Communication

ISSN: 2455-8532
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJBCC

https://journalspub.com/journal/IJBCC/

Research IJBCC

Bot Defender: A Collaborative Defense Framework for Botnet Intrusion Mitigation

Vrushali Didshere[1,*], Preeti Suryawanshi[2], Samradnyi Gaikwad[3]

Abstract

Botnet attacks represent a significant threat to cybersecurity, compromising vast numbers of devices and causing extensive harm. BOT DEFENDER is a novel collaborative defense framework designed to mitigate botnet intrusions effectively. This framework leverages the power of collective intelligence, integrating data from multiple sources to detect and respond to botnet threats in real-time. By utilizing advanced machine learning algorithms, BOT DEFENDER can identify anomalous network behavior indicative of botnet activities, allowing for swift intervention. The framework's collaborative nature ensures a comprehensive defense strategy, enhancing the resilience of individual systems through shared threat intelligence. Experimental results demonstrate that BOT DEFENDER significantly reduces the impact of botnet intrusions, showcasing their potential as a robust solution for modern cybersecurity challenges. Bot Defender, a collaborative framework that protects against botnet attacks. Bot Defender combines a proposed network traffic analyzer and machine learning technique to prevent botnet attacks. The proposed network traffic analyzer performs an in-depth traffic analysis to detect bots and filter out all the traffic from the identified bots. It significantly reduces network traffic by filtering out a huge amount of traffic from the bots and transfers significantly reduced amounts of traffic to the machine learning model for further analysis. Machine learning models, such as DT and XGBOOST, are powered by a novel feature selection technique, an extended dataset construction technique inspired by human learning patterns and a stacking ensemble-based machine learning model to detect bots. This proposed work exhibits a consistent performance of the proposed machine learning model. Finally, to evaluate the performance of Bot Defender, we design and develop a live botnet attack strategy.

Keywords: Collaborative framework, network traffic analyzer, machine learning, Bot detection, live botnet attack strategy

INTRODUCTION

As the Internet of Things (IoT) continues its rapid expansion, too does the landscape it inhabits, with botnets emerging as a significant risk. These automated networks of compromised devices pose a serious challenge to the security and stability of online platforms and services. To combat this threat, machine learning (ML) and deep learning (DL) techniques have been proposed as effective tools for identifying and categorizing botnet attacks within the IoT ecosystem [1–4].

Leveraging datasets, like UNSW-NB15 and employing preprocessing methodologies, such as SMOTE-Over Sampling to address class imbalances, ML-based solutions offer promising avenues for defense. Enter Bot Defender, a cybersecurity solution engineered to safeguard digital infrastructures from the perils of malicious

***Author for Correspondence**
Vrushali didshere
E-mail: vrushalididshere.skn.entc@gmail.com

[1]Associate Professor, Department of E&TC, SKNCOE, SPPU, Pune, Maharashtra, India
[2]Assistant Professor, Department of E&TC, SKNCOE, SPPU, Pune, Maharashtra, India.
[3]Student, Department of E&TC, SKNCOE, SPPU, Pune, Maharashtra, India

Received Date: March 10, 2025
Accepted Date: September 09, 2025
Published Date: December 30, 2025

Citation: Vrushali Didshere, Preeti Suryawanshi, Samradnyi Gaikwad. Bot Defender: A Collaborative Defense Framework for Botnet Intrusion Mitigation. International Journal of Broadband Cellular Communication. 2025; 11(2): 6–11p.

bot activity.

By employing advanced algorithms and real-time behavioral analysis, Bot Defender can discern between benign and malicious bot behavior, staying one step ahead of evolving threats. Its multi-layered approach integrates signature-based detection, behavioral analysis, and anomaly detection, enabling it to effectively thwart malicious bot activity while minimizing disruptions to legitimate user interactions. Moreover, Bot Defender's seamless integration with other security tools provides a comprehensive defense strategy against a wide array of cyber threats, ensuring the resilience of online platforms and applications in an increasingly hostile digital landscape [5–8].

LITERATURE REVIEW

Botnet defense strategies reveal a spectrum of approaches aimed at mitigating the pervasive threat posed by these networks of compromised devices. One recent framework, Bot Defender, offers a collaborative defense model leveraging network traffic analysis and machine learning. This innovative approach addresses the pressing need to safeguard infrastructures and organizations from the damaging effects of botnet attacks. However, existing research highlights certain gaps in the field [9].

Some surveys of botnet defense strategies emphasize collaborative approaches for early detection. While informative, these works may not delve deeply into specific frameworks like Bot Defender. Other studies have explored federated deep learning for detecting zero-day botnet attacks in IoT-edge devices, presenting collaborative approaches to enhance detection efficiency. However, their focus on IoT devices may limit the scope of broader collaborative defense frameworks [10].

Graph-based bot detection systems employing machine learning techniques have also been introduced. While collaborative aspects are implied, such systems do not explicitly address frameworks like Bot Defender. Similarly, deep learning-based detection systems may offer insights into collaborative defense mechanisms but do not explicitly focus on them [11].

Efficient IoT botnet detection systems using machine learning have been proposed as well. While some collaborative aspects may be present in their design, they are not the primary focus. Reinforcement learning-based botnet detection approaches could potentially be extended to collaborative defense strategies, but their emphasis on reinforcement learning may overshadow collaborative aspects [12, 13].

Novel approaches combining cooperative game theory with machine and deep learning for IoT botnet detection also suggest collaborative methods. While such integration demonstrates potential, these works may not explicitly address frameworks like Bot Defender. Overall, while existing literature offers valuable insights into botnet defense strategies, there remains a need for more research explicitly focusing on collaborative defense frameworks like Bot Defender [14].

SOFTWARE REQUIREMENT SPECIFICATIONS

External Interface Requirement

User Interface Application Based Malware Detection.

Hardware Interfaces

- *RAM: 8 GB:* As we are using Machine Learning Algorithm and Various High Level Libraries Laptop RAM minimum required is 8 GB.
- *Hard Disk:* 40 GB.
- *Processor: Intel i5 Processor IDE:* Spyder Best Integrated Development Environment as it gives possible suggestions at the time of typing code snippets that makes typing feasible and fast.
- *Coding Language: Python Version 3.5:* Highly specified Programming Language for Machine Learning because of availability of High-Performance Libraries.
- *Operating System: Windows 10:* Latest Operating System that supports all types of installation and development Environment.

Software Interfaces Operating System

- *Windows 10 IDE: Spyder Programming Language:* Python.

Non-Functional Requirement

Performance Requirements

The performance of the functions and every module must be well. The overall performance of the software will enable the users to work evidently. Performance of encryption of data should be fast. Performance of the provided virtual environment should be fast Safety Requirement. The application is designed in modules where errors can be detected and easily. This makes it easier to install and update new functionality if required.

Safety Requirement

The application is designed in modules where errors can be detected and fixed easily. This makes it easier to install and update new functionality if required.

- *Software Quality Attributes:* Our software has many qualities attribute that are given below:
  - *Adaptability:* This software is adaptable by all users.
  - *Availability:* This software is freely available to all users. The availability of the software is easy for everyone.
  - *Maintainability:* After the deployment of the project if any error occurs then it can be easily maintained by the software developer.
  - *Reliability:* The performance of the software is better which will increase the reliability of the Software.
  - *User Friendliness:* Since the software is a GUI application, the output generated is much user friendly in its behavior.
  - *Integrity:* Integrity refers to the extent to which access to software or data by unauthorized people can be controlled.
  - *Security:* Users are authenticated using many security phases, so reliable security is provided.
  - *Testability:* The software will be tested considering all the aspects.

DESIGN AND DRAWING

The process of building a Bot Defender, a robust framework designed to combat botnet attacks, involves several key stages aimed at ensuring its effectiveness and reliability.

In the initial stages, the focus lies on data preparation and understanding. This includes sourcing and utilizing datasets, like UNSW-NB15, employing techniques like SMOTE-Over Sampling, addressing class imbalances, and conducting exploratory data analysis to gain insights into the dataset's characteristics.

Subsequently, preprocessing steps, such as feature extraction, are employed to identify relevant data points distinguishing between bot and legitimate user activities. This phase involves leveraging supervised learning techniques to train models on the prepared datasets, ensuring that the Bot Defender can accurately categorize binary classes.

Further, attention is given to dataset balance to ensure accurate predictions for both bot and legitimate user activities. The dataset is then split into training and testing sets, enabling the model to be trained on one subset and evaluated on another to assess its generalization capabilities.

The model building process involves creating a system that integrates rule-based approaches, machine learning algorithms, and behavioral analysis to effectively identify and mitigate malicious bot activity. The model's performance is evaluated using selected metrics, such as accuracy, F1-score, recall, and precision, with insights gained through interpretation and analysis (Figure 1).

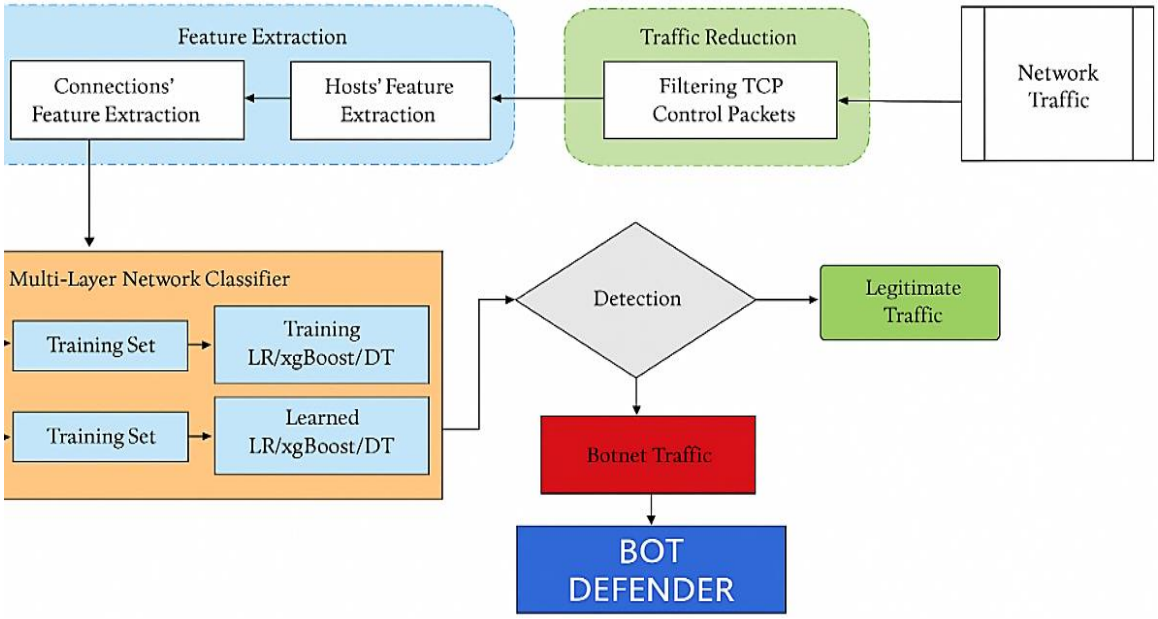

Figure 1. Bot Defender architecture for detecting botnet traffic.

Finally, the model's performance is validated and its generalization capabilities assessed, with findings documented comprehensively for reporting purposes. This systematic approach ensures the Bot Defender's ability to effectively protect against botnet attacks while adapting to evolving threats.

METHODOLOGY

Decision Tree Algorithm

- Implementing a decision tree algorithm as a classification method for distinguishing between legitimate and malicious bot activities.
- Leveraging the interpretability and versatility of decision trees in handling both categorical and continuous features.
- Emphasizing the need for complementary security measures alongside decision tree implementation due to the evolving threat landscape.
- Integrating decision trees with other machine learning techniques, rule-based systems, and behavioral analysis to enhance bot defense.
- Highlighting the importance of regular updates and improvements based on monitoring and feedback to maintain system robustness.

XGBoost Algorithm

- Utilizing XGBoost for its ability to handle complex patterns and adapt to changing bot behaviors in bot detection.
- Integrating XGBoost into a comprehensive bot defender system to enhance security and resilience.
- Leveraging XGBoost's high predictive accuracy and suitability for binary classification tasks common in bot detection.
- Outlining the process of gathering labeled historical web traffic data and dividing it into training and test sets for model evaluation.

Logistic Regression

- Employing logistic regression as a method for bot detection, focusing on evaluation metrics such as accuracy, precision, recall, and F1-score.
- Describing the deployment of the trained logistic regression model in real-time classification of user sessions within a bot defense system.

- Emphasizing the importance of continuous monitoring and model updates to adapt to evolving bot behaviors.
- Acknowledging logistic regression is one of many methods applicable to bot defense, with potential integration of other techniques like decision trees and neural networks.

EXPERIMENTATION PHASE

- Detailing the practical implementation of the designed botnet attack strategy in a controlled environment.
- Describing the setup of the experimental infrastructure, including a heterogeneous network of devices and various operating systems.
- Outlining the execution of the botnet attack and the generation of benign traffic by legitimate devices within the testbed.
- Explaining the monitoring and analysis of network traffic using dedicated tools to capture packets and detect anomalies.
- Highlighting the measurement of the impact of the botnet attack on network performance and the evaluation of defense mechanisms.
- Discussing the collection of empirical data throughout the experimentation phase and the evaluation of defense mechanisms based on performance metrics.
- Summarizing the interpretation of experimental results and deriving recommendations for enhancing network security and mitigating botnet threats.

APPLICATION

- *Website Security:* Protecting websites from automated threats like web scraping, credential stuffing, and account takeover attacks.
- *API Security:* Safeguarding APIs from bot-driven scraping and attacks by enforcing rate limits, analyzing request patterns, and blocking malicious bots.
- *E-commerce:* Preventing price scraping, inventory hoarding, and fraudulent transactions in e-commerce platforms to maintain sales and customer trust.
- *Content Protection:* Defending content from being scraped or plagiarized by bots, particularly crucial for news websites, blogs, and online publishing platforms.
- *Ad Fraud Prevention:* Identifying and blocking bots responsible for generating fake clicks and impressions on online ads, thus preventing ad fraud.
- *Credential Protection:* Detecting and blocking bots attempting to use stolen or guessed credentials to access user accounts, enhancing security and preventing unauthorized access.
- *Compliance and Regulatory Requirements:* Helping organizations comply with data protection and fraud prevention regulations by safeguarding against unauthorized access and data breaches

CONCLUSIONS

BOT DEFENDER is a novel collaborative defense framework designed to mitigate botnet intrusions effectively. This framework leverages the power of collective intelligence, integrating data from multiple sources to detect and respond to botnet threats in real-time. By utilizing advanced machine learning algorithms, BOT DEFENDER can identify anomalous network behavior indicative of botnet activities, allowing for swift intervention. The framework's collaborative nature ensures a comprehensive defense strategy, enhancing the resilience of individual systems through shared threat intelligence. Experimental results demonstrate that BOT DEFENDER significantly reduces the impact of botnet intrusions, showcasing their potential as a robust solution for modern cybersecurity challenges. Bot Defender, a collaborative framework that protects against botnet attacks. Bot Defender combines a proposed network traffic analyzer and machine learning technique to prevent botnet attacks. The proposed network traffic analyzer performs an in-depth traffic analysis to detect bots and filter out all the traffic from the identified bots. It significantly reduces network traffic by filtering out a huge amount of traffic from the bots and transfers significantly reduced amounts of traffic to the machine learning model for further analysis.

Acknowledgments

I take this opportunity to thank all those who have contributed to the successful completion of this Major Project. I would like to express my sincere thanks to my guide Prof. P. K. Suryawanshi who has encouraged us to work and provided valuable guidance wherever required. We express our immense pleasure and thankfulness to mini project coordinators, Mr. P. S. Kokare & Ms. M. M. Sonkhaskar who guided us on every possible stage. We also extend our gratitude to Dr. S. K. Jagtap (HOD of ENTC Department) who has provided facilities to explore this subject with more enthusiasm. We express our immense pleasure and thankfulness to Dr. A. V. Deshpande (Principal S.K.N.C.O.E) who has provided facilities to explore this subject with more enthusiasm. I like to thank all the teaching and non-teaching staff for their immense support and their cooperation.

REFERENCES

1. Newman P. The internet of things 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue. Bus Insider. 2020 [cited 2025 Sep 10]. Available from: https://www.businessinsider.com/.
2. Gillum J, Kao J, Larson J. Millions of Americans' medical images and data are available on the internet. Anyone can take a peek. ProPublica [Internet]. 2019 [cited 2025 Sep 10]. Available from: https://www.propublica.org/.
3. Threat landscape trends – Q1 2020. Symantec Enterprise Blogs. 2020 [cited 2025 Sep 10]. Available from: https://symantec-enterprise-blogs.security.com/.
4. Symantec ISTR. Internet security threat report (ISTR). Symantec Inc. 2019.
5. Osterweil E, Stavrou A, Zhang L. 20 years of DDoS: a call to action. arXiv [Preprint]. 2019 Apr [cited 2025 Sep 10]. Available from: https://arxiv.org/abs/1904.02739.
6. Saxena U, Sodhi J, Singh Y. An analysis of DDoS attacks in a smart home networks. In: 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence). 2020. p. 272–6. doi:10.1109/Confluence47617.2020.9058087.
7. Alzahrani S, Hong L. Generation of DDoS attack dataset for effective IDS development and evaluation. J Inf Secur. 2018;9(4):225–41. doi:10.4236/jis.2018.94016.
8. Anthi E, Williams L, Słowin´ska M, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT devices. IEEE Internet Things J. 2019;6(5):9042–53. doi:10.1109/JIOT.2019.2926365.
9. Khan AY, Latif R, Latif S, Tahir S, Batool G, Saba T. Malicious insider attack detection in IoTs using data analytics. IEEE Access. 2020;8:11743–53. doi:10.1109/ACCESS.201.2959047.
10. Ahmad Z, Khan AS, Shiang CW, Abdullah J, Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Trans Emerg Telecommun Technol. 2020;e4150. doi:10.1002/ett.4150.
11. Sarker IH, Shahriar B, Watters P, Ng A. Cybersecurity data science: An overview from machine learning perspective. J Big Data. 2020;7(1):1–29. doi:10.1186/s40537-020-00318-5.
12. Soe YN, Santosa PI, Hartanto R. DDoS attack detection based on simple ANN with SMOTE for IoT environment. In: 2019 Fourth International Conference on Informatics and Computing (ICIC). 2019. p. 1–5. doi:10.1109/ICIC47613.2019.8985853.
13. Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P. Network intrusion detection for IoT security based on learning techniques. IEEE Commun Surv Tutor. 2019;21(3):2671–701. doi:10.1109/COMST.2019.2896380.
14. García-Teodoro P, Díaz-Verdejo J, Maciá-Fernández G, Vázquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Comput Secur. 2009;28(1):18–28.

