iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67486

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Command and Control Traffic Detection and Mitigation in Botnet Driven Networks

Mrs. K. Harini[1], A. Jyothsna[2], J. Salman Raju[3], G. Navyatha[4], M. Vidya Sagar[5]
[1]*Assistant Professor, Dept of CSE, Raghu Engineering College*
[2, 3, 4, 5]*Dept of CSE, Raghu Institute of Technology*

Abstract: ***In the evolving landscape of cybersecurity, the threat of hackers exploiting system vulnerabilities remains a persistent challenge.***
The cyber kill chain outlines the series of steps attackers follow to infiltrate and compromise systems. A critical phase in this chain involves the establishment of a Command and Control (C2) server, through which malicious actors maintain control over the compromised systems and transfer beacons to exfiltrate information. This project introduces a novel technique aimed at disrupting the cyber kill chain by detecting and mitigating the establishment of C2 paths by using scanning tools. By integrating a proactive detection mechanism, the system identifies attempts to establish C2 communication channels in real-time. Upon detection, a dialogue box is immediately triggered, alerting the user to the suspicious activity. The user is then prompted to provide authentication via biometric verification or password entry, adding an additional layer of security. This approach not only enhances the detection capabilities of the system but also empowers users to take timely action, thereby preventing unauthorized data transfer to attackers.
The project's implementation focuses on developing a code module that seamlessly integrates with existing security frameworks, providing a robust defense against advanced persistent threats (APTs) and significantly reducing the risk of successful cyber intrusions.
Index Terms: Botnet Detection, Command and Control Traffic, Network Security, Traffic Mitigation, Anomaly Detection, Cybersecurity

I. INTRODUCTION

In recent years, botnets have become one of the most prominent threats to network security, enabling cybercriminals to carry out a wide range of malicious activities, including Distributed Denial of Service (DDoS) attacks, data theft, and ransomware distribution. Central to the operation of a botnet is the Command and Control (C&C) infrastructure, which facilitates communication between the botmaster and the compromised machines, or bots, under its control. These C&C channels are crucial for the botnet's command execution, making them a key target for detection and mitigation efforts. The stealthy nature of C&C traffic, coupled with the use of sophisticated techniques such as encryption, traffic obfuscation, and dynamic IP addressing, presents a significant challenge in detecting and disrupting these malicious activities.

The ability to accurately detect and mitigate C&C traffic is essential to safeguarding the integrity of networked systems. Existing methods of C&C detection often face limitations in terms of scalability, accuracy, and the ability to detect traffic from advanced botnets that employ advanced evasion strategies. Traditional signature-based methods are increasingly ineffective in dealing with the evolving tactics used by botmasters. As a result, new approaches that leverage behavioral analysis, machine learning algorithms, and anomaly detection techniques have emerged as promising solutions to identify C&C traffic patterns that deviate from normal network behavior.

This research aims to address these challenges by developing a robust framework for detecting and mitigating C&C traffic in botnet-driven networks. The study explores the use of network traffic analysis, combined with advanced machine learning techniques, to identify subtle and sophisticated indicators of C&C activity. In addition, the research investigates effective mitigation strategies that can reduce the impact of botnet-driven attacks while minimizing disruptions to legitimate network operations. By improving the accuracy and efficiency of detection systems, this research seeks to enhance the overall security of networked environments and contribute to the ongoing efforts to combat botnet-related cyber threats.

II. RELATED WORK

Botnet detection has been a critical area of research, with various approaches proposed over the years. Sharma [1] provides a comprehensive survey on botnet detection and mitigation techniques in large-scale networks, categorizing methods into signature-based, anomaly-based, and machine learning-based approaches.

Patel et al. [2] explore machine learning techniques for botnet traffic detection, comparing classifiers like Decision Trees, Random Forests, and Support Vector Machines (SVMs) to evaluate their effectiveness in distinguishing malicious traffic.

Jain et al. [3] extend this research by implementing deep learning models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), demonstrating their superior performance in detecting encrypted botnet traffic.

Feily et al. [4] classify detection techniques into host-based and network-based approaches, discussing heuristic detection and behavior-based analysis.

Zhu et al. [5] further analyze botnet architectures and C&C strategies, evaluating anomaly detection and honeypot-based methods.

García et al. [6] conduct an empirical comparison of botnet detection methods, assessing the trade-offs between accuracy, computational complexity, and false positive rates.

Meidan et al. [7] introduce N-BaIoT, a network-based IoT botnet detection framework leveraging deep autoencoders to identify compromised devices based on network behavior anomalies.

Li et al. [8] provide a survey on botnet architectures and C&C mechanisms, including centralized and P2P botnets. They analyze detection techniques such as network flow analysis and anomaly-based methods, highlighting their effectiveness in real-world scenarios.

Gu et al. [9] propose BotSniffer, a tool that identifies C&C channels in botnet-infected networks by analyzing traffic patterns, particularly for centralized botnets using HTTP and IRC protocols.

Kugisaki et al. [10] explore statistical traffic analysis techniques for botnet detection, identifying anomalies in packet size, connection intervals, and IP distributions.

Kumar et al. [11] highlight the use of Nepenthes honeypots for botnet detection, demonstrating their effectiveness in capturing and analyzing malware samples.

García et al. [12] provide an extensive review of network-based botnet detection techniques, emphasizing the importance of hybrid approaches that integrate multiple detection methods for improved accuracy.

III. PROBLEM STATEMENT

With the increasing prevalence of botnet attacks, traditional network security methods struggle to detect and prevent evolving cyber threats in real-time. Signature-based and rule-based intrusion detection systems (IDS) fail to recognize zero-day attacks, leading to high false positives, poor scalability, and delayed responses. The need for an AI-driven, real-time detection system that accurately classifies network traffic as normal or botnet-infected is crucial to strengthen cybersecurity defenses and mitigate risks effectively.

IV. EXISTING SYSTEM

The traditional approach to botnet detection relied on rule-based and signature-based IDS like Snort and Suricata, which struggled against evolving threats and zero-day attacks due to the need for constant updates. Anomaly-based methods, using statistical thresholds and heuristic analysis, suffered from high false positive rates. Early machine learning models, such as Logistic Regression and Decision Trees, lacked feature selection, data balancing, and real-time detection. Additionally, the absence of automated response mechanisms and inefficiency in handling large-scale traffic limited their practicality for real-time botnet detection.

V. PROPOSED SYSTEM

The Hybrid Detection and Mitigation Model (HDMM) is proposed to address the challenges of detecting and mitigating Command and Control (C&C) traffic in botnet-driven networks. This AI-powered, real-time framework enhances detection accuracy, scalability, and response efficiency by integrating machine learning, anomaly detection, and traffic analysis. The system preprocesses network traffic by removing irrelevant features, handling missing values, and encoding categorical attributes to improve model learning. Optimized feature selection and data balancing techniques further refine detection performance. A real-time processing module continuously analyzes network traffic, while an interactive alert system provides instant threat notifications, allowing users to take immediate action. By combining adaptive detection with effective mitigation strategies, HDMM significantly improves cybersecurity defenses against evolving botnet threats.

VI. ALGORITHMS

The proposed system uses four machine learning algorithms for botnet detection. Decision Tree (DT) is a simple and interpretable model that classifies network traffic based on feature splits. Random Forest (RF), an ensemble method, improves accuracy by combining multiple decision trees, reducing over fitting. Naive Bayes (NB) is a probabilistic classifier that assumes feature independence, making it efficient for detecting botnet traffic. K-Nearest Neighbors (KNN) is a distance-based algorithm that classifies network traffic by comparing it with the nearest data points, making it useful for anomaly detection. These models work together to enhance detection accuracy, minimize false positives, and improve real-time classification performance.

These algorithms are implemented on various datasets to evaluate their effectiveness. The Bot-IoT dataset is designed for IoT botnet detection and includes labeled traffic from attacks like DDoS and Mirai botnets. The CICIDS 2017 dataset contains diverse network attack traffic, including botnet, DDoS, port scanning, and brute force attacks, along with normal traffic for comparison. The CTU-13 dataset features real-world botnet traffic, including Mirai and Zeus botnets, making it valuable for training and testing detection models that identify command-and-control traffic.

The table below presents the classification performance metrics (accuracy, precision, recall, F1-score, and AUC) of the model on the Bot-IoT, CICIDS 2017, and CTU-13 datasets.

Dataset	Accuracy	Precision	Recall	F1-Score	AUC
Bot-IoT	98.6%	97.8%	99.2%	98.5%	0.985
CICIDS 2017	97.4%	96.2%	98.1%	97.1%	0.978
CTU-13	98.2%	97.5%	98.7%	98.1%	0.986

VII. MODEL WORKFLOW

1) Traffic Collection: Raw network traffic is captured from various sources.
2) Preprocessing: Data is processed and feature extraction occurs to convert raw packet data into meaningful features.
3) Detection: The traffic is analyzed using a hybrid approach combining machine learning-based detection for known patterns and anomaly-based detection for novel threats.
4) Mitigation: Upon detection of botnet traffic, appropriate mitigation techniques (DNS sinkholing, IP blacklisting, traffic filtering) are triggered in real time.
5) Continuous Monitoring: The system continually monitors network traffic, updating detection models and mitigation strategies based on evolving botnet tactics.

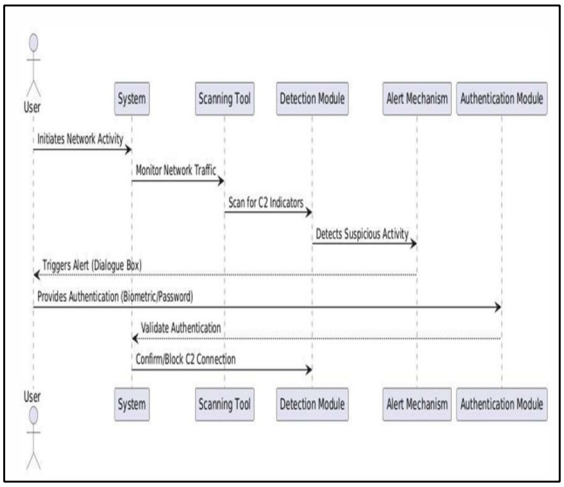


Fig 1 : Sequence Diagram

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

VIII. RESULT

1) Precision

Precision assesses the share of appropriately classified cases among those identified as fine. therefore, the formulation for calculating precision is expressed as:

"Precision = True positives/ (True positives + False positives) = TP/(TP + FP)"

$$\text{Precision} = \frac{True\ Positive}{True\ Positive + False\ Positive}$$

2) Recall

Recall is a metric in machine learning that measures the ability of the model to identify all relevant instances of a particular class. It is the ratio of correctly predicted positive observations to overall real positives and provides information on the completeness of the model when capturing the instances of the class.

$$Recall = \frac{TP}{TP + FN}$$

3) Accuracy

Accuracy is the ratio of accurate predictions in a class take a look at, assessing the overall precision of a model's predictions.

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN}$$

4) F1 Score

F1 - Score is a metric of evaluation of machine learning that measures the accuracy of the model. It combines the score and induction of the model. The accuracy metric calculates how many times the model has created the correct prediction throughout the data file.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$

TP (True Positive): Correctly identified botnet C&C traffic.
TN (True Negative): Correctly identified benign traffic.
FP (False Positive): Benign traffic misclassified as botnet traffic.
FN (False Negative): Botnet traffic misclassified as benign traffic.

The figures below illustrate the accuracy, recall, precision, and F1-score of the selected machine learning algorithms used for botnet detection training.

```
Accuracy score: 94.24408571615807 %
Botnet traffic recall score: 0.9646246279970802
Botnet traffic precision score: 0.9694914106413237
Botnet traffic f1 score: 0.9670518962188209
```

Fig 2 : Decision Tree Classifier


```
Accuracy score: 94.01253850018567 %
Botnet traffic recall score: 0.9673985063731821
Botnet traffic precision score: 0.963546269057393
Botnet traffic f1 score: 0.9654685451060825
```

Fig 3 : K-Nearest Neighbors

```
Accuracy score: 61.43459415265266 %
Botnet traffic recall score: 0.41047784827896006
Botnet traffic precision score: 0.5980202879581152
Botnet traffic f1 score: 0.4868111743748543
```

Fig 4 : Naive Bayes

```
Accuracy score: 94.3155470537021 %
Botnet traffic recall score: 0.969060587343478
Botnet traffic precision score: 0.9757007654993838
Botnet traffic f1 score: 0.9723693403349034
```

Fig 5 : Random Forest Classifier

The figures below represent a system generates simulated network traffic and triggers a real-time pop-up alert for potential botnet activity. The authentication prompt allows users to manually approve or block suspicious traffic, enhancing security.

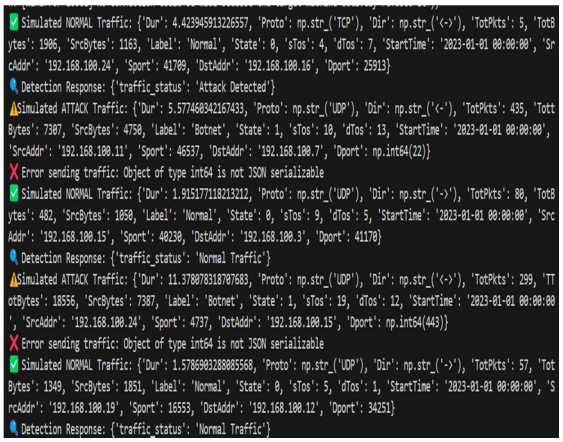


Fig 6 : Generating Fake Network Traffic

```
Predicted: Botnet for 192.168.100.24
blocked_ips: set()
user_decision Allow
127.0.0.1 - - [11/Mar/2025 20:20:30] "POST /detect HTTP/1.1" 200 -
Predicted: Normal for 192.168.100.15
blocked_ips: set()
127.0.0.1 - - [11/Mar/2025 20:20:32] "POST /detect HTTP/1.1" 200 -
Predicted: Normal for 192.168.100.19
blocked_ips: set()
127.0.0.1 - - [11/Mar/2025 20:20:34] "POST /detect HTTP/1.1" 200 -
Predicted: Normal for 192.168.100.20
blocked_ips: set()
127.0.0.1 - - [11/Mar/2025 20:20:36] "POST /detect HTTP/1.1" 200 -
Predicted: Botnet for 192.168.100.20
blocked_ips: set()
user_decision Block
127.0.0.1 - - [11/Mar/2025 20:20:40] "POST /detect HTTP/1.1" 403 -
127.0.0.1 - - [11/Mar/2025 20:20:42] "POST /detect HTTP/1.1" 403 -
```

Fig 7 : Detecting Malicious Traffic

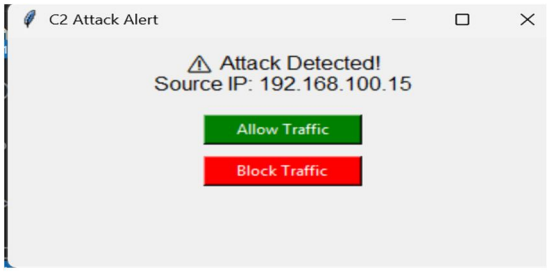


Fig 8 : Alert when Malicious Traffic is Detected

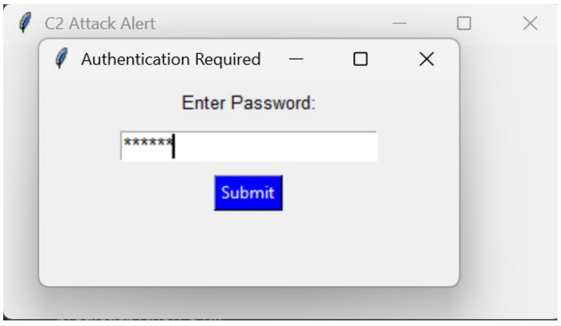


Fig 9 : Password Authentication

IX. FUTURE SCOPE

Future research on HDMM could focus on adaptive detection mechanisms using AI-driven techniques like unsupervised and reinforcement learning. Integrating it with intrusion detection systems and firewalls would create a multi-layered defense. Real-time threat intelligence sharing could improve botnet detection speed. Enhancing false positive mitigation through deep learning could boost accuracy. Advanced anomaly detection methods would help identify stealthy botnet attacks. Cross-layer analysis across network stacks could improve detection of evasive threats. Deploying HDMM in distributed, edge, and IoT environments would enhance scalability and efficiency. Long-term real-world testing would ensure robustness against evolving cyber threats.

X. CONCLUSION

This paper presents the HDMM has shown promising results in detecting and mitigating botnet C&C traffic, further improvements are needed to adapt the model to evolving threats, resource-constrained environments, and complex real-world conditions. By addressing the limitations outlined above and focusing on the suggested future enhancements, the HDMM can be evolved into a more robust, adaptive, and efficient system for securing modern networks against the ever-growing threat of botnet-driven attacks.

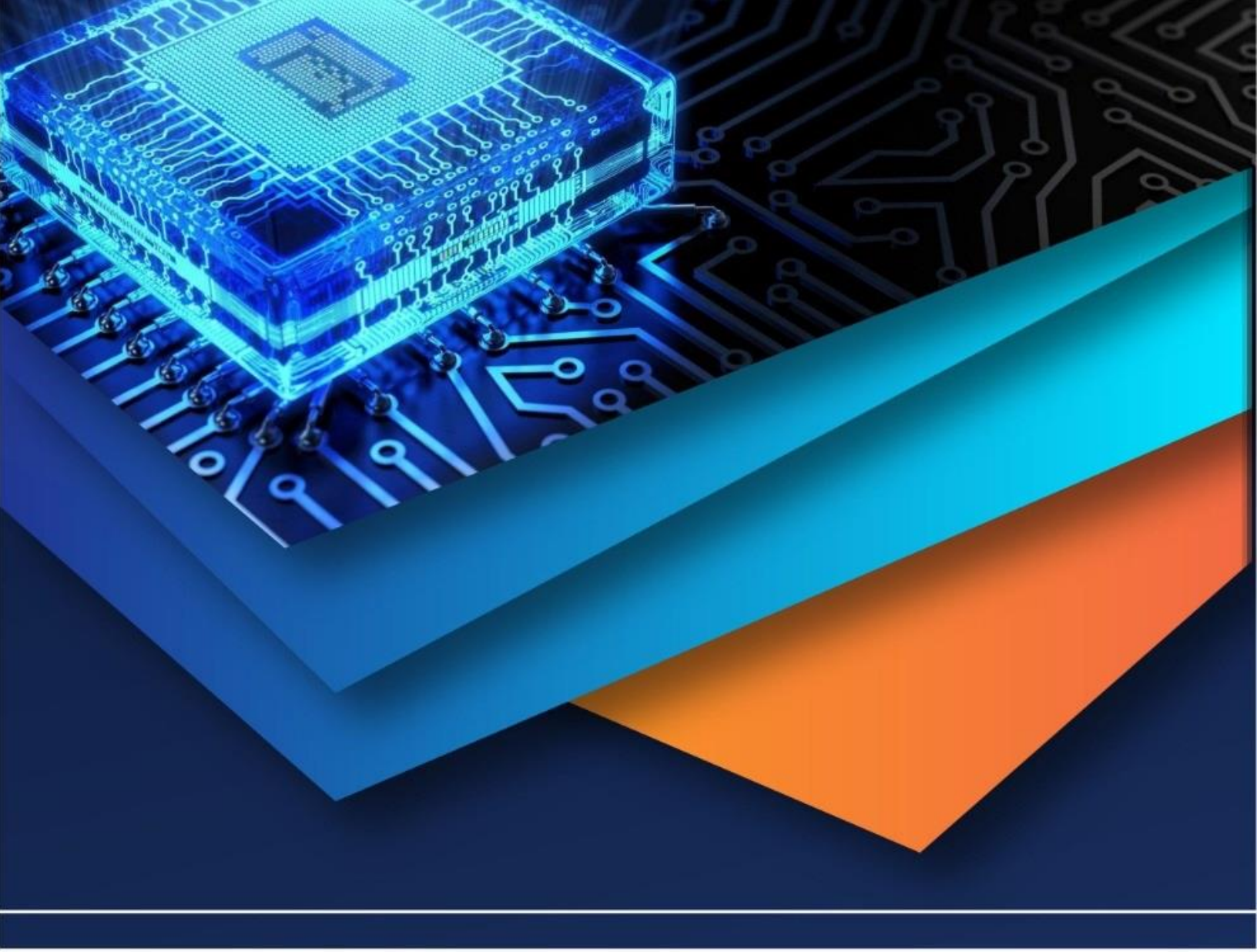
REFERENCES

[1] S Sharma, "Detection and Mitigation of Botnets in Large-Scale Networks: A Survey," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 975-986, Sept. 2019.
[2] R. Patel, M. Gupta, and N. Aggarwal, "Botnet Traffic Detection using Machine Learning Algorithms," *IEEE Access*, vol. 8, pp. 134345-134358, 2020.
[3] A. K. Jain, P. Kumar, and V. Singh, "Deep Learning Techniques for Botnet Traffic Detection," *Journal of Cyber Security Technology*, vol. 4, no. 1, pp. 31-45, Feb. 2021.
[4] M. Feily, A. Shahrestani, and S. Ramadass, "A survey of botnet and botnet detection," in Emerging Security Information, Systems and Technologies, 2009. SECURWARE'. 2009, pp. 268–273.
[5] Z. Zhu, G. Lu, Y. Chen, Z. Fu, P. Roberts, and K. Han, "Botnet research survey," in Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International. IEEE, 2008, pp. 967–972.
[6] S. García, M. Grill, J. Stiborek, and A. Zunino, "An Empirical Comparison of Botnet Detection Methods," *Computers & Security*, vol. 45, pp. 100-123, Sept. 2014.
[7] Y. Meidan et al., "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12-22, July-Sept. 2018.
[8] C. Li, W. Jiang, and X. Zou, "Botnet: Survey and case study," in Innovative Computing, Information and Control (ICICIC), 2009 Fourth International Conference on. IEEE, 2009, pp. 1184–1187.

[9] Y. Kugisaki, Y. Kasahara, Y. Hori, and K. Sakurai, "Bot detection based on traffic analysis," in Intelligent Pervasive Computing, 2007. IPC. The 2007 International Conference on. IEEE, 2007, pp. 303–306.

[10] S. Kumar, R. Sehgal, P. Singh, and A. Chaudhary, "Nepenthes honeypots based botnet detection," arXiv preprint arXiv:1303.3071, 2013.

[11] S. Garc´ıa, A. Zunino, and M. Campo, "Survey on network-based botnet detection methods," Security and Communication Networks, vol. 7, no. 5, pp. 878–903, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY