International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.48047/INTJECSE/V15I5.23 ISSN: 1308-5581 Vol 15, Issue 05 2023

HONEYPOT WITH MACHINE LEARNING BASED DETECTION FRAMEWORK FOR DEFENDING IoT BASED BOTNET DDoS ATTACKS

Mr.G.ANIL KUMAR
anil02.gardasu@gmail.com
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

BANDARU GOVARDHAN
bandarugovardhan6@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

MOHD KHAJA MOINUDDIN
khajamohd179@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

PEDDINTI ROHITH
goudrohith05@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

SAI VINEET KUMAR
Saivineet300@gmail.com
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SREYAS INSTITUTE OF ENGINEERING AND TECHNOLOGY

ABSTRACT

This project proposes a honeypot with machine learning based detection framework to defend against IoT based botnet DDoS attacks. The honeypot server acts as a decoy between the centralized server and the IoT network, and uses machine learning algorithms such as SVM, KNN, Random Forest, Decision Tree and Neural Network to classify the requests as normal or malicious. The honeypot server also extracts information from the attackers and informs the centralized server and the IoT network to block them. The paper claims that this approach can solve zero-day DDoS attacks and outperforms the existing signature-based detection methods. The paper uses real IoT data to train and test the machine learning models, and reports that SVM, KNN and Neural Network achieve the best performance.

INTRODUCTION

There are several honeypot-based approaches are present in the literature for defending DDoS. The concept of the signature matching method had been used as a detection framework in some of these approaches. Malware is detected on the basis of signatures obtained from their corresponding generated log files from the honeypot. This type of detection was able to deal with only stored signatures and its variations, hence throw a limitation on dealing with an unknown and wider range of malware families. Another solution is anomaly-based detection which does not make use of rules, but a threshold is set for normal user behavior and any deviation from it leads to a declaration of possible malicious behavior. Such systems do suffer from high false positive rates because attackers now can imitate normal behavior too.
Moreover, a machine learning based solution is capable to deal with such problem due to its ability to learn and teach over time. Thus, a more accurate classification with a smaller number of false positive can

be achieved by training the model with effective and updated data. The machine learning concept is used to better utilize the dynamic data produced by honeypot and increase the predictability for future attacks.

The widespread adoption of Internet of Things (IoT) devices has revolutionized various aspects of modern life, from smart homes to connected vehicles. However, this burgeoning connectivity has also created a vast and complex attack surface for cyber threats. One particularly concerning threat is the rise of botnet Distributed Denial-of-Service (DDoS) attacks, which utilize large numbers of compromised IoT devices to overwhelm legitimate targets with traffic. These attacks can cripple businesses, disrupt critical infrastructure, and cause widespread financial losses.

Traditional security measures, such as firewalls and intrusion detection systems, often struggle to effectively detect and mitigate botnet DDoS attacks, particularly against sophisticated and evolving attack techniques. This is because these attacks often employ low-signature reconnaissance to probe for weaknesses before launching a full-scale assault. As a result, zero-day attacks, which exploit vulnerabilities not yet known to security vendors, can cause significant damage before effective countermeasures can be deployed.

To address these challenges, we propose a novel approach that combines honeypot technology with machine learning techniques to enhance the detection and mitigation capabilities of IoT networks. Honeypots are decoy systems designed to attract and deceive attackers, allowing security analysts to observe their behavior, gather intelligence about their attack methods and tools, and ultimately disrupt their efforts. Machine learning algorithms, on the other hand, can analyse the captured data to identify patterns and anomalies indicative of malicious activity.

LITREATURE SURVEY

There are several honeypot-based approaches are present in the literature for defending DDoS. The concept of the signature matching method had been used as a detection framework in some of these approaches. Malware is detected on the basis of signatures obtained from their corresponding generated log files from the honeypot. This type of detection was able to deal with only stored signatures and its variations, hence throw a limitation on dealing with an unknown and wider range of malware families. Another solution is anomaly-based detection which does not make use of rules, but a threshold is set for normal user behavior and any deviation from it leads to a declaration of possible malicious behavior. Such systems do suffer from high false positive rates because attackers now can imitate normal behavior too. Moreover, a machine learning based solution is capable to deal with such problem due to its ability to learn and teach over time. Thus, a more accurate classification with a smaller number of false positive can be achieved by training the model with effective and updated data. The machine learning concept is used to better utilize the dynamic data produced by honeypot and increase the predictability for future attacks. Many machine learning methods have also been proposed to identify DDoS based on the selection of statistical features using several supervised learning algorithms like SVM, NaïveBayes, etc. However, these methods require extensive network expertise for selecting appropriate features out of the dataset and usually are limited to only one or several DDoS vectors. In addition, they require regular updates of the system to keep it functioning in diverse situations. Another machine learning based solution was proposed to detect DDoS using deep learning models like: Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory Neural Network (LSTM), and Gated Recurrent Unit Neural Network (GRU). A network-based anomaly detection method was proposed which extracts behavior snapshots of the network and uses deep autoencoders to detect anomalous network traffic emanating from compromised IoT devices. However, deep learning models need a large amount of data to train itself for producing accurate outcomes. In spite of that, they have extremely computationally expensive and complex training procedure and often require a significant amount of time to learn. IoT devices cannot afford such extensive procedures as they are quite constrained in terms of resources as well as in providing real-time services to the user.

PROPOSEDSYSTEM

A honeypot is a decoy system that mimics the behavior of a real IoT device and attracts attackers to interact with it. By doing so, the honeypot can collect valuable information about the attack patterns,

sources, and techniques. The proposed system uses the data generated by the honeypot as a dataset for training a machine learning model that can classify the traffic as normal or malicious. The proposed system can detect Zero-Day attacks.The proposed system aims to enhance the security of Internet of Things (IoT) devices by introducing a comprehensive defense mechanism against Distributed Denial of Service (DDoS) attacks orchestrated by IoT-based botnets. The system leverages a Honeypot, a decoy IoT device designed to attract malicious activities, coupled with a sophisticated Machine Learning-based detection framework.

The Honeypot serves as a deceptive target within the IoT network, emulating the behavior of a legitimate device. It captures and analyzes incoming traffic, allowing for the identification of malicious patterns and activities. This decoy system not only diverts potential attacks away from actual IoT devices but also provides valuable insights into the tactics, techniques, and procedures employed by emerging IoT botnets.The Machine Learning-based detection framework is integrated with the Honeypot to analyze the traffic patterns and distinguish between normal and malicious behavior. By continuously learning and adapting to new attack vectors, the framework enhances its detection capabilities over time. This dynamic approach allows the system to stay ahead of evolving threats, providing a proactive defense mechanism against the rapidly changing landscape of IoT-based DDoS attacks.

Key features of the proposed system include real-time monitoring, anomaly detection, and automated response mechanisms. The Machine Learning model refines its understanding of normal network behavior, enabling it to identify deviations indicative of DDoS attacks. When a potential threat is detected, automated responses can be triggered, such as isolating the affected device or adjusting network configurations to mitigate the impact of the attack.The significance of this proposed system lies in its ability to not only detect and mitigate ongoing attacks but also contribute to threat intelligence by continuously analyzing and learning from new attack patterns. As IoT devices become increasingly ubiquitous, securing them against sophisticated DDoS attacks is paramount. The Honeypot with a Machine Learning-based detection framework offers a robust defense strategy, safeguarding the integrity and functionality of IoT ecosystems.

RESULT

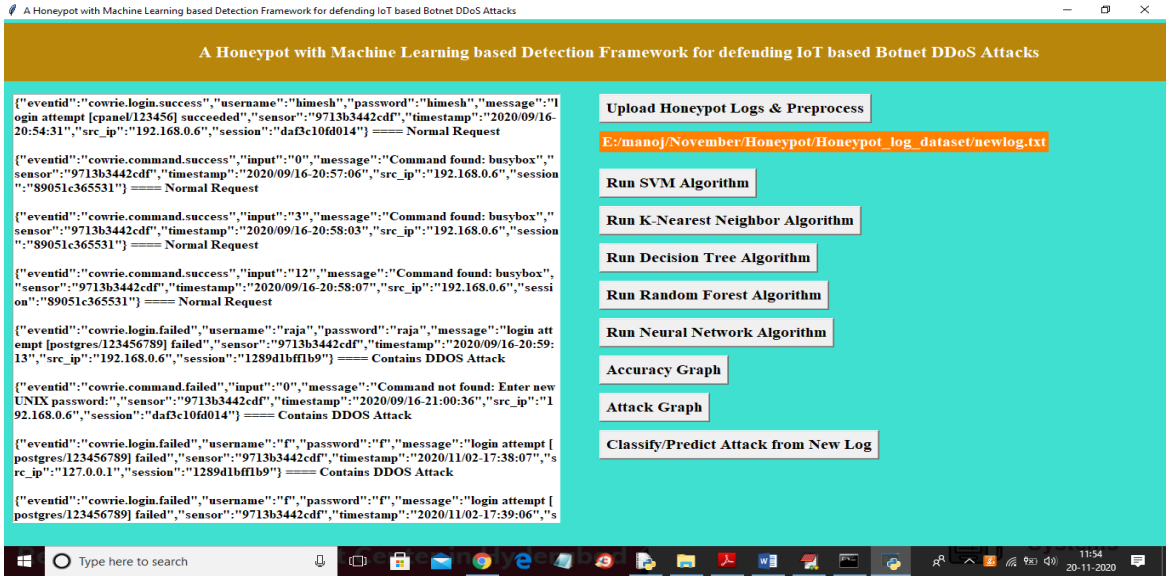

Fig 1 Generated Output 1

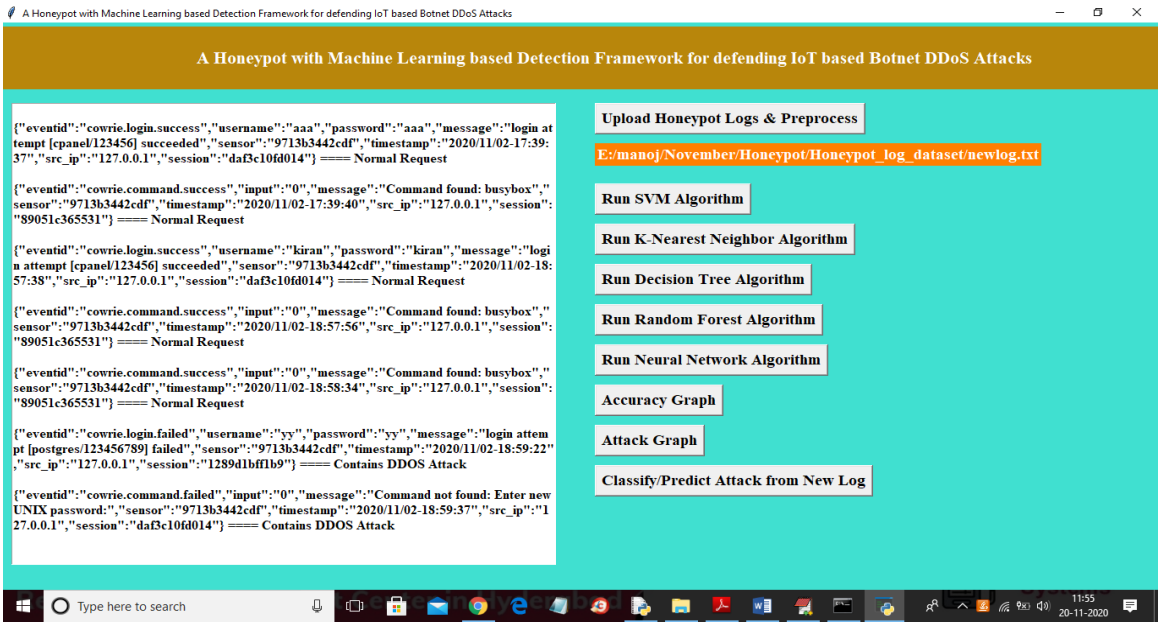

Fig .2 Generated Output 2

In above screen ML analyse each request and then mark that request signature as normal or DDOS attack. At each request line after equals to symbol we can see ML detection result. In above screen scroll down to view all request result

CONCLUSION

Internet-of-things is the biggest reason for the modernization of the real world in terms of technology. But it is also the main reason for the increasing number of cyber-attacks especially DDoS attacks. That's why defending against such attacks that use IoT as a medium to harm network security has become the primary concern in the field of Internet Security. A number of defense mechanisms have been proposed in the concerned field to make the IoT network immune to such attacks but they become incapable of handling new variants of IoT botnet attacks. We came up with a honeypot-based solution for the DDoS detection which uses real-time machine learning detection framework. Use of honeypots will ensure the logging of newly coming malware features which will be utilized by ML-based detection framework to train their classifiers effectively. For the future scope, we need to extend this approach to the next level where we can find out the open challenges or issues by implementing over the real-time scenarios. There is also scope for employing a cloud server to deal with extremely resource-constrained IoT devices. Finally, we can come up with a comparative analysis of our proposed solution by evaluating its performance in contrast to other proposed models.

REFERENCES

[1]. K. Chen, S. Zhang, Z. Li,Yi Zhang, Q.Deng, Sandip Ray, Yier Jin, “Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice” Journal of Hardware and Systems Security, vol. 2, Issue 2, pp. 97–110, (2018).

[2]. W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," IEEE Internet of Things Journal. 2018.

[3]. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142 (2017).

[4]. Honeypots and the Internet of Things. Available at https://securelist.com/honeypots-and-the-internet-of-things/78751.

[5]. Hastie, T., Tibshirani, R., & Friedman, J. Unsupervised learning. In The elements of statistical learning (pp. 485-585). Springer, New York, NY (2009).

[6]. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in Computer, vol. 50, no. 7, pp. 80-84 (2017).

[7]. Dougherty, J., Kohavi, R., & Sahami, M. Supervised and unsupervised discretization of continuous features. In Machine Learning Proceedings 1995, pp.194-202 (1995).

[8]. Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In Security and Privacy (SP), IEEE Symposium on (pp. 305-316). IEEE (2010).

[9]. M. Anirudh, S. A. Thileeban And D. J. Nallathambi, "Use of Honeypots for Mitigating DoS Attack Targeted on IoT Networks," 2017 International Conference On Computer, Communication And Signal Processing (ICCCSP), Chennai, Pp. 1-4, (2017).

[10]. Rieck, K., Holz, T., Willems, C., Dussel, P., & Larkov, P. (2008, July). Learning and classification of malware behavior. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (pp. 108-125). Springer, Berlin, Heidelberg.

[11]. Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. Automated classification and analysis of internet malware. In International Workshop on Recent Advances in Intrusion Detection Springer, Berlin, Heidelberg, pp. 178-197 (2007).

[12]. Binkley, J. R., & Singh, S. An Algorithm for Anomaly-based Botnet Detection. SRUTI, 6, 7-7. (2006).

[13]. Song, Y., Keromytis, A. D., & Stolfo, S. J. U.S. Patent No. 8,844,033. Washington, DC: U.S. Patent and Trademark Office. (2014).

[14]. The New Threat: The IoT DDoS Invasion.

[15]. https://www.a10networks.com/sites/default/files/resource-files/A10-TPS-GR-The_New_Threat_The_IoT_DDoS_Invasion.pdf.

[16]. Zammit, DA machine learning based approach for intrusion prevention using honeypot interaction patterns as training data. University of Malta, 1-55 (2016).