



Faculty of Engineering

Program Title: Master of Science in Artificial Intelligence

Semester: Summer 2024

Academic Year: 2024

Module Title: Research Methodology in Computer Science

- Module Code: AI800

Instructor Name: Dr. Mohammed Anbar

Report About:

Real-Time IoT Botnet Detection Using Machine and Deep Learning for Scalable Security

Student ID: 242001458

Student Name: Omar Abu Amra

Table of contents

Topic	Page number
Problem Statement	3-4
Research Objectives:	4-5
References	6

Problem Statement:

The Current proposal using advance machine learning and deep learning methods to detect and reduce botnet attacks in IoT networks.

Because of the varied nature of IoT devices and their limited computational capacity, sophisticated botnet assaults are becoming more and more common on IoT networks. These assaults pose serious risks to individual users, large-scale IoT deployments, and national security since they cause major disruptions, security breaches, and the possible penetration of key infrastructure. Even with advances in intrusion detection systems (IDS), real-time detection and mitigation of botnet attacks is still a major problem, especially in diverse and dynamic IoT contexts.

The rapid growth of IoT devices in a variety of fields, including smart cities, healthcare, and industrial systems, amplifies the possibility of harm that botnet attacks might cause. For IoT networks to function in a safe, dependable, and trustworthy manner a prerequisite for the developing Internet of Everything (IoE) effective detection and mitigation of these threats are not just desired, but also necessary. It is predicted that IoT security breaches would have a billion-dollar yearly economic impact, therefore reinforcing how critical it is to have strong defenses.

Existing methodologies for identifying botnet assaults in IoT networks encompass an intrusion detection system utilizing deep learning is employed to detect DDoS botnet attacks in IoT networks. This system achieves exceptional accuracy and precision by employing a deep neural network model. (Jithu et al., 2021). An ensemble learning model is employed to detect botnets in IoT environments. This model achieves a remarkable accuracy rate of 100% and significantly reduces the number of required features to just 20. It utilizes a combination of supervised, unsupervised, and regression learning approaches. (Rezaei, 2021). BotIDS is an advanced intrusion detection system that utilizes deep learning algorithms to effectively identify and detect botnet assaults in IoT networks. It has been proven to outperform previous methods, with an impressive validation accuracy of 99.94%. (Idrissi et al., 2021). A cooperative machine learning model was developed to detect IoT botnets at an early stage. The model achieved an accuracy of 99.37% when tested on a dataset consisting of 5023 botnets and 3888 benign samples. (Nguyen et al., 2022). The ELBA-IoT ensemble learning model surpasses current cutting-edge techniques for identifying botnet assaults in IoT networks, attaining a remarkable accuracy of 99.6% while incurring a minimal inference overhead of 40 as. (Abu Al-Haifa and Al-Dalanie, 2022). An

ensemble deep transfer learning approach was used to detect IoT malware, resulting in an accuracy of 93.58% on a dataset consisting of 3000 malicious and 3000 benign samples. (Kadhim et al., 2022).

Despite these developments, the present approaches fall lacking in several critical areas. insufficient ability to change or adjust in the face of novel or unusual conditions. The quickly changing nature of botnet attacks and the wide variety of IoT devices and protocols frequently present difficulties for current designs. Restricted scalability: Several proposed solutions face major difficulties when scaled to cover large, heterogeneous IoT networks. Limited real-time capabilities the fluid nature of IoT environments makes real-time detection and reaction essential, yet current solutions generally fall lacking in this regard. There is not enough representation in the dataset. A large number of models are trained using small datasets that come up short of capturing the richness and diversity of actual IoT botnet attacks.

Research Objectives

Research that focuses primarily on developing machine learning models that can scale and adapt to meet the diversity and dynamic nature of IoT networks is desperately needed in order to address these serious shortcomings. creating and utilizing larger, more inclusive datasets that faithfully represent real-world IoT botnet attack scenarios. developing machine learning models that can scale and adjust to the many and ever-changing IoT network conditions. improving feature extraction and selection techniques to offer effective real-time response and detection capabilities. Algorithms that are lightweight and efficient can be developed so that they can be employed with high detection accuracy on Internet of Things devices with limited resources.

To propose and Assure diversity and applicability to actual situations by compiling an extensive dataset that encompasses a broad spectrum of IoT botnet attack patterns. The diversity required to train models that can accurately identify the entire range of IoT botnet attacks is frequently lacking from current datasets. The accuracy and dependability of detection algorithms will be increased dramatically with a larger dataset.

To design and construct a scalable intrusion detection system that may be used to successfully implement resource limitations and heterogeneous device management across large-scale IoT networks. A scalable solution that can safeguard networks of different sizes and compositions is required due to the quick expansion and diversity of IoT deployments, which highlights a significant weakness in present security methods.

To develop and analyze new methods for feature extraction and selection that balance detection accuracy and computational efficiency in IoT devices with limited resources. One major problem in existing IoT security systems is providing real-time detection on resource-limited IoT devices, which requires efficient feature selection.

To develop and incorporate real-time detection features into the suggested architecture to guarantee prompt detection and handling of botnet threats in ever-changing Internet of Things settings. Real-time detection is essential for successful security because of the dynamic nature of IoT networks and the possibility for botnet infections to spread quickly. This solves a major flaw in many existing systems.

To evaluate how well different deep learning and machine learning models including Deep Learning hybrid approaches work to improve intrusion detection systems' efficiency and accuracy in identifying threats on Internet of Things networks. Pushing the limits of existing IoT security capabilities, comparative study of various models and hybrid method exploration can result in more effective detection strategies.

To design and use a collaborative learning approach to identify and isolate threats early in their lifespan, protecting privacy and cutting down on communication overhead, in order to enable the early detection of IoT botnet attacks. Reducing the effects of botnet assaults requires early discovery. A critical gap in IoT security can be filled by collaborative techniques, which can make use of distributed IoT systems to increase detection speed and accuracy.

The main obstacles in IoT botnet detection are intended to be methodically addressed by this study framework, which covers everything from data representation to model deployment and evaluation. By accomplishing these goals, we hope to: Improve IoT security by creating botnet detection systems that are more precise, effective, and flexible. Boost the overall security posture of IoT ecosystems by offering workable solutions that can be integrated into actual IoT deployments. Provide significant methods and insights to the cybersecurity community at large, especially when addressing situations with varying resources. Create a foundation for next studies on intelligent and adaptable IoT security systems.

References:

- Al-Haija, Q. A., & Al-Dala'ien, M. (2022). ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. *Journal of Sensor and Actuator Networks*, 11(1).
<https://doi.org/10.3390/jsan11010018>
- Alshamkhany, M., Alshamkhany, W., Mansour, M., Khan, M., Dhou, S., & Aloul, F. (2020). Botnet Attack Detection using Machine Learning. *Proceedings of the 2020 14th International Conference on Innovations in Information Technology, IIT 2020*, 203–208.
<https://doi.org/10.1109/IIT50501.2020.9299061>
- Idrissi, I., Boukabous, M., Azizi, M., Moussaoui, O., & Fadili, H. El. (2021). Toward a deep learning-based intrusion detection system for iot against botnet attacks. *IAES International Journal of Artificial Intelligence*, 10(1), 110–120. <https://doi.org/10.11591/ijai.v10.i1.pp110-120>
- Jithu, P., Shareena, J., Ramdas, A., & Haripriya, A. P. (2021). Intrusion Detection System for IOT Botnet Attacks Using Deep Learning. *SN Computer Science*, 2(3). <https://doi.org/10.1007/s42979-021-00516-9>
- Kadhim, Q. K., Al-Sudani, A. Q. A. S., Almani, I. A., Alghazali, T., Dabis, H. khalid, Mohammed, A. T., Talib, S. G., Mahmood, R. A., Sahi, Z. T., & Mezaal, Y. S. (2022). IOT-MDEDTL: IoT Malware Detection based on Ensemble Deep Transfer Learning. *Majlesi Journal of Electrical Engineering*, 16(3), 47–54.
<https://doi.org/10.52547/mjee.16.3.47>
- Nguyen, G. L., Dumba, B., Ngo, Q. D., Le, H. V., & Nguyen, T. N. (2022). A collaborative approach to early detection of IoT Botnet. *Computers and Electrical Engineering*, 97.
<https://doi.org/10.1016/j.compeleceng.2021.107525>
- Rezaei, A. (2021). Using Ensemble Learning Technique for Detecting Botnet on IoT. *SN Computer Science*, 2(3). <https://doi.org/10.1007/s42979-021-00585-w>