



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:

literature Review Detection System for IOT Botnet Attacks

Student ID: 242001458

Student Name: Omar Abu Amra

Table of contents

Topic	Page number
literature Review Detection System for IOT Botnet Attacks	3-5
Critical Analysis	4
Connections & Conflicts	5-6
Synthesis Matrix for Literature Review	7-9
References	10

literature Review Detection System for IOT Botnet Attacks:

This study paper presents a deep learning-based intrusion detection method to catch IoT botnet episodes, especially DDoS episodes. The writers developed a Deep Neural Network (DNN) model using the BoT-IoT dataset, which includes both normal and pretend attack traffic from a real IoT network circumstances. The dataset was preprocessed and normalized utilizing min-max scaling. The DNN model was trained and assessed employing various metrics, including accuracy, precision, recall, F-score, and AUC-ROC curve. The outcomes deliver high performance, with a precision of 0.947 and an AUC of 0.98. The key findings show that the offered DNN model outperforms existing techniques in detecting IoT botnet attacks with elevated accuracy and precision. Two major restrictions of this study are that The focus is primarily on DDoS attacks, potentially neglecting different classes of IoT botnet episodes, and The model's performance in real-world, dynamic IoT environments may differ from the simulated dataset used for training and testing.(Jithu et al., 2021)

This study aimed to develop an ensemble learning model for optimizing botnet detection accuracy on IoT machines while underrating required features. The experimenters mixed artificial neural networks (ANN) and decision trees (DT) after considering 17 device learning algorithms. They employed a dataset of 990,517 domain names (790,745 standard, 199,772 malicious) with 204 features, which was decreased to 20 essential features. The ensemble approach reached 100% accuracy in catching botnets and bots, with a true positive rate of 20.17% and a true negative rate of 79.83%. The main constraints were that the study concentrated exclusively on domain name-based detection, potentially ignoring other kinds of botnet activity. The model's interpretation was not pushed on real-time network gridlock, which could introduce further challenges in live circumstances.(Rezaei, 2021).

This study presents a deep learning-based intrusion detection method called BotIDS to notice botnet attacks in IoT networks. The experimenters operated convolutional neural networks (CNNs), corresponding to performance in other deep learning techniques like RNN, LSTM, and GRU. They employed the Bot-IoT dataset, which includes about 3.6 million network traffic logs affecting an IoT domain with normal traffic and ten classes of botnet episodes. The CNN model gained 99.94% guarantee accuracy and 0.58% validation loss, with forecast time beneath 0.34 ms.

The key results are that the CNN-based approach surpassed other deep learning techniques for this IoT intrusion detection mission. The primary restrictions noted are that The study only used one dataset for evaluation, and Real-world testing in an actual IoT environment was not conducted (Idrissi et al., 2021).

This study paper presents a collaborative machine-learning method for premature detection of IoT botnets. The authors design a model that integrates numerous features from technique calls, network manners, and machine performance to notice malicious movement in the premature phases of the botnet lifecycle. The model is assessed on a 5023 IoT botnet illustrations dataset and 3888 benign samples, achieving 99.37% accuracy. Key results contain the significance of using a collaborative late fusion approach to combine different feature sets and the capability to notice hurtful behavior earlier than full-time series data methods. The primary constraints are The dependency on features collected through a custom sandbox domain, which may restrict generalizability to real-world IoT devices—an insufficiency of comparison to other state-of-the-art IoT botnet detection methods to contextualize the performance gains. (Nguyen et al., 2022)

This research paper suggests ELBA-IoT, an ensemble learning model for noticing botnet attacks in IoT networks. The examination utilizes the N-BaIoT-2021 dataset, incorporating 611,359 regular traffic and 7,737 samples of botnet traffic (4,737 Bashlite and 3,000 Mirai) from five IoT appliances. The writers utilize three decision tree approaches (AdaBoosted, RUSBoosted, and bagged) and assess their ensemble model employing different performance metrics. The results show that ELBA-IoT achieves a high detection accuracy of 99.6% with lower inference overhead (40 μ -seconds), exceeding other state-of-the-art methods. The primary constraints of this study are The dependence on a single dataset, which may restrict the model's generalizability to other IoT environments, and The absence of real-time testing in an existing IoT network environment, which could deliver more insights into the model's functional performance. (Al-Haija & Al-Dala'ien, 2022)

This research document offers a novel method for IoT malware detection employing ensemble deep transfer learning. The approach preprocesses binary malware data into grayscale images and employs two pre-trained CNN models (ResNet101 and VGG16) as feature extractors. The pulled features are combined and provided into a classifier. The study utilized a dataset of 6,000 samples (3,000 malicious and 3,000 benign) gathered from two IT firms in Iraq. The suggested method

reached 93.58% accuracy, 94.39% precision, and 92.67% recall on the test set. The primary benefits are the benefit of transfer learning to optimize training with narrow data and the model's competitive performance connected to earlier works, particularly regarding inference time (0.012 seconds). Nevertheless, two fundamental limitations are the moderately small dataset size corresponding to some other studies in the field, which may restrict generalizability, and the absence of comparison with more recent state-of-the-art malware detection approaches, which could deliver a better complete evaluation of the presented approach's effectiveness. (Kadhim et al., 2022)

Critical Analysis:

The combined aim of these research papers is to introduce state-of-the-art machine learning and deep learning model-related studies that can be utilized for IoT botnet attack detection and intrusion detection so that more efficient Intrusion Detection System (IDS) design in an IoT network could occur. The studies used datasets like combined IoT and simulated network traffic Bot-IoT, which introduced benchmarks in the reviewed approaches performance with metrics such as accuracy, precision, recall (or True Positive Rate), F1 score, etc. They also provide ROC curves of the mentioned metrics for methods under study, all to prove the feasibility of the studied techniques proposed. Their papers generally say that their use of deep learning and ensembles furthers the state-of-the-art in detecting IoT botnet attacks compared to Traditional methods, with reasonable accuracy and performance metrics. Although not explicitly mentioned, these works are extensions of the IoT security research and deal with drawback contexture within customary intrusion detection strategies for IoT networks. The underlying assumption is that machine learning and deep learning (more formally called "end-to-end" training with inference), in particular, can learn narrow patterns in network traffic, implying normal vs. malicious behavior of an IoT device or group thereof! These include multiple models such as Deep Neural Networks (DNN), ensemble learning techniques, and transfer learning methods. This paper's strengths were presenting the recent IoT datasets and exploring the inherent security challenges in a precisely specified domain. However, some of the potential limitations may be overfitting to specific datasets, or it can get computationally complex for resource-limited IOT devices and, in a few cases, has never been tested in real life. Instead, these papers offer positive measures for enhancing IoT security using elaborate machine learning methods. However, more research regarding their practicality in real-world implementation and resource efficiency is required to corroborate the conclusions.

Connections & Conflicts:

Significance of IoT Security: All articles underscore the critical importance of protecting IoT devices from botnet assaults, highlighting the vulnerabilities of the devices' heterogeneous and resource-constrained design.

Methods of Machine Learning and Deep Learning: The majority of research recommends applying machine learning (ML) and deep learning (DL) to identify botnet activity. To improve detection accuracy, several articles explicitly use deep neural networks (DNNs).

Usage of the Bot-IoT Dataset: Several publications discuss using this dataset, which is intended for simulating and examining different kinds of assaults in IoT contexts. This similarity points to a shared resource that facilitates the testing and development of detection methods.

Anomaly Detection: Several studies suggest anomaly-based detection systems that use ML/DL to find anomalies in typical traffic patterns are likely successful in identifying botnet tendencies.

Conflicts: Detection Performance and Accuracy: Although some studies indicate excellent performance and accuracy with their models, others may give conflicting conclusions, posing concerns about the repeatability and generalizability of findings across diverse contexts or datasets.

Efficiency vs. Complexity: While some studies support more sophisticated models that attain high detection rates, others may support more straightforward, more efficient models that function as expected but are more straightforward to implement in IoT environments with limited resources.

Limitations of the dataset: Opinions regarding the adequacy of currently available datasets for training robust models may differ. While some articles may examine dataset variety in detail, others may draw attention to the limits of datasets such as UNSW-NB15 compared to Bot-IoT.

Overarching Concept for IoT Applications: The suggested techniques' efficacy may differ depending on the IoT application(e.g., healthcare, smart homes), resulting in disagreements on the findings' generalizability outside the particular settings examined.

Synthesis Matrix for Literature Review:

Study	Authors	Year	Research Design	Key Findings /Results	Methodology	Limitations
Study1	Kadhim QAl-Sudani AAImani IAIghazali TDabis HMOhammed A Talib SMahmood RSahi ZMezaal Y	2022	Quantitative, Experimental	Based on the evaluation results and performance analysis, our ensemble deep transfer learning method for IoT using malware is robust while also boasting high precision (F1) with an efficient computational cost. Accuracy: 93.58% Precision: 94.39% Recall: 92.67% F1-Score: 93.52% AUC-ROC: 0.97 + 0.012-second inference time	The methodology consisted of preprocessing binary malware data into images, then used to perform transfer learning with pretrained CNN models that evaluated upon the test set using standard classification metric. Data set obtained from two IT companies in Iraq (Jiasaz, Lucid) The dataset consists of malware and benign/non-malicious samples collected from Ubuntu 20.04.2. Dataset size is Total of six thousand samples three thousand malware samples three thousands of benign/ non-malicious samples. Eighty percent Training set - 3540 samples, 20% evaluate set (1200 samples). 8-bit sequences, after conversion of binary malware data. Converted into Grayscale Images Mean and std/appropriate normalizations. Two CNN models: ResNet101 and VGG16.Pretrained models on ImageNet grayscale form. Merged feature maps from the two models. Bidirectional LSTMs replace the RNN Encoder with a maxpool output, accompanied by Fully connected classification head. As in the case of transfer learning, ResNet101 frozen until last 4 blocks, VGG16First,3 block of the Model. Models fine-tuned with end-to-end on target data. Trained	small dataset: with a total of only six thousand (or in general just N) samples, half malicious and non-malicious each, the data pool limited for deep learning purposes. And the model may become too specialized to be useful against a broad range of IoT malware. The hardware bottleneck: The study is conducted on an Nvidia GeForce GTX 1050 GPU which could have limited them to train bigger models and larger batch sizes. Image Conversion: Transforming binary to grayscale, although creative can be better with the loss of important structural information available in original data from devices.
Study2	A1-Haija, Qasem Abu, A1-Dala'ien, Mu'Awya	2022	Quantitative, Experimental	Detection accuracy of 99.6%. Binary classification (Normal vs. malicious) achieved 99.6% accuracy. Ternary classification (normal vs. Bashlite vs. Mirai) reached 99.5% accuracy. Multi-class classification (10 classes) attained 99.4% accuracy. Low inference overhead of 40 microseconds per sample. 115 statistical features extracted from network traffic were used. Features included packet-based, time-based, and connection-based statistics. (AUC) of 0.999 for binary classification. High True Positive Rate (TPR) and low False Positive Rate (FPR) across all classification tasks.	This research used a set of processes, which included preprocessing the N-BaIoT-2021 dataset, developing individual decision tree models and an ensemble model, training and testing the model, and evaluating model performances using different criteria. An ensemble approach is used to enhance the detection of botnet attacks in an IoT network. It focused on the N-BaIoT-2021 dataset, which includes both IoT regular traffic and botnet-attacking traffic from infected devices. The dataset size in the study Total of 619,096 samples, 611,359 benign traffic samples and 27,737 botnet traffic samples (22,000 Bashlite + 3,000 MIRAI) All 619,096 samples in the dataset were included. The processing module carried out the data preparation, a preprocessing step for IoT traffic raw data. Converted preprocessed data to Word vector features table with labels Algorithms Used in Developing Modeling in the Study. They proposed an ensemble learning technique called ELBA-IoT. Three decision tree techniques were employed (AdaBoosted, RUSBoosted, and bagged decision trees). Ensembled these evaluations of Acceptance testing Simulation Phase MNMN Training in the study Implementation done using MATLAB and splitting into	Limited dataset, lack of comparison with other anomaly detection techniques, no real-world testing, limited attack types, no false positive analysis, computational overhead not fully addressed, lack of adversarial testing, and limited explainability.

Study3	Rezaei, Amirhossein	2021	Quantitative, Experimental	An ensemble learning method for detecting botnets in IoT networks that was highly effective. They utilized the approach and obtained 100% precision in detecting botnets and bots. The RMSE of the test findings was 0.0.	The methodology employed was a selection of features, testing of various machine learning algorithms, and the optimal ensemble model to minimize the features required but maintain the IoT botnet feature identification accuracy maximized. The data was taken from three databases, Kaggle, Github, and Cert, and both standard domain names and malicious domain names were used. The study used the entire dataset of 990,517 domain names. The relationship of the data was then analyzed with a research tool (matrices, heatmaps, histograms). A backward deletion technique was also used to choose the most appropriate set of features. Meanwhile, the number of required features was reduced to 20. Lastly, the 'Protocol' characteristic was converted to an integer to classify with a numerical digit. For instance, the position is UDP, the number is 1, 254, and the position is 2, TCP is three, and ICMP is four. The multitudes of machine learning algorithms were examined to understand the dataset and how to work with it properly. The four most successful algorithms, ANN, DT, GMM, and HC, had the best performances. Therefore, the dataset was divided to review the 90/10, 80/20, and 70/30 splits. Meanwhile, the 5-fold cross-validation was used to validate the criterion. There were several metrics computed for performance, such as accuracy, TPR, FPR, TNR, FNR Classification measures in the study $TPR = TP / (TP + FN)$, $FPR = FP / (FP + TN)$, $TNR = TN / (TN + FP)$, $FNR = FN / (FN + TP)$. The key innovation is the collaborative late fusion model that enables early detection of IoT botnets by combining multiple feature types, without requiring full execution data, allowing for faster and earlier detection compared to previous approaches. The authors used a V-Sandbox environment in the study to capture several dynamic features for IoT Botnets and benign samples such as network flow data, system calls data, and resource utilization.	The scholars could have cherry-picked methods that would support their 100% accuracy hypothesis. Utilizing only three differences botnets behavior may not cover all botnet behaviors.
Study4	Nguyen, Giang L.; Dumba, Brantio; Ngo, Quoc Dung; Le, Hai Viet; Nguyen, Tu N.	2021	Quantitative, Experimental	The proposed collaborative machine learning model achieved 99.37%. The model aims for early detection without requiring entire time-series data during malware execution. Features extracted from system calls, network behavior, and device performance.	The study did not include data for the complete execution, rather only during a window to provide early warning. The study utilized a dataset comprising 5023 IoT botnets and 3888 benign samples. The dataset used in the study consisted of 8911 samples, including 5023 malware and a business-as-usual number of benign (3888) samples. The researchers extracted vital features from the collected data, like system call sequences, network flow statistics, or device resource usage metrics. The study also conducted feature engineering to transform the input of machine learning models, as shown in. So, the authors in this study introduced a shared machine learning model combining different single-model classifiers via late fusion. The study reports the training of individual classifiers on distinct sets of features (network, system calls, resource usage) extracted from the data.	The selected system calls, network behavior, and device performance-based features might not all entail IoT botnet behaviors, such as stealthy command and control communication or polymorphic malware. The study needs to specify what types of IoT devices are included in their dataset

Study5	Jithu, R; Shareena, Jisuma; Ramdas; Aiswarya; Haripriya, A. P.	2021	Quantitative, Experimental	high-performing, lightweight DNN model for detecting DDoS botnet attacks in IoT networks The proposed deep neural network (DNN) model achieved high performance metrics: Precision: 0.947 Recall: 0.946 F-score: 0.947 Accuracy: 0.947	The approach concentrated on creating a DNN-based intrusion detection system to detect DDoS botnet attacks in IoT networks, employed the BoT-IoT dataset, and analyzed the performance of several metrics. This study was performed on the BoT-IoT dataset, generated in a natural network environment at Cyber Range Lab by UNSW Canberra Cyber. It consists of the standard and botnet traffic data. The paper explains that they are based on a subset of attack data (DDoS). The study does not mention the particular number of participants that they used. The authors discuss reducing the attack data into a 1:7 ratio of regular to malicious traffic entries. Data is processed by checking missing values and handling missing ones if present. We abstracted DDoS attack data from average traffic data and Trimmed attack = balanced dataset. Removes environment-specific attributes and Scales numeric features using min-max scaling. Protocols (categorical columns one-hot encoded) The deployed model eventually became a DNN model. ReLU activation function and feature columns were used based on the input layer. Multiple hidden layers: 20 nodes in the first and 12 in the second layers. <i>The model used for the testing -</i>	The dataset is generated by the lab and may not reflect an actual IoT network or attacks. This study may paint at most half the DDoS attack part and overlooks other types of IoT botnet attacks. Model developed on a single dataset (BoT-IoT), unclear how it would generalize to other datasets or real-world environments.
Study6	Idrissi, Idrissi; Boukabous, Mohammed; Azizi, Mostafa Moussaoui, Omar, Fadili, Hakim El	2021	Quantitative, Experimental	The proposed BotIDS model based on convolutional neural networks (CNN) achieved a very 99.94% and a low validation loss of 0.58%. Compared to other deep learning techniques like simple RNN, LSTM, and GRU, the CNN-based BotIDS model demonstrated superior classification performance. The prediction execution time of the BotIDS model was less than 0.34 ms.	The methodology introduced consisted of preprocessing the IoT traffic dataset, establishing and comparing deep learning models, and evaluating the performance regarding detecting different botnet attack types. The study used the following methods to collect data. The Bot-IoT dataset was explicitly developed for IoT systems by replicating the network environment at the university's Cyber Range Lab of UNSW Canberra Cyber, provided normal and malicious traffic data with six different attack types and ten attack subcategories. The original dataset contained 72 million records, but we used a 5% "full-feature" data sample of approximately 3.6 million records and a "10 best features" version. The sample size was not explicitly stated, but the dataset was a whole dataset of 3.6 million records. Moreover, it converted nominal data and IP addresses to numeric, merged the attack categories into single fields, implemented one-hot-encoding on attack categories, normalized the data, converted it into an image data shape, and split the data between 75% training and 25% testing. The model BotIDS, designed using a CNN-based approach, was developed and trained on 75% of the data and tested on the remaining 25%. Performances were evaluated by measuring validation accuracy, validation loss, and prediction execution time. BotIDS achieved 99.94% validation accuracy, 0.58% validation loss, and a prediction time of less than 0.34ms.	The study's bias in performance metric is a clear area for further investigation and improvement. The system's focus on accuracy as the primary evaluation benchmark, while neglecting the challenges of imbalanced datasets in cybersecurity applications, presents an opportunity for the field to evolve and improve.

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>