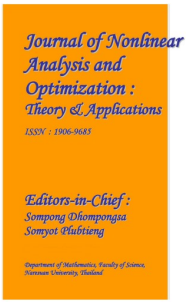
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Special Issue. 1, No.01 : 2024
ISSN :**1906-9685**



HYBRID DEEP LEARNING FOR BOTNET ATTACK DETECTION USING LSTM AND CNN

[1]Maligireddy Yashaswini, [2]Bhukya Rajesh, [3]Kathi Karthik,
[4]Vasikarla Bhavan Teja, [5] G.Venu Gopal Rao,[1,2,3,4]UG Scholar, Department of CSE (AI&ML)
[5]Assistant Professor, Department of CSE (AI&ML)
CMR Institute of Technology, Hyderabad, Telangana, India-501401

ABSTRACT

Cloud computing is perhaps the most enticing innovation in the present figuring situation. It gives an expense-effective arrangement by diminishing the enormous forthright expense of purchasing equipment foundations and processing power. Fog computing is an additional help to cloud infrastructure by utilizing a portion of the less-registered undertaking at the edge devices, reducing the end client's reaction time, such as IoT. However, most of the IoT devices are resource-constrained, and there are many devices that cyber attacks could target. Cyber-attacks such as bottleneck, Dos, DDoS, and botnets are still significant threats in the IoT environment. Botnets are currently the most significant threat on the internet. A set of infected systems connected online and directed by an adversary to carry out malicious actions without authorization or authentication is known as a botnet. A botnet can compromise the system and steal the data. It can also perform attacks, like Phishing, spamming, and more. To overcome the critical issue, we exhibit a novel botnet attack detection approach that could be utilized in fog computing situations to dispense with the attack using the programmable nature of the software-defined network (SDN) environment.We carefully tested the most recent dataset for our proposed technique, standard and extended performance evaluation measures, and current DL models. To further illustrate overall performance, our findings are cross-validated. The proposed method performs better than previous ones in correctly identifying 99.98% of multi-variant sophisticated bot attacks. Additionally, the time of our suggested method is 0.022(ms), indicating good speed efficiency results.

Keywords: Botnet Iot Attack, LSTM, CNN, Auto encoder.

http://doi.org/10.36893/JNAO.2024.V15I1N01.001-007

INTRODUCTION: To bring the expected result for Bot-Net attacks in the network devices a new develop dataset is applied. The dataset contains that normal traffic flows and several numerous of cyber-attacks traffic flows in botnets attacks. For the accurate traffic and for the develop effective dataset, the realistic test bed is used for to develop this dataset with the effective information features and also for the improvement of ML model performance and effective prediction model, mostly it were extracted and added it with the extracted features datasets. However, for the best results, the extracted features datasets are labelled as attack flow, categories, and subcategories. Nowadays, the Internet technology is growing up in day to day, and the varies devices are connected with this technology. By introducing this technology, daily life becomes more comfortable and well-organized. On the one side, these technologies are developing numerously but with this rapid development and popularization of internet devices causes the increasing number of cyber-attacks in the desktops is called the Bot-Net Attacks. Still it lacks the security in their internet connection software because most of them have not enough storage and computational resource for robust security mechanisms. In this project, it proposed a machine learning (ML) based botnet attack detection mechanism with sequential detection architecture. Its approach is adopted to implement a lightweight detection system with a high performance. Botnet is a network software bots designed to do malicious activities on the target network which are controlled using command and control protocol by the single unit is called the bot master. Bots are infected computers which is controlled remotely by bot master without any sign of being hacked and are used to perform malicious activities. Botnet size varies from small botnet to the large botnets where small botnet consists of few hundred bots and large botnets consists of 50,000 bots. Hackers can attack the system data without any noticeable indication of their presence. To secure these devices against botnet attacks, ML algorithms have been applied to develop Network Intrusion Detection Systems (NIDS). This NIDS can install at the strategic points within a network. Specifically, Deep Learning, an advanced ML approach, gives the unique capacity for automatic extraction of data from large-scale and high-speed network traffic integrated by interconnecting heterogeneous computer devices. Considering the resource constraints in these devices, NIDS techniques applied in classical networks devices which are not efficient for botnet detection in networks because of high computation and memory requirements. In order to produce an efficient Deep Learning method for botnet attack

detection in networks, large network traffic information is required to accept efficient classification performance. The processing and analysing the high-dimensional network traffic data can make the course of dimensionality. Also, training Deep Learning models with high-dimensional data can cause Hughes phenomena. High-dimensional of data process is complex and it requires huge computational resources and memory capacity. Some of the devices do not have sufficient space to store big network traffic data required for Deep Learning. Therefore, there is a need for end-to-end DL-based botnet detection method to reduce the high dimensionality of big network traffic and also detect the complexity and recent botnet attacks accurately based on low-dimensional network traffic information. Currently, Bot-Net dataset is the most relevant publicly available dataset for botnet attack detection in networks. The original feature dimensionality of the Bot-Net dataset is 43, and the memory space required for this network traffic data is 1.085 GB. So far, feature dimensionality reductions methods are applied to the Bot-Net dataset were all based on feature selection techniques.

RELEATED WORKS: Although several types of datasets are available in network intrusion detection. They have several challenges, like lack of reliable labels, redundancy of network traffic, low attack diversity, and missing ground truth. For instance, NSL-KDD and KDD Cup99 datasets are most popularly applied, but they are out dated, and they are not reflect the current normal and the attack scenarios. The usage of the DEFCON-8 dataset is limited because of low number of benign traffic models. These attack scenarios in UNIBS dataset are limited to DOS, Bot-Net dataset is the most related dataset which is publicly available for network devices botnet attack detection in the systems. To realise this dataset, an network test bed was set up to generate benign and malicious network traffic using heterogeneous communication protocols like User Datagram Protocol (UDP), Reverse Address Resolution Protocol (RARP), Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), Internet Protocol version6 ICMP (IPv6-ICMP) and Internet Group Management Protocol (IGMP). The test bed setup comprised a variety of IOT devices, including a weather station, smart fridge, remotely-activated garage door and smart thermostat. Also, millions of botnet attack traffic samples were included in Bot-Net. These attack traffic samples can be categorized into four IOT botnet scenarios, namely: DDOS, DOS and information theft. To ensure a fair comparison, feature dimensionality reduction methods that do not include benign network

traffic traces and all the four botnet attack scenarios in the Bot-IOT dataset were not included in this paper. For instance, did not consider the DOS attack scenario. Also, the performance of the method in detecting benign network traffic was not reported. In a similar work, the authors did not evaluate the procedure of the proposed method. In another work did not evaluate the procedure of the proposed method with the network traffic data in the BOTNET dataset. In summary, the state-of-the-art methods in the related work focused on the selection of specific features from available network traffic information available in the Bot-IOT dataset. However, this approach may likely affect the efficiency of botnet attack detection in IOT networks because the classifiers will not have access to some relevant network information during training, validation, and testing. Consequently, the feature selection approach may lead to low botnet attack detection accuracy and a high false alarm rate in IOT networks. On the other hand, LAE decreases the dimensionality of big IOT network traffic data and produces a low-dimensional latent space feature representation at the hidden layer without losing useful intrinsic network information.

EXISTING SYSTEM

Several researchers are focusing on detecting botnet attacks these days [28]_[30]. The main requirement in botnet detection is identifying the infected devices before they can exploit the network by initiating malicious activity. Authors propose numerous methods that claim to secure the network against botnet attacks. These approaches focus on anomaly detection schemes using artificial intelligence, primarily ML and DL algorithms. In various research approaches, authors [21]_[23] used ML and hybrid ML techniques for botnet detection such as BayesNet (BN), Support Vector Machine (SVM), J48, Decision Tree (DT), and Naive Bayes (NB). Furthermore, Machine Learning methods are categorized as the supervised, the unsupervised, or the semi-supervised learning.

Parakash *et al.* performed experiments using three well-known machine learning algorithms to detect DDoS packets: K-Nearest Neighbors algorithm (KNN), SVM, and NB. The findings show that the KNN performs better in detecting DDoS attacks having 97% accuracy, while SVM and NB algorithms achieve 82% and 83% accuracy, respectively [33]. In [34], the authors proposed a detection scheme that uses the SVM algorithm with their own proposed idle timeout adjustment algorithm (IA). They demonstrated the way their proposed methodology outperforms and achieves better results. In another work, [35] uses, NB, SVM and neural network. Results show that the neural network

and NB models performed outclass and achieved 100% accuracy, while the SVM model was at 95% accuracy. Ye *et al.* [36] also used the SVM algorithm and achieved an average accuracy of 95.24%. In [37], authors performed experiments using various algorithms such as Naive Bayesian and decision tree classifier algorithms. They achieved a 99.6% detection accuracy rate. DL algorithms are the subset of ML. That can deal with large datasets and unstructured data. ML algorithms do not provide better results for extensive data produced by IoT devices and unstructured data [38]. Hence DL algorithms are preferable for IoT compared to traditional ML algorithms such as KNN, SVM, NB, and others. Different DL and hybrid DL approaches are applied for detecting various kinds of malware in IoT devices [39]_[41]. In [42], the authors described a technique for defending the IoT environment against malware and cyber attacks, such as DDoS, brute force, bot, and infiltration. This strategy makes use of DL in SDN.

DISADVANTAGES

- An existing system is not hybrid deep learning detection policy to improve the efficiency and effectiveness of the SDN-based fog computing architecture. Results show that the proposed scheme works better and provides a better detection rate.
- can't customize the policies and applications dues to its programmable nature.

PROPOSED SYSTEM

- The system suggests an efficient deep learning framework for detecting Botnet attacks in an SDN-based fog computing environment.
- The practical experiment is performed on N_BaIoT Dataset, which comprises both Botnet attack and benign samples.
- The proposed technique is evaluated against well-known performance evaluation metrics of the machine and deep learning algorithms known as precision, F1-score, recall, accuracy, and so forth.
- For unbiased results, we also applied the technique of 10-fold-cross-validation.

ADVANTAGES

System can manage the secure connection for thousands of devices connected over the fog for data transmission.

System can provide real-time monitoring and awareness with low latency.

System can dynamically balance the load with its flexible architecture.

CONCLUSION: This system was proposed for efficient botnet detection in networks using deep learning algorithms such as LSTM and CNN. The effectiveness of this method was validated by performing extensive experiments with the most relevant publicly available dataset in binary and multi-class classification scenarios. By using this CNN the result will get more accurate and precision also comparing to the LSTM.

REFERENCES:

1. A. O. Akmandor, Y. Hongxu, and N. K. Jha, "Smart, secure, yet energyefficient, internet-of-things sensors," IEEE Transactions on Multi-Scale Computing Systems, vol. 4, no. 4, pp. 914–930, 2018.

2. D. E. Denning, "An intrusion-detection model," IEEE Transactions on software engineering, no. 2, pp. 222–232, 1987.

3. J. Qiu, L. Du, D. Zhang, S. Su, and Z. Tian, "Nei-tte: Intelligent traffic time estimation based on fine-grained time derivation of road segments for smart city," IEEE Transactions on Industrial Informatics, 2019

4. J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," IEEE Internet of Things Journal, 2020

5. X.-G. Luo, H.-B. Zhang, Z.-L. Zhang, Y. Yu, and K. Li, "A new framework of intelligent public transportation system based on the internet of things," IEEE Access, vol. 7, pp. 55 290–55 304, 2019.

6. Z. Tian, X. Gao, S. Su, and J. Qiu, "Vcash: A novel reputation framework for identifying denial of traffic service in internet of connected vehicles," IEEE Internet of Things Journal, vol. 7, no. 5, pp. 3901– 3909, May 2020.

1. M.Ganga Eswari, D.Vijayasekar, and, S.Dhanalakshmi,, "Criminal Identification Using Biometric Traits in Image Processing", International Journal of Applied Engineering Research Technology(IJAER), ISSN 0973-4562 Vol. 10 No.85 (2015), October 2015,PP 265-268 (SCOPUS/Annexure-II Journals)

2. D.Vijayasekar, S.Dhivya, and S.Dhanalakshmi, "Wiener Filter Operation on Blurred Images", International Journal of Applied Engineering Research Technology(IJAER), ISSN 0973-4562 Vol. 10 No.85 (2015), October 2015,PP 197-200 (SCOPUS/Annexure-II Journals)

3. Shiva Prasanth.A, and S.Dhanalakshmi,, "Automated Testing Tools for Different Coverage Metrics", International Journal of Advanced Innovative Research (IJAIR), Volume 5, Issue 10, ISSN: 2278-7844, October 2016, PP 120-123

4. K.Sindhu, and S.Dhanalakshmi,, "Disclosure of Malevolent in MANET: A Survey", International Journal of Research in Technological Studies(IJRTS),Volume 4,Issue 1,ISSN:2348-1439,December 2016,PP 31-34 (SCOPUS/Annexure-II Journals)

18. S. M. Babu, P. P. Kumar, B. S. Devi, K. P. Reddy, M. Satish and A. Prakash, "Enhancing Efficiency and Productivity: IoT in Industrial Manufacturing," *2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA)*, Hamburg, Germany, 2023, pp. 693-697, doi: 10.1109/ICCCMLA58983.2023.10346807.
19. Prakash, S. M. Babu, P. P. Kumar, S. Devi, K. P. Reddy and M. Satish, "Predicting Consumer Behaviour with Artificial Intelligence," 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA), Hamburg, Germany, 2023, pp. 698-703, doi: 10.1109/ICCCMLA58983.2023.10346660.

1.Kumbala Pradeep Reddy; Sarangam Kodati; Thotakura Veeranna; G. Ravi, "6 Machine Learning-Based Intelligent Video Analytics Design Using Depth Intra Coding," in Big Data Management in Sensing: Applications in AI and IoT , River Publishers, 2021, pp.77-86.