ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 3, 2024

A HYBRID DEEP LEARNING APPROACH FOR BOTTLE NECK DETECTION IN IOT

[1] K VENKATESH, [2]P.PAVAN KUMAR

(Assistant Professor), MSC, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

[2]MSC, scholar, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

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.

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

1.INTRODUCTION

One of the most significant issues for the network system to be efficient and reliable while doing transactions over the IoT is security [1]. The tremendous growth of IoT in different fields, i.e., surveillance, healthcare, transportation, manufacturing industry, education, and others, encourages securing IoT infrastructure to improve its performance. Earlier IoT devices generate data through various types of sensors, and it becomes tidy for the cloud servers to handle or process these transactions efficiently. Fog computing is among the newly proposed schemes that could be utilized to add preferred features to the IoT infrastructure [2]. Fog computing is competent in doing some regional analysis of information [3] before communicating the aggregated data to the cloud server. It helps in keeping the latency constraints in some time compelled real-time issues, making them appropriate for IoT-based applications such as vehicular ad-hoc networks (VANETs) [4]_[11]. These advancements towards using fog servers in IoT infrastructure motivate the adversaries to target the fog server with malicious intent to lower its performance. Hence, security and protection of the system are among the major issues that can affect the performance of fog computing [12]. In this regard, availability is among the core security requirements for offering services to the actual customer applications according to their interest. However, this is constantly tested by the adversaries by launching different types of attacks, such as DoS or DDoS attacks [13]. An individual or a group can perform these attacks. If a group performs it, it is named ``botnet,'' while if an individual launches it, it is known as ``bot-master.'' [14]. The bot-master is the attacker node that can launch several types of attacks on the server, such as Phishing, spam, Click fraud, and others. A command-and-control channel remotely controls a botnet. The command-and-control channel is a system the adversary uses to control by sending messages and commands to a compromised system. The adversary can steal the data through these commands and manipulate the infected network [8]. In a botnet attack, some `n' number of compromised nodes are controlled by a bot-master, and they launch an attack on the server from different compromised systems.

In the fog computing paradigm security is still challenging task, and various security schemes are proposed to make it resilient against vulnerabilities. However, most of the schemes focus on flexibility and continuous monitoring of the fog server. Software-denied networking (SDN) is used at fog servers to address flexibility, and continuous monitoring issues [15]. SDN is an emerging networking paradigm that assists in making the network more flexible that can help in managing the network, analyzing the traffic, and assisting in the routing control architectures [16], [17] as there is a separate control plan that provides a flexible device management policy. Hence, an SDN-based fog computing environment provides centralized control to the fog computing system. The characteristics of the SDN based fog computing system are discussed below V

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

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

_ SDN can dynamically balance the load with its flexible architecture. _ SDN can customize the policies and applications dues to its programmable nature. [18]

The software-denied network plays a vital role as its network control architecture can be directly programmable through the command requests. SDN based fog computing architecture can assist in analyzing and managing IoT devices. The motivation behind SDN is to give consistency to network management through partitioning the network into the data plane and the control plane. SDN can add programmability, adaptability, and versatility to the fog computing system. In high-speed networks, discovering the botnet attack is a significant concern [19]. The proposed work shows the methodology through which the botnet attack is identified with a high detection rate which can be used in SDN to enhance the security of fog computing. Deep learning (DL) based detection approach in the SDN-based fog computing application can be a better counterattack to improve the overall performance of the system [20]. DL strategy is adaptable to conditions to recognize the abnormal behavior of the network. We proposed a hybrid deep learning detection policy to improve the efciency and effectiveness of the SDN-based fog computing architecture. Results show that the proposed scheme works better and provides a better detection rate.

2. 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.

3. 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 canprovide real-time monitoring and awareness with low latency.

System can dynamically balance the load with its flexible architecture.

4. OUTPUTSCREENS

5. CONCLUSION

SDN-based fog computing architectures are the trending networking paradigms for several applications based on the IoT infrastructure. Fog computing systems are vulnerable to various types of Botnet attacks. Hence, there is a need to integrate a security framework that empowers the SDN to monitor the network anomalies against the Botnet attacks. DL algorithms are considered more effective for the IoT-based infrastructures that work on unstructured and large amounts of data. DL based intrusion detection schemes can detect Botnet attacks in the SDN-enabled fog computing IoT system.

We created a framework that utilizes a hybrid DL detection scheme to identify the IoT botnet attacks. It is trained against the dataset that contains normal and malicious data, and then we used this framework to identify botnet attacks that targeted different IoT devices. Our methodology comprises a botnet dataset, a botnet training paradigm, and a botnet detection paradigm.

Our botnet dataset was built using the N_BaIoT dataset, which was produced by driving botnet attacks from the Gafgyt and Mirai botnets into six distinct types of IoT devices. Five attack types, including UDP, TCP, and ACK, are included in both Gafgyt and Mirai attacks. We developed a botnet detection based on three hybrid models_ DNN-LSTM, CNN2D-LSTM, and CNN2D-CNN3D. Using this training model as a foundation, we developed a botnet detection paradigm that can recognise significant botnet attacks. The botnet detection approach is part of a multiclass classification model that can distinguish between the sub-attacks and innocuous data. The fact-finding analysis showed that our hybrid framework DNN-LSTM model had the highest accuracy of 99.98% at identifying the gafgyt and Mirai botnets in the N_BaIoT environment. In 2014 and 2016, the gafgyt

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT
ISSN2454-9940
www.ijasem.org
Vol 18, Issue 3, 2024

and Mirai botnets essentially targeted home routers and IP cameras. The NBaIoT dataset we used for our experiments revealed that rather than the type of IoT devices, the type of training models has a more significant impact on botnet detection performance. We think creating DNN-LSTM-based IoT botnet detection models would be an
excellent strategy to enhance botnet identification for different IoT devices.

In the future, we have in mind to compare the performance of the proposed hybrid algorithm to that of other IoT datasets with a more considerable number of nodes. Further, there is a need to test more combinations of DL algorithms and traditional machine learning algorithms.

SDN-based fog computing architectures are the trending networking paradigms for several applications based on the IoT infrastructure. Fog computing systems are vulnerable to various types of Botnet attacks. Hence, there is a need tointegrate a security framework that empowers the SDN to monitor the network anomalies against the Botnet attacks. DL algorithms are considered more effective for the IoT-based infrastructures that work on unstructured and large amounts of data. DL based intrusion detection schemes can detect Botnet attacks in the SDN-enabled fog computing IoT system.

We created a framework that utilizes a hybrid DL detection scheme to identify the IoT botnet attacks. It is trained against the dataset that contains normal and malicious data, and then we used this framework to identify botnet attacks that targeted different IoT devices. Our methodology comprises a botnet dataset, a botnet training paradigm, and a botnet detection paradigm.

Our botnet dataset was built using the N_BaIoT dataset, which was produced by driving botnet attacks from the Gafgyt and Mirai botnets into six distinct types of IoT devices. Five attack types, including UDP, TCP, and ACK, are included in both Gafgyt and Mirai attacks. We developed a botnet detection based on three hybrid models_ DNN-LSTM, CNN2D-LSTM, and CNN2D-CNN3D. Using this training model as a foundation, we developed a botnet detection paradigm that can recognise significant botnet attacks. The botnet detection approach is part of a multiclass classification model that can distinguish between the sub-attacks and innocuous data. The fact-finding analysis showed that our hybrid framework DNN-LSTM model had the highest accuracy of 99.98% at identifying the gafgyt and Mirai botnets in the N_BaIoT environment. In 2014 and 2016, the gafgyt and Mirai botnets essentially targeted home routers and IP cameras. The NBaIoT dataset we used for our experiments revealed that rather than the type of IoT devices, the type of training models has a more significant impact on botnet detection performance. We think creating DNN-LSTM-based IoT botnet detection models would be an excellent strategy to enhance botnet identification for different IoT devices.

In the future, we have in mind to compare the performance of the proposed hybrid algorithm to that of other IoT datasets with a more considerable number of nodes. Further, there is a need to test more combinations of DL algorithms and traditional machine learning algorithms.

6. REFERENCE

[1] Z. Hussain, A. Akhunzada, J. Iqbal, I. Bibi, and A. Gani, ``Secure IIoTenabled industry 4.0," *Sustainability*, vol. 13, no. 22, p. 12384, Nov. 2021.

[2] R. K. Barik, H. Dubey, K. Mankodiya, S. A. Sasane, and C. Misra, ``Geo-Fog4Health: A fog-based SDI framework for geospatial health big data analysis," *J. Ambient Intell. Hum. Comput.*, vol. 10, no. 2, pp. 551_567, Feb. 2019.

[3] S. Khan, S. Parkinson, and Y. Qin, ``Fog computing security: A review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, pp. 1_22, Dec. 2017.

[4] J. Malik, A. Akhunzada, I. Bibi, M. Talha, M. A. Jan, and M. Usman, ``Security-aware data-driven intelligent transportation systems," *IEEE Sensors J.*, vol. 21, no. 14, pp. 15859_15866, Jul. 2021.

[5] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, ``A cooperative quality-aware service access system for social internet of vehicles," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2506_2517, Aug. 2018.

[6] X. Wang, Z. Ning, M. C. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, ``Privacy-preserving content dissemination for vehicular social networks:

Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1314_1345, 2nd Quart., 2019.

[7] Z. Ning, Y. Li, P. Dong, X. Wang, M. S. Obaidat, X. Hu, L. Guo, Y. Guo, J. Huang, and B. Hu, ``When deep reinforcement learning meets 5Genabled vehicular networks: A distributed of_oading framework for traf_c big data," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1352_1361, Feb. 2020.

[8] X.Wang, Z. Ning, and L.Wang, ``Of_oading in internet of vehicles: A fogenabled real-time traf_c management system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4568_4578, Oct. 2018.

[9] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya, ``Fog data: Enhancing telehealth big data through fog computing," in *Proc. ASE BigDataSocialinform.*, 2015, pp. 1_6.

[10] W. U. Khan, T. N. Nguyen, F. Jameel, M. A. Jamshed, H. Pervaiz, M. A. Javed, and R. Jäntti, ``Learning-based resource allocation for backscatter-aided vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, early access, Nov. 18, 2021, doi: 10.1109/TITS.2021.3126766.