AN APPROACH BASED ON HYBRID DEEP LEARNING TO IDENTIFY BOTTLENECKS IN THE INTERNET OF THINGS

[1]IPPALAPALLI VENKATA NARASIMHA,[2]H.MADHUSUDHANA RAO

[1]Student,[2]Assistant professor MCA,M.Phill,(Ph.D)

Department of CSE

ABSTRACT:

Computing in the cloud is now regarded as one of the most fascinating developments in the field of information technology.

It provides a cost-effective solution by lowering the massive upfront costs of acquiring equipment foundations and processing power. This results in the creation of a more cost-effective arrangement. The term "fog computing" refers to an extra kind of assistance that may be provided to cloud infrastructure in the form of the utilisation of a part of the less-registered task carried out at the edge devices. This helps to decrease the response time required by the end client for services such as IoT. However, the majority of IoT devices have limited access to resources, and there are a large number of devices that might be targeted by cyberattacks. The Internet of Things (IoT) ecosystem is still vulnerable to severe dangers posed by cyberattacks such as bottleneck, DoS, DDoS, and botnets. The greatest major risk that presently exists on the internet is posed by botnets. A botnet is a network of infected computers that are commanded by an adversary to carry out harmful activities without the need for authorisation or authentication. These computers are linked to the internet. The system may be compromised by a botnet, which would then take the data.

It is also capable of launching attacks such as spamming, phishing, and others. We provide a fresh method for the detection of botnet attacks that is capable of being implemented in fog computing scenarios. This method makes use of the customizable character of an environment that is defined by software-defined networks (SDN), which enables it to circumvent the threat posed by the major problem. We gave our suggested method, conventional as well as extended performance assessment metrics, and the most recent DL models a thorough workout on the most recent dataset. Cross-validation is used to our results to provide a clearer picture of the overall performance.

The newly suggested approach is superior to those that came before it in terms of its ability to accurately detect 99.98% of multi-variant sophisticated bot assaults. In addition, the time taken by our recommended approach is 0.022 milliseconds, which indicates excellent outcomes in terms of speed and efficiency.

INDEX TERMS Intrusion detection, fog security, software-defined networks, deep learning, the Internet of Things, and botnets.

I.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-defined 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:

- 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-defined 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 efficiency and effectiveness of the SDN-based fog computing architecture. Results show that the proposed scheme works better and provides a better detection rate.

A. RESEARCH CONTRIBUTIONS

The research contribution includes the comprehensive evaluation of botnet attacks for different IoT devices and evolving cyber threats in IoT using the dataset N_BaIoT 2018. Our proposed hybrid technique comprises two DL algorithms: DNN and LSTM. We rigorously evaluate the proposed mechanism with standard performance metrics (i.e., Recall, Accuracy, F1-Score, Precision, AU-ROC, etc.). The presented hybrid scheme results show better detection accuracy with low computational complexity. The contributions of this research work are as given below:

- We suggest 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.

The paper’s organization is as follows; section II introduces related literature. Section III shows the security issues in Fog computing. Section IV provides information about Deep Learning and its algorithms. Section V details our proposed system and the methodology used for detection and experimentation, such as Dataset, detection phase, evaluation phase, and experiment. While Section VI comprises the experimental results and our assessment results. Finally, section VII provides the conclusion and defines the future map.

II.LITERATURE SURVEY:

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. ML algorithms face challenges like scalability, learning from massive data, and low-value density data. To convert big data into usable intelligence in the face of an ever-growing big data universe, ML must develop and improve. Massive data is developing exponentially, so ML must develop and evolve to turn big data into valuable insight. 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. They used the CICIDS2018 dataset for the evaluation of the presented scheme. The proposed model achieved 99.87% accuracy, 0.0554% FPR, with a testing time of only 18.9ms. Likewise, in [43], using two-way LSTM to implement DL for evaluation demonstrates a new method for packet-level inspection on the IoT and networks. The authors utilized Mirai and normal IoT traffic generated in this paper for experiments. Consequently, the authors of [44] used SDN to deploy an detection mechanism system to safeguard the IoT and showed a testing success rate with 95% accuracy. They considered the KDD99 dataset for attack detection using the Restricted Boltzmann Machine for DoS, login, and Probe (RBM). Moreover, in [45], authors considered a hybrid model consisting of CNN and RNN. The proposed solution is based on network flow attributes. They applied the proposed model to two datasets, i.e., CTU13 and ISOT. These combined datasets form two classes, i.e., botnets and benign. The author of [16] offered an IoT based work that acknowledges the effectiveness of a DL-based algorithm (LSTM) for botnet attack detection. The study used data from various IoT devices from the N IoT 2018 dataset, which had a 99.90% detection rate. DL approaches are helpful for intrusion detection in SDN-based architectures [20], [46] [47]. DL methods are applied to identify botnet attacks in non-

SDN infrastructures [48] while requiring more research to analyze the feasibility and efficacy of using DL (CNN, RNN, and LSTM) algorithms to detect and mitigate botnet attacks on SDN controllers.The studies show that to effectively defend the system against newly developing threats, a centralised mechanism and intelligence are still needed. The accuracy of botnet malware detection varies for different algorithms applied to different datasets. In Table 2, several ML or DL based detection schemes are presented. It shows that the selected research area is among the emerging research trends in the field of IoT security. There is ongoing research in this area using different datasets [49]. As per our findings, a thorough study of the DL hybrid combinations is required to explore the possibility of increasing the accuracy and precision in the detection of botnet attacks such that it further achieves lower FPR in consuming less time. Hence, we tested various combinations of DL algorithms in our research work and concluded that the hybrid deep learning algorithm uses DNN [50] and LSTM [51] is effective. It also produces better outcomes compared to other strategies that have been suggested. Additionally, it completely pinpoints sophisticated and devastating multi-attacks in the IoT environment.

Edge computing, IoT, and Industry 4.0 have advanced and developed quickly in recent years. Recently, there have been many cloud-based service providers (Cisco, VMware, IBM, Juniper, Big Switch Networks, Versa Networks, Colt Technology, and Lumina SDN) who have shifted from the traditional network paradigm towards Software-Defined Fog (SD-FoG) [52]. The fog server is the fundamental part of the system as it holds critical information related to IoT devices, accumulating and storing the client’s data. The basic architecture of the fog paradigm is depicted in Figure 1, representing edge devices connected with fog servers for communication. Numerous distributed fog and edge servers are deployed to offer services over the network to millions of consumers, whereas; the fog servers are connected to cloud servers. The openness and accessibility of the network assets through these devices make fog computing vulnerable. Fog computing has created a new security conundrum due to its significant distribution properties, heterogeneity, mobility, and restricted resources. Because of its limited computing capability, the Fog would struggle to implement a comprehensive security solution to detect and prevent attacks.

III.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 and Mirai botnets essentially targeted home routers and IP cameras. The N_BaIoT 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.

REFERENCES

[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, ‘‘GeoFog4Health: 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 offloading framework for traffic big data,’’ IEEE Trans. Ind. Informat., vol. 16, no. 2, pp. 1352–1361, Feb. 2020. [8] X. Wang, Z. Ning, and L. Wang, ‘‘Offloading in internet of vehicles: A fogenabled real-time traffic 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 BigData Socialinform., 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.