International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 328-331 www.ijaem.net ISSN: 2395-5252

Classification of Network Cyber Attack in Fog Layer Using Machine Learning

Ms. Snehal Devidas Wahane, Dr. R. R. Keole
Department OF Computer Science and Engineering HVPM COET Amravati, India.
Associate Professor & HEAD Department OF Information Technology and Engineering HVPM COET Amravati, India.

Submitted: 15-04-2021 Revised: 28-04-2021 Accepted: 30-04-2021

ABSTRACT: Attack and Anomaly detection in Internet of Things (IoT) Instruction is raising concern in the domain of Internet of Things (IoT) ,The now days daily network traffic in a smart city via loT systems is increasing new cybersecurity challenges to connection IoT devices are being connected to the sensors or actuator that are directly connected to massive cloud servers.
The developers need to enhance new techniques for infected loT devices. Machine learning models have been compared to predicts attacks and anomalies on the IoT system accurately. In this proposed research work, to address the loT cyber security threats, An Anomaly Detection loT (AD-IoT) system is used, which is intelligent anomaly detection based on machine learning algorithm.
Keywords: AD - Anomaly Detection, IoT - in Internet of Things, IDS-, Intrusion Detection Systems, NIDS- Network Based Instruction Detection Systems.

I. INTRODUCTION:

The Internet of Things (IoT). Automated network system , the IoT is an umbrella term, covering a multitude of devices and technologies that have both Internet capabilities, and serve some primary function, such as: home automation, including smart air conditioning system, smart fridge, smart oven and smart lamps, etc. Smart devices are gaining popularity in our homes that also make our life more easy and comfortable , the increased deployment of such smart devices brings an increase in potential security risks. In recent years, massive use of IOT devices can complex the IOT network. However, the number of loT devices over heterogeneous variety types of services, technologies, devices, and protocols (e.g. Wireless, Wired, Satellite, cellular, Bluetooth, etc.) leads to the complexity of managing future IoT networks.

Therefore, this integration protocol with the internet leaves serious cybersecurity threats and vulnerabilities for attacking the information of the daily activities of citizen's lives. These cyber threats can obtain unauthorized access to the IoT devices without the knowledge of either the eligible user or administrator (e.g. Miria botnet) and due to this the fog layer is introduced. Fog layer is used to reduce the energy consumption, latency and storage. The AD-IoT system is designed to monitor all IoT traffic in a distributed fog layer and alert the administrator or service provider.

II. LITERATURE REVIEW AND RELATED WORK

- **Security Issues, Challenges,and Open Problems in the Internet of Things:**

In conclusion, they believe this survey may provide an important contribution to the research community, by documenting the current security status of this very dynamic area of researchand motivating researchers interested in developing new schemes to address security in the context of the Internet of Things.
M. M. Hossain, M. Fotouhi, and R. Hasan,[1] A survey has been done in the most important security aspects of the Internet of Things with emphasis on what is being done and what are the issues that require further research. Their work explores the overall security architecture of IoT followed by security issues related to interoperability of heterogeneous objects.

- **Attack Detection in Fog-to-Things Computing:**

T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho,[2] In this paper, they have implemented a deep learning algorithm for detecting network intrusion and evaluated their NIDS model. Although the results are not yet good enough to be adopted in any commercial product or an alternative solution for signature-based IDS, the approach still has significant potential land advantages for further development. By comparing the results with those of other classifiers, we have shown the potential of using deep learning for the flow-based anomaly detection system. In the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 328-331 www.ijaem.net ISSN: 2395-5252

context of the SDN environment, the deep learning approach also has potential.

This is attributed to the centralized nature of the controller and the flexible structure of SDN. The basic information about network traffic can be extracted easily by the controller an evaluated by the deep learning intrusion detection module. To improve the accuracy, they will analyze the traffic and propose other types of features. With the flexibility of the SDN structure, they can extract many features that contain more valuable information or focus on one specific type of attack, like DDoS, to increase the accuracy of the NIDS. They will also try to adjust our DNN model for better performance (e.g., varying the number of hidden layers and hidden neurons).

Abeshu and N. Chilarnkurti [3], proposed a distributed deep-learning-driven fog-to-things computing attack detection scheme using publicly available NSL-KDD dataset. A pretrained stacked autoencoder has been employed in feature engineering, while softmax was used for classification. To compare our model with shallow algorithms, metrics such as accuracy, DR, and ROC curve have been used for system evaluation, and accuracies over varied worker nodes are considered for scalability measure.

The authors propose a novel distributed deep learning scheme of cyber-attack detection in Fog-to-things Computing. Their experiments have shown that deep models are superior to shallow models in detection accuracy, false alarm rate, and scalability.

- **Intrusion Detection in Internet of Things:**

B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, [4] Internet of Things (IoT) is a new paradigm that integrates the Internet and physical objects belonging to different domains such as home automation, industrial process, human health and environmental monitoring. It deepens the presence of Internet connected devices in our daily activities, bringing, in addition to many benefits, challenges related to security issues. For more than two decades, Intrusion Detection Systems (IDS) have been an important tool for the protection of networks and information systems.

In this paper, they presented a survey about IDS research efforts for IoT.They proposed a taxonomy to classify these papers, which is based on the following attributes: detection method, IDS placement strategy,security threat, and validation strategy. They observed that the research of IDS schemesfor IoT is still incipient. The proposed solutions do not cover a wide range of attacksand IoT technologies. Moreover, it is not clear which detection method and placementstrategies are more adequate for IoT systems. Finally, validation strategies are not wellconsolidated.

- **Analysis of Problem.**

IoT devices have been growing exponentially with multiple heterogeneous devices. This leads to increase IoT vulnerabilities to serve attack vectors that can target the IoT victims and use them to steal personal information or launch an attack over a network.

Proposed Work and Objectives.

1. To increase or improve a security over a network.
2. To study different type of cyberattacks.
3. To study machine learning algorithm for Cyberattacks Classification.

In Smart city architecture, based on the advantage of fog computing to reduce the latency between cloud and IoT sensor. It comprises of three layers that include application layer, fog layer and IoT sensor layer. The Fog layer is a major component of the smart city architecture, which ensures processing and aggregation of the data.

AD-IoT system promises to intelligently detect zero-attacks and IoT botnets in distributing detection in the fog layer. This AD-IoT system design model is supposed to consist of several components involving a massive amount of IoT devices connected to distributed fog network privately or publicly in a smart city. Detecting from this intelligent model distributed at each fog node, it should detect the new attacks to alert the cloud server management. AD-IoT Security Gateway IDS System is placed on a master fog node that can intelligently monitor the communication among the network traffic data. AD-IoT system is based on the ensemble methods, which are used to improve the performance of algorithm in system model.

Desired Implications

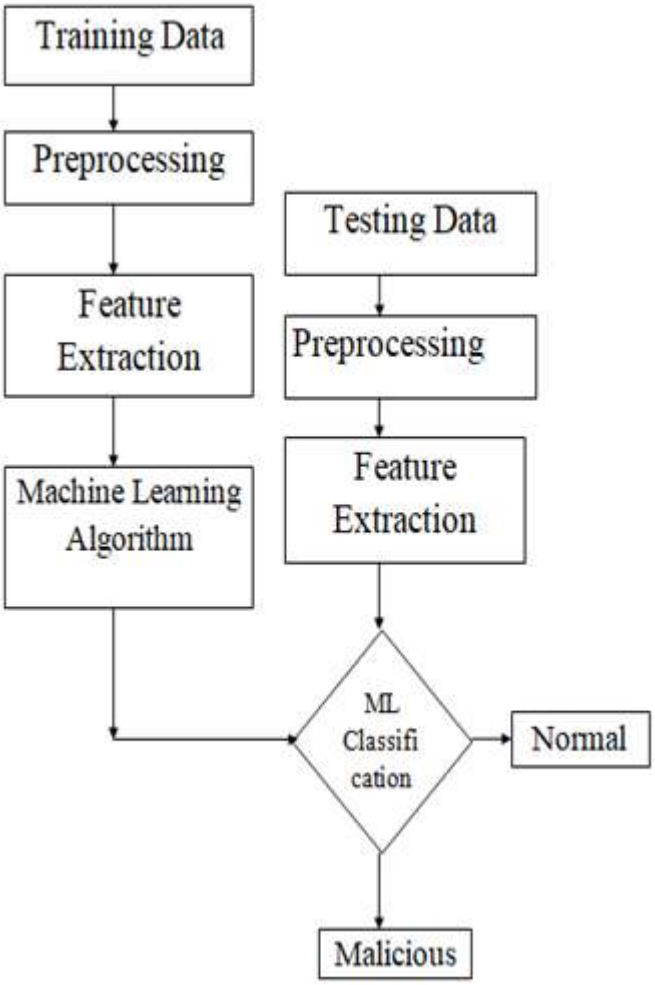
Cyberattacks can find the vulnerable IoT devices either in private or public networks. NIDS can utilize machine learning algorithm (e.g. Random Forest, SVM, Perceptron, etc)to classify and detect malicious behavior in the IoT fog network. This can be done by applying the NIDS system through use of the anomaly detection method based on the machine learning algorithms, which uses statistical analysis to clean and prepare data for an intelligently predictive model.

Thus, AD-IoT approach can enhance the performance for effectively detecting the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 328-331 www.ijaem.net ISSN: 2395-5252

cyberattacks in fog node in smart city, rather than detecting in the cloud layer, which guarantee a lightweight feature, less latency, and lower consumption than the cloud layer, which has a massive amount of data in a big infrastructure smart city.

Fig: Working Diagram:



REFERENCES

[1]. M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21-28.

[2]. T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," in Wireless Networks and Mobile Communications (WINCOM), 2016 International Conference on. IEEE, 2016, pp. 258-263.

[3]. A. Abeshu and N. Chilarnkurti, "Deep learning: the frontier for distributed attack detection in fog-to-things computing," IEEE CommunicationsMagazine, vol. 56, no. 2, pp. 169-175, 2018.

[4]. B. B. Zarpelao, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things;' Journal of Networkand Computer Applications, vol. 84, pp. 25-37, 2017.

[5]. M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home iot using openflow," in Availability, Reliability and Security (ARES), 2016 11th InternationalConference on. IEEE, 2016, pp. 147-156.

[6]. M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19-31,

2016. [l] J. Howell. Number of connected iot devices will surge to 125 billion by 2030, ihs markit says - ihs technology. [Online]. Available: https://technology.ihs.com/596542/, last accessed: 11/07/2018.

[7]. S. Prabavathy, K. Sundarakantham, and S. M. Shalinie, "Design of cognitive fog computing for intrusion detection in internet of things," Journal of Communications and Networks, vol. 20, no. 3, pp. 291-298, 2018.

[8]. N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 data set," Information Security Journal: A GlobalPerspective, vol. 25, no. 1-3, pp. 18-31, 2016.