Review on Deep Learning Based IoT Intrusion Detection System

Rajeswari Somasundaram and P Karthikeyan

February 1, 2022

REVIEW ON DEEP BASED IOT INTRUSION DETECTION SYSTEM

ABSTRACT

One of the goals of smart environments is to improve human life quality in terms of comfort and efficiency. The Internet of Things (IoT) standard has lately evolved into a smart environment technology. The key concerns in any real-world smart environment based on the IoT prototype are security and privacy. Security flaws in IoT-based systems could lead to security concerns infecting smart environment applications. As a result, there is a substantial need for IoT-specific intrusion detection systems (IDSs) to prevent IoT-related security threats that exploit only a handful of these security flaws. Traditional IDSs may not be a solution for IoT environments due to the restricted computation and storage capabilities of IoT devices, as well as the protocols employed. The increased awareness of vulnerabilities and associated attack pathways has an impact on a number of security goals. The major goal is to construct three abstraction levels of features, namely packet-based, unidirectional-based, and bidirectional-based features, that are determined. The evaluation process is carried out using a MQTT simulated dataset. The experimental findings indicated that ML models are capable of meeting the ID needs of MQTT-based networks.

INTRODUCTION

The Internet of Things (IoT) is a network of physical objects with sensors, software, and communication that can communicate with other networked devices over the internet. Because of the pervasive nature of these devices and the ease with which they can be monitored and controlled from afar, there has been a rapid development in the creation of a variety of novel applications in a variety of domains, including smart home devices, wearable devices, health monitoring devices, connected industrial and manufacturing sensors and equipment, energy management devices, and so on. The security of devices and the protection of data from cyberattacks are major concerns in IoT systems.

Cyberattacks are the deliberate exploitation or illegal access to another person's or organization's information or infrastructure. Due to the heterogeneity of devices and protocols, as well as direct internet exposure, protecting IoT devices from assaults is difficult. Sensors in smart surroundings work together to carry out functions. Smart environments can be extended with the use of wireless sensors, wireless communication systems, and IPv6. Smart cities and smart homes, as well as smart healthcare and smart services, are examples of such environments. Smart items become more effective when IoT systems and smart surroundings are combined. IoT systems, on the other hand, are vulnerable to a variety of security threats, including denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. IoT services and smart environment applications in an IoT network might be severely harmed by such attacks. Because IoT communication protocols and technologies differ from those used in traditional IT, their security solutions should as well. Despite several endeavours in this sector, many obstacles and research concerns remain open, according to a review of a wide range of scholarly publications.

LITERATURE REVIEW

Most of the research papers have represented the work of various machine learning based algorithms are used in movie recommendation systems, most of the research involved K-Nearest Neighbourhood (KNN) and the Deep Learning algorithms, King et al, developed that there is still a lack of a comprehensive and cohesive perspective to ensure IoT security. The study looked at multinational projects in the field and found that most of them are focused on building and executing IoT-specific applications. Machine learning algorithms are acceptable because they are adapted in various applications such as data classification.

Reduction strategies proposed for IT networks are not suitable for IoT environments, and some Machine Learning models have been developed to identify attacks based on IoT traffic designs [1].

Gendreau et al stated that the obscurity and low accessibility of many of these devices in this vast heterogeneous network will make it difficult to holistically monitor information flow. Nonetheless, to safeguard networks, unauthorized intruders must be detected within the constraints of each type of device or subnetwork before any system information can be disseminated. To understand and illustrate IDS platform differences and the current research trend towards a universal, cross-platform distributed approach, the survey starts with an historical examination of intrusion detection systems [2].

Domingo at el proposed that Smartphones are the reference platforms being equipped with an accelerometer sensor and elements of the IoT[3]. The work surveys and compares accelerometer signals classification methods to enable IoT for the aforementioned functions. The considered methods are support vector machines (SVMs), decision trees, and dynamic time warping, the SVM-based approaches show an accuracy of above 90%.

Chaabouni et al demonstrated that the IoT security threats and challenges for IoT networks by evaluating existing defense techniques. Also the main focus is on IoT NIDS deployed via ML since learning algorithms have a good success rate in security and privacy. The implementation of the NIDS in IoT context considering IoT limitations. Moreover, the this enables security individuals differentiate IoT NIDS from traditional ones[4].

Liang Xiao et al investigated that The Internet of Things (IoT), which connects a range of devices to networks to enable upgraded and intelligent services, must safeguard user privacy and resist assaults including spoofing, denial of service (DoS), jamming, and eavesdropping. Review IoT security solutions based on machine-learning (ML) approaches such as supervised learning, unsupervised learning, and deep learning. To ensure data privacy, ML-based IoT authentication, access control, secure offloading, and malware detection approaches are used [5].

DATASET

This section provides a description of the dataset generated by the MQTT sensors simulation is described in this section. The dataset includes four attack scenarios as well as normal operation. Four attacks are carried out by the attacker, each of which is recorded separately.

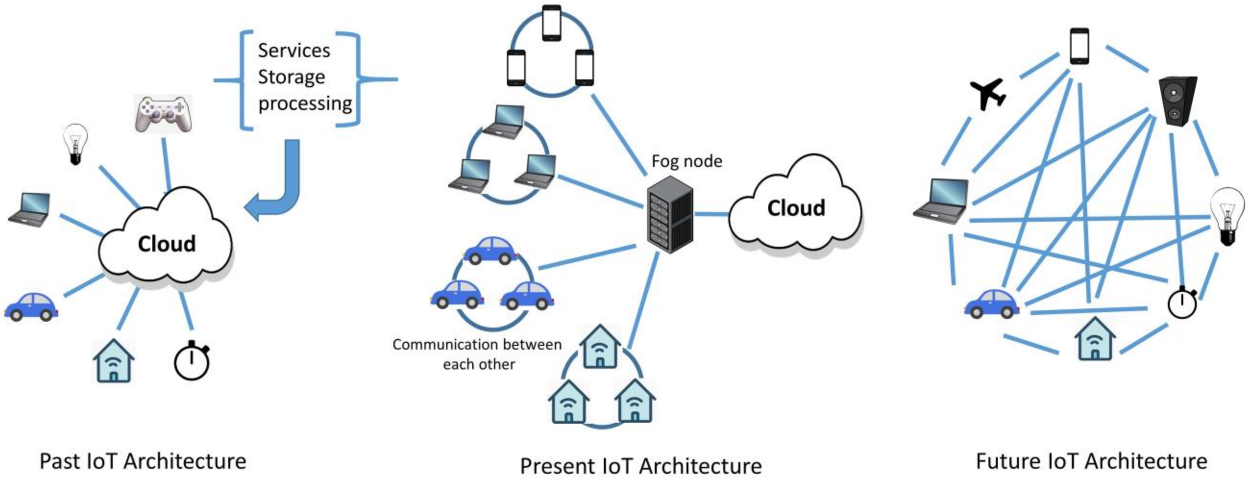
The attack types are:

- Aggressive scan (Scan A)
- 3User Datagram Protocol (UDP) scan (Scan sU)
- Sparta SSH brute-force (Sparta)
- MQTT brute-force attack (MQTT BF)

Tcpdump was used to collect the data. By recording Ethernet traffic and subsequently exporting to pcap _les, the packets are collected. The following instruments were used:

- Virtual machines are used to simulate the network devices.
- Nmap is used for the scanning attacks.
- VLC is used to simulate the camera feed stream.
- MQTT-PWN is used for the MQTT brute-force attack.

Existing IDS have been shown to be unsuccessful at detecting a wide range of threats, including zero-day attacks, as well as reducing false alarm rates (FARs). As a result, regardless matter how exact the intrusion detection (ID) method is, malicious attempts might undermine IDS stability. The IDS architecture. An ensemble-based model for intrusion detection will be constructed using multiple ML classification algorithms such as DT, J48, and SVM with nine most significant and crucial features in the KDD99 dataset of intrusion detection.



An examination of industrial IoT applications, as well as basic IoT validation technologies and multi-layer designs. Because of the Internet of Things' unique qualities, such as deployment, mobility, and complexity, such a standard would have serious security weaknesses that could not be accepted in the industrial IoT sector. It focuses primarily on the security difficulties associated with IoT middleware, as well as a comprehensive study of related existing protocols and their security vulnerabilities, as well as the special problems associated with IoT device localization and placement. Security approaches for IoT security include software defined networking (SDN) and network function virtualization (NFV). Despite the fact that there are numerous studies in this field, they are all focused on a single topic.

Physical access attacks include replacing nodes or their batteries, as well as reprogramming nodes. When it comes to network attacks, the author distinguishes between active and passive attacks. Active attacks, on the other hand, change, discard, or misdirect data packets in order to disrupt network node connection. An active attack can readily damage a large number of IoT devices since a network is made up of peripherally deployed units that communicate with each other using multi hop communication. Of course, whether or not an IDS detects all attacks is a key criterion for its effectiveness. In addition, the IDS should only report actual assaults, not harmless behaviour that has been misinterpreted as an attack. The ratio of an IDS's alarms to the actual appearance of attacks is especially important.

Reference	Method	Merits	Demerits	Dataset
1	Dynamic hierarchical network CNN byte method	In user behaviour analytics it detects the important features without any human supervision	Convolutional neural network exploits gradient and imbalance the class in IDS	CNN
2	Cross-platform distributed approach	To safeguard the network from the intruders	The accuracy rate is low	IDS and IoT
3	SVM based approach	Easy and effective way to monitor the information flow	Accuracy is less than 90%	Dynamic wrapping
4	IoT defense techniques	IoT NIDS deployed via ML	Chances of malicious	Traditional techniques of NIDS

			activities in NIDS is high	
5	ML-based IoT authentication	Improves the security and privacy of the data flow	Multiple ML techniques were used	KDD, J48

PROPOSED METHOD

A Log-based IDS to predict if the network log is an attack or not. Log Analysis for Intrusion Detection is the process used to detect attacks on a specific environment using log files as the primary source of information. Selecting relevant feature is an important problem in learning systems. KDD dataset is used for benchmarking intrusion detection problem based on network traffic logs. The elimination of the insignificant features simplified the problem and did not hurt the detection rate and the accuracy rate will be 98%.

CONCLUSION

Deep learning, as an intelligent technique, offers a solution to the IoT network intrusion detection challenge. A deep learning-based intrusion detection solution for IoT networks that classifies traffic flow. The literature review in this study is based on the collection of many research publications that have demonstrated the application of machine learning algorithms in intrusion detection systems, with the KDD dataset being largely utilised to minimise network traffic logs.

REFERENCE

1. King J, Awad AI (2016) A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 40(1):133–143

2. Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90

3. M. C. Domingo, “An overview of the internet of things for people with disabilities,” Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2017

4. Chaabouni, Nadia, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. (2019) "Network Intrusion Detection for IoT Security based on Learning Techniques." IEEE Communications Surveys & Tutorials.

5. Xiao, Liang, Xiaoyue Wan, Xiaozhen Lu, Yanyong Zhang, and Di Wu. (2018) "IoT security techniques based on machine learning." arXiv preprint arXiv:1801.06275

6. I. Onat and A.Miri, “An intrusion detection system for wireless sensor networks,” in Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob ’05), vol. 3, pp. 253–259, IEEE Computer, Qu´ebec, Canada, August 2019.

7. Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A survey on security and privacy issues in internet-of-things,” IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, Oct 2019

8. Weber M, Boban M (2016) Security challenges of the internet of things. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija. pp 638–643.

9. Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). Procedia Comput Sci 61:46–51

10. Liu L, Xu B, Zhang X, Wu X (2018) An intrusion detection method for internet of things based on suppressed fuzzy clustering. EURASIP J Wireless Communication Network 2018(1):113

11. D. E. Boubiche and A. Bilami, “Cross layer intrusion detection system for wireless sensor network,” International Journal ofNetwork Security & Its Applications, vol. 4, no. 2, p. 35, 2012.

12. R. Bao, I. Chen, M. Chang, and J. Cho, “Hierarchical trust management forwireless sensor networks and its applications to trust-based routing and intrusion detection,” IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169–183, 2019.

13. T. Roosta, S. Shieh, and S. Sastry, “Taxonomy of security attacks in sensor networks and countermeasures,” in Proceedings of the 1st IEEE International Conference on System Integration and Reliability Improvements, vol. 25, pp. 13–15, 2020.

14. I. Ud Din, M. Guizani, B. Kim, S. Hassan, and M. Khurram Khan, “Trust management techniques for the internet of things :a survey,” *IEEE Access*, vol. 7, pp. 29763–29787, 2019.

15. Chaabouni, Nadia, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. (2019) "Network Intrusion Detection for IoT Security based on Learning Techniques." IEEE Communications Surveys & Tutorials.

16. Hassan, Wan Haslina. (2019) "Current research on Internet of Things (IoT) security: A survey." Computer Networks 148: 283-294.

17. Abdel-Basset, M., Manogaran, G., Mohamed, M.: Internet of things (IoT) and its impact on supply chain: A framework for building smart, secure systems. Future Generation Computer Systems 86, 614{628 (2018).

18. Hindy, H., Brosset, D., Bayne, E., Seeam, A.K., Tachtatzis, C., Atkinson, R., Bellekens, X.: A taxonomy of network threats and the e_ect of current datasets on intrusion detection systems. IEEE Access 8, 104650{104675 (2020)

19. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.L., Iorkyase, E., Tachtatzis, C.,Atkinson, R.: Threat analysis of IoT networks using artificial neural network intrusion detection system. In: 2016 International Symposium on Networks, Computers and Communications (ISNCC). pp. 1{6. IEEE (2019).

20. Ali B, Awad AI (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. 86, 619{628 (2020).