IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⋇ Impact Factor 7.105 ⋇ Vol. 9, Issue 5, May 2022

DOI: 10.17148/IARJSET.2022.9592

NETWORK INTRUSION DETECTION SYSTEM BY SUPERVISED MACHINE LEARNING

Keerthi P[1], Gagan K M[2], M V Suhas[3], Mahendra R[4]

Assistant Professor, Department of Information Science & Engineering,

Atria Institute of Technology, Bengaluru, India[1]

Student, Department of Information Science & Engineering, Atria Institute of Technology, Bengaluru, India[2,3,4]

Abstract: People from all over the world can connect over the Internet. Network attacks are a risk in this Internet environment. The risk of integrity and confidentiality has risen in tandem with the density of information and its global reach. Breach of security has gotten way too regular. As a result, network security is becoming increasingly important these days. Accidental network interference can be avoided by using network protection. It's made up of network intrusion detection software that monitors the activity on the network. To track traffic from source to destination apps, NIDS is strategically placed throughout the network. The computer would do its best to screen both inbound and outbound traffic, but this would cause traffic congestion, decreasing the system's overall performance. Machine learning approaches such as logistic regression, Naive Bayes, K-Nearest Neighbour, and Decision Trees were applied in the domain of intrusion detection for our research.

Keywords: Network intrusion, Machine learning, Host Intrusion Detection System, Network security

I. INTRODUCTION

Information systems are now a vital component of all businesses, regardless of their size or industry. Nonetheless, the data kept and services provided by these information systems make them viable targets for a variety of attacks. These attacks can have devastating repercussions due to their wide variety and specificity to systems. In this environment, computer security has emerged as a serious concern, and research in this area is growing. To provide a level of safety that fits the needs of modern living, several instruments and methods are devised. The Intrusion Detection System is one of these tools (IDS). IDS are tools that are used to detect attempted network attacks as well as anomalous activities and behaviours that are intended to disrupt the system's normal operation. Network-based intrusion detection systems (NIDS), host-based intrusion detection systems (HIDS), and hybrid intrusion detection systems (HIDS) are the three types of intrusion detection systems. In addition, by monitoring all network traffic, harmful activity can be detected. In general, IDS systems are set up by setting the network interface card to promiscuous mode, Machine Learning (ML) based IDS systems based algorithms such as K-means, Hidden Markov Model and Self Organizing Maps (SOM); Neural networks, decision trees, Naive Bayes and Support Vector Machine. Deep learning (DL) has recently transformed a number of fields, delivering state-of-the-art results in areas such as computer vision and natural language processing.

II. REVIEW OF THE LITERATURE

New security vulnerabilities in the network develop one after another as computer network technology advances, making it increasingly difficult to ignore. A vital duty for today's network administrators is to successfully prevent harmful network hackers from penetrating, ensuring that network systems and computers are safe and functioning properly Deep learning was used to construct a network intrusion detection system. This method uses a deep confidence neural network to extract features from network monitoring data, and then a BP neural network as the top level classifier to classify intrusion types [1].

The experimental results suggest that RNN-IDS is well suited to modelling a classification model with high accuracy, and that its performance in binary and multiclass classification is superior to that of classic machine learning classification methods. The RNN-IDS model improves the intrusion detection accuracy. Introduce an intrusion detection system that uses an upgraded recurrent neural network (RNN) to detect the type of intrusion in the suggested system [2].

DOI: 10.17148/IARJSET.2022.9592

Nowadays, the internet is a frequently used platform by individuals all over the world. As a result, science and technology have progressed. According to many surveys, network intrusion has been steadily increasing in recent years, resulting in personal privacy theft and becoming a major attack platform. Unauthorized action on a computer network is known as network intrusion. As a result, an effective intrusion detection system is required. Rapid advancements in the realm of communication have resulted in a massive growth in network size and data. As a result, many new attacks are being developed, making it difficult for network security to detect breaches accurately. Furthermore, intruders with the intent of launching various attacks within the network cannot be overlooked. An intrusion detection system (IDS) is a tool that inspects network traffic, integrity, and availability to protect the network from possible invasions. Deep learning (DL)-based IDS systems are being tested as potential solutions for quickly detecting breaches throughout a network [3].
The intrusion detection system idea presents a taxonomy based on well-known deep learning techniques used in network-based intrusion detection system (NIDS) systems. In terms of the proposed approach, evaluation measures, and dataset selection, recent trends and breakthroughs in deep learning based NIDS are discussed. Mobile risks are fast increasing in tandem with the massive increase in the number of mobile users. Mobile malware can be used to steal private information, install backdoors, launch ransomware attacks, and deliver premium SMSs, among other things [4].
In order to detect sophisticated threats and limit false positives, the model can also be combined with classic intrusion detection systems. The use of a semi-supervised clustering algorithm can significantly improve the performance of fully unsupervised clustering methods. As a result, network security has become an indisputable component of the network system. Currently, one of the domains in which neural networks are being intensively explored for increasing overall computer network security and data privacy is the financial sector [5].

CONCLUSION

We have presented a practical and efficient Network Intrusion Detection System using classification and deep learning technique which can also be implemented on other machine learning algorithms and can be used on existing systems. Intrusion detection is a practical and practical approach for providing a specific service. Definition of defense in our large and current networks (possible uncertainty) Computer and networking programs. Intrusion monitoring systems are based on host audit-trail and network traffic analysis and are designed to detect threats, preferably in real time.

REFERENCES

[1] "Incremental anomaly –based intrusion detection system using limited labelled data," in Web Research (ICWR),2019 3rd International Conference on, pp. 178-184, P. Alaei and F. Noorbehbahani.
[2] M. Saber, S. Chadli, M. Emharraf, and I.EI Farissi,’’Modeling and implementation approach to evaluate the intrusion detection system,’’ in International Conference on Networked systems, 2018,pp.513-517.
[3] M. Tavallaee, N. Stakhanova, Towards a meaningful evaluation of anomaly-based intrusion detection algorithms," Ghorbani," Part C (Applications and Reviews), IEEE Transactions on Systems, Man, and Cybernetics, vol.. 40, no. 5,pp. 516-524,2018.
[4] LeCun, Yann, Yoshua Bengio, and Geoffffrey Hinton (2015). “Deep learning”. In: nature 521.7553, pp. 436–444.
[5] Adetunmbi, Adebayo O, and others (2008). "Identifying network infiltration using a rough set and the k-nearest neighbour method." International Journal of Computing and Information Technology Research, vol. I2.1, pp. 60–66.
[6] Li, Wei (2004). “Using genetic algorithm for network intrusion detection”. In: Proceedings of the United States department of energy cyber security group 1, pp. 1– 8.