INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of Second International Conference on Advancements in Research and Development (ICARD 2021)

Deep Learning Approach For Intelligent Intrusion Detection System

Maneesha M [1], Savitha V[2], Jeevika S[3],Nithiskumar G[4], Sangeetha K[5]
[1,3,4]UG Scholar, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India.
[2,5]Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, India.
manokrish2099@gmail.com[1], jeevikajeevi16@gmail.com[2], nithishatm07@gmail.com[3], profvsavithacse@gmail.com[4], Sangithaprakash@gmail.com[5]

Abstract

This paper focuses on preventing cyber attacks, which are common on any device connected to the internet. In order to create an intrusion detection system (IDS) that can recognise and differentiate cyber-attacks at the network and host levels in a timely and automated manner, machine learning techniques are widely used. A deep neural network (DNN) is a form of deep learning model being researched for use in developing a scalable and efficient intrusion detection system (IDS) capable of detecting and classifying unexpected and unpredictable cyber-attacks.Since network behaviour is constantly changing and attacks are evolving at a rapid pace, it is critical to analyse various datasets that have been produced over time using both static and dynamic approaches. This type of research helps in the discovery of the most effective detection algorithm.

Keywords: Intrusion detection system, Cyber Attacks, Deep Neural Networks

1. Introduction

Information and communications technology (ICT) systems and networks carries different datas from various users to prevent attacks. These attacks can be manual and machine generated, diverse and are gradually advancing in obfuscations resulting in undetected data breaches.

With the advancement of hardware, software, and network topologies, including recent advances in the Internet of Things, such cyber attacks are constantly evolving with very algorithm. Malicious cyber attacks pose significant security risks, necessitating the development of a new, versatile, and effective system. An intrusion detection system (IDS) is a proactive intrusion detection method that detects and classifies intrusions, attacks, and violations of security policies at the network and host level infrastructure in real time. Intrusion detection is divided into two categories: network-based intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS)..Infrastructure needs to be levelled as soon as possible. Intrusion detection is divided into two categories: network-based intrusion detection systems (NIDS) and host-based intrusion detection systems.sensors in the immediate vicinity While NIDS examines the contents of each packet in network traffic flows, HIDS relies on data from log files, which include sensor logs, device logs, programme logs, file systems, disc resources, user account information, and other information. Many businesses use a combination of NIDS and HIDS.Network behaviours are collected using network equipment through mirroring by networking devices such as switches, routers, and network taps, and analysed to identify attacks and potential threats hidden within network traffic. HIDS is an IDS system that detects attacks by using system activities in the form of various log files running on the local host machine. An intruder uses a specific service to gain access to the target device during the exploitation process. Abusing, subverting, or violating are all terms that can be applied to a service. The final step is pillage, in which an attacker's malicious activities can include data theft, CPU time theft, and impersonation. An attack is now described as a series of behaviour that has the potential to compromise a resource's confidentiality, data integrity, availability, or any other security policy. An IDS system's primary goal is to detect all of these forms of attacks in order to protect computers and networks from malicious activity [1-5].

2. Problem Identification

2.1. Aim of the Paper

This paper is proposed mainly to reduce cyber-attacks which is of various types. Through machine learning we can gather huge amounts of data on known cyber attacks and apply the results to the existing security protocols. Rapid response times are critical for avoiding the worst effects of cyber attacks. **The longer a breach goes undetected, deeper the affect for owners**, for instance, the more data will be compromised, which can be costly to companies of the all sizes. Predictive analytics can give remote hands teams the advance notice to actively combat hacking attempts.

2.2. Stages of Compromise: An Attacker’s View

Unauthorized users, also known as attackers, are the most common perpetrators of intrusions. An intruder may use the Internet to gain remote access to a device or render a service unusable. Understanding how to successfully attack a device is needed for effective intrusion detection. An assault can be divided into five stages in general. Reconnaissance, exploitation, reinforcement, consolidation, and pillage are the five phases. During the first three stages, an attack can be detected; but, once it enters the fourth or fifth level, the device is completely compromised. As a result, distinguishing between normal activity and an attack is extremely difficult. An assault is launched during the reconnaissance processs.This attempts to gather knowledge about reachable hosts and facilities, as well as the operating system and device versions currently in use. An intruder uses a specific service to gain access to the target device during the exploitation process. Abusing, subverting, or violating are all terms that can be applied to a service.Stolen password or dictionary attacks are examples of exploiting services, while SQL injection is an example of subversion abuse. The key pillars of information protection are confidentiality, data integrity, and availability. In terms of information security, authenticity and transparency are also relevant. In general, attacks against secrecy address passive attacks such as eavesdropping, while attacks against honesty address active attacks such as device scanning attacks.'Probe' and availability, for example, resolve attacks that cause network services to be inaccessible to regular users, such as denial of service ('DoS') and distributed denial of service ('DDoS'). IDS systems only have a small ability to detect eavesdropping attacks. An attack known as a 'probe' can be launched from either [6-10].

3. Proposed System

3.1. Software System

Users will benefit from this software because it will protect them from cyber or malware attacks. When this programme is mounted on a Smartphone, it keeps track of all the websites that the user visits and keeps an eye on any new devices that are inserted into that device. If the programme detects an attack or irregular and suspicious data, it automatically notifies the user of the problem and provides information about the attack so that the user understands where the problem originated with a few simple details such as IP address and type of malware.

3.2. Network-Based Intrusion Detection Systems (NIDS)

A network-based intrusion detection system (NIDS) watches for malicious traffic on a network. NIDS typically require promiscuous network access in order to analyse all traffic, including all unicast traffic. Figure 1 shows a typical NIDS architecture. NIDS are passive devices that monitor traffic without interfering with it. The NIDS uses a different network interface (read/write) to sniff the firewall's internal interface in read-only mode and send alerts to an NIDS Management server.

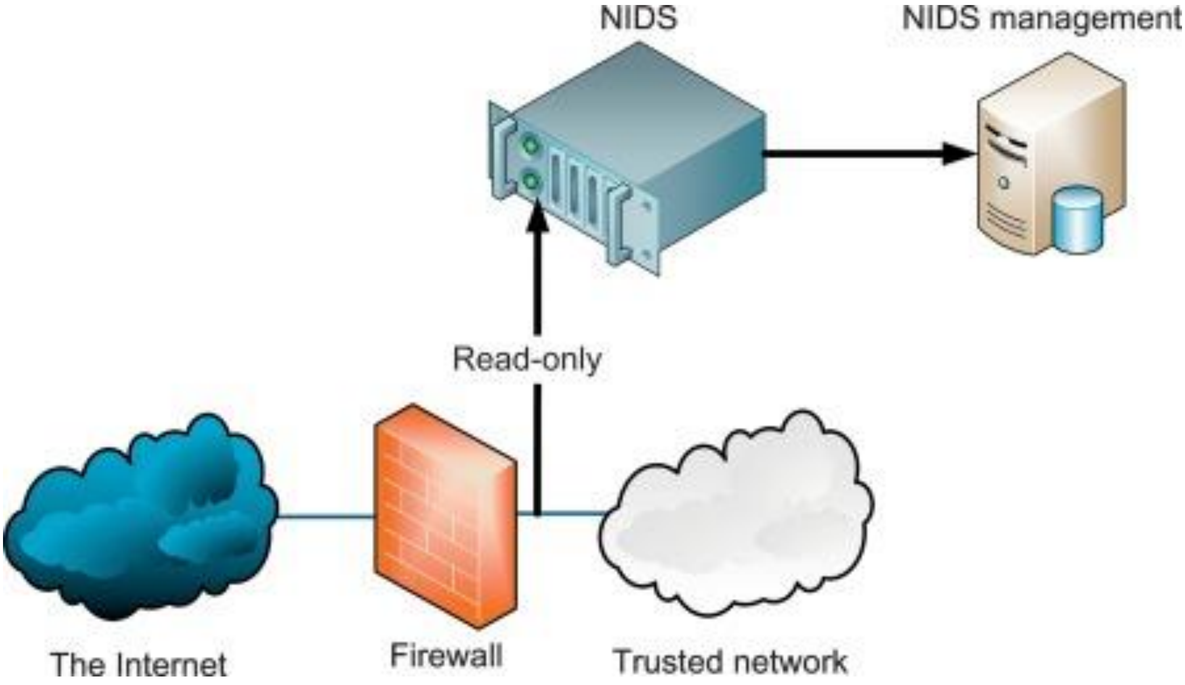

Fig.1.NIDS architecture

3.3. Deep Learning Approaches

Deep neural networks are successful in supervised learning, Unsupervised learning, Reinforcement learning, as well as hybrid learning.

a. Supervised Learning

In supervised learning, the input variables represented by X are converted into output variables represented by Y using an algorithm that learns the mapping function f.

The aim of the learning algorithm is to approximate the mapping function so that a new input's output (Y) can be predicted (X). The error from the predictions made during planning may be used to correct the results. Learning can be stopped until all of the inputs have been conditioned to generate the desired output. Random Forest is used to classify and solve regression problems. Regression is used to solve regression problems, Support Vector Machines are used to classify data, and Regression is used to solve regression problems.

b.Unsupervised Learning

In unsupervised learning, we have the input data only and no corresponding output to map. This learning aims to learn about data by modeling the distribution in data. Algorithms can be able to discover the exciting structure present in the data. Clustering problems and association problems use unsupervised learning.

c.Reinforcement Learning

The algorithm is trained using reinforcement learning, which employs a reward and punishment scheme. The algorithm or agent learns from its surroundings in this situation. When the agent performs well, he is rewarded, and when he performs poorly, he is penalised. Consider a self-driving vehicle, where the agent is rewarded for safely arriving at the destination and penalised for going off-road. In the case of a chess programme, the reward condition could be victory and the punishment could be being checkmated. The agent seeks to optimise the benefit while minimising the cost. The algorithm is not instructed on how to perform the learning in reinforcement learning.

d.Hybrid Learning

Hybrid learning architectures combine generative (unsupervised) and discriminative (supervised) learning elements. A hybrid deep neural network can be created by combining different architectures. They're used to recognise human actions using action bank features, and they're supposed to yield significantly better performance.

Conclusions

As a final thought, The proposed architecture converts system call traces to a ngram vector representation model first. The input feature vectors are then reduced in size using a dimensionality reduction method that selects only those n-gram terms whose frequencies are greater than a predefined threshold value. Finally, deep learning is used to process the dimensionality reduced vectors in order to decide if the corresponding system call traces are natural and intrusive. The proposed framework reliably distinguishes the natural and intrusive device processes while minimising overall computational overheating, according to experimental findings on the benchmark ADFA-LD dataset.

References

[1] Ozgur and H. Erdem, "A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015", PeerJ PrePrints, vol. 4, Apr. 2016.

[2] D. Larson, "Distributed denial of service attacks–holding back the flood", Netw. Secur., vol. 2016, no. 3, pp. 5-7, 2016.

[3] T. Kim, B. Kang, M. Rho, S. Sezer and E. G. Im, "A multimodal deep learning method for Android Malware detection using various features", IEEE Trans. Inf. Forensics Secur., vol. 14, no. 3, pp. 773-788, Mar. 2019.

[4] A. Saracino, D. Sgandurra, G. Dini and F. Martinelli, "Madam: Effective and efficient behavior-based android malware detection and prevention", IEEE Trans. Dependable Secure Comput., vol. 15, no. 1, pp. 83-97, Jan. 2018.

[5] A. Gharib, I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "An evaluation framework for intrusion detection dataset", Proc. Int. Conf. Inf. Sci. Secur. (ICISS), pp. 1-6, Dec. 2016.

[6] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity", IEEE Access, vol. 6, pp. 35365-35381, 2018.

[7] M. Tang, M. Alazab, Y. Luo and M. Donlon, "Disclosure of cyber security vulnerabilities: time series modelling", Int. J. Electron. Secur. Digit. Forensics, vol. 10, no. 3, pp. 255-275, 2018.

[8] D. Larson, "Distributed denial of service attacks–holding back the flood", Netw. Secur., vol. 2016, no. 3, pp. 5-7, 2016.

[9] .S. Huda, J. Abawajy, M. Alazab, M. Abdollalihian, R. Islam and J. Yearwood, "Hybrids of support vector machine wrapper and filter based framework for malware detection", Future Gener. Comput. Syst., vol. 55, pp. 376-390, Feb. 2016.

[10]A. Javaid, Q. Niyaz, W. Sun and M. Alam, "A deep learning approach for network intrusion detection system", Proc. 9th EAI Int. Conf. Bio-Inspired Inf. Commun. Technol. (BIONETICS), pp. 21-26, 2016.