WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

NETWORK INTRUSION DETECTION SYSTEM.

Ms.P.Vimala M.E.[1], Rishi Ragul R[2], Nethaaji M[3], Ruthria Kannan K[4], Prakashmani K.[5]

[1 2 3 4 5] **Dhirajlal Gandhi College Of Technology, Salem.**

A B S T R A C T

Network Security is to protect computer network against hacking, misuse, unauthorized changes to the system and securing a computer network infrastructure. Network attack is the intrusion or threat can be defined as any deliberate action that attempts unauthorized access, information manipulation, or rendering the system unstable by exploiting the existing vulnerabilities in the system. Intrusion Detection system (IDS) / Intrusion Prevention System (IPS) has become a prerequisite in computer networks. IDS/IPS is a device or software application that monitors network or system activities for malicious activities. Present network intrusion detection system is not able to detect the new attacks due to variety of reasons like volume of data, diversity of data, low frequency attacks etc. This project reduces the human effort needed to develop the model like data pre processing, feature selection and it is an hybrid mode that is it identify both signature based and behavioural based attacks . But deep learning is the only solution to above listed problems. This project is based on developing a deep learning model and integrating it with software. In this project's functionality include intrusion detection, malware detection, traffic analysis. This model is trained on NSL dataset which is standard all over the world with the help of this project we can make the network more secure and free of attacks.

Keywords: Network attack, IDS, Deep learning model, Hybrid mode.

1. Introduction

We are in the midst of a deep learning revolution. Unprecedented success is being achieved in designing deep neural network models for building computer vision and Natural Language Processing (NLP) applications. But there's still one field that isn't quite riding this success wave. The application of deep learning in Information Security (InfoSec) is still very much in its nascent stages. But InfoSec is one of the most crucial fields every data scientist should pay attention to. Malware detection and network intrusion detection are two areas where deep learning has shown significant improvements over the rule-based and classic machine learning-based solutions.

Getting labeled data for new network attack can be expensive. In particular, the promise of self-taught learning and unsupervised feature learning is that if we can get our algorithms to learn from" unlabeled" data, then we can easily obtain and learn from massive amounts of it. This unsupervised deep learning algorithm helps to detect new network attacks for which there is no labeled data.

Deep learning cannot solve all the InfoSec problems because it needs extensive labeled datasets. Unfortunately, no such labeled datasets are readily available. However, there are several InfoSec use cases where the deep learning networks are making significant improvements to the existing solutions. Malware detection and network intrusion detection are two such areas where deep learning has shown significant improvements.

2. Literature survey

2.1 HYBRID INTRUSION DETECTION SYSTEM DESIGN FOR COMPUTER NETWORK SECURITY

AUTHOR : SIMRANJEET SINGH

The paper was published in April 2018 this paper they proposed a hybrid IDS by combining the two approaches in one system. The hybrid IDS is obtained by combining packet header anomaly detection (PHAD) and network traffic anomaly detection (NETAD) which are anomaly-based IDSs with the misuse-based IDS Snort which is an open-source project. The hybrid IDS obtained is evaluated using the MIT Lincoln Laboratories network traffic data (IDEVAL) as a testbed. Evaluation compares the number of attacks detected by misuse based IDS on its own, with the hybrid IDS obtained combining anomaly-based and misuse based IDSs and shows that the hybrid IDS is a more powerful system.. Nowadays with the spreading of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide network security. There are various threat sources including software bugs mostly as the operating systems and software used becomes more functional and larger in size. Intruders who do not have rights to access these data can steal valuable and private information belonging to network users. Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them. It is very clear that firewalls are not enough to secure a network completely because the attacks committed from outside of the network are stopped whereas inside attacks are not. This is the situation where intrusions detection systems (IDSs) are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyse the security problems so that they are not repeated

2.2.USING GENETIC ALGORITHM FOR INTRUSION DETECTION

AUTHOR : WEI LI

This paper describes a technique of applying Genetic Algorithm (GA) to network Intrusion Detection Systems (IDSs). A brief overview of the Intrusion Detection System, genetic algorithm, and related detection techniques is presented. Parameters and evolution process for GA are discussed in detail. Unlike other implementations of the same problem, this implementation considers both temporal and spatial information of network connections in encoding the network connection information into rules in IDS. This is helpful for identification of complex anomalous behaviors. This work is focused on the TCP/IP network protocols. When an intruder attempts to break into an information system or performs an action not legally allowed, we refer to this activity as an intrusion (Graham, 2002; see also Jones and Sielken2000). Intruders can be divided into two groups, external and internal. The former refers to those who do not have authorized access to the system and who attack by using various penetration techniques. The latter refers to those with access permission who wish to perform unauthorized activities. Intrusion techniques may include exploiting software bugs and system misconfigurations, password cracking, sniffing unsecured traffic, or exploiting the design flaw of specific protocols (Graham, 2002). An Intrusion Detection System is a system for detecting intrusions and reporting them accurately to the proper authority. Intrusion Detection Systems are usually specific to the operating system that they operate in and are an important tool in the overall implementation an organization's information security policy (Jones and Sielken,2000), which reflects an organization's statement by defining the rules and practices to provide security, handle intrusions, and recover from damage caused by security breaches.

3. Existing System

The aim of this system to detect various attacks in the system for which there are lot of labeled data. Deep Learning has been used to train a model which can be used to detect the attacks in the network .Deep learning models like Recurrent neural network(RNN),convolutional neural network(CNN) and other neural networks are used in this application .Many of the existing systems is signature based detection system that is the system already knows the signature of the attack and it detects the attack based on the dataset that is used for training.

Disadvantages

- Produce a low level of accuracy
- Lack of appropriate data sets

Recommended system

To propose an intelligent algorithm for economic forecasting that uses Convolutional Neural Networks (CNN) to achieve goals. Our work estimates the correlation coefficient based on the spear method between gross domestic product (GDPR) and other economic statistics to find effective parameters for the growth and decline of GDPR, and also determine the returns from CNNs. To assess the effectiveness of the algorithm in predicting economic status, we studied nationally reported economic and disease statistics in India. Test results show about 96% and 89% accuracy about one and a few months ago. Our method can help governments propose effective policies to prevent economic damage.

Benefits

- Easy to predict behavioral changes
- It increases accuracy

4. System Architecture

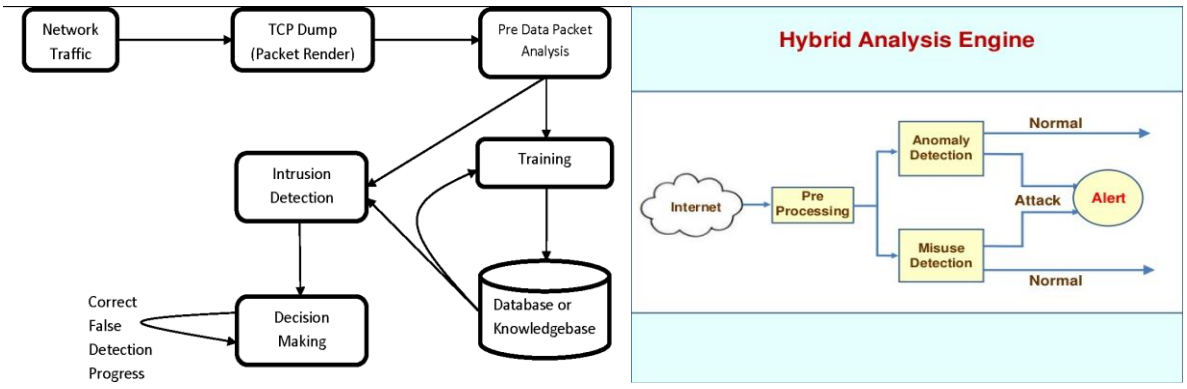

Fig. Architecture diagram of System

This project will affect everyone connected to the Internet The network intrusion detection techniques are important to prevent our systems and networks from malicious behaviours. However, traditional network intrusion prevention such as firewalls, user authentication and data encryption have failed to completely protect networks and systems from the increasing and sophisticated attacks and malwares. So hybrid model makes use of both signature and behaviour based method for detecting an attack. The project will analyse the data packets using TCP dump and send it through the deep learning model and check for intrusion detection if it identifies that there is an attack then it will block the site.

Objectives

- To analyze the data packets.
- To analyze the data packets in hybrid mode.
- To reduce the attack on the network traffic.
- To ensure the security of the system while transferring data packets.

Acknowledgements

We would like to express our deep and sincere gratitude to professor Ms P VIMALA ,M.E., for giving the opportunity and guidance throughout this research.

Conclusion

Network based IDS system is implemented using feed forward neural networks. NSL dataset is used for training the model. Pre-processing techniques like Scaling, Transformation and deep auto encoder have been carried out before supplying the data to the model. Captured the packets in real time network traffic using the Bro network analyser framework. Packet features like Source IP, Destination IP, frames, Port, Mac Address, format, Protocol type are extracted and analysed Model is saved and used by Flask API Server. We created a simple desktop application using Tkinter python module to record live network traffic. Then the Packet analysis and testing were done with the Already existing model so that it can detect any attack on the client side.

REFERENCES

[1]L. Karanam, K. K. Pattanaik, and R. Aldmour, “Intrusion Detection Mechanism for Large Scale Networks using CNN LSTM,” pp. 323–328, 2021.

[2] S. M. Sohi, J. Seifert, and F. Ganji, “RNNIDS : Enhancing Network Intrusion Detection Systems through Deep Learning,” Comput. Secur. pp. 102-151, 2020.

[3] Lin Chen et al., “a Novel Network Intrusion Detection System Based on CNN,” pp. 243–247, 2020.

[4] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, “Kitsune : An Ensemble of Autoencoders for Online Network Intrusion Detection,” no. February, pp. 18–21, 2018.

[5] J. Xu, Y. Wen, C. Yang, and D. Meng, “An Approach for Poisoning Attacks against RNN-Based Cyber Anomaly Detection,” pp. 1680–1687, 2020.

[6] M. A. Khan, “HCRNNIDS : Hybrid Convolutional Recurrent Neural,” 2021.

[7] A. Farrokhi, “Intrusion detection using reduced-size RNN based on feature grouping,” pp. 1185–1190, 2012.

[8] T. A. Tang, L. Mhamdi, D. Mclernon, S. Ali, R. Zaidi, and M. Ghogho, “Deep Recurrent Neural Network for Intrusion Detection in SDN-based Networks,” 2018 4th IEEE Conf. Netw. Softwarization Work., no. NetSoft, pp. 202–206, 2018.

[9] A. B. Dataset, “Towards the Development of Realistic Botnet Dataset.”

[10] F. Laghrissi, S. Douzi, K. Douzi, and Hssina, “Intrusion detection systems using long short -term memory (LSTM),” J. Big Data, 2021.

[11] ANANDARAJ, A. Peter Soosai; INDUMATHI, G.. "Enhanced Fuzzy Particle Swarm Optimization Load Distribution (EFPSOLD) for DDOS Attacks Detection and Prevention in Healthcare Cloud Systems. Journal of Internet Technology",. 21, n. 2, p. 435-445,mar.2020.ISSN2079-4029,2021.