International Journal of Research Publication and Reviews

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

Abnormality Detection System for Network Traffic

[1]Tamilselvi N, [2]Sangeetha V, [3]Nisha R, [4]Santhanalakshmi K

[1,2,3]B.E. Computer Science and Engineering (Final year), [4]Assistant Professor, B.E, M.Tech,
Department of Computer Science and Engineering, Paavai Engineering College, Paavai Institutions, Paavai Nagar, NH-44, Pachal – 637018. Namakkal Dist., India

ABSTRACT

The amount of people on the networks is growing very rapidly because of the advances of the network technologies. A large amount of transmission information has been generated and passed over the network. However, this data is at risk of being attacked and intruded. To prevent network intrusions, security measures should be taken to prevent any anomalies and identify potential threat from the network. Network security researchers and labs have done much network security research. The major aim of this study was to do a noninvasive inspection, which would provide a large general mechanism on the recent advancement in abnormality detection. Recent research on new technologies and future possibilities of anomaly detection were reviewed in the study as published in the last 5 years. Specifically, the literature review dealt with the systems that are used for detection of anomalies in network traffic. These applications included Wireless Sensor Networks (WSN), Internet of Things (IoT), High Performance Computing, Industrial Control Systems (ICS) and Software Defined Networking (SDN) environments. The review ends with a few unresolved issues that need to be solved to enhance anomaly detection systems.

KEYWORDS: Network technologies, Network traffic, Security measures, Anomaly detection, Network intrusions, Non-invasive inspection, Abnormality detection, Wireless Sensor Network (WSN), Internet of Things (IOT), High Performance Computing, Industrial Control Systems (ICS), Threat detection, Network security, Unresolved.

HIGHLIGHTS:

- Increasing Network Usage and Security Risks: With the rapid growth in network usage, there is a significant rise in data transmission, making networks more vulnerable to attacks and intrusions, thus requiring effective anomaly detection systems.
- Focus on Recent Advances: The study reviews the latest research (past five years) in anomaly detection technologies, particularly applications like IoT, WSN, ICS, and SDN, highlighting both progress and unresolved challenges.

INTRODUCTION

The rise of the internet and the increasing number of connected devices have made network traffic an essential part of our daily lives. We rely on it to carry out various activities, such as streaming videos and making payments online. However, as the amount of data that's transmitted over the network keeps growing, it has become harder to maintain its reliability and security. Due to the increasing number of attacks on the network, many companies and organizations are now becoming more concerned about the security of their networks. An important technique for protecting networks is anomaly detection, which is a process that can identify anomalous behavior in a wide range of network data. This type of detection can be applied to various aspects of network data such as user activity logs and network traffic. There are two types of techniques used for this type of detection: machine learning-based and statistical-based. Methods that are statistical-based can identify deviations from the expected behavior. On the other hand, methods that are machine learning-based use algorithms to learn from the patterns of normal behavior. A failure to detect network anomalies can lead to various issues, such as data breaches and system downtime. These can be caused by various factors, such as hardware failures, malicious attacks, and software bugs. If left undetected, these can affect an organization's operations and financial security. A successful cyberattack can have severe consequences, such as the theft of sensitive data or the disruption of vital infrastructure.

The goal of this study is to analyze the performance of three different algorithms: the Support Vector Machine, the Random Forest, and the Artificial Neural Network. In addition, we will explore the impact of the feature selection on these algorithms' performance. This study aims to analyze the various techniques used for detecting network anomalies and their effectiveness in improving the security of networks. The KDD NSL dataset, which is a widely used research tool in network security, contains traffic data that has been simulated to attack different types of DoS attacks. This was created by NIST to support research related to intrusion detection systems. The KDD NSL data set contains about 4.9 million records that have been labeled as either "normal" or "DoS, Probe, R2L, U2R". It features 41 features, such as service type, destination IP addresses, flags, and protocol type. One of the main benefits of utilizing the KDD-NSL dataset is its vast number of labeled examples. This makes it an ideal training and testing ground for machine learning models. Furthermore, it contains a wide variety of attacks, which can be used to evaluate the algorithms' performance. The goal of this study is to analyze the performance of deep learning and machine learning algorithms when it comes to detecting DoS attacks. By focusing on this attack, we hope to gain a deeper understanding of how different techniques can identify it. The KDD-NSL dataset can provide us with an opportunity to thoroughly study deep learning algorithms and machine learning models when it comes to identifying network anomalies. The results of this research will be beneficial in helping organizations protect their networks from cyberattacks.

OBJECTIVE

A failure to detect network anomalies can lead to various issues, such as data breaches and system downtime. These can be caused by various factors, such as hardware failures, malicious attacks, and software bugs. If left undetected, these can affect an organization's operations and financial security. A successful cyberattack can have severe consequences, such as the theft of sensitive data or the disruption of vital infrastructure. Apart from financial losses, a company's reputation can also be damaged. An organization's ability to detect network anomalies is very important to prevent cyberattacks and ensure the integrity of its networks.

PROCEDURE

1. Login Page

2.Click to open the Home Dashboard

3.Select Security Scan Process

4.Upload Traffic Data to Filter Process

5.Select DoS Attack Data File Load

6.Scan To Result View

7.View Anomaly Detection Result

SUMMARY OF ISSUES

- Difficulty distinguishing between normal and abnormal traffic due to behavioral variability.
- High false positive rates can lead to wasted resources.
- Manual investigation of flagged events is time-consuming and costly.
- Current systems struggle to detect zero-day or unknown attacks effectively.

PROBLEM DEFINITION

With the rapid growth in internet usage and connected devices, network traffic volumes have surged. This has made it increasingly difficult to monitor and secure networks against cyber threats such as Denial-of-Service (DoS) attacks.

Traditional security measures often fail to detect novel or evolving threats, emphasizing the need for advanced, adaptive anomaly detection systems to identify irregular patterns in network traffic in real-time.

EXISTING SYSTEM

n recent years, the number of unknown attacks has increased rapidly both from inside and outside the organization. So, it has become imperative to provide customers and users secure access to the network and at the same time keeping the network attack free. That is why IDS (Intrusion Detection System) was introduced. The extensive increase of attacks has the potential for extremely negative impacts on individuals and society. Therefore, intrusion detection in network traffic has recently become an emerging research that is attracting tremendous attention. Therefore there is a need to build a platform to detect anomalies.

DISADVANTAGES

- One of the most challenging factors is distinguishing between abnormal and normal traffic.

- Since the behavior of the network can vary depending on various factors, such as the time of day and the user's behavior, it is not easy to define a standard for normalization.
- This can be caused by the mistake of identifying legitimate traffic as anomalous. It can be very time-consuming and costly to investigate.

PROPOSED SYSTEM

The proposed system employs machine learning and deep learning algorithms (SVM, Random Forest, ANN) to detect anomalies in network traffic using the KDD-NSL dataset. The system automates the detection of suspicious behavior based on historical and simulated attack data. It includes:

- Data preprocessing
- Feature selection (including PCA)
- Classification and prediction using trained models
- Real-time alert generation for detected threats

ADVANTAGE:

- Anomaly detection helps prevent cyber threats and ensure network reliability by identifying unusual traffic patterns that may signal security breaches or unauthorized access.
- Anomaly-based IDS can identify previously unseen threats by learning what "normal" behavior looks like on a network and then flagging deviations as potential anomalies.
- The benefits of using machine learning for network traffic anomaly detection are numerous. It allows organizations to detect threats that traditional security measures might miss, providing an additional layer of secure.

PROCEDURE

1. Login Page

2.Click to open the Home Dashboard

3.Select Security Scan Process

4.Upload Traffic Data to Filter Process

5.Select DoS Attack Data File Load

6.Scan To Result View

7.View Anomaly Detection Result

SYSTEM REQUIREMENT SPECIFICATION

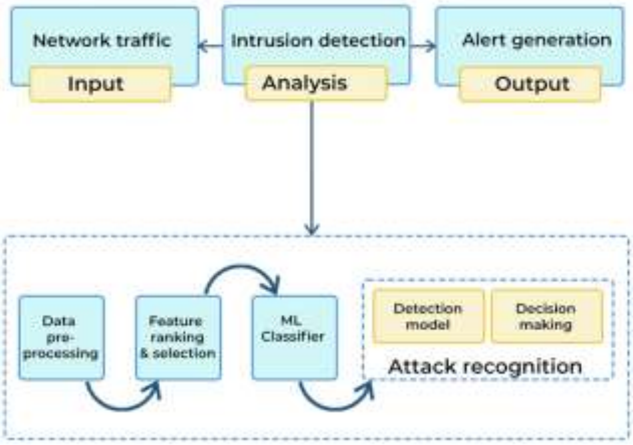
HARDWARE REQUIREMENT:

System	: Pentium IV 2.4 GHz
Hard Disk	: 500 GB
Monitor	: 15 VGA colour
RAM	: 4GB

SOFTWARE REQUIREMENT:

Operating System	: Windows- 10/11
Frontend	: Streamlit 3.0

SYSTEM ARCHITECTURE



CONCLUSION

On the use of deep learning and machine learning techniques to detect anomalous events in network traffic. We utilized the KDD-NSL dataset and three popular algorithms namely, the SVM, ANN, and Random Forest. We also utilized feature selection methods to improve the performance. The results of our study revealed that the three algorithms that were used to detect network anomalies were able to perform well in terms of their accuracy, recall, F1-score, and precision. Furthermore, the selection of features led to a significant increase in the performance of the algorithms. The findings of this study show that deep learning and machine learning methods can effectively identify network anomalies. They also suggest that feature selection can help improve the performance of these techniques. Due to the increasing volume of network data and the complexity of the situation, cyber-attacks are becoming more prevalent

REFERENCE

[1] S. H. A. H. Baddar, A. Merlo, and M. Migliardi, “Anomaly detection in computer networks: A state-of-the-art review,” J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl., vol. 5, no. 4, pp. 29–64, 2021.

[2] Y. Xin et al., “Machine Learning and Deep Learning Methods for Cybersecurity,” IEEE Access, vol. 6, pp. 35365– 35381, 2019, doi: 10.1109/ACCESS.2018.2836950.

[3] S. Y. Huang and Y. N. Huang, “Network traffic anomaly detection based on growing hierarchical SOM,” Proc. Int. Conf. Dependable Syst. Networks, pp. 10–11, 2020, doi: 10.1109/DSN.2013.6575338.

[4] Z. Du, L. Ma, H. Li, Q. Li, G. Sun, and Z. Liu, “Network Traffic Anomaly Detection Based on Wavelet Analysis,” Proc. - 2018 IEEE/ACIS 16th Int. Conf. Softw. Eng. Res. Manag. Appl. SERA 2018, pp. 94–101, 2021, doi: 10.1109/SERA.2018.8477230.

[5] O. I. Sheluhin and I. Y. Lukin, “Network Traffic Anomalies Detection Using a Fixing Method of Multifractal Dimension Jumps in a Real-Time Mode,” Autom. Control Comput. Sci., vol. 52, no. 5, pp. 421–430, 2022, doi: 10.3103/S0146411618050115.

[6] B. J. Radford, L. M. Apolonio, A. J. Trias, and J. A. Simpson, “Network Traffic Anomaly Detection Using Recurrent Neural Networks,” pp. 1–7, 2023, [Online]. Available: http://arxiv.org/abs/1803.10769.

[7] M. Mantere, M. Sailio, and S. Noponen, “Network traffic features for anomaly detection in specific industrial control system network,” Futur. Internet, vol. 5, no. 4, pp. 460–473, 2019, doi: 10.3390/fi5040460.

[8] M. A. A. Naser, “Network Traffic Analysis based on collective anomaly detection,” pp. 1141–1146, 2020.

[9] F. Iglesias and T. Zseby, “Analysis of network traffic features for anomaly detection,” Mach. Learn., vol. 101, no. 1–3, pp. 59–84, 2021, doi: 10.1007/s10994-014-5473-9.

[10] T. Andrysiak, Ł. Saganowski, and W. Mazurczyk, “Network anomaly detection for railway critical infrastructure based on autoregressive fractional integrated moving average,” Eurasip J. Wirel. Commun. Netw., vol. 2016, no. 1, 2022, doi: 10.1186/s13638-016-0744-8.