Chapter 9
Intrusion Detection System Using Deep Learning

Meeradevi
M.S. Ramaiah Institute of Technology, India

Pramod Chandrashekhar Sunagar
M.S. Ramaiah Institute of Technology, India

Anita Kanavalli
M.S. Ramaiah Institute of Technology, India

ABSTRACT

With recent advancements in computer network technologies, there has been a growth in the number of security issues in networks. Intrusions like denial of service, exploitation from inside a network, etc. are the most common threat to a network's credibility. The need of the hour is to detect attacks in real time, reduce the impact of the threat, and secure the network. Recent developments in deep learning approaches can be of great assistance in dealing with network interference problems. Deep learning approaches can automatically differentiate between usual and irregular data with high precision and can alert network managers to problems. Deep neural network (DNN) architectures are used with differing numbers of hidden units to solve the limitations of traditional ML models. They also seek to increase predictive accuracy, reduce the rate of false positives, and allow for dynamic changes to the model as new research data is encountered. A thorough comparison of the proposed solution with current models is conducted using different evaluation metrics.

DOI: 10.4018/978-1-7998-8161-2.ch009

1. INTRODUCTION TO INTRUSION DETECTION SYSTEM

The Intrusion Detection System (IDS) is a platform which enables network traffic for malicious behavior as well as sends warnings while it detects it (*Liao et al., 2013*). It is a software program that checks a network or device for potentially malicious behavior or regulation violations. Any malicious behavior or breach is usually identified to an admin or centralized via a security information and event management (SIEM) system. The SIEM framework combines data from various supplies and utilizes alert filtering methods to discriminate between malicious and false warnings. While intrusion detection systems track networks for detecting sensitive activities, they are vulnerable to false alarms. As a result, when companies first install their IDS products, they must fine-tune them. It entails correctly configuring intrusion prevention systems to distinguish between natural network traffic and malicious behavior. Intrusion detection mechanisms also track network packets accessing the device to identify suspicious activity and send out alert alerts automatically.

1.1 Motivation

In this digital era every device is connected with internet. We are heavily dependent on these devices for our day to day needs. With this there will be a lot of security and intrusion threats on these systems. The research work carried out on intrusion detection system addresses many techniques using machine learning. Existing IDSs still confront hurdles in improving recognition rate, lowering number of false positives, and detecting unknown intrusions. Many academics have concentrated on building IDSs that use machine learning techniques to overcome the difficulties mentioned above. Machine learning algorithms can automatically detect the key differences between regular and aberrant data. Deep learning has achieved impressive results and has become a hotspot for study. So in this work, the deep neural network is implemented to solve the limitations of traditional ML models.

2. TYPES OF IDS

Intrusion Detection Systems are categorized into fivetypes:

2.1 Network Intrusion Detection System (NIDS)

Network intrusion detection systems (NIDS) are installed at a predetermined point inside the network to inspect traffic from several network devices. It monitors all passing traffic on the subnet and compares it to a database of documented attacks.