Chapter 1
Securing Metaverse Platforms Using Machine Learning-Based Intrusion Detection Systems

K. Muthamil Sudar
http://orcid.org/0000-0001-9640-3477
Mepco Schlenk Engineering College, India

ABSTRACT

The increasing number of cyber threats requires more sophisticated and intelligent security solutions than the conventional signature-based Intrusion Detection Systems (IDS). Against the background of growing big data, high-speed networks, and dynamically changing attack vectors, Machine Learning (ML) has become a revolutionary technology to augment IDS by allowing systems to learn from past experiences, recognize patterns, and detect previously unseen attacks in real-time. This chapter discusses the application of Machine Learning methods to the development and design of contemporary IDS. When it comes to intrusion detection, ML algorithms such as decision trees, support vector machines, neural networks, k-nearest neighbors, and ensemble methods are really useful and help to identify known and unknown threats. The chapter on intrusion detection takes a look at the different types of learning, supervised, unsupervised, and semi-supervised, and in terms of datasets like NSL-KDD.

DOI: 10.4018/979-8-2600-2313-6.ch001

INTRODUCTION

Background and Motivation

Business and society over the past two decades, the sheer number of interconnected systems has exploded, and with it, the exposure to cyber threats, as the internet has come to be the backbone of global communication. As a result, individual, governmental, and corporate users are all facing a rising tide of system sabotage, identity theft, and cyberattacks. More often, these attacks now involve sophisticated approaches that completely bypass traditional security measures, making traditional rule-based and signature-based approaches a challenge to stay on top of. A very effective response to cyberattacks is now at the temperament of any modern security setup and is an intrusion detection system. These systems are there to monitor behaviour on a system or network and alert to signs of something abnormal. Conventional IDS models have used a lot of rules and pre-programmed signatures to pick out known threats, but struggle to keep up with the changing landscape of cyberattacks. Well-known patterns of attack turn up every day, and lots of them do not fit into any pre-existing categories, which is why we need flexible and adaptable detection techniques. Machine learning has been hailed as one of the promising ways to address this challenge. By teaching themselves to learn from data, machine learning systems can identify complex patterns, anomalies, and brand-new threats, and do not rely on fixed rules.

Limitations of Traditional IDS

They have a number of disadvantages when traditional Intrusion Detection Systems are in use. They're based on signatures, which are pre-programmed attack patterns, and use a database to match these signatures to incoming data. They're great for repeated attacks, but completely blind to zero-day threats, or attacks that do not yet have a signature (Duaa et al., 2025), which is basically anything we have not seen before. Coming hotfooting into a system, these sorts of attacks can wreak havoc, and the high rate of false positives is yet another problem with rule-based systems. Sometimes analysts get overwhelmed when legitimate user behavior is flagged as suspicious. The response to real threats may be delayed as a result. Furthermore, it takes a lot of time and effort to update rule sets and signature databases manually. Attackers can evade detection by taking advantage of this delay. By identifying behavior that deviates from a “normal” profile, heuristic-based or anomaly detection systems attempt to address some of these problems. But it's not always easy to define what is “normal.” Concerning intrusion detection systems, they are still prone to producing a lot of false alarms, especially in cases where the user