Chapter 9
IDSCI: An Advanced Machine Learning-Based Intrusion Detection System for Cloud Infrastructure

Arvind Mewada
Bennett University, India

Mohd Aquib Ansari
https://orcid.org/0000-0002-9083-1523
Galgotias University, India

Shahnawaz Ahmad
https://orcid.org/0000-0002-3989-9928
Bennett University, India

Sushil Maurya
Siksha 'O' Anushandhan, India

Lalit Kumar
https://orcid.org/0000-0002-8441-1696
MCAET, India

ABSTRACT

The increase in cloud usage has created intricate security problems, highlighting a higher need for preventative measures against security breaches. Classic intrusion detection systems (IDS) are challenged in cloud settings because of the environment's moving and scattered nature, which leads to great rates of incorrect identification and poor optimisation. This research presents an IDSCI capable of deploying an advanced IDS, which IDSCI achieves by applying a hybrid deep learning model

DOI: 10.4018/979-8-3373-1832-5.ch009

that uses convolutional neural networks (CNN) with bidirectional long short-term memory (BiLSTM). The model improves detection accuracy by using robust cloud support for intrusion detection optimisation, guaranteeing strong protection of the cloud-based infrastructure. IDSCI has effectively achieved 98.5% detection accuracy with NSL-KDD and CICIDS2017 datasets, considerably better than traditional IDS systems. These findings illustrate this system in increasing the effectiveness of cloud security through higher detection rates, lower misuse alarms, and real-time counteractive action against threats.

1. INTRODUCTION

The rise of cloud computing has greatly shifted how organisations design and manage their information technology (IT) systems. Cloud services' unparalleled scalability, flexibility, and cost-efficiency make them indispensable to running any modern corporation. Nonetheless, there are considerable security risks associated with them. Cloud infrastructures' active, decentralised, and multi-user structure renders them liable to cyberattacks. The safeguarding of confidential information and system integrity can only be ensured through the implementation of thorough security protocols.

An IDS serves the purpose of observing system and network activity for any harmful actions or violations of predefined rules, highlighting its significance in cybersecurity. At the same time, cloud systems present challenges for traditional IDS implementations (Takabi, Joshi, & Ahn, 2010). The traditional IDS is ineffective due to the complexity of cloud environments, the volume of data and the rate of changes that occur within it. One of these quite pervasive problems is the increase in false positives, lack of sophistication, lack of scalability, and inability to foresee unforeseen threats. Instead of using complicated techniques, machine learning (ML) offers a much more effective approach to enhancing IDS functionality in the cloud. Learning from data allows systems to rise to emerging threats, leading to an increase in the efficacy and precision of intrusion detection (Shenfield, Day, & Ayesh, 2018; Mewada, Gedam, Reddy, & Khan, 2010). Such intelligent IDS eliminate threats by understanding their operational environment without human intervention requirements. Usually, such systems are based on supervised, unsupervised, and deep learning. This study seeks to find ways to build effective machine learning-based IDS for clouds sensitive to these systems' specific features.

Traditional Intrusion Detection Systems (IDS) struggle to effectively secure cloud environments due to their dynamic, distributed nature, leading to high false positive rates, limited scalability, and inefficiency in detecting emerging threats. Existing IDS solutions often fail to capture complex attack patterns in real time,