Artificial Intelligence Review
https://doi.org/10.1007/s10462-021-10037-9

A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions

Ankit Thakkar[1] · **Ritika Lohiya**[1]

Abstract

With the increase in the usage of the Internet, a large amount of information is exchanged between different communicating devices. The data should be communicated securely between the communicating devices and therefore, network security is one of the dominant research areas for the current network scenario. Intrusion detection systems (IDSs) are therefore widely used along with other security mechanisms such as firewall and access control. Many research ideas have been proposed pertaining to the IDS using machine learning (ML) techniques, deep learning (DL) techniques, and swarm and evolutionary algorithms (SWEVO). These methods have been tested on the datasets such as DARPA, KDD CUP 99, and NSL-KDD using network features to classify attack types. This paper surveys the intrusion detection problem by considering algorithms from areas such as ML, DL, and SWEVO. The survey is a representative research work carried out in the field of IDS from the year 2008 to 2020. The paper focuses on the methods that have incorporated feature selection in their models for performance evaluation. The paper also discusses the different datasets of IDS and a detailed description of recent dataset CIC IDS-2017. The paper presents applications of IDS with challenges and potential future research directions. The study presented, can serve as a pedestal for research communities and novice researchers in the field of network security for understanding and developing efficient IDS models.

Keywords Intrusion detection system · Machine learning · Deep learning · Swarm and evolutionary computation · Feature selection · Performance measures · Challenges · Future research directions and applications

Abbreviations

DNN	Deep Neural Network
DBN	Deep Belief Network
SDN	Software Defined Network

✉ Ritika Lohiya
18ftphde30@nirmauni.ac.in

Ankit Thakkar
ankit.thakkar@nirmauni.ac.in

[1] Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India

Published online: 01 July 2021