Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

An Improved Network Intrusion Detection Method Based On CNN-LSTM-SA

Bian Hui[1, 2], Kang Leng Chiew[2*]

[1] Qinyuan (Jiangsu) Technology Co., Ltd., China
[2] Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Malaysia

ARTICLE INFO

Article history:
Received 12 October 2023
Received in revised form 8 December 2023
Accepted 19 March 2024
Available online 25 April 2024

Keywords:
Network intrusion detection; Machine learning; Deep learning; Long short-term memory

ABSTRACT

Network intrusion detection is an essential component of contemporary cybersecurity strategies, and the development of efficient techniques to accurately identify malicious activities has become a priority. This study investigates the performance of various conventional machine learning algorithms, including decision trees, naive Bayes, naive Bayes trees, random forest, random trees, MLP, and SVM, in detecting network intrusions using binary and multi-classification approaches. Furthermore, the study proposes a deep learning method, CNN-LSTM-SA, which consistently outperforms conventional machine learning techniques in terms of precision, recall, F1 score, and overall accuracy for network intrusion detection. Specifically, the proposed method combines CNN and LSTM with SA in machine learning theory to extract more optimized, strongly correlated features. The proposed method is evaluated using the benchmark NSL-KDD database. The results indicate that the CNN-LSTM-SA method holds great potential in enhancing the efficacy of network intrusion detection systems.

1. Introduction

The Internet has become the main infrastructure for people's daily lives and work, and its importance in politics, culture, economy, military and other fields has been continuously demonstrated. It has become a powerful driving force for promoting economic and social development in the 21st century [1-3]. With the popularization of the Internet, various network services and applications have emerged and penetrated into all aspects of people's work and life. Along with the rapid development of the Internet and Internet-based applications, the network environment has become increasingly complex, resulting in many issues related to network security. Intrusion detection, as a major component of network security measures, can actively defend against network attacks and respond before the network is harmed, playing a very important role. In today's rapidly developing information technology era, it is an urgent task to effectively combat attacks and ensure the security of Internet-based information systems [4]. Due to the complexity and diversity of attackers' behaviors, it is very difficult to model both normal and attack behaviors by identifying

[*] *Corresponding author.*
E-mail address: klchiew@unimas.my

https://doi.org/10.37934/araset.44.1.225238