Advancing IoT Security with a Hybrid Deep Learning Model for Network Intrusion Detection

Publisher: IEEE

Rigzen Norbu ; Arun Kumar M ; Ramanathan S ; Nagendra Kumar D ; Jigmet Dolkar ; Subalakshmi Sujitha K **All Authors**

Abstract:
Intrusion detection systems play a pivotal role in safeguarding computer networks from a plethora of cyber threats. Traditional methods have demonstrated effectiveness, b... **View more**

Metadata

Abstract:
Intrusion detection systems play a pivotal role in safeguarding computer networks from a plethora of cyber threats. Traditional methods have demonstrated effectiveness, but the evolving nature of attacks demands novel approaches that can capture intricate patterns and relationships within network data. In this paper, we propose a groundbreaking CNN-Transformer hybrid deep learning model for Network Intrusion Detection Systems (NIDS) prediction, utilizing the Canadian Institute of Cyber Security dataset. The hybrid architecture capitalizes on the strengths of both Convolutional Neural Networks (CNNs) and Transformers. CNNs excel at capturing spatial features in data, making them suitable for identifying local patterns in network traffic. On the other hand, Transformers are adept at capturing global contextual relationships, thereby handling complex temporal dependencies in network sequences. By fusing these two powerful architectures, we achieve a comprehensive model capable of discerning both local anomalies and global attack trends. Our model is extensively evaluated on the Canadian Institute of Cyber Security dataset, and the results are nothing short of remarkable. We achieve an unprecedented accuracy of 99.4%, showcasing the efficacy of the proposed hybrid approach in the context of real-world network traffic. Furthermore, the model demonstrates a robust ability to generalize across diverse attack scenarios, effectively minimizing false positives and false negatives. As cyber threats continue to evolve, the significance of innovative models that offer superior detection accuracy and robust generalization cannot be

More Like This

overstated. This work not only furthers the field of intrusion detection but also underscores the potential of hybrid deep learning architectures in addressing complex cybersecurity challenges.

Published in: 2023 International Conference on Energy, Materials and Communication Engineering (ICEMCE)

Date of Conference: 14-15 December 2023

DOI: 10.1109/ICEMCE57940.2023.10434006

Date Added to IEEE *Xplore*: 21 February 2024

Publisher: IEEE

ISBN Information:

Conference Location: Madurai, India

Contents

Intrusion Detection Systems (IDS) have become a pivotal component in the defense against the escalating complexity of cyber threats in today's interconnected world. These systems play a crucial role in identifying and mitigating unauthorized access, malicious activities, and potential breaches within computer networks. Traditional IDS approaches, often relying on rule-based methods or statistical models, have exhibited efficiency to some extent. However, the evolving landscape of cyber-attacks necessitates innovative techniques that can effectively decipher the intricate patterns and relationships hidden within network data. This paper introduces a pioneering approach aimed at significantly enhancing the performance of Network Intrusion Detection Systems (NIDS) through the fusion of Convolutional Neural Networks (CNNs) and Transformers, two powerful deep learning architectures. While both CNNs and Transformers have individually demonstrated remarkable success across various domains, their integration within the context of NIDS offers the potential to capture both local and global characteristics of network traffic data. The deep learning-based Network Intrusion Detection System (NIDS) leveraging Convolutional Neural Networks (CNN) and Bidirectional Long Short-Term Memory (LSTM)[1] captures both temporal and spatial data characteristics effectively. It exhibited a high detection rate and a low false positive rate when evaluated using the NSLKDD dataset [2].

More Like This

Network Intrusion detection approach based on convolutional neural network
2022 4th International Conference on Communications, Information System and Computer Engineering (CISCE)
Published: 2022

Network Intrusion Detection Model Based on Convolutional Neural Network
2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)
Published: 2021

Show More