A Genetic Algorithm-Optimized Hybrid Deep Learning Framework for Accurate and Robust Intrusion Detection in Cloud Computing

Sabria Ahmed Ben Naser
School of Basic Science, Libyan Academy for Postgraduate Studies, Misurata, Libya

Farij Omer Ehtiba
Faculty of Information Technology, Misurata University, Misrata, Libya

Haitham Saleh Ben Abdelmula
Libyan Center for Electronic Systems, Programming and Aviation Research, Libya

Abdulhkim Alhadi Anaiba
Libyan Center for Electronic Systems, Programming and Aviation Research, Libya

Abstract:
The rapid expansion of cloud computing has broadened the cyber threat landscape, making intrusion detection increasingly difficult due to the scale, speed, and complexity of network traffic in dynamic cloud environments. This paper presents A Genetic Algorithm-Optimized Hybrid Deep Learning-driven Intrusion Detection System (GA-HDLIDS) that combines Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, and an attention mechanism to model both spatial and temporal patterns in network data. A Genetic Algorithm (GA) is integrated to automate hyperparameter optimization, eliminating manual tuning and significantly boosting classification accuracy. Evaluated on the CSE-CIC-IDS2018 dataset, the baseline model (HDLIDS) achieves 99.19% (multi-class) and 99.57% (binary) accuracy. The OHDLIDS model substantially outperforms existing methods, reaching 99.97% and 99.99% accuracy, respectively, with F1 scores above 99.9%. Moreover, the model generalizes effectively to an unseen dataset (CSE-CIC-IDS2019) without retraining, attaining 90.91% accuracy, confirming its robustness in real-world scenarios. All experiments prevent data leakage through strict training-testing separation. These results establish OHDLIDS as a highly accurate, scalable, and practical solution for intrusion detection in evolving cloud computing environments.

Keywords:
Cloud Computing, Cyber Security, Deep Learning, Genetic Algorithm, Hybrid Model.