International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Intrusion Detection Using IOT with Deep Learning

Prachi Bhimrao Jadhav

Deogiri Institute Of Engineering And Management Studies, Aurangabad, Maharashtra, India
Department Of Computer Science And Engineering

Abstract
The rapid expansion of the Internet of Things (IoT) has led to a surge in interconnected devices, increasing the risk of cyber threats. Traditional intrusion detection systems (IDS) often fail to handle the complexity and dynamic nature of IoT network traffic. This paper introduces a hybrid deep learning model that integrates convolutional neural networks (CNN), long short-term memory (LSTM), and artificial neural networks (ANN) to enhance intrusion detection performance. Trained on the BoT-IoT dataset, the proposed system achieves high accuracy and reliability, demonstrating its effectiveness in identifying malicious activity in IoT environments.

Keywords
Internet of Things (IoT), Intrusion Detection System (IDS), Cybersecurity in IoT, Deep Learning, Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), Artificial Neural Networks (ANN), Hybrid Deep Learning Models, Network Traffic Analysis, Anomaly Detection, Supervised Learning, BoT-IoT Dataset, IoT Network Security, Sequential Data Modeling, Real-Time Threat Detection

1. Introduction
The Internet of Things (IoT) has revolutionized the digital landscape by interconnecting a vast number of devices. While beneficial, this interconnectivity introduces new cybersecurity threats. Intrusion detection systems (IDS) are essential for detecting and mitigating such threats. Conventional intrusion detection systems struggle to cope with the evolving and variable patterns of IoT network traffic. Deep learning, especially hybrid models, offers a promising alternative by learning complex patterns in data. This paper explores a CNN + LSTM + ANN based model for IoT-based intrusion detection.

2. Methodology
Our proposed model combines CNN for spatial pattern recognition, LSTM for sequential learning, and ANN for final classification. The BoT-IoT dataset, which includes normal and various attack types such as DoS, DDoS, and data theft, was preprocessed using normalization and one-hot encoding. The model was trained using cross-entropy loss and optimized with the Adam optimizer. Evaluation metrics included accuracy, precision, recall, and F1-score.

3. Results And Discussion

On evaluating with the BoT-IoT dataset, the hybrid architecture produced the following outcomes:

- Accuracy: 98.7%

- Precision: 98.5%

- Recall: 98.8%

- F1-score: 98.65%

The confusion matrix reveals a strong ability to correctly identify intrusions with minimal false positives. The combination of CNN, LSTM, and ANN proved effective in capturing various data characteristics.

4. Conclusion

This research presents a hybrid CNN + LSTM + ANN model for intrusion detection in IoT networks using the BoT-IoT dataset. The proposed model demonstrates strong accuracy and adaptability, indicating its potential for real-time use in intelligent IoT-enabled environments. Future work includes testing on other datasets and exploring lightweight architectures for edge deployment.

References

1. Moustafa, Nour, and Jill Slay. 'The BoT-IoT Dataset: Building a realistic environment for IoT-based attacks.' IEEE 2019.
2. Hochreiter, Sepp, and Jürgen Schmidhuber. 'Long short-term memory.' Neural computation 1997.
3. LeCun, Yann, et al. 'Gradient-based learning applied to document recognition.' Proceedings of the IEEE, 1998.
4. Goodfellow, Ian, et al. 'Deep learning.' MIT press, 2016.
5. Bengio, Yoshua, et al. 'Learning long-term dependencies with gradient descent is difficult.' IEEE Transactions, 1994.