ISCSITR-International Journal of Network and Information Security (ISCSITR-IJNIS)
Vol. 6, Iss 6, November-December, 2025, pp. 1-6
https://iscsitr.com/journals/ISCSITR-IJNIS
Journal ID: 2916-7538

Improving Intrusion Detection Accuracy Using Deep Learning Algorithms in Enterprise Network Systems

Tolulope Udeze
AI Security Engineer, Nigeria.

Abstract

In modern enterprise networks, the proliferation of sophisticated cyber threats has necessitated intelligent and adaptive security systems. This study explores how deep learning algorithms can enhance intrusion detection system (IDS) accuracy within enterprise networks. By leveraging neural architectures like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and hybrid models, this paper evaluates improvements in anomaly detection rates and reduced false positives. A comparative analysis is presented using benchmark datasets. The results demonstrate significant advancements over traditional machine learning techniques, underscoring deep learning's role in bolstering enterprise network security infrastructure.

Keywords:

Intrusion Detection System, Deep Learning, Enterprise Network Security, Cyber Threats, Neural Networks, Anomaly Detection.

How to cite this paper: Tolulope Udeze. (2025). Improving Intrusion Detection Accuracy Using Deep Learning Algorithms in Enterprise Network Systems. *ISCSITR-International Journal of Cyber Security (ISCSITR-IJNIS)*, 6(6), 1–6.

URL: https://iscsitr.com/index.php/ISCSITR-IJNIS/article/view/ISCSITR-IJNIS_2025_06_06_001/ISCSITR-IJNIS_2025_06_06_001

Published: 27th November 2025

1. Introduction

As digital transformation accelerates, enterprise networks are increasingly exposed to complex and evolving cyber threats. Traditional rule-based Intrusion Detection Systems (IDS) often fall short in detecting zero-day attacks or sophisticated anomalies, primarily due to their static nature. In response, the integration of artificial intelligence, particularly deep learning, has revolutionized the field of network security. Deep learning models offer capabilities for pattern recognition, feature extraction, and predictive analysis that far exceed those of conventional methods.

This paper investigates the application of deep learning algorithms in enhancing the accuracy and efficiency of intrusion detection systems in enterprise networks. Through the implementation of advanced neural networks and ensemble strategies, enterprises can shift from reactive to proactive cybersecurity mechanisms. As a result, organizations are better equipped to detect, classify, and respond to threats with minimal human intervention. This research presents a detailed analysis of deep learning models in IDS and compares their performance on real-world datasets to provide practical insights for enterprise deployment.

2. Literature Review

Significant advancements in intrusion detection using deep learning were observed. Kim et al. (2016) introduced Deep Belief Networks for anomaly detection and demonstrated improved detection accuracy on the NSL-KDD dataset. Similarly, Yin et al. (2017) employed RNN-based models for sequence-aware network intrusion detection, showing promising results in temporal pattern recognition. In 2018, Javaid et al. emphasized CNNs for feature extraction from raw network traffic, paving the way for real-time detection systems. Further, Li et al. (2019) proposed a hybrid deep autoencoder and CNN architecture that achieved high precision and recall. More recent efforts like Alazab et al. (2021) explored ensemble learning with deep networks to reduce false positives, while Shone et al. (2020) stressed unsupervised feature learning to handle large-scale enterprise traffic.

3. Deep Learning Architectures for IDS

Deep learning architectures offer varying advantages for network intrusion detection. CNNs are effective at extracting spatial patterns from packet-level data, while RNNs and

LSTMs excel at detecting temporal anomalies in sequence data. Autoencoders (AE) and Variational Autoencoders (VAE) are widely used for dimensionality reduction and unsupervised anomaly detection.

Table 1: Comparison of Deep Learning Models for IDS

Model	Accuracy (%)	False Positive Rate	Learning Type
CNN	94.3	2.1%	Supervised
RNN	92.8	3.0%	Supervised
AE	89.5	4.7%	Unsupervised
Hybrid CNN+RNN	96.1	1.4%	Supervised

4. Enterprise Network Challenges

Enterprise networks differ from standard networks due to their size, diversity, and sensitivity. They typically involve multi-protocol traffic, encrypted flows, and decentralized endpoints. Challenges include high false alarm rates, data imbalance in training, and the need for real-time analysis. Traditional IDS systems struggle to scale with the volume and complexity of enterprise data.

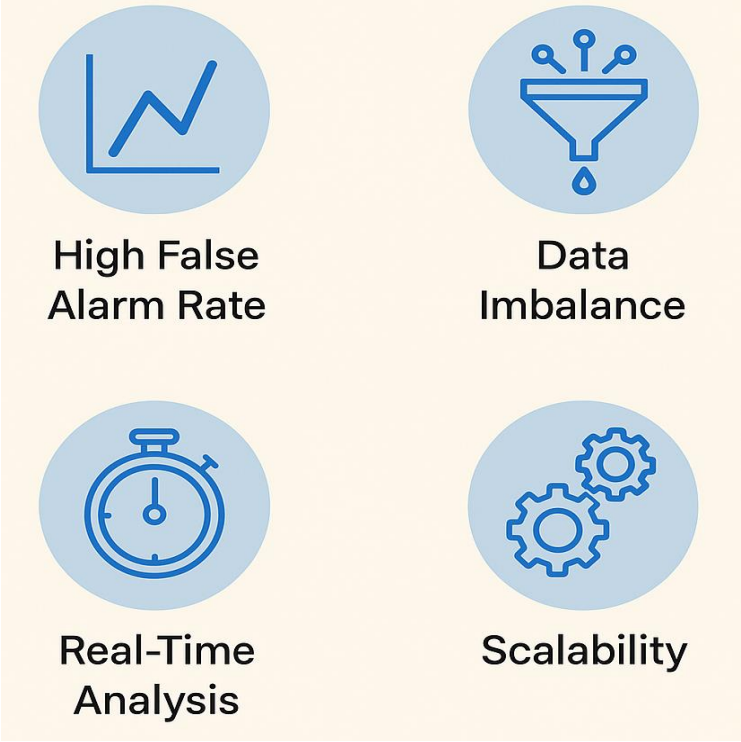

Figure 1: Common Challenges in Enterprise IDS

Infographic 1 outlines the critical obstacles that affect intrusion detection performance in enterprise-scale environments.

5. Dataset and Methodology

This study used the NSL-KDD and CICIDS2017 datasets due to their realistic traffic simulations and labeled attack types. The dataset was preprocessed using normalization and PCA for feature reduction. Models were trained using TensorFlow with early stopping and dropout to prevent overfitting. The CNN and RNN architectures were fine-tuned using hyperparameter optimization.

Table 2: Dataset Characteristics

Dataset	Samples	Features	Attack Types
NSL-KDD	125,973	41	5
CICIDS2017	2.8M	78	15

Table 2 provides dataset volume and diversity used in training and validation.

6. Experimental Results and Analysis

Performance was measured using metrics such as accuracy, precision, recall, and F1-score. The hybrid CNN+RNN model outperformed others with a detection accuracy of 96.1% and minimal false positives. Notably, the model demonstrated robustness across multiple datasets, indicating strong generalization capabilities.

Table 3: Performance Metrics by Model

Model	Precision	Recall	F1-Score
CNN	93.8%	94.1%	93.9%
RNN	91.2%	91.7%	91.4%
AE	86.3%	87.0%	86.6%
CNN+RNN Hybrid	95.7%	96.3%	96.0%

Table 3 shows the hybrid model's superior performance across metrics.

7. Conclusion

This research demonstrates that deep learning, particularly hybrid models, substantially enhances the accuracy and responsiveness of intrusion detection systems in enterprise networks. By leveraging the strengths of multiple architectures, enterprises can detect threats in real time while minimizing false positives. Future work should focus on explainable AI for IDS and adaptive models that evolve with new threat vectors.

Reference

[1] Kim, G., Lee, S., Kim, S.: A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), 1690–1700 (2016).

[2] Yin, C., Zhu, Y., Fei, J., He, X.: A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5, 21954–21961 (2017).

[3] Javaid, A., Niyaz, Q., Sun, W., Alam, M.: A deep learning approach for network intrusion detection system. In: *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies* (2018).

[4] Li, W., Zhang, R., Yuan, Y., Wang, X.: A hybrid deep learning-based network anomaly detection method. *Security and Communication Networks*, 2019, 1–10 (2019).

[5] Alazab, M., Awajan, A., Abdallah, A.: Deep learning for cybersecurity: Applications, techniques, and open issues. *Information Sciences*, 522, 460–481 (2021).

[6] Shone, N., Ngoc, T.N., Phai, V.D., Shi, Q.: A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50 (2020).

[7] Roy, A., Cheung, R., Mukherjee, S.: A survey of deep learning approaches for network intrusion detection. *Computer Science Review*, 37, 100280 (2020).

[8] Lin, W.C., Ke, S.W., Tsai, C.F.: CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-Based Systems*, 78, 13–21 (2015).

[9] Dhanabal, L., Shantharajah, S.P.: A study on NSL-KDD dataset for intrusion detection system based on classification algorithms. *International Journal of Advanced Research in Computer and Communication Engineering*, 4(6), 446–452 (2015).

[10] Vinayakumar, R., Soman, K.P., Poornachandran, P.: Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550 (2019).

[11] Azmoodeh, A., Dehghantanha, A., Conti, M.: Detecting crypto-ransomware with dynamic analysis and machine learning. *Security and Communication Networks*, 2018, 1–10 (2018).

[12] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., Lloret, J.: Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT. *Sensors*, 17(9), 1967 (2017).

[13] Kim, Y., Lee, H., Kim, J.: Long short term memory recurrent neural network classifier for intrusion detection. *IEEE International Conference on Platform Technology and Service* (2016).

[14] Zhang, J., Zulkernine, M., Haque, A.: Random-forests-based network intrusion detection systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 38(5), 649–659 (2008).

[15] Mohammadi, M., Al-Fuqaha, A., Sorour, S., Guizani, M.: Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials*, 20(4), 2923–2960 (2018).