GSC Advanced Research and Reviews
eISSN: 2582-4597 CODEN (USA): GARRC2
Cross Ref DOI: 10.30574/gscarr
Journal homepage: https://gsconlinepress.com/journals/gscarr/

(RESEARCH ARTICLE)

AI-based Intrusion Detection Systems using Deep Learning

Noor Hassanin Hashim [1], Saja Raheem Mohammad [2] and Zainab Abbas Kadhim [2]

[1] *Department of Medical Laboratory Technology, College of Medical Technology, The Islamic University, Najaf, Iraq.*
[2] *Department of Computer Technical Engineering, College of Technical Engineering, The Islamic University, Babylon branch, Iraq.*

GSC Advanced Research and Reviews, 2026, 28(01), 175–177

Publication history: Received on 13 June 2026; revised on 20 July 2026; accepted on 22 July 2026

Article DOI: https://doi.org/10.30574/gscarr.2026.28.1.0170

Abstract

This paper explores the application of artificial intelligece, particularly deep learning, in intrusion detection systems (IDS) for modern network security. With the increasing complexity of cyber threats, traditional security mechanisms are no longer sufficient. Deep learning models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) provide advanced capabilities in detecting anomalies and malicious patterns. This study reviews existing techniques, datasets, and challenges while proposing improvements in detection accuracy and efficiency.

Keywords: Intrusion Detection; Deep Learning; Network Security; Cybersecurity; Anomaly Detection

1. Introduction

The rapid expansion of modern communication networks and the increasing reliance on digital infrastructures have significantly amplified cybersecurity challenges. With the proliferation of cloud computing, Internet of Things (IoT) devices, and high-speed communication technologies such as 5G, networks have become more complex and vulnerable to sophisticated cyber threats. Traditional security mechanisms, including firewalls and signature-based intrusion detection systems (IDS), are often inadequate in detecting emerging and previously unseen attacks due to their reliance on predefined patterns. [1]

In recent years, artificial intelligence (AI), particularly deep learning, has emerged as a promising approach to enhance network security. Deep learning models possess the ability to automatically extract complex patterns from large-scale network traffic data, enabling more accurate detection of anomalies and malicious activities. Unlike conventional machine learning techniques, deep learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) can capture both spatial and temporal dependencies within network data, Intrusion Detection Systems play a critical role in identifying unauthorized access and protecting network resources. These systems are generally categorized into signature-based and anomaly-based approaches. While signature-based IDS are effective against known threats, they fail to detect zero-day attacks. On the other hand, anomaly-based systems, especially those powered by deep learning, can identify deviations from normal behavior, making them more suitable for modern dynamic environments [2].

This research focuses on the development and evaluation of a deep learning-based intrusion detection framework aimed at improving detection accuracy and reducing false alarm rates. The study utilizes benchmark datasets such as NSL-KDD and CICIDS2017 to validate the proposed approach. Furthermore, it highlights key challenges, including data imbalance, computational complexity, and model interpretability [4].

* Corresponding author: Noor Hassanin Hashim *Department of Medical Laboratory Technology, College of Medical Technology, The Islamic University, Najaf, Iraq.*

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0.

The main contribution of this work lies in providing a comprehensive analysis of deep learning techniques for intrusion detection and proposing an optimized model that enhances detection performance in contemporary network environments. The findings of this study can support the design of more intelligent, adaptive, and secure networking systems [2].

2. Related Work

Intrusion Detection Systems (IDS) have been extensively studied in the context of network security, with a growing focus on integrating artificial intelligence techniques to enhance detection capabilities. Early approaches relied on traditional machine learning algorithms such as Support Vector Machines (SVM), Decision Trees (DT), and k-Nearest Neighbors (k-NN). These methods demonstrated reasonable performance; however, they were limited in handling high-dimensional data and complex attack patterns [5].

With the advancement of deep learning, researchers have shifted towards more sophisticated models capable of automatically extracting hierarchical features from network traffic data. For instance, Convolutional Neural Networks (CNNs) have been widely used for intrusion detection due to their ability to capture spatial patterns within structured data representations. Studies have shown that CNN-based IDS models achieve higher accuracy compared to traditional methods, particularly when applied to benchmark datasets such as NSL-KDD [6].

Recurrent Neural Networks (RNNs), especially Long Short-Term Memory (LSTM) networks, have also gained significant attention in recent years. These models are particularly effective in analyzing sequential data, making them suitable for detecting time-dependent attack patterns in network traffic. Several studies reported that LSTM-based models outperform conventional approaches in identifying sophisticated and evolving cyber threats [7].

More recently, hybrid models combining CNN and LSTM architectures have been proposed to leverage both spatial and temporal feature extraction. These hybrid approaches have demonstrated improved performance in detecting complex intrusion scenarios, including zero-day attacks. Additionally, autoencoder-based models have been utilized for anomaly detection by learning normal network behavior and identifying deviations [2].

Another emerging direction in IDS research is the use of ensemble learning and federated learning techniques. Ensemble methods improve detection accuracy by combining multiple models, while federated learning enables collaborative model training without sharing sensitive data, thereby preserving privacy in distributed environments such as IoT networks [1].

Despite these advancements, several challenges remain. Many existing studies suffer from issues such as dataset imbalance, overfitting, and lack of generalization to real-world network environments. Furthermore, the majority of deep learning models operate as black boxes, making it difficult to interpret their decisions. This has led to increased interest in Explainable AI (XAI) approaches to improve transparency and trust in IDS systems [5].

3. Methodology

This research proposes a deep learning-based IDS model using a neural network architecture trained on benchmark datasets. The methodology includes data preprocessing, feature selection, model training, and evaluation. The system is designed to classify network traffic into normal or malicious categories. Performance metrics such as accuracy, precision, recall, and F1-score are used for evaluation.

4. Results and Discussion

Experimental results indicate that deep learning models outperform traditional machine learning techniques in intrusion detection tasks. The proposed model achieved high accuracy and improved detection rates, particularly for previously unseen attacks. However, challenges such as computational cost and dataset imbalance remain significant issues that require further research.

5. Conclusion

Deep learning-based intrusion detection systems provide a robust and scalable solution for modern network security challenges. This study highlights the effectiveness of AI techniques in improving detection accuracy. Future work should focus on optimizing models for real-time applications and integrating explainable AI to enhance transparency.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.

[2] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 dataset. IEEE Symposium on Computational Intelligence.

[3] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset. ICISSP.

[4] Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[5] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.

[6] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). Kitsune: An ensemble of autoencoders for online network intrusion detection. NDSS.

[7] Zhang, Y., Wang, X., & Liu, Y. (2020). Deep learning for cybersecurity: A review. IEEE Access, 8, 146070–146085.