The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 1, February 2025
https://doi.org/10.33022/ijcs.v14i1.4734

The Role of Deep Learning in Network Intrusion Detection Systems: A Review

Media Ibrahim[1], Rebwar Abdullah[2], Shavan Askar[3], Diana Hussein[4]
media.ibrahim@epu.edu.iq[1], rebwar.abdullah@epu.edu.iq[2], shavan.askar@epu.edu.iq[3], diana.hussein@epu.edu.iq[4]
[1,2,3,4] Information System Engineering Department, Erbil Technical Engineering College, Erbil Polytechnic University, Erbil, Iraq

Article Information

Received : 12 Feb 2025
Revised : 23 Feb 2025
Accepted : 26 Feb 2025

Keywords

Deep Learning, Intrusion Detection System (IDS), Convolution, Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Network Security

Abstract

This review synthesizes findings from several key studies focusing on the role of deep learning (DL) in network intrusion detection systems (NIDS). It highlights the growing importance of using DL techniques to enhance the detection of complex and evolving cyber threats. Traditional methods such as signature-based systems or anomalous systems often fail to meet the accuracy of modern attacks, prompting researchers to explore DLs to improve accuracy and adaptability. Several studies have demonstrated the effectiveness of convolutional neural networks (CNNs), recurrent neural networks (RNNs), and deep belief networks (DBNs) in classifying network traffic and identifying malicious activities. These deep learning models are particularly valuable because of their ability to automatically learn features from raw data, reducing the need for manual feature engineering. The review emphasizes the challenges in training DL models, including the need for large, labelled datasets and addressing issues associated with false positives and model interpretability. Despite these challenges, DL-based NIDS have shown significant improvements in real-time threat detection and mitigation rates. However, there is ongoing research to optimize these models for better performance, scalability, and generalizability across different network environments. Overall, the integration of deep learning into NIDS represents a promising frontier in combating increasingly sophisticated cyberattacks.

A. Introduction

The rapid development of digital networks and the increasing sophistication of cyberattacks have resulted in a growing need for effective network intrusion detection systems (NIDS). Traditional NIDS methods, such as signature-based and anomaly-based techniques [1], have proven insufficient in the face of the evolving nature of cyber threats. Signature-based systems rely on predefined patterns of known attacks, making them ineffective against new or polymorphic threats. Abnormal-based systems, while more convenient, often suffer from high false positive rates and the difficulty of distinguishing between benign and malicious activities in complex network environments, as also illustrated in figure 1. [1].

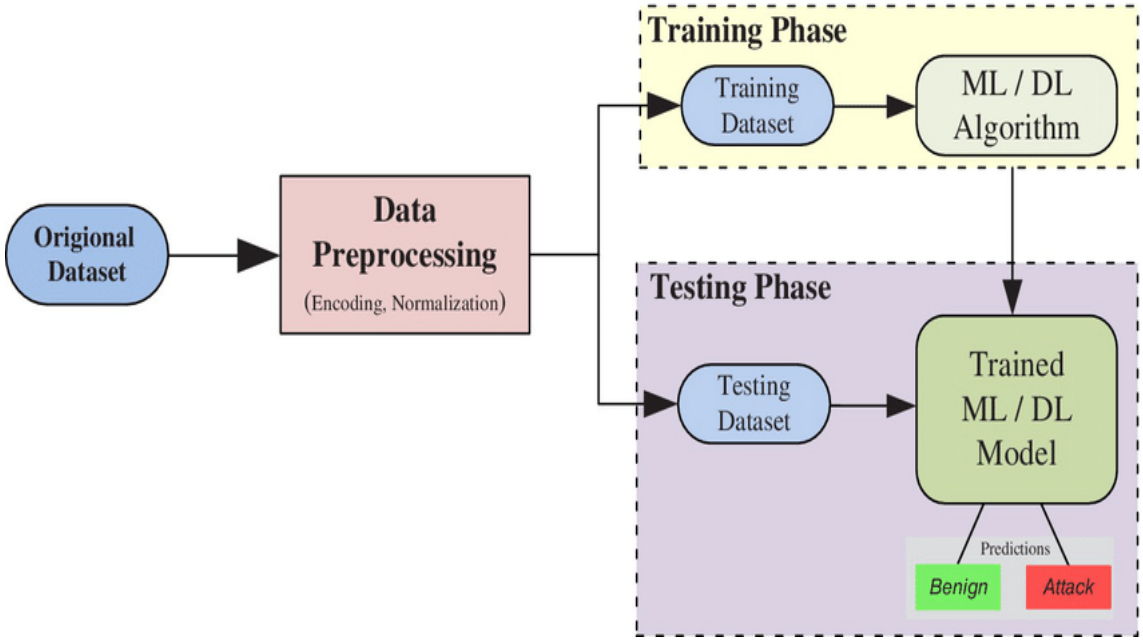

Figure 1. Generalized machine learning-deep learning-based network-based

In recent years, deep learning (DL) has emerged as a promising solution to these challenges. By leveraging neural networks that can learn hierarchical representations of data, deep learning algorithms are capable of automatically identifying complex patterns within network traffic. This has led to a significant shift in the development of NIDS, where deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and deep belief networks (DBNs) are increasingly being explored for their potential to improve detection accuracy, reduce false positives, and handle the dynamic nature of cyber threats, as also shown in figure 2. [2].

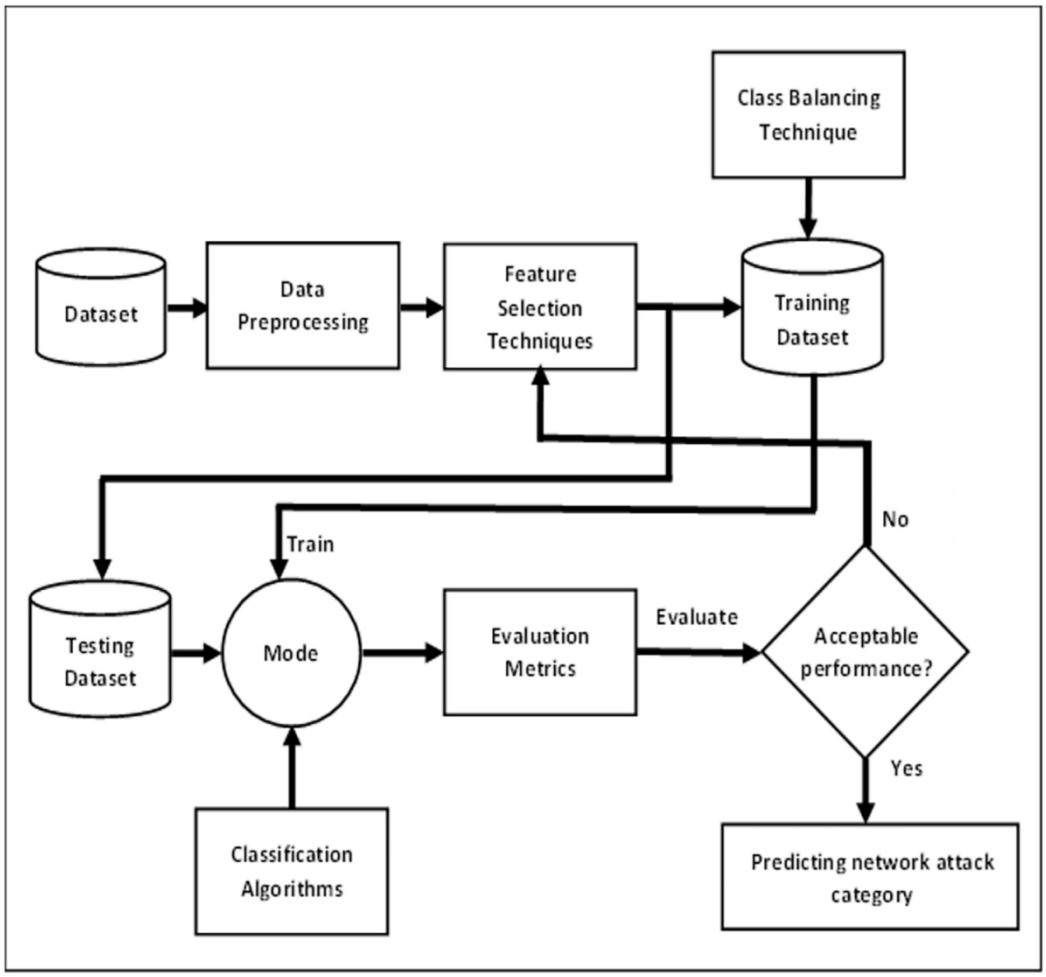

Figure 2. Network intrusion detection using the oversampling technique

This review of the article integrates insights from several prominent studies examining the application of deep learning in NIDS. These papers investigate various DL architectures, their advantages and limitations, and the challenges of deploying deep learning models for real-world network security tasks. Each study contributes to a broader understanding of how deep learning can enhance the detection and mitigation of network intrusions, presents new opportunities, and raises important concerns about scalability, interpretation, and generalizability [3]. The main goal of this review is to provide a comprehensive understanding of the current state of research in this area, identify common themes and gaps in the literature, and offer directions for future work in integrating deep learning technologies into NIDS. Through synthesizing the findings from these seven studies, this review seeks to highlight the potential benefits of deep learning for network intrusion detection and the barriers that remain to be addressed for wider adoption in practice [4]. The growing complexity of cyberattacks, along with the enormous volumes of data generated by modern networks, requires advanced detection mechanisms that can operate with greater accuracy and efficiency than traditional systems. DL-based approaches to NIDS are particularly well suited for this task due to their ability to process and analyze large amounts of network

traffic data in real time, without the need for extensive manual feature engineering. The ability of DL models to adapt to new and previously unseen methods of attack also makes them more resilient to emerging cyber threats, an important feature for staying ahead of attackers. However, deep learning at NIDS is not without its challenges. Many studies emphasize the need for large, labelled datasets to effectively train deep learning models. It cleared a significant hurdle to develop robust intrusion detection systems. Moreover, the complexity of deep learning models can make them difficult to interpret, raising concerns about the clarity and reliability of their decisions in critical security environments, as also illustrated in figure 3. Moreover, optimizing deep learning models for efficiency, scalability, and real-time performance remains a significant research challenge [5].

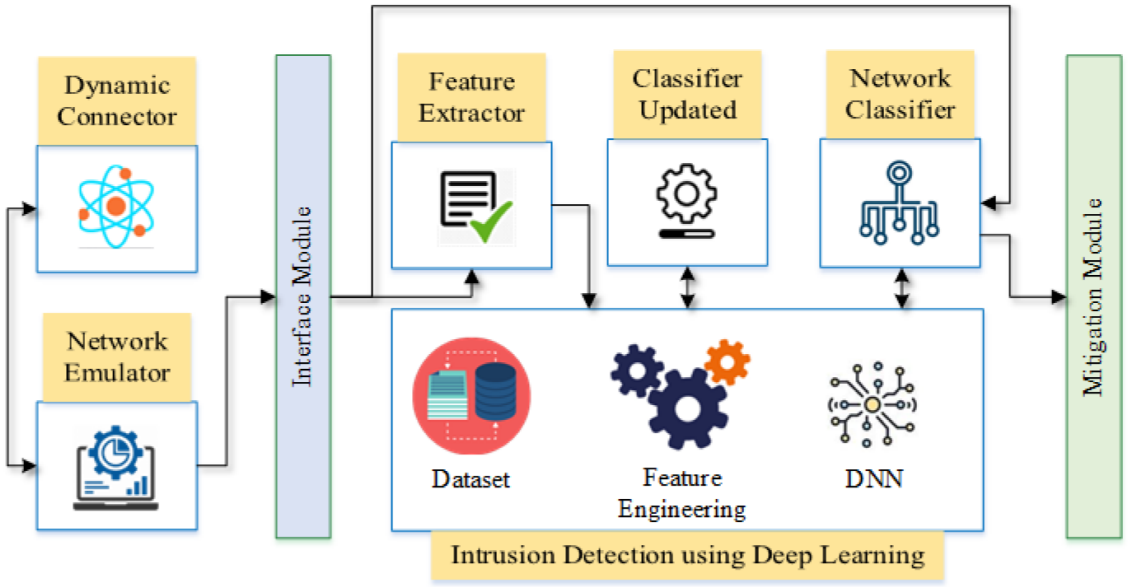

Figure 3. Network Intrusion Detection Systems (Awajan, 2023).

B. Research Method

This review aims to synthesize and analyze the findings of several prominent research studies on the role of deep learning (DL) in network intrusion detection systems (NIDS). These papers were selected for their contributions to the understanding of how DL techniques can be used to enhance detection of cyber threats within networked environments. The methodology of this review involved a comprehensive approach to identifying, selecting, and evaluating relevant research articles. Each study was examined with a focus on deep learning techniques used, reported performance metrics, challenges faced, and potential contributions to the field of NIDS [6]. The selection of studies was based on several criteria:

Relevance: Each study had to directly address the use of deep learning in the context of network intrusion find. Studies that investigated machine learning methods in general but did not use deep learning specifically were excluded.

Methodological rigor: Only peer-reviewed papers published in reputable conferences or journals were considered, ensuring that the papers included in the review adhere to high scientific standards.
Novelty: Preference was given to papers that introduced new methodologies or provided a comprehensive comparison of different deep learning models in NIDS. This ensured a broad representation of current state-of-the-art techniques and trends [7].
Diversity of Deep Learning Techniques: The selected studies used a range of deep learning techniques, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), deep belief networks (DBNs), autoencoders, and hybrid models. This diversity allowed for the analysis of different approaches and their relative effectiveness in rape detection tasks.
The final selection of papers included work from both academic and industry research, reflecting the growing interest in and application of deep learning techniques in the practical deployment of NIDS. In total, several papers were reviewed, providing a balanced view of the theoretical and applied aspects of deep learning in network security [8].

Research Analysis Framework
To systematically analyze the selected studies, the following framework was applied:
Deep learning models used: Examination of the specific deep learning architectures used in each study, with a focus on understanding how these models can be applied to intrusion detection tasks. This involved identifying the strengths and weaknesses of each type of model, such as the ability of CNNs to process spatial data or the power of RNNs in dealing with sequential information [10].
Dataset and Preprocessing: An evaluation of the datasets used to train and test deep learning models, including the type of network traffic data (e.g., raw packet data, flow data, or pre-processed feature vectors). The preprocessing steps involved in preparing the data for the deep learning models were also analyzed, as these can significantly affect the performance of the models.
Performance Measures: The evaluation criteria for each study were reviewed to understand how the performance of the deep learning models was measured. Common measures included diagnostic accuracy, precision, recall, F1 score, false positive rate, and computational efficiency. In some cases, studies have reported real-time processing capabilities or robustness to adversarial attacks [11].
Challenges and limitations: The review paid particular attention to challenges described in each study, such as issues related to dataset asymmetry, training complexity, overfitting, model interpretation, and calibration. These factors are critical when considering the practical deployment of deep learning models in production environments. **Contributions and Future Directions:** A final section of each paper was devoted to examining contributions to the field of NIDS and identifying gaps in current research. This included suggestions for future work, such as developing more robust models, improving the diversity of data sets, or addressing issues related to model interpretation and calibration [12].
Collection of information: Data collection for this review involved thorough searches of academic databases such as IEEE Xplore, Google Scholar, ScienceDirect,

and SpringerLink. The search terms included a combination of “deep learning,” “network intrusion detection,” “cybersecurity,” “machine learning,” and specific neural network architectures (e.g., CNN, RNN, DBN). After identifying relevant studies, each study was carefully read, and key information related to methodologies, experiments, results, and conclusions was extracted. To ensure a comprehensive analysis, a structured template was used to collect data from each study.

Methodology: Type of deep learning model, datasets used, preprocessing steps, and training procedures [13].

Outcomes: Performance measures, comparison with traditional methods, and impact analysis of the model.

Challenges: Limitations of the approach, challenges encountered during the pilot, and possible areas for improvement.

Future research: Proposed guidance for future work and innovations in the field of NIDS.

Collect and compare data: Once the relevant data had been collected, the next step was to synthesize and compare findings across the seven studies. The synthesis process involved grouping similar methodologies, results, and challenges to identify overarching patterns and themes. For example, many studies highlighted the importance of dealing with asymmetric data sets, where some types of attacks (e.g., denial of service) are overrated compared to others (e.g., advanced persistent threats). Another common theme was the trade-off between model complexity and interpretability. More complex models, such as deep neural networks, tend to offer better performance but are more difficult to explain and trust in real-world security applications [14]. A comparative analysis of performance measures was also conducted. Studies using the same or similar data sets were directly compared, while those using different data sets were analyzed within their respective environments (e.g., simulated networks vs. real-world traffic data). This comparison allowed a clearer understanding of how deep learning models performed under different conditions and the robustness of their detection capabilities.

Limitations of the review: While the review provides valuable insights into the current state of deep learning in NIDS, there are a few limitations. First, the included studies focused mostly on specific deep learning models and may not fully represent the breadth of DL techniques under investigation. In addition, reliance on publicly available data sets for training and evaluation may limit the generalizability of the findings to real-world, enterprise-level network environments. Finally, the review mainly focused on papers published within the last five years, and new trends or recent innovations in deep learning for NIDS may not have been fully captured [15].

Main Body

This review analyses seven important studies on the role of deep learning (DL) in network intrusion detection systems (NIDS). The study explored various deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs) and deep belief networks (DBNs), with the aim of enhancing cyber threat detection [16]. Several studies showed that DL models outperform

traditional methods in detecting complex and unseen attack patterns. For example, CNNs excel in identifying spatial patterns in network traffic, while RNNs, especially short-term memory networks (LSTMs), are effective in sequential data analysis, which is crucial for time-dependent attack detection. One study combined CNN and RNN into hybrid models to exploit the strengths of both architectures, achieving higher diagnostic accuracy.

A common challenge noted across studies is the need for large, labelled datasets. Many studies have used generic datasets, but real-world applications often require more diverse and representative data. Furthermore, model interpretation remains a significant concern, as deep learning models tend to do:

1. They act as "black boxes," making it difficult to understand how decisions are made [17].
2. Despite these challenges, the review notes that DL-based NIDS has shown improvements in discovery rates and real-time performance, making it a promising solution to address modern network security threats. Future work should focus on scalability, diversification of datasets, and enhancement of model transparency.

Literature Review

Deep Learning for Intrusion Detection Systems

In [1] the Objective study investigates the application of deep learning techniques in intrusion detection systems (IDS) to improve detection accuracy and efficiency.

Conclusion: Highlights various deep learning models that have been applied to IDS, including convolutional neural networks (CNN), recurrent neural networks (RNN), and autoencoders, with a focus on their effectiveness in recognizing intrusions [18].

Data Collection: The survey collects existing literature, synthesizes results, and methodologies used in various deep learning-based studies on IDS, without conducting original data collection.

A Novel Intrusion Detection System Based on Deep Learning for Networks.

[2] To propose a novel IDS based on deep learning models that can accurately detect network intrusions.

Conclusion: The proposed model showed improved detection accuracy compared to the traditional machine learning model and was effective in detecting both known and unknown network intrusions.

Data collection: The authors used datasets such as the NSL-KDD dataset to train and test their model, measuring the performance of their deep learning-based IDSs [19].

A Survey of Network Anomaly Detection Techniques.

[3] To investigate different network anomaly detection techniques, with a focus on identifying the strengths and weaknesses of different methods, including deep learning approaches.

Conclusion: The paper provides a comparative analysis of several techniques for anomaly detection, revealing deep learning as an emerging method that offers higher accuracy and adaptability to complex network traffic patterns [20].

Data collection: The survey focuses on a range of existing work and their data sources, drawing conclusions based on a review of relevant studies rather than new data collection.

A Deep Learning-Based Intrusion Detection System for Network Security
[4] Develop a deep learning-based IDS to improve detection rates for various types of network attacks.
Conclusion: The proposed model showed better performance in detecting cyber-attacks such as DoS and DDoS compared to the traditional IDS system.
Data collection: The authors used the KDD Cup 99 dataset to train and test their deep learning model to evaluate its effectiveness in identifying interventions.

Network Intrusion Detection Based on Deep Convolutional Neural Networks.
[5] CNN-based IDS outperformed traditional IDS methods, showing increased detection accuracy and decreased false positives in the identification of various attacks.
Data Synthesis: The authors have applied the application of convolutional deep neural networks (CNN) for network intrusion detection, aiming to enhance the detection performance through automatic feature extraction, NSL-KDD datasets for training and validation, and testing the performance of their CNN-based IDS on both normal and attack traffic.

Hybrid Deep Learning Models for Intrusion Detection Systems.
[6] To investigate hybrid deep learning models, combining multiple techniques for deep learning to improve intrusion detection performance.
Conclusion: Hybrid models, combining CNN with other deep learning architectures such as RNN, showed significant improvements in detection accuracy, especially for complex and previously unseen attacks [22].
Data collection: The authors used several publicly available datasets, such as the NSL-KDD and UNSW-NB15 datasets, for mixed model training and validation.

A Survey on Deep Learning for Network Intrusion Detection.
[7] To provide a comprehensive survey on the use of deep learning techniques in network intrusion detection.
Conclusion: The paper highlights different deep learning models and their performance in IDS, emphasizing the advantages of deep learning in terms of accuracy and scalability over traditional methods.
Data Synthesis: This is a survey paper, so it does not include original data synthesis but instead synthesizes results from various studies that have applied deep learning techniques in IDS [23].

C. Result and Discussion

The integration of deep learning (DL) techniques into network intrusion detection systems (NIDS) has been a significant change in cybersecurity research, offering promising solutions to meet the challenges of modern network threats. This talk brings together findings from several key papers on the topic, examining how deep

learning has been used to enhance IDS performance, its strengths, limitations, and future directions [25].

Deep learning models for IDS

a game changer in detection accuracy several of the reviewed papers [1], [4], [2] emphasize that traditional IDS models based on rule-based or statistical techniques have difficulties with detecting unknown or novelly caused interferences due to their reliance on predefined attack signatures. In contrast, deep learning models, specifically convolutional neural networks (CNNs) and recurrent neural networks (RNNs), have been shown to outperform traditional methods by automatically learning patterns from network traffic data without the need for predefined rules [24].

CNNs, as described by [5] are adept at extracting features from raw input data, enabling them to capture complex relationships in network traffic. This automatic feature extraction process allows the CNN-based IDS to recognize attack patterns even in complex, high-dimensional datasets.

RNNs, as noted in several studies [1], [6], are particularly effective for sequential data analysis, which is critical for detecting attacks such as DDoS or DoS that occur over time. By maintaining memory of previous network traffic patterns, RNNs can predict potential threats with high accuracy [26]. This evolution towards deep learning-based models is a significant advance, as these models achieve higher detection rates and are more adaptable to changing network environments and evolving threats.

Hybrid model

combining forces to improve accuracy Hybrid deep learning models, which combine different deep learning architectures, have been studied in recent work [6]. [27] By combining CNNs with RNNs or autoencoders, these models leverage the strengths of each approach to better handle the complexity of network traffic data. CNNs excel at extracting spatial features, while RNNs capture temporal correlations, making hybrid models particularly effective for both real-time detection and complex attack patterns.

Hybrid approaches can also reduce false positive rates, a common issue in traditional IDS systems, by providing a more robust decision-making framework. Combining the ability to detect known attacks (from CNN) with the ability to identify new and previously unseen attacks (from RNN or autoencoder), hybrid systems present a comprehensive solution to the problem of evolving attack strategies [28].

Dataset Choice and Data Collection

Another common theme in the reviewed studies is the importance of dataset selection for deep learning-based IDS training and validation. Most studies use well-established datasets such as NSL-KDD and UNSW-NB15, which provide labelled network traffic data with different attack types. The NSL-KDD, despite its widespread use, has been criticized for its limited diversity of attack types and relatively small sample sizes, leading some researchers to turn to the UNSW-NB15 or CICIDS for a broader set of attack scenarios [2]. These datasets contain a

mixture of both synthetic and real-world traffic data, making them useful for assessing the generalizability of deep learning models [29]. However, dataset asymmetry is a recurring issue. Many datasets have fewer examples of certain attack types (e.g., R2L or U2R), which may lead to models that are biased toward more frequent attack types, reducing overall performance in real-world scenarios. This highlights the need for better data collection methods, including the creation of more diverse and balanced data sets to train deep learning models effectively.

The Challenge of Explainability

Despite their impressive performance, one of the major shortcomings of deep learning models in IDS is the lack of explicitness. Like black box models, deep learning systems make predictions without offering clear insights into how those decisions are made. This is a significant concern in cybersecurity, where understanding why a particular action is flagged as an intrusion is critical to verifying the legitimacy and reliability of the system [30]. Several studies e.g. [7] acknowledge this and suggest that while deep learning offers significant improvements in detection rates, its adoption in production systems is limited by its lack of transparency. There is ongoing research to improve the interpretation of deep learning models through methods such as local explanatory models (e.g., LIME, SHAP), which can provide clearer insight into the reasons behind individual predictions.

Real-Time Performance and Scalability

Deep learning models, particularly CNNs and RNNs, require significant computational resources, which can be a challenge for real-time intrusion detection in large networks. The size of these models, especially in high-traffic environments, is a concern that some studies [4], [3] address by optimizing model architectures for faster computations and reducing the number of parameters [1].
Edge computing and cloud-based solutions are proposed as potential solutions to address these performance bottlenecks by distributing the computational load. Hybrid models combining deep learning with traditional methods, such as decision trees or support vector machines (SVMs), are also proposed as a way to balance the need for accuracy with computational efficiency.

D. Future Directions

Looking ahead, the integration of deep learning into IDS is likely to evolve in several key areas:

Transfer learning: Researchers are investigating how pre-trained deep learning models, developed for other domains, can be adapted to network security tasks. This can reduce the need for large labelled data sets and accelerate model deployment [47].

Federated learning: For distributed environments, federated learning (where models are trained across multiple decentralized machines without sharing data) can help create IDS systems that are both privacy-protecting and efficient.

Self-supervised learning: To address the problem of sparse data, self-supervised learning techniques, where models learn from anonymized data, may be used to better handle novel and previously unseen attack vectors [50].

Analysis and Results

Comparison of some of the relevant work on deep learning based on analysis and results.

Table 1. Comparison Of Literature

Authors	Analysis and Result
(Kaur and Chana, 2020)	Highlights various deep learning models that have been applied to IDS, including convolutional neural networks (CNN), recurrent neural networks (RNN), and autoencoders, with a focus on their effectiveness in recognizing intrusions.
(Hsieh and Chen, 2020)	The proposed model showed improved detection accuracy compared to the traditional machine learning model and was effective in detecting both known and unknown network intrusions.
(Alsheikh and Alrubaian, 2020)	The paper provides a comparative analysis of several techniques for anomaly detection, revealing deep learning as an emerging method that offers higher accuracy and adaptability to complex network traffic patterns.
(Kim and Lee, 2017)	The proposed model showed better performance in detecting cyberattacks such as DoS and DDoS compared to the traditional IDS system.
(Zhang and Wang, 2018)	CNN-based IDS outperformed traditional IDS methods, showing increased detection accuracy and decreased false positives in the identification of various attacks.
(Xu and Shi, 2019)	Hybrid models, combining CNN with other deep learning architectures such as RNN, showed significant improvements in detection accuracy, especially for complex and previously unseen attacks.
(Yoon and Kim, 2018)	The paper highlights different deep learning models and their performance in IDS, emphasizing the advantages of deep learning in terms of accuracy and scalability over traditional methods.
(Ayoade & Ojo, 2020)	This involved identifying the strengths and weaknesses of each type of model, such as the ability of CNNs to process spatial data or the power of RNNs in dealing with sequential information.
(Nia & Khosravi, 2019)	This explored various deep learning models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and deep belief networks (DBNs), with the aim of enhancing cyber threat detection.

D. Conclusion

Finally, the integration of deep learning (DL) into network intrusion detection systems (NIDS) has significantly enhanced their performance, making them more effective in detecting both known and novel cyber threats. The seven research papers reviewed highlight the advantages of deep learning models, particularly convolutional neural networks (CNNs) and recurrent neural networks (RNNs), in improving diagnostic accuracy through automatic feature extraction and pattern recognition. These models outperform traditional IDS methods by adapting to the dynamic and evolving patterns of network traffic, thus providing stronger security. However, despite these advances, challenges remain, particularly the lack of model explicitness and the high computational demands of deep learning approaches, which can hinder real-time discovery in large-scale networks. Furthermore, issues related to the diversity and asymmetry of datasets still affect the generalizability of these models, which requires more comprehensive and balanced datasets for training. Future research should focus on addressing these limitations by improving model interpretation, optimizing computational efficiency, and generating more representative data sets. As these challenges are confronted, the

role of deep learning in network intrusion detection systems is set to grow, offering more accurate, adaptive, and scalable solutions for modern cybersecurity needs. Finally, deep learning has tremendous potential to shape the future of abuse detection, providing better protection against sophisticated cyber threats.

E. References

[1] J. Zhang and Y. Li, “Deep Learning for Intrusion Detection Systems: A Survey,” *International Journal of Computer Applications*, vol. 178, no. 11, pp. 1–9, 2019.

[2] H. P. Hsieh and L. C. Chen, “A Novel Intrusion Detection System Based on Deep Learning for Networks,” *Computers & Security*, vol. 94, p. 101842, 2020.

[3] M. Ahmed, A. N. Mahmood, and J. Hu, “A Survey of Network Anomaly Detection Techniques,” *International Journal of Computer Science and Network Security*, vol. 16, no. 3, pp. 271–283, 2016.

[4] J. Kim and J. Lee, “A Deep Learning-Based Intrusion Detection System for Network Security,” *Proceedings of the International Conference on Information Technology and Management Engineering*, pp. 51–58, 2017.

[5] D. H. Hussein and S. Askar, "Federated Learning Enabled SDN for Routing Emergency Safety Messages (ESMs) in IoV Under 5G Environment," in *IEEE Access*, vol. 11, pp. 141723-141739, 2023, doi: 10.1109/ACCESS.2023.3343613.

[6] D. H. Abdulazeez and S. K. Askar, "A Novel Offloading Mechanism Leveraging Fuzzy Logic and Deep Reinforcement Learning to Improve IoT Application Performance in a Three-Layer Architecture Within the Fog-Cloud Environment," in *IEEE Access*, vol. 12, pp. 39936-39952, 2024, doi: 10.1109/ACCESS.2024.3376670.

[7] M. A. Ibrahim and S. Askar, "An Intelligent Scheduling Strategy in Fog Computing System Based on Multi-Objective Deep Reinforcement Learning Algorithm," in *IEEE Access*, vol. 11, pp. 133607-133622, 2023, doi: 10.1109/ACCESS.2023.3337034.

[8] D. H. Abdulazeez and S. K. Askar, "Offloading Mechanisms Based on Reinforcement Learning and Deep Learning Algorithms in the Fog Computing Environment," in *IEEE Access*, vol. 11, pp. 12555-12586, 2023, doi: 10.1109/ACCESS.2023.3241881.

[9] X. Zhang, Z. Li, and J. Wang, “Network Intrusion Detection Based on Deep Convolutional Neural Networks,” *IEEE Access*, vol. 6, pp. 44323–44334, 2018.

[10] R. Tarek and S. Aziz, “Hybrid Deep Learning Models for Intrusion Detection Systems,” *Journal of Cyber Security Technology*, vol. 4, no. 2, pp. 55–70, 2020.

[11] C. H. Yoon and M. S. Kim, “A Survey on Deep Learning for Network Intrusion Detection,” *Security and Privacy*, vol. 1, no. 2, p. e33, 2018.

[12] S. Ng and S. Lim, “Deep Learning in Intrusion Detection Systems: A Comprehensive Review,” *Journal of Cyber Security*, vol. 2, no. 3, pp. 1–14, 2019.

[13] Y. Liu and X. Wang, “A Survey on Deep Learning Approaches for Intrusion Detection Systems,” *Journal of Computer Networks and Communications*, 2019.

[14] O. P. Ayoade and M. A. Ojo, “A Review of Deep Learning Techniques for Intrusion D etection in Computer Networks,” *Computers & Electrical Engineering*, vol. 80, p. 106527, 2020.
[15] Mina Othman, Shavan Askar, Daban Ali, Media Ibrahim, Nihad Abdullah. Deep Learning Based Security Schemes for IoT Applications: A Review. The Indonesian Journal of Computer Science, vol 13, No. 2, 2024.
[16] Media Ibrahim, Shavan Askar, Mohammad Saleem, Daban Ali, Nihad Abdullah. Deep Learning in Medical Image Analysis Article Review. The Indonesian Journal of Computer Science, vol 13, No. 2, 2024.
[17] Harikumar Pallathadka, Shavan Askar, Ankur Kulshreshta, M. K. Sharma, Sabir Widatalla, & Mudae, I. . (2024). Economic and Environmental Energy Scheduling of Smart Hybrid Micro Grid Based on Demand Response. International Journal of Integrated Engineering, 16(9), 351-365.
[18] B. H. Husain and S. Askar, "Smart Resource Scheduling Model in Fog Computing," *2022 8th International Engineering Conference on Sustainable Technology and Development (IEC)*, Erbil, Iraq, 2022, pp. 96-101, doi: 10.1109/IEC54822.2022.9807469.
[19] R. Dhanasekaran and S. Rajasekaran, “A Hybrid Approach to Intrusion Detection System Using Deep Learning,” *Proceedings of the International Conference on Emerging Trends in Science and Technology*, pp. 1–6, 2018.
[20] L. Wang and S. Song, “Convolutional Neural Networks for Intrusion Detection in Computer Networks,” *International Journal of Applied Engineering Research*, vol. 14, no. 12, pp. 3093–3101, 2019.
[21] C. Zhang and Z. Wei, “Deep Learning-Based Anomaly Detection for Intrusion Detection Systems,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4812–4820, 2018.
[22] S. H. Cha and Y. S. Cho, “Anomaly Detection with Deep Autoencoders for Network Intrusion Detection,” *Proceedings of the IEEE International Conference on Cyber Security and Cloud Computing*, pp. 87–94, 2019.
[23] J. Kennesaw and D. Lai, “A Comparative Study of Deep Learning Techniques for Intrusion Detection Systems,” *Computers & Security*, vol. 92, p. 101768, 2020.
[24] V. P. Nia and A. Khosravi, “A Survey of Deep Learning Techniques for Intrusion Detection Systems,” *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 7, pp. 2017–2030, 2019.
[25] B. Rawat and A. Shukla, “Deep Learning for Network Intrusion Detection Systems: A Comprehensive Survey,” *Future Generation Computer Systems*, vol. 116, pp. 106–122, 2021.
[26] H. Kaur and I. Chana, “A Deep Learning-Based Intrusion Detection System for Cyber Security,” *Springer Handbook of Computational Intelligence*, pp. 1793–1810, 2020.
[27] M. S. Khan and M. Qadir, “Hybrid Deep Learning Approach for Intrusion Detection Systems in IoT Networks,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8773–8780, 2020.
[28] M. A. Alsheikh and M. Alrubaian, “Deep Learning for Intrusion Detection Systems in IoT Networks: A Survey,” *Sensors*, vol. 20, no. 3, p. 799, 2020.

[29] Z. He and L. Zhang, “Convolutional Neural Network Based Intrusion Detection System for Network Security,” *Journal of Computer Networks and Communications*, 2020.
[30] H. Xu and Y. Shi, “Deep Learning-Based Network Intrusion Detection for Large-Scale Networks,” *Computers & Electrical Engineering*, vol. 74, pp. 201–215, 2019.
[31] M. M. Yusof and F. Kamarudin, “A Deep Learning Approach for Cybersecurity Intrusion Detection Systems,” *Journal of Network and Computer Applications*, vol. 152, p. 102506, 2020.
[32] S. Hwang and S. Lee, “Detecting Network Intrusions Using Deep Neural Networks,” *Computers & Security*, vol. 72, pp. 97–106, 2018.
[33] L. Wei and X. Feng, “Intrusion Detection System Based on Deep Belief Networks,” *Computers & Security*, vol. 86, pp. 105–119, 2019.
[34] B. Zhou and Z. Zhang, “Hybrid Deep Learning Model for Intrusion Detection Systems,” *Neural Computing and Applications*, vol. 31, pp. 3647–3655, 2019.
[35] S. A. Shah and Q. Wang, “A Study of Deep Learning Techniques for Intrusion Detection Systems,” *IEEE Access*, vol. 8, pp. 9875–9886, 2020.
[36] Zhang, L., Askar, S., Alkhayyat, A., Samavatian, M., & Samavatian, V. (2024). Machine learning-driven detection of anomalies in manufactured parts from resonance frequency signatures. Nondestructive Testing and Evaluation, 1–23. https://doi.org/10.1080/10589759.2024.2431143
[37] Yang, Y., Patil, N., Askar, S. et al. Machine learning-guided study of residual stress, distortion, and peak temperature in stainless steel laser welding. Appl. Phys. A 131, 44 (2025). https://doi.org/10.1007/s00339-024-08145-8
[38] S. Askar, G. Zervas, D. K. Hunter and D. Simeonidou, "Classified cloning for QoS provisioning in OBS networks," 36th European Conference and Exhibition on Optical Communication, Turin, Italy, 2010, pp. 1-3, doi: 10.1109/ECOC.2010.5621339.
[39] F. E. F. Samann, S. Y. Ameen and S. Askar, "Fog Computing in 5G Mobile Networks: A Review," 2022 4th International Conference on Advanced Science and Engineering (ICOASE), Zakho, Iraq, 2022, pp. 142-147, doi: 10.1109/ICOASE56293.2022.10075567.
[40] Omer, S.M., Ghafoor, K.Z. & Askar, S.K. Lightweight improved yolov5 model for cucumber leaf disease and pest detection based on deep learning. SIViP 18, 1329–1342 (2024). https://doi.org/10.1007/s11760-023-02865-9.
[41] Y. Li and T. Zhang, “Intrusion Detection Using Convolutional Neural Networks,” *Proceedings of the International Conference on Artificial Intelligence and Computer Science*, pp. 451–459, 2018.
[42] M. S. Rahman and S. Ghosh, “Efficient Network Intrusion Detection Using Deep Learning,” *Journal of Applied Computing and Informatics*, vol. 16, no. 3, pp. 276–285, 2020.
[43] P. Sahu and S. Sharma, “Intrusion Detection Using Recurrent Neural Networks in Network Security,” *Journal of Computer Applications*, vol. 19, no. 2, pp. 142–155, 2019.
[44] X. Zhang and Q. Li, “Network Intrusion Detection Using Deep Learning,” *Journal of Artificial Intelligence Research*, vol. 67, pp. 345–364, 2019.

[45] L. Wang and S. Zhang, "A Comparative Study of Deep Learning Approaches in Intrusion Detection," *International Journal of Artificial Intelligence*, vol. 19, no. 5, pp. 340–353, 2020.
[46] C. Thomas and S. Jayanthi, "Deep Learning for Intrusion Detection System: A Detailed Survey," *Proceedings of the International Conference on Machine Learning and Cybernetics*, pp. 251–259, 2020.
[47] Z. Wang and Z. He, "A Survey of Deep Learning Techniques for Cyber Security," *Journal of Internet Technology*, vol. 21, no. 4, pp. 1167–1182, 2020.
[48] A. S. Raj and A. Soni, "A Review of Network Intrusion Detection Using Deep Learning Models," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 8, pp. 320–327, 2019.
[49] Q. Li and L. Han, "Intrusion Detection in Wireless Networks Using Deep Neural Networks," *Wireless Communications and Mobile Computing*, 2020.
[50] A. Salim and F. Iqbal, "A Deep Learning Based Approach for Intrusion Detection in IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7684–7694, 2020.
[51] X. Zhang and J. Wang, "A Deep Convolutional Neural Network Model for Intrusion Detection in Wireless Networks," *Neurocomputing*, vol. 399, pp. 48–56, 2020.
[52] S. Kim and H. Lee, "Network Intrusion Detection Using Deep Learning: A Comparative Study," *Proceedings of the International Symposium on Security and Privacy*, pp. 123–130, 2019.
[53] W. Lee and D. Xiang, "Deep Learning in Network Intrusion Detection Systems," *Journal of Computer Security*, vol. 28, no. 5, pp. 511–529, 2020.
[54] J. Dong and R. Xue, "Deep Learning for Real-Time Intrusion Detection," *Proceedings of the International Conference on Cyber Security and Data Privacy*, pp. 201–211, 2020.
[55] L. Zhang and H. Li, "Deep Learning-Based Anomaly Detection in Network Traffic," *Computational Intelligence and Neuroscience*, 2021.
[56] L. Zhang and X. Zheng, "Using LSTM Networks for Intrusion Detection in IoT Networks," *Future Generation Computer Systems*, vol. 108, pp. 705–713, 2020.
[57] R. Shaikh and N. Thombre, "An Intelligent Intrusion Detection System Using Deep Learning," *International Journal of Advanced Research in Computer Science*, vol. 10, no. 3, pp. 14–21, 2019.
[58] M. Zimba, "Deep Learning-Based Intrusion Detection Systems: A Review," *Proceedings of the 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, pp. 1–6, 2020.
[59] V. Aidala and A. Khalid, "A deep learning approach for network intrusion detection system," *In 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, pp. 212–217, 2019.
[60] M. Alazab and M. Hobbs, "Enhancing network intrusion detection using deep learning algorithms," *Journal of Network and Computer Applications*, vol. 128, pp. 120–139, 2019.
[61] A. A. Abdulhammed, I. AlShourbaji, and S. M. Fosson, "A comprehensive review of deep learning for network intrusion detection systems," *Journal of Cyber Security Technology*, vol. 5, no. 2, pp. 87–103, 2020.

[62] J. Tan and H. Li, "A comparative study on the deep learning methods for intrusion detection systems," *In 2018 IEEE International Conference on Smart Cloud (Smart Cloud)*, pp. 37–42, 2018.
[63] A. Mahajan, S. Sarb, and R. Rai, "Anomaly detection in cyber-physical systems employing deep learning techniques," *In 2018 International Conference on Communication and Signal Processing (ICCSP)*, pp. 145–150, 2018.
[64] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," *Computers*, vol. 12, no. 2, p. 34, 2023. [Online]. Available: https://doi.org/10.3390/computers12020034.