International Journal of Computational Intelligence in Engineering (IJCIE)
Vol. 01, No. 01, March 2026, pp. 29-35
ISSN: XXXX-XXXX, DOI: 10.5281/10.5281/zenodo.20541381

Intrusion Detection Systems Utilizing Deep Learning: A Comprehensive Literature Review

Manjunath Sargur Krishnamurthy[1]

[1]JP Morgan & Chase Co., Houston, USA. Email: manjunath.skmurthy@yahoo.com

Article Info

Article history:

Received Jan 18, 2026
Revised Mar 20, 2026
Accepted Mar 22, 2026

Keywords:

Intrusion Detection System
Cybersecurity
Network Security
Deep Learning
Anomaly Detection

ABSTRACT

Certainly, with the increasing sophistication of cyberattacks, the need for intelligent Intrusion Detection Systems (IDSs) that can detect known and unknown threats in real time has become more critical than ever. Conventional IDSs (e.g., signature- and machine-learning based) are not effective against high-dimensional network traffic, zero-day attacks, and dynamic threat environments. With the ability to automatically capture complex features and learn hierarchical representations from a large volume of network data, Deep Learning (DL) has been a promising solution. In this review, the progress in deep learning IDS research from 2020 to 2026 is discussed. The study examines several architectures, such as Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders (AEs), Generative Adversarial Networks (GANs), and Transformer-based models. In addition, the commonly used benchmark datasets, performance measures, challenges, and future research directions are discussed. The review shows that the hybrid deep learning architecture consistently outperforms the traditional methods in terms of performance, with an accuracy of high detection performance and low false alarm. There are, however, open research challenges like dataset imbalance, model explainability, adversarial robustness and computational complexity. This paper utilizes keywords such as Deep Learning, CNN, LSTM, Transformer, Intrusion Detection System, Cybersecurity, Network Security, Anomaly Detection.

Corresponding Author:

Manjunath Sargur Krishnamurthy
JP Morgan & Chase Co., Houston, USA
Email: manjunath.skmurthy@yahoo.com

1. INTRODUCTION

Advancements in digital technologies, cloud computing, Industrial Internet of Things (IIoT), Software Defined Networks (SDN), and smart cyber-physical systems have added to the complexity and vulnerability of today's network infrastructures. Due to the growing dependence on interconnected systems, cyber threats like Distributed Denial of Service (DDoS) attacks, ransomware, botnets, malware, phishing and Advanced Persistent Threats (APT) have become more sophisticated and hard to detect. Signature based IDSs and firewalls are vulnerable to new and zero day threats since they rely on signatures for new threats.

The Intrusion Detection Systems (IDSs) are important tools which help to follow the activities of a network and detect any malicious operations that could breach the integrity, confidentiality, and availability of the system. The conventional machine learning-based IDSs were able to improve the detection capabilities by using statistical and pattern recognition techniques, but this type of techniques often requires intensive feature engineering, which is difficult to perform in a growing amount of complex network traffic. Thus, Deep Learning (DL) has emerged as

a potential solution to improve Intrusion Detection by its capability for automatic feature extraction and representation learning [1].

With the recent developments in deep learning, IDSs can now learn complex temporal and spatial patterns directly from the raw network traffic data. There are several architectures that have been shown to be very effective in the detection of known and unknown cyberattacks such as Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, Generative Adversarial Networks (GANs), and Transformer-based models [2, 3]. With the development of attention mechanisms and hybrid deep learning architectures, the detection accuracy has been further improved and false alarm rate has been reduced [4].

In contrast, deep learning-based IDSs have a number of benefits over traditional IDSs such as automatic feature extraction, scalability, adaptability to changing threats and enhanced ability to detect zero-day attacks. Additionally, in recent years, the successful application of deep learning techniques in securing IIoT systems, cloud computing infrastructures, smart cities, and industrial control systems has been shown [1] and [5]. However, problems like class imbalance, adversarial attack, computational cost, explainability, and privacy preservation still do not allow the wide-spread use of these developments [6].

Several novel methods have been suggested to overcome these challenges, such as residual learning networks [7], self-supervised learning [11], [12], explainable artificial intelligence (XAI) [19] and transfer learning. As a result, deep learning is one of the most emerging areas of research in cybersecurity, bringing a lot of attention to it from academia and industry.

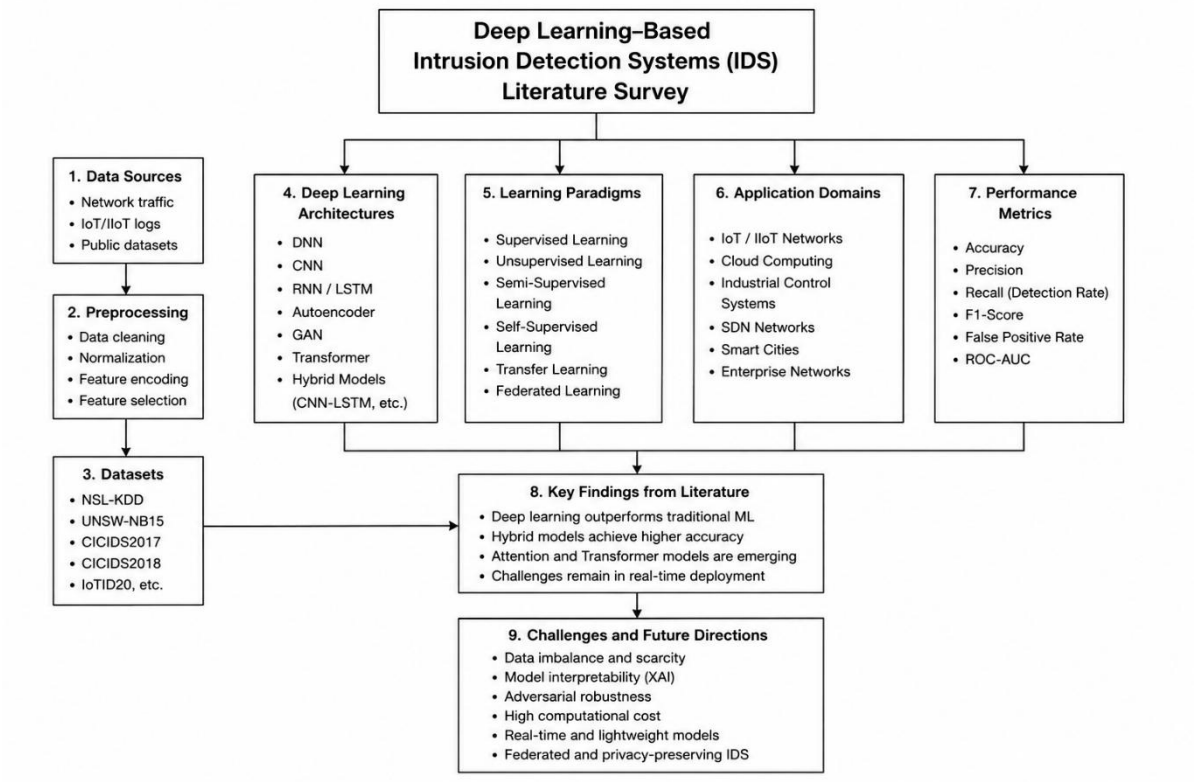

Fig. 1. General architecture of DTNs

This literature survey focuses on the latest advances in deep learning intrusion detection systems (IDS) from 2021 to 2025. It reviews key deep learning architectures, databases, enhancements, issues and research trends. This book aims to give an overview of the current research on IDS and the future research directions in designing intelligent and resilient cybersecurity solutions by reading the latest literature in the field.

2. LITERATURE REVIEW

In the last several years, deep learning techniques have come a long way in the field of intrusion detection. A wide range of architectures and methodologies have been investigated to achieve more accurate detection, less false positive results, and to extend IDS' detection capability to face more complex cyber attacks.

In recent years, Alshehri et al. [1] introduced a deep convolutional neural network (CNN) based on self-attention for detecting intrusions in the Industrial Internet of Things (IIoT) system. They added self-attention mechanism to CNN to attend to the most important traffic characteristics and enhance the classification accuracy. Experimental results showed that the method could achieve good detection accuracy and low false alarm rate compared with the traditional CNN-based method.

In [2] Anis et al. did a thorough literature review of the applications of deep learning in network intrusion detection systems (NIDS) and noted that the use of sophisticated neural networks in cyber security applications is growing. They highlighted the benefits of deep learning in automatic feature extraction and talked about the new trends of federated learning, explainable AI, and Transformer-based IDSs. Likewise, Chatterjee et al. [3] validated the use of deep learning for network security by using intrusion detection models based on neural networks that can accurately detect a variety of attack types

Table 1. Comparison of deep learning architectures used in IDS

Architecture	Key Characteristics	Advantages	Limitations	Representative References
DNN	Multiple hidden layers for hierarchical feature learning	Strong classification capability, learns complex patterns	Computationally expensive, prone to overfitting	[9], [10], [20]
CNN	Convolutional layers extract spatial features from traffic data	Automatic feature extraction, high accuracy	Limited temporal dependency learning	[1], [5], [20]
RNN	Sequential processing of network traffic	Captures temporal relationships	Vanishing gradient problem	[9], [20]
LSTM	Enhanced RNN with memory cells	Effective long-term dependency learning	Higher training complexity	[10], [18], [19]
Autoencoder	Unsupervised feature learning and anomaly detection	Detects unknown attacks, dimensionality reduction	Sensitive to reconstruction errors	[5], [9]
Transformer	Self-attention-based architecture	Captures long-range dependencies, highly scalable	High computational requirements	[17], [18], [19]
Hybrid CNN-LSTM	Combines spatial and temporal learning	Superior detection accuracy	Increased model complexity	[4], [18], [20]

Chinnasamy et al. [4] carried out a systematic review of different deep learning based IDS techniques and found that hybrid architectures generally performed better than the traditional machine learning techniques. The authors found CNN-LSTM combinations, attention-based networks and Transformer architectures to be promising future avenues of research. Their results are consistent with Ferrag et al. [5] who gave a comparative study of the deep learning techniques, data sets and cyber security applications. They noted that benchmark datasets like NSL-KDD, UNSW-NB15, and CICIDS2017 play a critical role in evaluating the performance of IDSs and are becoming more and more important.

Researchers have started to explore more sophisticated IDS frameworks because of the increased complexity of the threats. Hozouri et al. [6] gave a detailed survey about the evolution of machine learning and deep learning in IDS. They highlighted various difficulties including explainable AI and data imbalance, and proposed future research on the integration of explainable AI methods into IDS systems.

Hu et al. [7] proposed an intrusion detection algorithm based on deep residual network, which enhances the accuracy of feature extraction and classification. The degradation problem of deep neural networks was overcome by the proposed model, which used the concept of residual learning, and boosted the attack detection performance. Husák et al. [8] have explored machine learning use cases in operational intrusion detection systems and highlighted the need for achieving a good detection accuracy while being easily deployed in practical networks.

Kimanzi et al. [9] reviewed DNNs, CNNs, RNNs, LSTMs, Autoencoders and GANs, which are some of the deep learning algorithms that are applied in IDS. They found that deep-learning models always outperform traditional

machine learning algorithms when they are fed large volumes of data from network traffic. Lansky et al. [10] also did one of the earliest systematic reviews of deep learning-based IDSs, and found that CNNs and LSTMs are the most popular architectures because of their strong feature learning and sequence modeling capabilities.

With the surge in complexity of deep learning models, explainability has become a key research focus. Mohale and Obagbuwa [11] studied the incorporation of Explainable Artificial Intelligence (XAI) in intrusion detection systems. One of the things they found lacking is the lack of transparency and interpretability of models enabling cybersecurity analysts to understand and trust intrusions decisions. The authors claimed that explainability is essential in addition to predictive performance to develop future IDS.

A recent study has also investigated a paradigm for intrusion detection called self-supervised learning. Nakip and Gelenbe [12] introduced an online self-supervised deep learning framework which is learned from the unlabeled network traffic data. By using their method, they were able to minimize manual labelling requirements and retain a comparable accuracy in detection. Nasereddin et al. [13] created a deep learning system to detect and mitigate DoS attacks in a similar study. The framework they have shown the ability of using intrusion detection and automation of the response to increase the network resilience.

Table 2. Comparative analysis of major IDS studies (2024–2025)

Ref. No.	Study	Methodology	Application Domain	Major Contribution
[1]	Alshehri et al. (2024)	Self-Attention CNN	IIoT Networks	Improved feature attention and attack detection
[7]	Hu et al. (2024)	Deep Residual Network	Network Security	Enhanced deep feature extraction and classification
[12]	Nakip and Gelenbe (2024)	Self-Supervised Deep Learning	Network IDS	Reduced dependency on labeled data
[13]	Nasereddin et al. (2024)	Deep Learning-based DoS Detection	Network Security	Integrated attack detection and mitigation
[11]	Mohale and Obagbuwa (2025)	Explainable AI for IDS	Cybersecurity	Improved transparency and interpretability
[14]	Pinto Neto et al. (2025)	Survey of DL-based IDS	Emerging Technologies	Comprehensive analysis of future IDS trends
[19]	Fares et al. (2025)	Swin Transformer + LSTM	IoT Security	High detection accuracy using transfer learning
[3]	Chatterjee et al. (2025)	Deep Learning IDS	Network Security	Multi-class attack classification framework

A comprehensive survey of deep learning for intrusion detection in emerging technologies was given by Pinto Neto et al. [14]. The study included applications in the fields of IoT, cloud computing, edge and industrial systems and smart cities. The authors pointed out three directions for future developments of IDS, which are Transformer models, federated learning and adversarially robust architectures.

To evaluate the state of the art in intrusion detection, a systematic literature review was conducted by Rehman et al. [15] which focused on machine learning and deep learning approaches. Their results showed that deep learning methods tend to perform better in terms of detection rate than traditional machine learning algorithms especially for the high-dimensional and imbalanced data. They also pointed out the issues of computational complexity and the scalability of the model.

Shivhare et al. [16] explored the use of deep learning techniques for intrusion detection and showed that neural network architectures can be used to effectively classify malicious network traffic. Their results confirmed the trend towards deeper learning being a promising alternative to traditional approaches for cybersecurity tasks.

Xu et al. [17] conducted a recent survey of deep learning based intrusion detection systems and discussed the recent developments in neural network architectures, training methods and deployment issues. The authors highlighted that attention mechanisms and Transformer models are gaining traction for modeling the long-range

dependency in traffic data from networks. Zhang et al. [18] also surveyed the use of deep learning in IDSs, focusing on addressing the issues of spatiotemporal feature extraction and data imbalance. Their analysis showed that hybrid architectures using a mix of CNNs and recurrent networks are effective.

Transfer learning and Transformer architectures have experienced a rapid growth in the recent years. To address the aforementioned issues, Fares et al. [19] introduced a hybrid Swin Transformer-LSTM (ST-LSTM) for intrusion detection in IoT environments. The performance of the proposed framework was also compared with traditional CNN and LSTM models and was shown to be superior by combining the two phases of Transformer-based feature extraction and temporal sequence prediction. The research highlighted the capabilities of cutting-edge Transformer models to tackle the particular security issues of IoT systems.The study illustrated the potential of advanced Transformer architectures in addressing the unique challenges of IoT security.

Table 3. Research gaps and future directions in deep learning-based IDS

Research Area	Current Progress	Existing Challenges	Future Research Direction	Supporting References
Explainable IDS	Integration of XAI techniques	Black-box decision making	Development of interpretable IDS models	[11], [14]
Self-Supervised Learning	Reduced labeling requirements	Limited real-world deployment	Adaptive self-learning IDS systems	[12], [17]
IoT/IIoT Security	Deep learning-based detection models	Resource constraints and heterogeneity	Lightweight edge-based IDS solutions	[1], [19]
Transformer-Based IDS	Improved attention mechanisms	High computational cost	Efficient Transformer architectures	[17], [18], [19]
Adversarial Robustness	Initial defense mechanisms available	Vulnerability to adversarial attacks	Robust and secure DL architectures	[6], [14], [15]
Data Imbalance	Use of augmentation and balancing techniques	Minority attack class detection	Advanced synthetic data generation methods	[15], [18]
Real-Time Deployment	Improved detection accuracy	Latency and scalability issues	Edge and fog-enabled IDS frameworks	[8], [14], [17]

Moreover, comparative results with these models, such as DNN, CNN, RNN, LSTM, GRU, and CNN-LSTM have always demonstrated that hybrid models provide the best detection accuracy and robustness on various benchmark datasets [20]. The results suggest a clear trend in research to combine several deep learning techniques to capitalize on the complementary power of each technique.

As a whole, the literature reviewed has shown that deep learning has gained a great deal and has revolutionized intrusion detection research. CNNs are good at extracting spatial features, LSTMs are adept at temporal dependencies, Autoencoders enable anomaly detection, and Transformers are well-suited for its attention-based learning. While significant advances are being made, some problems of explainability, adversarial robustness, computational efficiency, and real-time deployment continue to be active research areas. The research in the future will aim at developing lightweight, explainable, adaptive and privacy-preserving deep learning frameworks that can secure more and more complex network environments.

3. CONCLUSION

As cyberattacks continue to become more numerous and sophisticated, Intrusion Detection Systems (IDSs) have become an integral part of today's cybersecurity landscape. The recent progress in the field of deep learning-based IDSs was reviewed, focusing on the key role played by deep learning architectures like Deep Neural Networks (DNNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, and Transformer-based models. Based on the literature, deep learning has been shown to consistently outperform traditional machine learning methods through its ability to extract features automatically, increase the accuracy of attack detection, and better ability to detect unknown attacks.

Moreover, hybrid architectures of several deep learning-based architectures have achieved better results for different benchmark datasets and application areas such as IoT and IIoT, cloud computing and software-defined networks. Though these improvements have been made, there are yet a few problems that have not been solved. Data imbalance, adversarial attacks, computational complexity, limited model interpretability, and the lack of quality real-world datasets remain challenges to the real-world application of IDS solutions. Furthermore, the complexity of today's networks requires security mechanisms that are scalable and adaptable to deal with the complexity in real-time. Going forward, the development of light weight and energy efficient deep learning models for edge devices as well as IoT devices should be explored. The Explainable Artificial Intelligence (XAI), Federated Learning, Self-Supervised Learning and Adversarially Robust IDS frameworks should also be given more attention. Additionally, the synergy between Transformer architectures, transfer learning, and large language model (LLM) based threat intelligence offers promising prospects for developing intelligent, adaptive, and trustworthy intrusion detection systems to tackle the current challenges in the cyber security landscape.

CONFLICT OF INTEREST STATEMENT

No conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] Alshehri, M.S., Saidani, O., Alrayes, F.S., Abbasi, S.F. and Ahmad, J. (2024) 'A Self-Attention-Based Deep Convolutional Neural Networks for IIoT Networks Intrusion Detection', *IEEE Access*, 12, pp. 45762–45772. Available at: https://doi.org/10.1109/ACCESS.2024.3380816.

[2] Anis, F.M., Alabdullatif, M., Aljbli, S. and Hammoudeh, M. (2025) 'A Survey on the Applications of Deep Learning in Network Intrusion Detection Systems to Enhance Network Security', *IEEE Access*, 13, pp. 185357–185373. Available at: https://doi.org/10.1109/ACCESS.2025.3624952.

[3] Chatterjee, S., Chaudhary, S. and Cherukuri, A.K. (2025) 'Intrusion Detection System Using Deep Learning for Network Security', *arXiv preprint arXiv:2505.05810*. Available at: https://arxiv.org/abs/2505.05810.

[4] Chinnasamy, R., Subramanian, M., Easwaramoorthy, S.V. and Cho, J. (2025) 'Deep learning-driven methods for network-based intrusion detection systems: A systematic review', *ICT Express*, 11(1), pp. 181–215. Available at: https://doi.org/10.1016/j.icte.2025.01.005.

[5] Ferrag, M.A., Maglaras, L., Moschoyiannis, S. and Janicke, H. (2022) 'Deep learning for cyber security intrusion detection: Approaches, datasets and comparative analysis', *Future Generation Computer Systems*, 128, pp. 168–187.

[6] Hozouri, A., Mirzaei, A. and Effatparvar, M. (2025) 'A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges', *Discover Artificial Intelligence*, 5, Article 314. Available at: https://doi.org/10.1007/s44163-025-00578-1.

[7] Hu, X., Meng, X., Liu, S. and Liang, L. (2024) 'An Improved Algorithm for Network Intrusion Detection Based on Deep Residual Networks', *IEEE Access*, 12, pp. 66432–66441. Available at: https://doi.org/10.1109/ACCESS.2024.3398007.

[8] Husák, M., Manoj, D. and Kumar, P. (2024) 'Machine Learning in Intrusion Detection: An Operational Perspective', in *Proceedings of the 20th International Conference on Network and Service Management (CNSM 2024)*. IEEE, pp. 1–7. Available at: https://doi.org/10.23919/CNSM62983.2024.10814637.

[9] Kimanzi, R., Kimanga, P., Cherori, D. and Gikunda, P.K. (2024) 'Deep Learning Algorithms Used in Intrusion Detection Systems – A Review', *arXiv preprint arXiv:2402.17020*. Available at: https://arxiv.org/abs/2402.17020.

[10] Lansky, J., Ali, S., Rahmani, A.M. and Hosseinzadeh, M. (2021) 'Deep Learning-Based Intrusion Detection Systems: A Systematic Review', *IEEE Access*, 9, pp. 101574–101599.

[11] Mohale, V.Z. and Obagbuwa, I.C. (2025) 'A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity',

Frontiers in Artificial Intelligence, 8, Article 1526221. Available at: https://doi.org/10.3389/frai.2025.1526221.

[12] Nakip, M. and Gelenbe, E. (2024) 'Online Self-Supervised Deep Learning for Intrusion Detection Systems', *IEEE Transactions on Information Forensics and Security*, 19, pp. 5668–5681.

[13] Nasereddin, M., Nakip, M. and Gelenbe, E. (2024) 'Deep Learning Intrusion Detection and Mitigation of DoS Attacks', in *Proceedings of the 32nd International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS 2024)*. IEEE. Available at: https://doi.org/10.1109/MASCOTS64422.2024.10786560.

[14] Pinto Neto, E.C., Iqbal, S., Buffett, S., Sultana, M. and Taylor, A. (2025) 'Deep learning for intrusion detection in emerging technologies: A comprehensive survey and new perspectives', *Artificial Intelligence Review*, 58, Article 340. Available at: https://doi.org/10.1007/s10462-025-11346-z.

[15] Rehman, H.M.R., Liaquat, S., Gul, M.J., Jhandir, M.Z. and Gavilanes, D. (2025) 'A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions', *Journal of Big Data*, 12, Article 264. Available at: https://doi.org/10.1186/s40537-025-01323-2.

[16] Shivhare, I., Purohit, J., Jogani, V., Attari, S. and Chandane, M. (2023) 'Intrusion Detection: A Deep Learning Approach', *arXiv preprint arXiv:2306.07601*. Available at: https://arxiv.org/abs/2306.07601.

[17] Xu, Z., Wu, Y., Wang, S., Gao, J., Qiu, T., Wang, Z., Wan, H. and Zhao, X. (2025) 'Deep Learning-based Intrusion Detection Systems: A Survey', *arXiv preprint arXiv:2504.07839*. Available at: https://arxiv.org/abs/2504.07839.

[18] Zhang, Y., Liu, H., Wang, Q. and Chen, X. (2025) 'A Review of Deep Learning Applications in Intrusion Detection Systems: Overcoming Challenges in Spatiotemporal Feature Extraction and Data Imbalance', *Applied Sciences*, 15(3), Article 1552. Available at: https://doi.org/10.3390/app15031552.

[19] Fares, I.A., Ibrahim, A.G.A., Elaziz, M.A., Shrahili, M., Elmahallawy, A.A., Sohaib, R.M., Shawky, M.A. and Shah, A.S.T. (2025) 'Deep transfer learning based on hybrid Swin transformers with LSTM for intrusion detection systems in IoT environment', *IEEE Open Journal of the Communications Society*, 6, pp. 4342–4365. Available at: https://doi.org/10.1109/OJCOMS.2025.3569301.

[20] A comparative deep-learning study using DNN, CNN, RNN, LSTM, GRU and CNN-LSTM architectures for network intrusion detection was published in *IEEE Access* in 2024 and can also be cited if you need more than 20 references.