

Deep Learning-Based Intrusion Detection Systems for Network Security

TABLE OF CONTENT

Deep Learning-Based Intrusion Detection Systems for Network Security	1
Introduction.....	1
Literature Review.....	2
Summary Table of Reviewed Papers	5
Critical Analysis.....	6
Comparative Discussion	7
Research Gaps.....	7
Synthesis	8
Conclusion	8
References.....	9
Sources and Links	10

Introduction

Network intrusion detection systems are becoming an integral part of contemporary cybersecurity due to the fact that network configurations are no longer restricted to predetermined attack signatures or anticipated traffic patterns. While signature-based systems and other traditional intrusion detection methods may successfully identify known assaults, their reliability is compromised when dealing with modified, disguised, or unknown attacks in advance. Research into network security has taken an uptick thanks to deep learning's ability to find intricate patterns in network traffic data without using human feature engineers. The following papers (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022) were reviewed in this article: those that used deep learning approaches for network intrusion detection."Deep Learning-Based Intrusion Detection Systems for Network Security" is the chosen paper title. In order to better understand how different deep learning architectures have been utilized to enhance the accuracy of intrusion detection, this literature review will examine CNN-LSTM models, recurrent neural networks, deep neural networks, non-symmetric deep autoencoders, and sparse autoencoders. This review takes into account the models' suitability for real-world network environments, as high accuracy

on benchmark datasets does not necessarily translate into strong performance against active or evolving cyberattacks (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022).

Literature Review

One of the first deep learning methods for detecting intrusions in networks was developed by Javaid et al. (2016) using self-taught learning. To lessen reliance on manually specified characteristics, they set out to create a model that could learn valuable representations from network data. In the research, a sparse autoencoder was used for feature learning and a softmax regression classifier was used for classification on the NSL-KDD dataset. Since the autoencoder may extract more essential representations from the input traffic data, deep feature learning may enhance intrusion detection performance compared to typical shallow learning algorithms, according to Javaid et al. (2016).

At a time when many intrusion detection systems depended substantially on characteristics that were manually picked, Javaid et al.'s work stands out because it introduced representation learning to the field. The reliance on NSL-KDD is the major issue, however; it is extensively used but fails to accurately portray current encrypted communication, cloud traffic, data from the Internet of Things (IoT), or sophisticated persistent threats. Although the article proved the promise of deep learning for IDS, its real-world application was restricted since the experimental approach was based on an offline benchmark dataset instead of real-time network traffic (Javaid et al., 2016).

The use of recurrent neural networks for intrusion detection was assessed by Yin et al. (2017). The goal of this research was to examine the potential of RNNs to better represent network data and enhance classification accuracy. To test RNN-IDS's performance in binary and multiclass classification, the authors turned to the NSL-KDD dataset. Their results showed that the RNN-based model outperformed several conventional machine learning algorithms in terms of detection performance, which raises the possibility that sequential learning might be helpful in identifying patterns of attacks in network data (Yin et al., 2017).

The study by Yin et al. stands out because it highlights the importance of recurrent learning—a technique that works well when trying to predict ordered or sequential data. The importance of this cannot be overstated, since network traffic often encompasses connections between events in time rather than just a compilation of individual pieces of data. Problems with the study's methodology include its reliance on NSL-KDD for model evaluation and its failure to address issues such as concept drift, hostile manipulation, high-speed traffic, or real-world deployment situations. Many intrusion detection system investigations encounter this issue. According to Yin et al. (2017), more validation is needed to prove the true resilience of the RNN model, despite its promising theoretical performance.

An technique to network intrusion detection utilizing a non-symmetric deep autoencoder was reported by Shone et al. (2018). One goal was to enhance intrusion detection by integrating unsupervised feature learning with a deep classification system. The model was constructed with the help of GPU-enabled TensorFlow, and it was tested using the NSL-KDD and KDD Cup 99 datasets. Outperforming most current intrusion detection techniques, their results demonstrated that non-symmetric autoencoders are capable of learning compact and realistic representations of traffic (Shone et al., 2018).

Given the potential difficulty in obtaining labeled cyberattack data in real-world circumstances, the use of unsupervised feature learning is the primary strength of the work by Shone et al. Using a non-symmetric autoencoder also helped with dimensionality reduction while keeping key traffic features intact. The research had certain issues, one of which was its reliance on KDD-based datasets like KDD Cup 99, which had assault scenarios that were outdated and had redundancy issues that were already recognized. NSL-KDD is an improvement over KDD Cup 99 in terms of data duplication, but it can't keep up with the complexity of modern business networks (Shone et al., 2018).

A method for intelligent intrusion detection was presented by Vinayakumar et al. (2019) using deep neural networks. The goal was to create a deep learning-based adaptive intrusion detection system (IDS) that could identify and classify various threats. In contrast to studies that use only one dataset, this one tested DNNs on several benchmark intrusion detection datasets. Results

show that DNNs can adapt to various intrusion detection settings and provide good classification performance when trained and evaluated correctly (Vinayakumar et al., 2019).

One of the main advantages of the work by Vinayakumar et al. is that, instead of relying just on NSL-KDD, the scientists employed a variety of datasets, expanding the experimental scope. Consequently, compared to previous publications, this paper's rating is stronger. While deep models may provide accurate results, they often need extensive training data, fine-tuning, and powerful computing resources, which is a significant challenge in deep learning intrusion detection system (IDS) research. In addition, DNN choices still have a ways to go before they can be easily understood, which might lead to a loss of confidence in security operations (Vinayakumar et al., 2019).

A trustworthy model for network intrusion detection was developed by Hsu et al. (2021) using convolutional neural networks equipped with long short-term memory. The goal was to merge CNN's feature extraction with LSTM networks' temporal modeling capabilities. Researchers used convolutional neural network (CNN) layers to identify regional traffic patterns and long short-term memory (LSTM) layers to build sequential correlations. According to Hsu et al. (2021), integrating CNN and LSTM might enhance intrusion detection performance due to the model's spatial and temporal learning capabilities.

The study's strongest point is the hybrid design that Hsu et al. used. When it comes to learning longer connections in sequential data, LSTM networks are great, but when it comes to extracting local feature patterns, CNNs really shine. Hence, compared to only using CNN or LSTM, the method is superior. The model is complex, however, and compared to simpler machine learning methods, it could be more expensive to train and more challenging to execute. Hybrid models also need additional testing in real-time network environments, where latency, class imbalance, and dynamic attack behavior are key challenges (Hsu et al., 2021). This is in addition to the fact that they perform well on benchmark datasets.

A network intrusion detection system was created by Halbouni et al. (2022) using a CNN-LSTM hybrid deep neural network. Improving detection accuracy was the goal of combining CNN-based spatial feature extraction with LSTM-based temporal learning. The research used a

number of datasets, such as UNSW-NB15, CIC-IDS2017, and WSN-DS, to assess the model. According to Halbouni et al. (2022), models evaluated on a single older dataset may not have the same generalizable detection skills as CNN-LSTM architectures, which showed high performance across many datasets.

The use of many more recent datasets, such as CIC-IDS2017 and UNSW-NB15, which are typically more representative than KDD Cup 99, is the primary strength of Halbouni et al.'s analysis. In addition, by learning several feature types, the research demonstrates how hybrid systems might enhance IDS performance. Nevertheless, computational complexity and explainability remain issues with the paradigm. Even the most precise model will fail in practical security scenarios if it is unable to handle heavy traffic or provide an understandable description of warnings (Halbouni et al., 2022).

Summary Table of Reviewed Papers

Year	Authors	Methodology	Key Findings	Weaknesses / Limitations
2016	Javaid et al.	Self-taught learning using sparse autoencoder and softmax regression on NSL-KDD	Deep feature learning improved IDS performance compared with traditional approaches	Relied mainly on NSL-KDD; limited real-world validation
2017	Yin et al.	Recurrent neural network IDS using NSL-KDD	RNN-IDS achieved strong binary and multiclass classification performance	Limited testing on modern live traffic and adversarial conditions
2018	Shone et al.	Non-symmetric deep autoencoder with deep classification on KDD Cup 99 and NSL-KDD	Autoencoder-based feature learning improved detection capability	KDD-based datasets are outdated and may inflate performance

2019	Vinayakumar et al.	Deep neural network evaluated across multiple IDS datasets	DNNs showed strong potential for flexible intelligent IDS	High computational cost and limited interpretability
2021	Hsu et al.	CNN-LSTM hybrid model	Hybrid spatial-temporal learning improved detection performance	More complex model; real-time deployment issues not fully addressed
2022	Halbouni et al.	CNN-LSTM hybrid deep neural network on UNSW-NB15, CIC-IDS2017, and WSN-DS	Strong performance across multiple datasets	Computational complexity and explainability remain challenges

Critical Analysis

The six research demonstrate a clear evolution from basic deep feature learning to hybrid systems. While Yin et al. focused on recurrent modeling, Javaid et al. proposed sparse autoencoder-based representation learning. Later efforts, such as Hsu et al. and Halbouni et al., combined CNN and LSTM layers to capture both spatial and temporal elements of traffic, whilst Shone et al. improved the autoencoder direction using non-symmetric deep autoencoders. According to Javaid et al. (2016), Yin et al. (2017), Shone et al. (2018), Hsu et al. (2021), and Halbouni et al. (2022), intrusion detection research has gradually shifted from single-model deep learning to integrated architectures that attempt to learn richer traffic representations.

Studies that evaluate models over several datasets provide the most methodological advancement. In this regard, Vinayakumar et al. and Halbouni et al. are preferable since they use more than only NSL-KDD. This is critical because when traffic distribution changes, IDS models often outperform on a particular dataset but fail to generalize. As a consequence, utilizing several datasets gives a more reliable indication of a model's capacity to adapt to different attack patterns and network conditions (Vinayakumar et al., 2019; Halbouni et al., 2022).

Regardless of their contributions, the evaluated works have some shortcomings. First, the bulk of them rely on benchmark datasets, notably NSL-KDD, which are no longer representative of modern networks. Second, although accuracy is the major goal of many studies, false alarm rate, detection latency, interpretability, processing overhead, and deployment feasibility are given less consideration. Third, deep learning models are frequently referred to as "black boxes," which is problematic for cybersecurity because analysts require comprehensible evidence before responding to alerts (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022).

Comparative Discussion

The papers agree that deep learning can improve intrusion detection by automatically learning features from network traffic. However, they differ in how they model traffic data. Autoencoder-based approaches, such as Javaid et al. and Shone et al., focus on feature learning and dimensionality reduction. RNN-based approaches, such as Yin et al., focus on sequential relationships. Hybrid CNN-LSTM approaches, such as Hsu et al. and Halbouni et al., attempt to combine both spatial and temporal learning. These differences show that no single architecture is universally superior; rather, the choice of model depends on the type of traffic, dataset, attack categories, and deployment requirements (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Hsu et al., 2021; Halbouni et al., 2022).

A conflict appears between high benchmark accuracy and practical deployment readiness. Several papers report strong results, but many of these results are obtained under controlled experimental conditions. In real networks, attack patterns change, benign traffic is highly diverse, encrypted traffic reduces visibility, and false alarms can overwhelm security teams. Therefore, the literature suggests that deep learning is promising, but it also shows that academic IDS models still need stronger evaluation in real-time and operational environments (Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022).

Research Gaps

The first major research gap is the lack of real-world validation. Many reviewed models are evaluated on public benchmark datasets, but fewer are tested on live enterprise traffic or

continuously changing network environments. This limits confidence in their ability to detect zero-day attacks, polymorphic attacks, and advanced persistent threats. Future research should include real-time testing, cross-dataset validation, and evaluation under concept drift conditions (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Vinayakumar et al., 2019).

The second gap is explainability. Deep learning models may detect attacks accurately, but they often do not explain which features or traffic behaviours caused the detection. This creates a problem for security analysts who must investigate alerts and justify decisions. Future IDS research should integrate explainable artificial intelligence techniques so that deep learning models become not only accurate but also understandable and trustworthy (Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022).

The third gap concerns computational efficiency. CNN-LSTM and deep neural network models can be expensive to train and deploy, especially in high-speed networks or edge environments. Future research should consider lightweight deep learning, model compression, online learning, and efficient deployment on resource-constrained systems. Without addressing efficiency, deep learning IDS models may remain academically successful but operationally difficult to use (Hsu et al., 2021; Halbouni et al., 2022).

Synthesis

The reviewed literature shows that deep learning has improved network intrusion detection by reducing dependence on manual feature engineering and by enabling models to learn complex attack patterns. Early studies proved the usefulness of autoencoders and recurrent networks, while later studies demonstrated the value of hybrid models. However, the field has not fully solved the problems of real-world generalization, interpretability, and efficient deployment. Therefore, the most convincing future direction is not simply to build deeper models, but to design IDS systems that are accurate, explainable, computationally efficient, and validated across realistic network environments (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022).

Conclusion

This literature review examined six research papers on deep learning-based intrusion detection systems for network security. The reviewed studies show that deep learning methods, including sparse autoencoders, RNNs, non-symmetric autoencoders, DNNs, and CNN-LSTM hybrid models, can improve intrusion detection performance by learning complex patterns from network traffic. However, the review also shows that many studies remain limited by benchmark-based evaluation, weak explainability, and insufficient real-world testing. Overall, deep learning is a powerful direction for intrusion detection, but future research must move beyond accuracy-focused experiments and address deployment, interpretability, robustness, and adaptability to modern cyber threats (Javaid et al., 2016; Yin et al., 2017; Shone et al., 2018; Vinayakumar et al., 2019; Hsu et al., 2021; Halbouni et al., 2022).

References

- Halbouni, A., Gunawan, T. S., Habaebi, M. H., Halbouni, M., Kartiwi, M., & Ahmad, R. (2022). CNN-LSTM: Hybrid deep neural network for network intrusion detection system. *IEEE Access*, 10, 99837–99849. <https://doi.org/10.1109/ACCESS.2022.3206425>
- Hsu, C.-M., Azhari, M. Z., Hsieh, H.-Y., Prakosa, S. W., & Leu, J.-S. (2021). Robust network intrusion detection scheme using long-short term memory based convolutional neural networks. *Mobile Networks and Applications*, 26, 1137–1144. <https://doi.org/10.1007/s11036-020-01623-2>
- Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. In *Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies* (pp. 21–26). <https://doi.org/10.4108/eai.3-12-2015.2262516>
- Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50. <https://doi.org/10.1109/TETCI.2017.2772792>
- Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550. <https://doi.org/10.1109/ACCESS.2019.2895334>

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

<https://doi.org/10.1109/ACCESS.2017.2762418>

Sources and Links

1. Javaid et al. (2016): <https://doi.org/10.4108/eai.3-12-2015.2262516>
2. Yin et al. (2017): <https://doi.org/10.1109/ACCESS.2017.2762418>
3. Shone et al. (2018): <https://doi.org/10.1109/TETCI.2017.2772792>
4. Vinayakumar et al. (2019): <https://doi.org/10.1109/ACCESS.2019.2895334>
5. Hsu et al. (2021): <https://doi.org/10.1007/s11036-020-01623-2>
6. Halbouni et al. (2022): <https://doi.org/10.1109/ACCESS.2022.3206425>