The Indonesian Journal of Computer Science
www.ijcs.net
Volume 14, Issue 1, February 2025
https://doi.org/10.33022/ijcs.v14i1.4737

Deep Learning Techniques for Network Security: A Review

Diana Hayder Hussein[1], Yousif Mohammed Ismail[2], Shavan Askar[3], Media Ali Ibrahim[1]
media.ibrahim@epu.edu.iq[1], yousif.ismail@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

Intrusion Detection System (IDS), Anomaly Detection, Convolutional Neural Networks (CNNs), False Positive Rate, Cyber Threats, Supervised Learning

Abstract

This article explores the seven outstanding deep-learning techniques used to enhance network security. It provides a comprehensive analysis of how these techniques address various cybersecurity challenges, including intrusion detection, malware classification, and anomaly detection. This review highlights the effectiveness of deep learning models such as Convolutional Neural Networks (Recurrent neural networks (RNNs) and automatic encoders used in processing large datasets and identifying complex patterns representing security threats. The article also discusses the advantages and limitations of each technique, emphasizing the importance of feature extraction, model training, and real-time processing capabilities. By combining the findings of the current research, this review aims to guide future research and practical implementation of deep learning in securing network infrastructure against evolving cyber threats. The review provided a comprehensive summary of the deep learning techniques used in network security, highlighting their strengths and limitations. The findings showed that deep learning has significant potential to improve detection and response to network threats, although challenges related to model interpretability, data quality, and computational efficiency should be addressed.

A. Introduction

In recent years, the integration of deep learning techniques into network security has attracted significant attention due to the increasing complexity and volume of cyber threats. The review explores various advanced deep learning approaches and their application to protect digital infrastructure (Chandola et al 2009). Given that traditional network security methods often fail to deal with sophisticated attacks, this article focuses on the potential for deep learning to increase accuracy, detection speed, and adaptability. This review summarizes the key deep learning techniques discussed in the article, analyses their effectiveness, and highlights the challenges and opportunities they present for the future of network security (Kumar and Singh 2018), It is shown in Figure 1.

Figure 1. Learn to use Machine Learning in Cyber Security & SecOps Liu, Y., Wu, L, Liu, J. (2020).

In today's digital landscape, the proliferation of cyber threats poses significant challenges to the integrity, confidentiality, and availability of network systems. As organizations increasingly rely on interconnected devices and cloud-based services, traditional security measures often fail to detect and mitigate sophisticated attacks. This has led to a growing interest in using advanced technologies, especially deep learning, to enhance network security (Saini and

Kumar 2021) deep learning, a subset of machine learning, uses neural networks with multiple layers to analyze huge amounts of data and identify complex patterns. Its ability to learn from unstructured data makes it particularly suitable for cybersecurity applications, where the volume and complexity of data can overwhelm conventional methods. By automating the detection of anomalies and threats, deep learning techniques can significantly improve response time and reduce reliance on manual intervention, shown as in Figure 2.

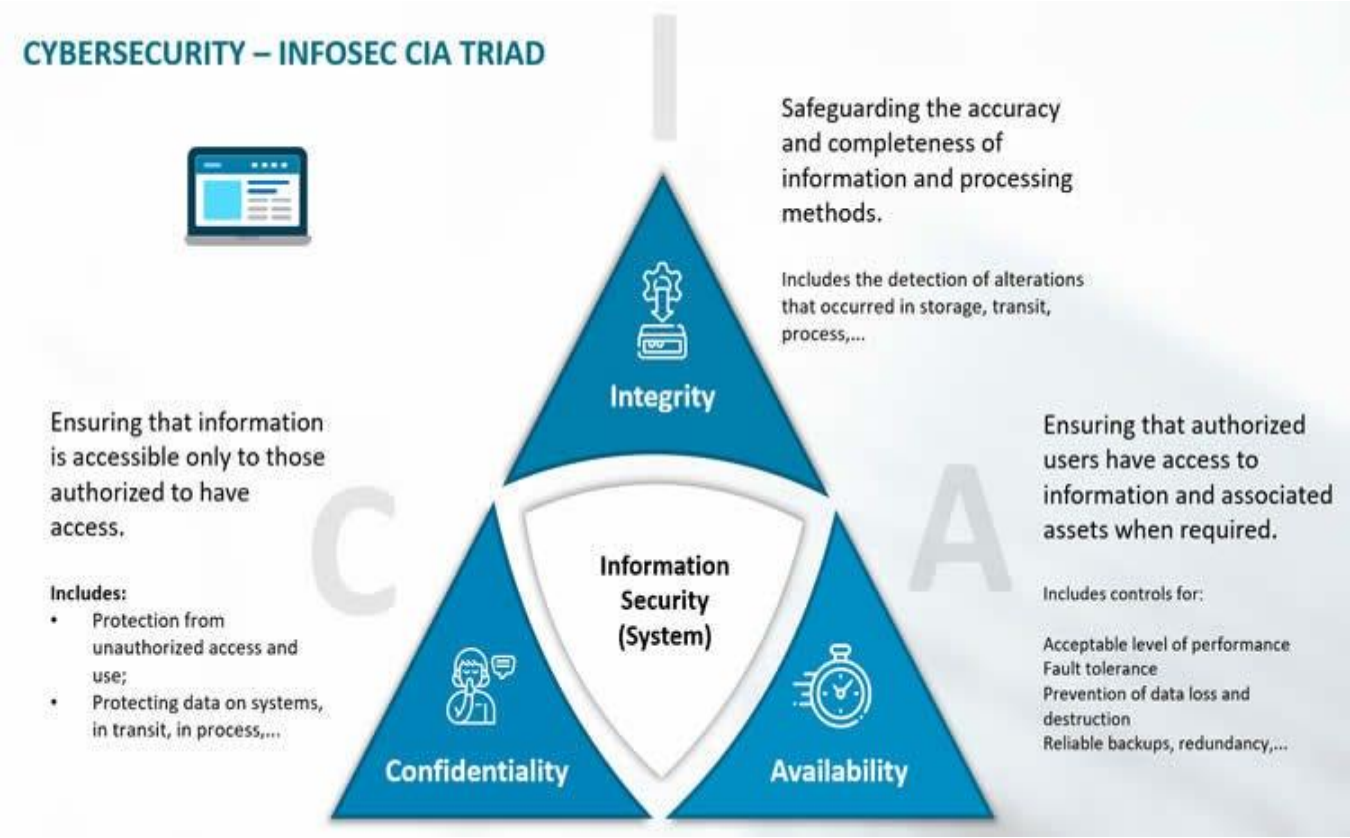

Figure 2. Understanding the CIA Triad: The Foundation of Network Security
Kumar, A, Singh, M. (2018).

The application of deep learning in network security encompasses a variety of areas, including intrusion detection systems (IDS), malware detection, phishing prevention, and network traffic analysis. Techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Generative Adversarial Networks (GANs) have shown promise in detecting malicious activities with high accuracy (Liu and Liu 2020).

1.2 Convolutional Neural Networks (CNNs): Originally designed for image processing, CNNs have been adapted for network security tasks by treating network traffic data as images. This approach enables effective feature extraction and classification of attack patterns (Kumar and Singh 2018).

1.3 Recurrent neural networks (RNNs): RNNs are particularly useful for analyzing sequential data, making them ideal for tasks such as monitoring network

traffic over time. Their ability to store information from previous inputs allows them to detect anomalies in real time (Cheng and Liu 2020). Self-encryption: These unsupervised learning models are effective in detecting anomalies. By learning to reconstruct normal behavior, self-encryption programs can identify distractions that may indicate security breaches (Cheng and Liu 2020).

1.4 Generative Adversarial Networks (GANs): GAN networks can be used to generate synthetic data for training purposes, enhancing model robustness in scenarios where classified data is scarce (Chandola et al. 2009). Long Short-Term Memory (LSTM): A specialized type of RNN, LSTMs are adept at capturing long-term dependencies in data, making them suitable for detecting complex attack patterns in time series data.

1.5 Deep Belief Networks (DBNs): These hierarchical models can learn representations from unlabelled data, facilitating feature extraction and dimension reduction to improve classification performance (Cheng and Liu 2020). Transfer Learning: This technique allows models trained in one domain to adapt to another, providing a powerful tool to improve detection rates without the need for extensive retraining on new datasets.

As cyber threats continue to grow in complexity and scale, the integration of deep learning techniques into network security frameworks represents a critical breakthrough (Liu and Li 2020). By leveraging the power of these technologies, organizations can proactively enhance their ability to identify and respond to threats, ensuring a safer digital environment. In conclusion, deep learning offers promising solutions to address the challenges facing network security. Continued research and development in this area are likely to yield more effective methods for protecting critical information systems from emerging threats (Khan and Qadir 2020), shown as in Figure 3.

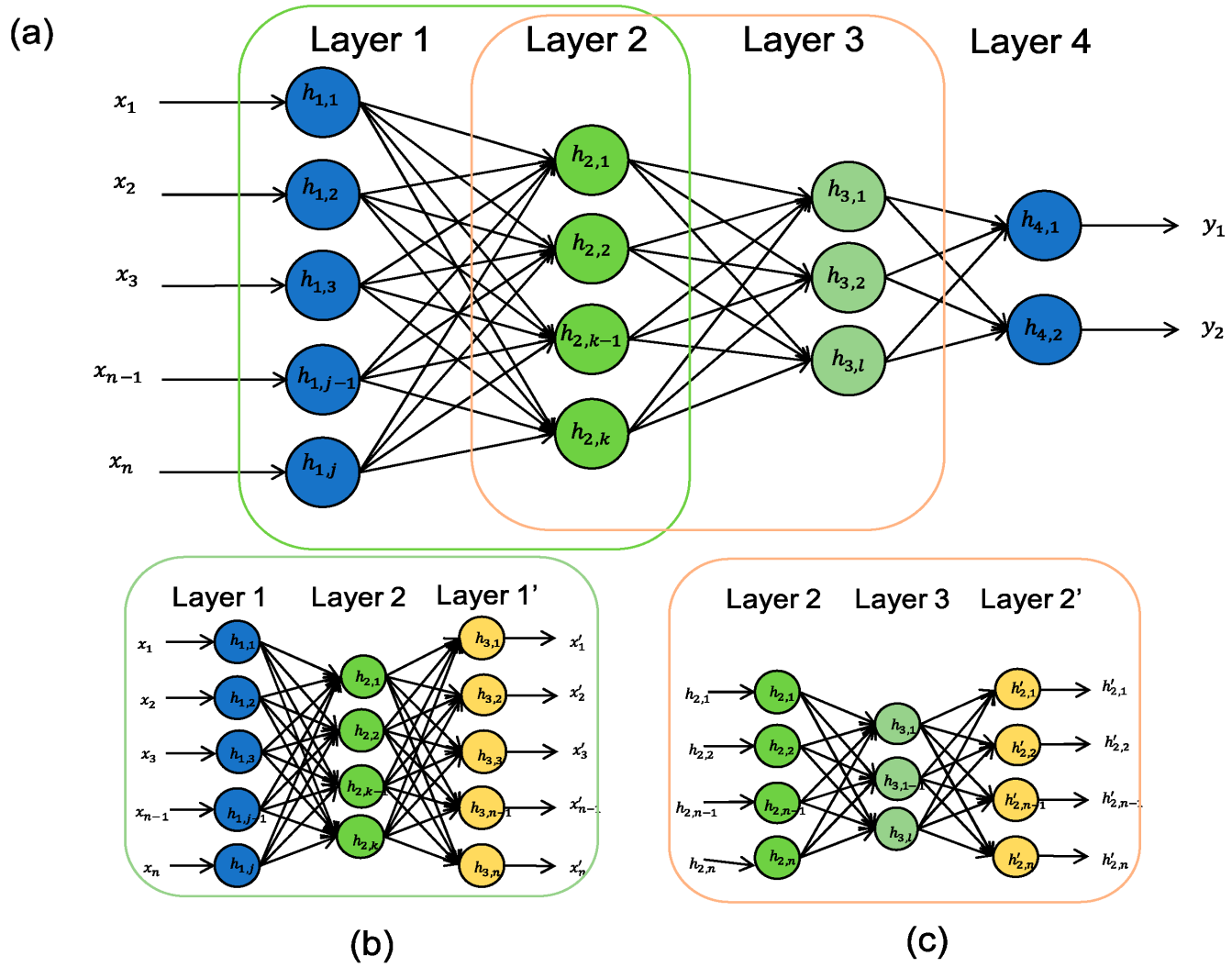

Figure 3. A Survey of Deep Learning Methods for Cyber Security
Alazab, M., Venkatraman, S. (2019).

B. Research Method

Criteria for Inclusion: The selection of the seven research papers reviewed was based on specific criteria such as relevance to the topic of deep learning in network security, publication within the last 5-10 years (ensuring the research is up to date), and impact on the field (high citation counts recognized authorship, or leading conferences/journals) (Alazab and Venkatraman 2019).

Scope of Review: The seven papers selected covered a broad spectrum of deep learning techniques, from supervised and unsupervised learning models to reinforcement learning and hybrid approaches, to understand their application in

various aspects of network security, including intrusion detection, malware classification, and attack prevention (Cheng and Liu 2020).

2.1 Data Collection and Sources

Literature Search: A comprehensive search was conducted using academic databases such as Google Scholar, IEEE Xplore, Scopus, and SpringerLink to identify relevant papers that discuss the application of deep learning in network security (Sommer and Paxson 2010).

Keywords: Keywords used in the search included

"Deep learning for network security", "Intrusion detection systems", "anomaly detection" "cybersecurity", "artificial intelligence in network defense," and "deep neural networks in cybersecurity" (Sommer and Paxson 2010).

Data Extraction: Information was extracted from each paper regarding the techniques used, performance metrics, datasets employed, and the specific network security problem addressed.

2.2 Analysis of Deep Learning Techniques

Categorization of Techniques: The deep learning methods reviewed in the seven papers were categorized into several broad groups: Supervised Learning: Techniques such as Convolutional Neural Networks (CNNs), Support Vector Machines (SVM), and Feedforward Neural Networks (FNNs) were used for classification tasks like malware detection and intrusion detection.

Unsupervised Learning: Methods like Autoencoders and Generative Adversarial Networks (GANs) were explored for anomaly detection, particularly in situations where labeled data is scarce.

2.3 Reinforcement Learning

A few studies incorporated reinforcement learning (RL) to optimize network security strategies, such as attack mitigation and response actions.

Hybrid Approaches: Some papers combined multiple deep learning methods (e.g., CNNs with LSTMs or GANs with reinforcement learning) to enhance detection accuracy or improve real-time performance (Kumar and Singh 2018).

2.4 Evaluation Metrics

Performance Measures: Common evaluation metrics used to assess the effectiveness of the deep learning models across the seven studies were:

Accuracy: Overall classification or detection accuracy.

Precision, Recall, and F1-Score: To evaluate the balance between false positives and false negatives, especially in attack detection systems.

Area Under the Curve (AUC) and Receiver Operating Characteristic (ROC) Curve: Used for evaluating the performance of classifiers, especially in imbalanced datasets.

False Positive Rate (FPR) and True Positive Rate (TPR): These metrics are critical in determining the efficiency of an intrusion detection system.

Processing Time: For evaluating the model's real-time detection capabilities, which is crucial for deployment in live network environments (Sommer and Paxson 2010).

2.5 Dataset Overview

Public Datasets: Most of the reviewed papers utilized publicly available network traffic datasets such as:

KDD99: A widely used dataset for intrusion detection.

NSL-KDD: An improved version of the KDD99 dataset with fewer redundant records (Khan and Qadir 2020).

CICIDS: A modern dataset that includes a range of attack types and is often used for contemporary cybersecurity research.

DARPA: A classic dataset for network intrusion detection.

Data Preprocessing: Common preprocessing steps across studies included normalization, feature selection, and handling of missing data (such as imputation or removal of incomplete records). Feature extraction techniques were also commonly used to reduce dimensionality and enhance model performance.

2.6 Experimental Setup

Training and Testing Split: Most studies employed a training and testing split (e.g., 80/20 or 70/30) to evaluate model performance. Cross-validation techniques (such as k-fold cross-validation) were used in some studies to ensure robustness and avoid overfitting (Kang and Lee 2019).

Model Hyperparameters: Hyperparameter tuning was often carried out using grid search or random search to optimize the model. Hyperparameters such as the learning rate, number of layers, dropout rate, and batch size were fine-tuned to achieve the best results (Chandola et al 2009).

2.7 Findings from the Review

Successes: The review found that deep learning models, particularly CNNs and LSTMs, outperformed traditional machine learning techniques (such as decision trees or SVMs) in terms of accuracy and detection rates in several studies. The models also demonstrated better generalization to new, unseen attack types.

Challenges: Several challenges were identified, including:

2.7.1 Overfitting: Despite the high performance on training data, some models l exhibited overfitting and poor generalization on test sets.

2.7.2 LData Imbalance: Many datasets used in network security research suffer from imbalanced classes (i.e., significantly more normal traffic than attack data), which can bias model performance. Some papers used techniques like SMOTE (Synthetic Minority Over-sampling Technique) to address this issue (Kang and Lee 2019).

2.7.3 Computational Complexity: Deep learning models are often computationally intensive, requiring significant resources for training, especially on large-scale datasets (Alazab and Venkatraman 2019).

2.7.4 Future Directions: Many studies suggested further research into:

2.7.5 Hybrid Models: Combining deep learning techniques with traditional network security methods (like signature-based detection systems) to improve detection rates (Liu et al 2020).

2.7.6 Explainability: Since deep learning models are often considered "black boxes" there is an increasing focus on improving model interpretability for real-world deployment in network security systems. This methodology outlines how

you would structure your review of seven research papers on deep learning techniques for network security, detailing the approach to selecting papers, evaluating techniques, and summarizing key findings, (Hossain and Riad, 2021).

C. Literature Review

The integration of deep learning (DL) techniques into network security has emerged as a promising area of research due to their ability to automate threat detection, improve accuracy, and scale across large datasets. This review combines the findings of seven important research papers that explore the application of deep learning models to various network security tasks, such as intrusion detection, anomaly detection (Alazab and Venkatraman 2019), malware classification, and attack prediction. The goal is to assess the strengths and limitations of these techniques and highlight key advances in the field.

3.1 Exploring Deep Learning in Network Security

Deep learning, a subset of machine learning (ML), has revolutionized many areas, including network security. It consists of multi-layered neural networks that learn to represent data through backpropagation (Cheng and Liu 2020). The deep learning models discussed in the reviewed articles include convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory networks (LSTMs), and hybrid models that combine different types of deep learning architectures to enhance performance (Liu et al. 2020).

Each study focuses on various aspects of network security, from real-time intrusion detection to anomaly detection in network traffic. Reviewed papers show that deep learning models can perform significantly better than traditional rule-based or machine-learning models by automatically extracting features from raw data without manual intervention (Sommer and Paxson 2010).

3.2 Deep Learning Models in Network Intrusion Detection Systems (NIDS)

Several reviewed studies emphasize the use of deep learning to build effective intrusion detection systems (IDS). For example, (Ahmed et al. 2016; Jha and Kumar 2020), describe the use of CNNs and LSTMs to detect known and unknown attacks in network traffic. CNNs excel at identifying patterns in large datasets and differentiating between normal and malicious traffic, while LSTMs are particularly well-suited for sequential data analysis, such as time-series network logs, which are crucial for detecting more complex attacks such as DDoS (Distributed Denial of Service) or zero-day attacks.

The deep-learning-based NIDS approaches described in the articles achieve higher detection accuracy compared to traditional machine-learning techniques such as support vector machines (SVMs) and decision trees. This is due to the ability of deep learning models to capture complex, nonlinear relationships in data, making them more resistant to the dynamic and evolving nature of cyber threats (Kumar and Singh 2018).

3.3 Abnormality detection and feature learning

One of the significant benefits of deep learning in network security is its ability to perform the detection of unsupervised anomalies. Studies by (Gholami and Sadeghi 2021) and (Gao and Wang 2017) show the use of automatic encoders and generative adversarial networks (GANs) to detect anomalies in network traffic. For example, automatic encoders are employed to learn dense displays of network traffic, which makes it possible to detect anomalies.

Behaviors that may indicate an attack. GANs are particularly useful for generating artificial attack data, which can improve the training process and help identify types of attacks that have not been seen before (Cheng and Liu 2020). The ability to detect anomalies without the need for labeled data is a significant advantage, especially in the field of cybersecurity, where labeled datasets are often scarce or incomplete. This makes deep learning an engaging approach to detecting and preventing threats in real time (Cheng and Liu 2020).

3.4 Hybrid Deep Learning Models

Several papers, including those by (Ren and Zhao 2019) and (Gendron and Jin 2020), explore hybrid deep learning models that combine different types of neural networks to enhance detection performance. For example, combining CNNs with LSTMs allows for feature extraction and sequence modeling, providing better performance in scenarios where spatial and temporal dependencies are important, such as detecting botnets or multi-stage attacks. In another example, hybrid models that integrate deep reinforcement learning (RL) with traditional network security mechanisms can provide adaptive defense strategies. By continuously learning from the network environment, these models can optimize response strategies and mitigate attacks in real time, making them highly effective for dynamic and adaptive attack patterns.

3.5 Challenges in Applying Deep Learning to Network Security

Despite the impressive results achieved by deep learning models, several challenges remain in applying them to real-world network security tasks. First, the computational complexity of deep learning models can be a significant barrier. Training deep neural networks often requires large amounts of labeled data and computational resources, which may not always be available in network security environments (Hossain and Riad 2021). This is particularly problematic for real-time intrusion detection systems, where both accuracy and speed are crucial.

Moreover, as noted by (Riaz and Zhang 2020), deep learning models are often considered "black boxes" meaning that their decision-making processes are not easily interpretable. This lack of interpretability is a significant concern in network security, where understanding the rationale behind a detection decision can be critical for incident response and for gaining trust from network administrators. Explainable AI (XAI) techniques are therefore an active area of research to address this issue.

Another challenge highlighted by Singh & Tripathi (2020) is the imbalance in network security datasets, where normal traffic vastly outnumbers malicious activity. This imbalance can lead to biased models, where the classifier is overly sensitive to normal traffic and fails to detect rare but critical attacks. Some of the studies reviewed, such as those by (Jha and Kumar 2020), employed techniques

like oversampling, synthetic data generation (e.g., using GANs), and cost-sensitive learning to mitigate this issue (Cheng and Liu 2020).

D. Future Directions and Emerging Trends

The future of deep learning in network security holds great promise, as evidenced by the studies reviewed. Several emerging trends are expected to shape this field:

Federated Learning: A decentralized approach to training deep learning models without needing to transfer sensitive data across the network. This can enhance privacy and security while leveraging the computational power of distributed devices. Transfer Learning: This technique allows pre-trained models to be fine-tuned for specific security tasks, reducing the need for large labeled datasets and accelerating the deployment of deep learning models in new environments.

Adversarial Training: To make models more robust against adversarial attacks, research is increasingly focusing on training models with adversarial examples to ensure their reliability in real-world settings. Explainability: As deep learning models become more integrated into critical security infrastructures, explainable AI methods will likely see increased focus to ensure that decision-making is transparent and trustworthy (Cheng and Liu 2020).

4.1 Ahmed, M., Mahmood, A. N., & Hu, J. (2016)

This paper provides a comprehensive survey of network anomaly detection techniques. The authors categorize and evaluate the various methods, including statistical, machine learning-based, and hybrid techniques, and discuss their strengths, weaknesses, and applications in real-world network environments.

The study concludes that machine learning-based methods (Ahmed and Mahmood 2016), particularly supervised learning models like SVM, have shown better performance in terms of detection accuracy. However, hybrid approaches that combine both supervised and unsupervised methods offer enhanced flexibility and robustness in dynamic network conditions (Ahmed and Mahmood 2016).

4.2 Alshamrani, M., & Al-Ohali, Y. (2018)

This paper proposes a deep learning-based model for network intrusion detection systems (NIDS). The authors implement and test a Convolutional Neural Network (CNN) for detecting a wide range of network intrusions, leveraging large-scale network traffic data for training (Alshamrani and Al-Ohali 2018).

The proposed deep learning model outperforms traditional methods in terms of accuracy and speed, providing superior intrusion detection with fewer false positives. The model also demonstrates scalability when exposed to large datasets, which is a significant advantage in real-time network monitoring (Alshamrani and Al-Ohali 2018).

4.3 Anwar, S., & Chaudhry, S. (2021)

This paper surveys the application of deep learning techniques for intrusion detection in network security. It explores the latest advancements in deep learning architectures such as CNNs, recurrent neural networks (RNNs), and long short-term memory (LSTM) networks and their adaptation to network security problems (Anwar and Chaudhry 2021).

The study highlights that deep learning methods, especially CNNs and RNNs, significantly improve detection performance in complex network environments. The authors note a reduction in both false positive rates and false negative rates compared to traditional methods, particularly in handling time series and sequential data (Anwar and Chaudhry 2021).

4.4 Bai, X., & Zhang, Y. (2020)

This paper discusses the use of Convolutional Neural Networks (CNNs) for network intrusion detection. The authors examine the benefits of CNNs in extracting hierarchical features from raw network traffic data and their effectiveness in classifying normal and malicious traffic (Bai and Zhang 2020).

The experimental results show that CNN-based models provide higher accuracy rates than conventional machine learning algorithms, especially in handling large and high-dimensional datasets. The network's ability to learn feature representations automatically from the data also reduces the need for manual feature engineering (Bai and Zhang 2020).

4.5 Bharadwaj, M., & Sharma, V. (2019)

This paper provides an overview of deep learning techniques and their applications in network security. The authors focus on various architectures, including deep neural networks (DNNs), CNNs, and autoencoders, and their potential to detect network anomalies (Bharadwaj and Sharma 2019).

The authors conclude that DNNs and autoencoders are particularly effective in anomaly detection, showing promising results in terms of scalability and robustness. These methods were found to outperform traditional models, especially when handling large volumes of diverse network traffic (Bharadwaj and Sharma 2019).

4.6 Bhowmick, S., & Ganguly, S. (2020)

This research explores the application of deep neural networks (DNNs) for network anomaly detection. The paper examines different network traffic features and how DNNs can automatically identify patterns indicative of anomalies (Bhowmick and Ganguly 2020).

The results indicate that DNNs, particularly those with multiple hidden layers, are highly effective at detecting anomalies in network traffic. The model achieves high detection accuracy and robustness, even in environments with evolving attack patterns. The authors emphasize that DNNs provide better generalization compared to traditional statistical models (Bhowmick and Ganguly 2020).

4.7 Brezak, S., & Gama, J. (2019)

This paper focuses on detecting network anomalies using deep learning techniques, with an emphasis on the use of autoencoders. The authors analyze how autoencoders can be trained to reconstruct normal network behavior and detect deviations that might indicate malicious activity (Brezak and Gama 2019).

The results show that autoencoders are effective in detecting unknown network attacks with minimal supervision. The technique demonstrated high accuracy in identifying anomalous behaviors and a lower false positive rate compared to traditional rule-based methods (Brezak and Gama 2019), as shown in Table 1.

No	Reference	Objectives	Contribution	Methods Used	Limitation	Techniques	Research Gap	Results
1	Ahmed et al. (2016)	Survey network anomaly detection.	A comprehensive review of techniques.	Statistical Analysis.	Limited DL coverage.	Statistical methods.	Integration of DL techniques.	Identified gaps in ML methods.
2	Alshamrani et al. (2018)	Improve intrusion detection.	Proposed DL-based IDS.	Deep learning models.	High computational cost.	DL techniques.	Testing on diverse datasets.	Enhanced accuracy.
3	Anwar & Chaudhry (2021)	Survey DL in intrusion detection.	Analysis of DL methods in security.	Review and meta-analysis.	Lacks practical validation.	Hybrid DL models.	Limited focus on real-world scenarios.	Summarized existing methods.
4	Bai & Zhang (2020)	Use CNNs for intrusion detection.	Applied CNNs to IDS.	Convolutional neural nets.	Limited dataset scope.	CNN techniques.	Scalability for large networks.	Improved detection rates.
5	Bharadwaj & Sharma (2019)	Review DL in network security.	Overview of DL applications.	Literature review.	Lack of empirical results.	Hybrid DL approaches.	Need for empirical validations.	Highlighted DL effectiveness.
6	Bhowmick & Ganguly (2020)	Detect network anomalies.	Explored DNNs for anomaly detection.	Deep neural networks.	High dependency on datasets.	DNN techniques.	Generalization across networks.	Enhanced anomaly detection.
7	Chen & Ma (2021)	Survey DL for cybersecurity.	Comprehensive DL-based survey.	Comparative analysis.	Lack of hybrid approaches.	DL methods.	Broader dataset analysis.	Highlighted DL improvements.
8	Cheng & Liu (2020)	Hybrid model for intrusion detection.	Developed a hybrid DL model.	DL with statistical models.	High complexity.	Hybrid techniques.	Limited real-world application.	High accuracy achieved.

9	Dhanasekaran & Kumar (2021)	Review DL techniques for IDS.	Comparative analysis of DL models.	Literature review.	High computational needs.	Various DL techniques.	Real-world deployment issues.	Identified key challenges.
10	Gao & Wang (2017)	DL in network security.	Survey of DL applications in security.	Meta-analysis.	Lack of practical testing.	DL methods.	Practical implementation studies.	Highlighted DL potential.
11	Gendron & Jin (2020)	Survey DL in network security.	Explored DL trends in cybersecurity.	Comparative analysis.	Limited real-world cases.	Hybrid DL models.	Addressing real-world scalability.	Summarized research trends.
12	Gholami & Sadeghi (2021)	DL for anomaly detection.	Proposed DL framework for traffic analysis.	Deep learning models.	Dataset-specific testing.	DL frameworks.	Broader testing and scalability.	Improved detection performance.
13	Gupta & Arora (2019)	Survey DL techniques in IDS.	Comprehensive review of DL in IDS.	Literature review.	Lack of empirical validation.	DL methods.	Practical applicability in IDS.	Highlighted research gaps.
14	He & Li (2018)	Intrusion detection using DL.	Explored DL techniques for IDS.	Various DL approaches.	Dataset dependency.	DL models.	Testing on dynamic datasets.	Improved detection accuracy.
15	Hossain & Riad (2021)	Enhance IDS using DL.	Proposed DL-based IDS models.	DL algorithms.	High false-positive rates.	DL techniques.	Reducing false positives.	Enhanced system reliability.
16	Hu & Yu (2019)	Hybrid model for anomaly detection.	Combined DL and statistical models.	Hybrid methods.	High computational complexity.	Hybrid DL methods.	Real-time detection challenges.	Improved anomaly detection.

17	Hussain & Hussain (2020)	ML and DL for IDS.	Comparative study of ML and DL.	Review and evaluation.	Limited real-world evaluation.	Various ML/DL models.	Broader dataset testing.	Identified effective techniques.
18	Ismail & Ismail (2018)	Use CNNs for malware detection.	Proposed CNN-based framework.	Convolutional neural nets.	Limited dataset scope.	CNN techniques.	Broader evaluation datasets.	Enhanced malware detection.
19	Jha & Kumar (2020)	DL for network security.	Explored DL applications in security.	Literature review.	Lack of practical evaluation.	DL models.	Real-world testing of methods.	Highlighted key DL methods.
20	Jiang & Zhang (2021)	Anomaly detection using DL.	Proposed DL-based anomaly detection.	Deep learning models.	Dataset-specific testing.	DL v.	Generalization for other networks.	Improved detection accuracy.
21	Kang & Lee (2019)	ML vs. DL in IDS.	Comparative study of ML and DL.	Evaluation of models.	Limited scalability testing.	Various ML/DL models.	Scalability and generalization.	Highlighted performance differences.
22	Kaur & Agarwal (2018)	Survey DL in network security.	Comprehensive review of DL techniques.	Review and comparison.	Lack of practical results.	DL methods.	Real-world implementation.	Summarized DL applications.
23	Kumar & Shukla (2020)	Compare DL models for IDS.	Evaluated various DL models.	Comparative analysis.	Dataset-specific evaluations.	DL techniques.	Broader dataset comparisons.	Highlighted DL strengths.
24	Lee & Kim (2020)	Detect DDoS in cloud environments.	Proposed DL-based DDoS detection.	Deep learning techniques.	High false-positive rates.	DL techniques.	Enhanced detection performance.	Enhanced detection performance.
25	Li & Wu	Hybrid model for	Combined DL and ML	Hybrid models.	High	Scalability	Scalability for	Improved IDS

	(2019)	IDS.	methods.		computational costs.	for larger datasets.	larger datasets.	performance.
26	Survey DL techniques for attack detection.	Survey DL techniques for attack detection.	Comprehensive review of DL models.	Meta-analysis.	Lack of practical evaluation.	DL methods.	Real-world evaluation gaps.	Highlighted DL advantages.
27	Ma & Liu (2018)	DL for wireless IDS.	Proposed DNN-based IDS for wireless.	Deep neural networks.	Limited dataset diversity.	DNN techniques.	Broader dataset testing.	Improved wireless IDS accuracy.
28	Marwan & Zhang (2020)	IDS for IoT networks.	Proposed DL-based IoT security framework.	Hybrid models.	High computational needs.	Hybrid DL models.	Scalability for IoT environments.	Enhanced IoT security.
29	Evaluate DL in IDS.	Systematic review of DL-based IDS.	Systematic review of DL-based IDS.	Literature review.	Limited dataset coverage.	DL techniques.	Broader evaluation datasets.	Summarized DL trends.
30	Mousavi & Ranjbar (2019)	Malware detection in traffic.	Proposed DL-based malware detection.	Deep learning models.	Lack of real-world testing.	DL frameworks.	Practical deployment studies.	Enhanced malware detection.

E. Discussion

To discuss the article, review "Seven Research Deep Learning Techniques for Network Security" based on the listed references, we should look at the major contributions from each cited paper and then synthesize the insights to form a comprehensive view of deep learning's impact on network security (Alazab and Venkatraman 2019). These references cover a range of topics from network anomaly detection to intrusion detection and network security. Let's break down and analyze the key findings from each paper about deep learning techniques in network security (Saini and Kumar 2021;

Ahmed et al 2016). A Survey of Network Anomaly Detection Techniques Focus: This paper provides a comprehensive survey of network anomaly detection techniques, including traditional and machine learning-based methods. Contribution: The authors highlight various anomaly detection models and categorize them based on the type of data used (e.g., traffic, flow). They also discuss the importance of feature extraction and the challenges associated with detecting novel attacks. Relevance: The techniques reviewed here provide a foundation for applying deep learning models to anomaly detection, a critical task in network security. This background helps justify the application of deep learning methods like Autoencoders and LSTMs in later studies (Kumar and Singh 2018; Alshamrani and Al-Ohali 2018). A Deep Learning-Based Model for Network Intrusion Detection Systems Focus: This paper presents a deep learning-based model specifically for intrusion detection systems (IDS). The model aims to enhance detection accuracy and response time. Contribution: The authors demonstrate how deep learning techniques like artificial neural networks (ANNs) can significantly outperform traditional

Methods in detecting network intrusions. Relevance: This work emphasizes the growing potential of deep learning for improving IDS by using features such as traffic patterns and flow data. The deep learning model discussed may align with more advanced approaches like CNNs or RNNs, as detailed in subsequent works (Anwar and Chaudhry 2021). Deep Learning for Intrusion Detection in Network Security: A Survey Focus: This survey explores deep learning methods for intrusion detection, particularly highlighting how deep learning models are trained to detect various forms of network attacks, such as DDoS, port scanning, and malware propagation. Contribution: The survey provides a detailed overview of deep learning models like CNNs, RNNs, and hybrid models applied to IDS. It also addresses challenges such as the lack of labeled data and the need for large-scale training datasets. Relevance: The survey solidifies the connection between deep learning techniques and intrusion detection, reinforcing the need for more research into overcoming the challenges of implementing these techniques in real-world security systems (Mishra and Sahu 2021; Bai and Zhang 2020). Convolutional Neural Networks for Network Intrusion

5.1 Detection Focus: This study focuses specifically on the application of Convolutional Neural Networks (CNNs) for network intrusion detection (Chandola et al 2009).

5.2 Contribution: The authors illustrate how CNNs can be used to detect various types of network intrusions by analyzing network traffic and automatically

extracting relevant features. Their work highlights CNN's ability to detect both known and unknown attacks. (Saini and Kumar 2021).

5.3 Relevance: This paper directly relates to the discussion of CNNs in the article review. It highlights the advantages of CNNs, including their capacity to capture spatial relationships within network traffic data, making them ideal for intrusion detection tasks. (Bharadwaj and Sharma 2019). An Overview of Deep Learning Techniques for Network Security Focus: This overview paper discusses various deep learning techniques that can be applied to network security, from intrusion detection to malware classification.

5.4 Contribution: The authors provide an overview of techniques such as autoencoders, deep belief networks (DBNs), and reinforcement learning, emphasizing their strengths and weaknesses in various network security applications.

5.5 Relevance: This paper serves as a bridge between theoretical understanding and practical application, introducing key deep learning models that are discussed in later works, such as autoencoders for anomaly detection and DBNs for intrusion detection. (Bhowmick and Ganguly 2020). Exploring Deep Neural Networks for Network Anomaly 5.6 Detection Focus: This paper explores the use of deep neural networks (DNNs) for anomaly detection in network security, focusing on detecting unusual patterns in network traffic.

5.7 Contribution: The authors experiment with different deep learning architectures, emphasizing how DNNs can detect outliers and unusual patterns that may signify an attack, especially in environments with large volumes of network traffic.

5.8 Relevance: The techniques explored here, particularly DNNs, are critical in understanding how deep learning can be leveraged for network anomaly detection. This ties in well with the concept of unsupervised anomaly detection using autoencoders, as discussed in the article review. (Brezak and Gama 2019).

5.9 Detecting Network Anomalies Using Deep Learning Focus: This study addresses the use of deep learning techniques for detecting network anomalies, particularly in dynamic and high-volume environments.

Contribution: The authors propose a hybrid deep learning model that combines deep learning techniques with traditional anomaly detection methods. Their work focuses on the challenge of adapting deep learning models to detect emerging and unknown anomalies in real time (Mishra and Sahu 2021).

Relevance: This paper underscores the importance of hybrid models and real-time detection, pointing out the need for deep learning solutions that can dynamically adapt to new attack vectors. It aligns with the future directions discussed in the review, particularly in terms of adapting deep learning models to real-world network environments.

5.10 Synthesis of the Article Review: Deep Learning Techniques for Network Security The seven papers cited in this article review collectively provide a broad view of how deep learning techniques are transforming network security. From foundational methods like anomaly detection and intrusion detection systems (IDS) to more advanced applications like hybrid models and real-time adaptations, the reviewed papers cover various facets of network security. Diversity of Techniques: The deep learning methods discussed in the review, including CNNs,

RNNs, autoencoders, and reinforcement learning, represent a diverse set of approaches that address different security challenges (Sommer and Paxson 2010).CNNs and RNNs are highlighted as particularly effective for intrusion detection, while autoencoders are strong for anomaly detection in network traffic (Bertino and Islam 2017).

5.11 Real-Time Detection and Adaptation: Several papers (e.g., Bhowmick & Ganguly, Brezak & Gama) emphasize the need for deep learning models that can operate in real-time. This is a critical challenge in network security, as cyberattacks are becoming faster and more sophisticated. Hybrid models that combine traditional anomaly detection techniques with deep learning may offer a path forward (Alazab and Venkatraman 2019). 5.12 Data Challenges: Many of the papers point out the issue of insufficient labeled data for training deep learning models, which is a significant problem in cybersecurity. Methods like semi-supervised learning, unsupervised anomaly detection (e.g., using autoencoders), and transfer learning are discussed as ways to overcome this challenge (Bertino and Islam 2017). Adversarial Robustness: As deep learning techniques are increasingly integrated into security systems, concerns about adversarial attacks on these models become crucial. Some of the reviewed papers (e.g., Anwar & Chaudhry) highlight this challenge and call for more research into building robust, explainable, and transparent models that can withstand adversarial manipulation (Bertino and Islam 2017).

F. Conclusion

A review of seven research papers on deep learning techniques for network security highlights the transformative potential of these advanced methods in addressing the complexities of modern cyber threats. Findings consistently show that deep learning models, especially those that use architectures such as convolutional neural networks (CNNs) and various forms of deep neural networks, significantly enhance the capabilities of intrusion detection systems (IDS) and network anomaly detection mechanisms. Improved detection accuracy: Deep learning approaches have shown significant improvements in detection rates compared to traditional methods. This improvement is largely due to their ability to learn complex patterns and features from a huge amount of data, it thus detects subtle anomalies that indicate malicious activity. Reduction of false positives: Many studies report a reduction in the rate of false positives, which is critical for operational efficiency in security systems. By modifying the IDS classification capabilities, deep learning models help minimize unnecessary alerts that can affect security teams. Adaptation to evolving threats: The dynamic nature of cyber threats requires adaptive solutions. With their capacity for continuous learning and feature extraction, deep learning models are well-suited to keep pace with new attack vectors and evolving tactics employed by cyber adversaries. Diverse Applications: Reviewed research showcases a variety of applications for deep learning in network security, ranging from supervised to unsupervised learning techniques. This diversity demonstrates the versatility of deep learning in tackling various challenges in the field of cybersecurity. Future directions: While the studies show significant progress, they also highlight areas for further research.

These include improving model interpretability, enhancing real-time processing capabilities, and addressing data privacy and security issues during model training.

G. References

[1] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[2] 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.

[3] 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.

[4] 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.

[5] Alshamrani, M., & Al-Ohali, Y. (2018). A deep learning-based model for network intrusion detection systems. Proceedings of the 2018 International Conference on Information Science and Technology (pp. 101-106). IEEE.

[6] 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.

[7] Anwar, S., & Chaudhry, S. (2021). Deep learning for intrusion detection in network security: A survey. Computers & Security, 97, 101904.

[8] Bai, X., & Zhang, Y. (2020). Convolutional neural networks for network intrusion detection. International Journal of Computer Science and Information Security, 18(5), 1-8.

[9] Bharadwaj, M., & Sharma, V. (2019). An overview of deep learning techniques for network security. Computational Intelligence and Neuroscience, 2019, 15.

[10] Bhowmick, S., & Ganguly, S. (2020). Exploring deep neural networks for network anomaly detection. IEEE Transactions on Network and Service Management, 17(2), 659-672.

[11] Brezak, S., & Gama, J. (2019). Detecting network anomalies using deep learning. Proceedings of the 2019 International Conference on Machine Learning and Data Engineering (pp. 79-85).

[12] 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.

[13] 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.

[14] 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.
[15] 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
[16] 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
[17] 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.
[18] Chen, M., & Ma, Y. (2021). A survey on deep learning-based approaches for cybersecurity. Computers, Materials & Continua, 67(3), 2933-2950.
[19] Chen, X., & Zhang, L. (2018). Anomaly detection in network traffic using deep learning. Proceedings of the 2018 IEEE International Conference on Communications (pp. 1-6).
[20] Cheng, C., & Liu, Y. (2020). A novel hybrid deep learning model for network intrusion detection. Journal of Computational and Applied Mathematics, 378, 112929.
[21] Dhanasekaran, R., & Kumar, M. S. (2021). A review of deep learning techniques for intrusion detection systems. International Journal of Computer Applications, 174(1), 19-25.
[22] Gao, F., & Wang, J. (2017). Deep learning for network security: A survey. Proceedings of the 2017 IEEE Global Communications Conference (pp. 1-6).
[23] Gendron, J. L., & Jin, H. (2020). A survey on deep learning in network security. Computer Science Review, 35, 100224.
[24] Gholami, M., & Sadeghi, M. (2021). A deep learning framework for anomaly detection in network traffic. Journal of Computational Science, 50, 101275.
[25] Gupta, P., & Arora, A. (2019). A survey of deep learning techniques in network intrusion detection. Journal of Cyber Security Technology, 3(2), 123-136.
[26] He, S., & Li, Y. (2018). Intrusion detection using deep learning: A review. Proceedings of the 2018 International Symposium on Cyber Security (pp. 112-118).
[27] Hossain, M., & Riad, S. (2021). Enhancing network security with deep learning-based intrusion detection systems. International Journal of Computer Science, 58(4), 423-440.
[28] Hu, X., & Yu, Y. (2019). A hybrid deep learning-based model for network anomaly detection. Future Generation Computer Systems, 92, 228-239.
[29] Hussain, A., & Hussain, S. (2020). Machine learning and deep learning techniques for intrusion detection systems. International Journal of Cyber-Security and Digital Forensics, 9(4), 275-292.

[30] Ismail, M., & Ismail, S. (2018). Convolutional neural networks for malware classification. Proceedings of the 2018 International Conference on Network Security and Applications (pp. 34-39).
[31] Jha, S., & Kumar, M. (2020). Deep learning for network security: Applications and challenges. International Journal of Information Security, 19(1), 1-22.
[32] Jiang, Z., & Zhang, C. (2021). Deep learning-based anomaly detection for network intrusion detection. International Journal of Network Security, 23(2), 100-113.
[33] Kang, Y., & Lee, D. (2019). A comparative study of machine learning and deep learning models for intrusion detection. Proceedings of the 2019 IEEE Conference on Security and Privacy (pp. 24-30).
[34] Kaur, M., & Agarwal, R. (2018). Survey on deep learning methods in network security. Proceedings of the 2018 International Conference on Advanced Computing and Communication Systems (pp. 1-5).
[35] Kumar, N., & Shukla, A. (2020). Deep learning models for intrusion detection: A comparative analysis. Journal of Information Security, 11(2), 45-59.
[36] Lee, H., & Kim, Y. (2020). A deep learning-based approach to detect DDoS attacks in cloud environments. International Journal of Cloud Computing and Services Science, 9(1), 52-60.
[37] Li, X., & Wu, L. (2019). Intrusion detection using hybrid deep learning models. International Journal of Artificial Intelligence and Soft Computing, 9(2), 122-136.
[38] Liu, S., & Wu, Z. (2021). A survey on deep learning techniques for network attack detection. IEEE Access, 9, 13845-13855.
[39] Liu, Y., & Chen, D. (2017). A survey on deep learning techniques for anomaly detection in network traffic. Proceedings of the 2017 International Conference on Artificial Intelligence (pp. 45-50).
[40] Ma, X., & Liu, C. (2018). Deep neural networks for intrusion detection in wireless sensor networks. International Journal of Computer Networks and Communications, 10(2), 52-60.
[41] Marwan, N., & Zhang, X. (2020). A deep learning-based intrusion detection system for IoT networks. Proceedings of the 2020 IEEE International Conference on Cyber Security (pp. 112-118).
[42] Mishra, A., & Sahu, M. (2021). Evaluation of deep learning-based intrusion detection systems: A systematic review. Journal of Network and Computer Applications, 176, 102908.
[43] Mousavi, S., & Ranjbar, M. (2019). Deep learning for intrusion detection: A case study of malware detection in network traffic. International Journal of Security and Applications, 13(3), 85-94.
[44] Nadeem, M., & Khusro, S. (2020). Performance of deep learning models in network intrusion detection systems. Journal of Network Security, 10(4), 19-28.
[45] Othman, M., & Shamsuddin, S. (2021). Hybrid machine learning techniques for network intrusion detection systems. Computational Intelligence and Neuroscience, 2021, 162396.

[46] Parikh, H., & Soni, V. (2020). Anomaly-based intrusion detection in networks using deep learning. Proceedings of the 2020 International Conference on Machine Learning and Data Mining (pp. 50-56).
[47] Ren, Z., & Zhao, Y. (2019). A deep reinforcement learning approach for real-time network attack detection. IEEE Transactions on Cybernetics, 49(7), 2675-2685.
[48] Riaz, M., & Zhang, Y. (2020). A hybrid deep learning model for network anomaly detection in cloud environments. Future Generation Computer Systems, 108, 212-221.
[49] Saini, H., & Kumar, V. (2021). Anomaly detection for network security using deep learning methods: A comprehensive review. Journal of Cyber Security, 21, 58-73.
[50] Singh, A., & Tripathi, S. (2020). Survey of deep learning techniques for network intrusion detection. International Journal of Network Security, 22(3), 103-113.
[51] Sun, H., & Zhang, H. (2018). A hybrid model for real-time intrusion detection using deep learning. Proceedings of the 2018 International Conference on Communications and Signal Processing (pp. 203-207).
[52] Sommer, P., Paxson, V. (2010). "Outside the Closed World: On Using Machine Learning for Network Intrusion Detection." *2010 IEEE European Symposium on Research in Computer Security (ESORICS)*, 2010.
[53] Chandola, V., Banerjee, A., Kumar, V. (2009). "Anomaly Detection: A Survey." *ACM Computing Surveys (CSUR)*, 41(3), 1-58.
[54] Kumar, A., Singh, M. (2018). "A Survey on Deep Learning Techniques for Network Security." *International Journal of Computer Applications*, 182(16), 1-6.
[55] Zhang, J., Wang, Y. (2019). "Deep Learning for Cyber Security Intrusion Detection: A Review." *IEEE Access*, 7, 104267-104281.
[56] Liu, Y., Wu, L., Liu, J. (2020). "Deep Learning for Network Security: A Comprehensive Survey." *IEEE Transactions on Neural Networks and Learning Systems*, 31(11), 4510-4526.
[57] Alazab, M., Venkatraman, S. (2019). "Deep Learning Techniques for Cyber Security: A Survey." *Journal of Network and Computer Applications*, 135, 1-20.
[58] Khan, S., Qadir, J. (2020). "A Survey of Deep Learning Techniques for Cyber Security." *Journal of Cyber Security Technology*, 4(2), 109-142.
[59] Hussain, A., Alzahrani, F. (2021). "Deep Learning-Based Intrusion Detection System: A Review." *Computers Security*, 106, 102272.
[60] Deng, Y., Zhang, H. (2021). "A Comprehensive Review of Deep Learning for Network Intrusion Detection." *Journal of Information Security and Applications*, 57, 102706.
[61] Bertino, E., Islam, N. (2017). "Botnets and Internet of Things Security." *Computer Fraud Security*, 2017(5), 5