International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 01, January-March 2026, pp: 19-28
ISSN: 3071-3358

# Deep Learning Approaches for Intrusion Detection in Intelligent Communication Networks; A Study

**Dr. Aamir Ullah Khan Lodhi**
University of South Florida, Florida, USA.
Email: dean.rnd.scet@gmail.com



***Abstract***
*The increasing integration of intelligent communication networks, including fifth-generation (5G), sixth-generation (6G), Internet of Things (IoT), cloud computing, edge intelligence, and software-defined networking, has significantly improved communication efficiency and connectivity. However, the rapid expansion of these advanced network infrastructures has also increased vulnerability to sophisticated cyberattacks, malicious intrusions, and security breaches. Traditional intrusion detection systems (IDS), which primarily rely on signature-based and rule-based mechanisms, often fail to identify emerging and complex threats in dynamic communication environments. Deep Learning (DL) approaches have emerged as effective solutions for intrusion detection due to their ability to automatically extract hidden patterns, analyze high-dimensional network traffic data, and detect anomalous behavior in real time. This study explores various deep learning techniques, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Autoencoders, Deep Belief Networks (DBN), and hybrid deep learning models for intrusion detection in intelligent communication networks. The paper examines the role of deep learning in enhancing attack detection accuracy, minimizing false alarm rates, improving scalability, and enabling adaptive threat intelligence in heterogeneous networking environments. Additionally, the research discusses challenges such as data imbalance, adversarial attacks, computational overhead, privacy concerns, and model interpretability in intelligent network security systems. By analyzing recent advancements and research developments, this study highlights the transformative potential of deep learning-based intrusion detection systems in strengthening cybersecurity frameworks for future intelligent communication networks. The findings demonstrate that deep learning techniques significantly improve intrusion detection performance, network resilience, and automated security response mechanisms, contributing to safer and more reliable communication infrastructures.*

***Keywords***
*Deep Learning, Intrusion Detection System (IDS), Intelligent Communication Networks, Cybersecurity, Network Security, Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Autoencoder, Deep Belief Network (DBN), Artificial Intelligence, Anomaly Detection, Internet of Things (IoT), 5G Networks, 6G Networks, Intelligent Systems.*

## 1. Introduction

The advancement of intelligent communication networks has significantly transformed digital communication systems across industries, governments, healthcare, education, transportation, and industrial automation. Emerging technologies such as 5G, 6G, Internet of Things (IoT), cloud computing, software-defined networking (SDN), and edge intelligence have enabled unprecedented levels of communication efficiency, automation, and smart decision-making capabilities. These technologies facilitate seamless data transmission, ultra-low latency communication, and high-speed connectivity, thereby supporting intelligent applications such as autonomous vehicles, smart healthcare, industrial automation, and intelligent urban infrastructure. However, this technological transformation has simultaneously increased cybersecurity vulnerabilities, exposing communication systems to sophisticated cyber threats and network intrusions. [2]

***Received:*** *27-12-2025*
***Revised:*** *29-01-2026*
***Accepted:*** *14-02-2026*
***Published:*** *28-02-2026*
***Citation:*** *" Deep Learning Approaches for Intrusion Detection in Intelligent Communication Networks", ijaicn, vol. 2, no. 1, pp. 19–28, Feb. 2026,*

The rapid increase in interconnected devices and distributed communication infrastructures has created complex attack surfaces that cybercriminals increasingly exploit. Traditional cybersecurity mechanisms struggle to protect intelligent communication networks due to the continuously evolving nature of cyberattacks.

Malicious activities such as denial-of-service attacks, phishing, malware injection, botnet attacks, ransomware, insider threats, and unauthorized data access continue to challenge network security systems.

Since intelligent communication networks process enormous volumes of dynamic and heterogeneous traffic data, conventional intrusion detection methods are often insufficient for detecting hidden or zero-day attacks effectively. [3]

Intrusion Detection Systems (IDS) play an essential role in identifying unauthorized activities, malicious intrusions, and abnormal network behavior. IDS are broadly categorized into signature-based and anomaly-based systems. Signature-based IDS detect attacks using predefined patterns stored in databases, while anomaly-based IDS identify deviations from normal network behavior. Although signature-based systems demonstrate high efficiency in recognizing known attacks, they perform poorly against unknown or evolving cyber threats. Similarly, traditional anomaly detection systems often suffer from high false alarm rates and inadequate learning capabilities. [4]

In recent years, Deep Learning (DL) has emerged as a transformative technology in cybersecurity and intrusion detection. Deep learning models possess superior capabilities in feature extraction, pattern recognition, and real-time threat analysis. Unlike conventional machine learning methods, deep learning algorithms can automatically learn meaningful representations from raw network traffic data without extensive manual feature engineering. This capability significantly enhances detection accuracy and allows systems to adapt to changing cyber threat environments. [5]

Various deep learning architectures have been applied in intrusion detection systems, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory (LSTM), Autoencoders, Deep Belief Networks (DBN), and hybrid deep learning frameworks. CNN models effectively identify spatial features in network traffic data, while RNN and LSTM architectures excel in analyzing sequential traffic behavior and time-dependent attack patterns. Autoencoders are widely used for anomaly detection by learning compressed representations of normal network activity, whereas DBN models support unsupervised learning for complex intrusion classification tasks. Hybrid architectures combine multiple techniques to improve performance and robustness. [6]

The application of deep learning in intelligent communication networks has shown significant improvements in intrusion detection accuracy, reduced false positive rates, enhanced scalability, and improved adaptability to dynamic network environments. Intelligent intrusion detection systems powered by deep learning support automated threat analysis and contribute to stronger cybersecurity resilience in modern communication ecosystems. However, despite these benefits, several challenges remain unresolved, including computational complexity, adversarial manipulation, limited training datasets, model transparency, and privacy-related concerns. [7]

This study aims to provide a comprehensive review of deep learning approaches for intrusion detection in intelligent communication networks. The paper examines the role of deep learning models in network security, evaluates their advantages and limitations, and highlights recent research developments and future opportunities for intelligent cybersecurity systems. [8]

## 2. Literature Review

*Goodfellow, Bengio, and Courville (2016)* presented a comprehensive foundation for deep learning, explaining the theoretical principles of neural networks, optimization techniques, and representation learning. Their work established the fundamental concepts that have enabled the development of advanced cybersecurity applications, including intelligent intrusion detection systems and automated threat analysis mechanisms [1].

*Stallings (2018)* discussed essential network security principles, including authentication, access control, cryptography, and intrusion detection technologies. The author highlighted the increasing complexity of cyber threats and emphasized the need for intelligent security frameworks capable of detecting sophisticated attacks in modern network environments [2].

*Scarfone and Mell (2007)* provided detailed guidelines for Intrusion Detection and Prevention Systems (IDPS), categorizing detection techniques into signature-based and anomaly-based approaches. Their work remains a key reference for understanding the operational requirements, deployment strategies, and performance considerations of intrusion detection systems in organizational networks [3].

*Liao, Lin, Lin, and Tung (2013)* conducted a comprehensive review of intrusion detection systems and analyzed various detection methodologies, including anomaly detection, misuse detection, and hybrid approaches. The study identified the strengths and limitations of traditional

IDS techniques and highlighted the need for more adaptive and intelligent detection mechanisms [4].

Goodfellow, Shlens, and Szegedy (2015) investigated adversarial examples in deep neural networks and demonstrated how small perturbations in input data can mislead machine learning models. Their findings revealed critical vulnerabilities in deep learning systems and emphasized the importance of robust model design for cybersecurity applications [5].

*LeCun, Bengio, and Hinton (2015)* explored recent advances in deep learning and demonstrated the effectiveness of deep neural networks in handling complex pattern recognition tasks. The authors highlighted the ability of deep learning models to automatically extract meaningful features from large datasets, making them suitable for intrusion detection and threat intelligence applications [6].

*Schmidhuber (2015)* presented an extensive overview of deep learning architectures, including convolutional neural networks, recurrent neural networks, and deep feedforward networks. The study discussed the evolution of neural network technologies and their potential applications in security analytics and anomaly detection [7].

*Sarker (2021)* introduced the concept of deep cybersecurity and examined how deep learning techniques can improve threat detection, malware classification, and intrusion detection. The study emphasized the growing role of artificial intelligence in strengthening cyber defense mechanisms and reducing response times to emerging threats [8].

*Buczak and Guven (2016)* reviewed data mining and machine learning techniques used in cybersecurity applications. Their survey analyzed classification, clustering, and anomaly detection methods and concluded that machine learning significantly enhances the accuracy and efficiency of intrusion detection systems when compared with conventional approaches [9].

*Vinayakumar, Soman, and Poornachandran (2019)* investigated deep learning models for network traffic prediction and intrusion detection. The authors demonstrated that deep neural networks can effectively learn traffic behavior patterns and accurately identify malicious activities in complex network environments [10].

*Kim, Lee, and Kim (2014)* proposed a hybrid intrusion detection framework that combined anomaly detection and misuse detection techniques. Their approach improved detection accuracy by leveraging the strengths of both methodologies while reducing false alarm rates commonly associated with standalone detection systems [11].

*Javaid, Niyaz, Sun, and Alam (2016)* developed a deep learning-based intrusion detection system using neural network architectures to classify network traffic. Experimental results showed that deep learning techniques achieved better detection performance and adaptability than traditional machine learning algorithms [12].

*Yin, Zhu, Fei, and He (2017)* introduced a recurrent neural network (RNN)-based intrusion detection model capable of capturing temporal dependencies in network traffic. The study demonstrated superior classification performance and enhanced detection capabilities for identifying complex cyberattacks [13].

*Shone, Ngoc, Phai, and Shi (2018)* proposed a deep learning framework integrating non-symmetric deep autoencoders with random forests for intrusion detection. The hybrid architecture effectively extracted relevant features from network traffic data and achieved high detection accuracy with reduced computational complexity [14].

*Diro and Chilamkurti (2018)* developed a distributed deep learning-based attack detection system for Internet of Things (IoT) environments. Their approach improved scalability and enabled efficient detection of malicious activities across distributed IoT networks, addressing security challenges associated with connected devices [15].

*Alrawashdeh and Purdy (2017)* focused on the development of an online anomaly intrusion detection system using deep learning techniques. Their study demonstrated the capability of deep neural networks to continuously monitor network traffic and identify abnormal behaviors in real-time environments [16].

*Tang, McLernon, Ghogho, Zaidi, and El-Hajjar (2020)* proposed a deep learning-based intrusion detection model for Software Defined Networking (SDN). The study showed that deep learning algorithms can effectively analyze SDN traffic patterns and improve attack detection performance while maintaining network flexibility and efficiency [17].

*Ferrag, Maglaras, Moschoyiannis, and Janicke (2020)* conducted a comparative study of deep learning techniques for cybersecurity intrusion detection. The authors evaluated various datasets, architectures, and performance metrics, concluding that deep learning methods consistently outperform traditional approaches in detecting modern cyber threats and network attacks [18].

## 3. Intelligent Communication Networks and Security Challenges

Intelligent communication networks represent advanced digital infrastructures that integrate artificial intelligence, automation, cloud computing, and smart communication technologies to enable seamless connectivity and intelligent data processing. These networks include 5G and 6G communication systems, IoT ecosystems, software-defined networking, edge intelligence, vehicular communication networks, and cloud-based

infrastructures. Such systems support large-scale device communication and autonomous operations while enabling efficient data sharing across multiple platforms. [16]

However, the growing complexity of intelligent communication systems introduces serious cybersecurity risks. Since billions of connected devices continuously exchange sensitive information, attackers exploit network vulnerabilities to gain unauthorized access, disrupt services, or steal confidential data. Common cybersecurity threats include DDoS attacks, malware injection, ransomware, phishing, data interception, spoofing, insider attacks, and botnet activities. [17]

One major challenge in intelligent communication networks is the dynamic nature of cyber threats. Traditional intrusion detection methods rely on predefined attack signatures and fail to recognize unknown attacks effectively. Additionally, network traffic generated by IoT and intelligent devices is highly heterogeneous, making feature extraction and attack classification increasingly difficult. Intelligent communication networks also demand low-latency security mechanisms capable of operating in real time without affecting network performance. [18]

Furthermore, intelligent communication infrastructures often operate under resource constraints, particularly in edge devices and IoT systems. Deep learning models require substantial computational resources, creating implementation difficulties in low-power environments. Privacy concerns also emerge when sensitive user information is processed for cybersecurity analysis. Therefore, intelligent and adaptive security solutions are required to ensure resilient communication infrastructures capable of resisting evolving cyber threats. [19]

## 4. Deep Learning Techniques for Intrusion Detection in Intelligent Communication Networks

Deep learning techniques have emerged as highly efficient solutions for intrusion detection due to their capability to analyze large-scale network traffic data, automatically extract hidden features, and identify complex attack behaviors with minimal human intervention. Unlike conventional machine learning approaches that depend heavily on manual feature extraction, deep learning models autonomously learn hierarchical representations from raw data, improving detection efficiency and classification accuracy. In intelligent communication networks such as 5G, 6G, IoT, cloud computing, and software-defined networking environments, deep learning enables adaptive and scalable cybersecurity frameworks capable of detecting both known and unknown attacks. [20]

### 4.1 Convolutional Neural Networks (CNN) for Intrusion Detection

Convolutional Neural Networks (CNN) are among the most widely adopted deep learning architectures for intrusion detection due to their strong capability in automatic feature extraction and classification. Originally developed for image recognition tasks, CNN models have demonstrated significant success in cybersecurity by identifying hidden traffic patterns and malicious behaviors in network communication datasets. CNN architectures consist of convolutional layers, pooling layers, and fully connected layers that collectively process multidimensional data and detect significant attack features. [21]

In intrusion detection systems, CNN models analyze network traffic packets and transform traffic attributes into structured representations for classification. The convolutional layer identifies hidden relationships among traffic features, while pooling mechanisms reduce dimensional complexity and improve computational efficiency. CNN-based intrusion detection systems have shown high effectiveness in detecting distributed denial-of-service (DDoS) attacks, malware activities, botnet intrusions, spoofing attacks, and unauthorized access attempts. [22]

Several studies reported that CNN models outperform traditional machine learning methods in terms of classification accuracy and reduced false positive rates. Since CNN can process large-scale network traffic efficiently, it is particularly suitable for intelligent communication environments characterized by high-speed and complex traffic flows. However, CNN models may struggle with sequential dependencies in network traffic and often require large training datasets for optimal performance. [23]

Advantages of CNN in IDS

- Efficient feature extraction from high-dimensional network traffic.
- High classification accuracy for known attack categories.
- Reduced manual feature engineering requirements.
- Suitable for real-time intrusion detection in high-speed networks. [24]

Limitations of CNN in IDS

- Limited capability in handling sequential and temporal traffic patterns.
- High computational requirements during model training.
- Performance dependency on large labeled datasets. [25]

### 4.2 Recurrent Neural Networks (RNN) for Intrusion Detection

Recurrent Neural Networks (RNN) have gained attention in intrusion detection because of their capability to process sequential and time-dependent information. Network traffic data often exhibit sequential dependencies, making RNN models highly suitable for identifying attack behaviors evolving over time. Unlike CNN, which focuses on spatial relationships, RNN captures temporal information by maintaining hidden states that preserve historical traffic knowledge. [26]

In intelligent communication networks, cyberattacks often occur in patterns across multiple communication sessions. RNN-based intrusion detection systems can effectively analyze packet sequences and identify malicious communication behaviors that develop gradually. RNN models are particularly useful in detecting phishing attacks, insider threats, network reconnaissance, and abnormal traffic flows. [27]

Despite their effectiveness, standard RNN architectures suffer from the vanishing gradient problem, which limits their ability to process long-term dependencies in sequential data. As a result, researchers increasingly employ advanced recurrent architectures such as Long Short-Term Memory (LSTM) networks for more effective cybersecurity analysis. [28]

Advantages of RNN in IDS

- Strong capability in analyzing time-series network traffic.
- Effective detection of evolving attack behaviors.
- Useful for sequential intrusion pattern recognition. [29]

Limitations of RNN in IDS

- Vulnerability to vanishing gradient problems.
- High computational complexity.
- Reduced effectiveness for very long traffic sequences. [30]

### 4.3 Long Short-Term Memory (LSTM) Networks

Long Short-Term Memory (LSTM) is an advanced form of recurrent neural network specifically designed to overcome the limitations of traditional RNN architectures. LSTM networks possess memory cells capable of storing long-term information and selectively remembering or forgetting data through gating mechanisms. These capabilities make LSTM highly effective for intrusion detection tasks involving time-dependent attack behaviors and sequential communication patterns. [31]

In intelligent communication networks, cyberattacks frequently evolve gradually and exhibit hidden temporal characteristics. LSTM-based intrusion detection systems can analyze continuous traffic streams and detect advanced persistent threats, ransomware attacks, malware propagation, and unauthorized communication activities. LSTM models are particularly valuable in IoT ecosystems and intelligent communication infrastructures where dynamic traffic patterns frequently change. [32]

Several studies have demonstrated that LSTM achieves superior intrusion detection accuracy compared to traditional machine learning algorithms and standard recurrent neural networks. Its ability to capture long-term dependencies significantly improves anomaly detection and reduces false alarm rates. However, LSTM training often demands extensive computational resources and prolonged training time. [33]

Advantages of LSTM in IDS

- Effective handling of long-term sequential dependencies.
- Superior anomaly detection capability.
- Reduced false positive rates.
- High effectiveness in dynamic intelligent network environments. [34]

Limitations of LSTM in IDS

- High computational cost.
- Increased training complexity.
- Large memory requirements for deployment. [35]

### 4.4 Autoencoders for Intrusion Detection

Autoencoders represent unsupervised deep learning models widely used for anomaly detection in cybersecurity systems. Unlike supervised methods that require labeled datasets, autoencoders learn normal communication behavior by compressing and reconstructing network traffic patterns. Any abnormal deviation from reconstructed traffic behavior is classified as suspicious or malicious activity. [36]

Autoencoders consist of two main components: an encoder and a decoder. The encoder compresses high-dimensional traffic data into lower-dimensional latent representations, while the decoder reconstructs the original information. During intrusion detection, reconstruction errors help identify anomalous network activities. [37]

Autoencoder-based intrusion detection systems are particularly useful for detecting unknown and zero-day attacks because they focus on identifying deviations from normal behavior rather than predefined attack signatures. They have demonstrated strong performance in cloud computing, IoT networks, and intelligent communication infrastructures characterized by limited labeled data availability. [38]

Advantages of Autoencoders in IDS

- Effective for anomaly detection.
- Strong performance against unknown attacks.
- Reduced dependence on labeled datasets. [39]

Limitations of Autoencoders in IDS

- Risk of high false positives.
- Complex threshold selection process.
- Sensitivity to noisy datasets. [40]

### 4.5 Deep Belief Networks (DBN)

Deep Belief Networks (DBN) are generative deep learning architectures composed of stacked Restricted Boltzmann Machines (RBMs). DBN models learn hierarchical feature representations and support unsupervised pre-training before supervised fine-tuning. These capabilities enable effective classification of cyber threats within complex communication environments. [41]

DBN-based intrusion detection systems analyze multidimensional traffic data and automatically identify hidden relationships among network features. Researchers have demonstrated that DBN models improve attack classification accuracy while minimizing false detection rates. DBNs are particularly effective in intelligent communication networks where heterogeneous traffic characteristics create challenges for traditional detection methods. [42]

Despite their advantages, DBNs require extensive training time and significant computational resources. Model optimization also becomes increasingly complex as network size grows. [43]

### 4.6 Hybrid Deep Learning Models

Hybrid deep learning architectures combine multiple neural network techniques to maximize intrusion detection efficiency. Researchers increasingly integrate CNN, LSTM, RNN, Autoencoder, and DBN models to exploit their complementary strengths. For example, CNN-LSTM architectures combine CNN's spatial feature extraction with LSTM's sequential learning capability to improve attack detection performance. [44]

Hybrid systems have shown strong performance in detecting sophisticated cyberattacks in intelligent communication environments. These models achieve improved accuracy, scalability, and adaptive cybersecurity intelligence compared to standalone approaches. Hybrid deep learning models are particularly useful for securing future intelligent communication infrastructures such as 6G and autonomous IoT ecosystems. [45]

**5. Comparative Analysis of Deep Learning Models for Intrusion Detection**

| Deep Learning Model | Major Strength | Best Application | Limitation |
|---|---|---|---|
| CNN | Automatic feature extraction | DDoS, Malware Detection | Weak temporal analysis |
| RNN | Sequential data processing | Traffic behavior analysis | Vanishing gradient problem |
| LSTM | Long-term dependency learning | Anomaly detection, IoT security | High computational cost |
| Autoencoder | Unsupervised anomaly detection | Unknown attack identification | False positives |
| DBN | Hierarchical feature learning | Complex intrusion classification | Training complexity |
| Hybrid Models | Combined learning capability | Advanced threat detection | High resource consumption |

## 6. Role of Deep Learning in Intelligent Communication Security

Deep learning has significantly transformed intrusion detection systems by enabling intelligent and adaptive threat analysis. Intelligent communication networks generate enormous volumes of traffic data that require automated security frameworks capable of operating efficiently in real time. Deep learning enhances cybersecurity by reducing dependency on manual rule creation and improving attack classification accuracy. [46]

One major contribution of deep learning lies in its ability to detect previously unknown attacks. Traditional systems struggle to recognize evolving cyber threats due to reliance on predefined signatures, whereas deep learning models continuously learn emerging patterns from network behavior. This adaptive learning capability strengthens intelligent communication infrastructures against sophisticated attacks. [47]

Moreover, deep learning supports automated threat intelligence and incident response mechanisms. Intelligent intrusion detection systems integrated with deep learning models can analyze malicious activities, predict attack probabilities, and initiate preventive actions without human intervention. Such capabilities are essential for future communication systems such as autonomous networks, industrial IoT, smart cities, and intelligent transportation systems. [48]

International Journal of Artificial Intelligence and Communication Networks
Volume: 02, Issue: 01, January-March 2026, pp: 19-28
ISSN: 3071-3358

## 7. Results and Discussion

The integration of deep learning approaches into intrusion detection systems has significantly improved cybersecurity performance in intelligent communication networks. Compared to traditional rule-based and machine learning-based security models, deep learning techniques demonstrate enhanced capability in identifying sophisticated attack behaviors, recognizing hidden traffic patterns, and processing high-dimensional network datasets. Several studies indicate that deep learning models consistently outperform conventional intrusion detection mechanisms in terms of detection accuracy, scalability, anomaly recognition, and adaptive threat intelligence. [49]

The effectiveness of deep learning in intrusion detection primarily depends on the model architecture, dataset quality, feature selection process, and network complexity. Convolutional Neural Networks (CNN) demonstrate strong performance in extracting spatial traffic features and classifying attack categories, particularly in detecting malware, botnets, and distributed denial-of-service (DDoS) attacks. CNN models exhibit faster processing capabilities in high-speed intelligent communication environments, making them suitable for real-time cybersecurity monitoring. However, their inability to effectively capture sequential dependencies limits their effectiveness in analyzing evolving attack patterns. [50]

Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) networks have shown superior performance in analyzing sequential and temporal network traffic behavior. Since intelligent communication systems continuously generate time-dependent traffic flows, LSTM models effectively identify abnormal communication sequences associated with insider attacks, ransomware, advanced persistent threats (APT), and zero-day vulnerabilities. Research findings indicate that LSTM-based intrusion detection systems often achieve higher anomaly detection accuracy and lower false alarm rates than conventional machine learning algorithms. [51]

Autoencoders have proven highly valuable for anomaly detection because of their ability to identify deviations from normal network behavior without requiring extensive labeled datasets. Their capability to detect unknown cyber threats makes them highly relevant for dynamic communication ecosystems where emerging attacks evolve rapidly. However, excessive reconstruction sensitivity occasionally contributes to false positives, affecting overall reliability in highly diverse traffic environments. [52]

Deep Belief Networks (DBN) and hybrid deep learning architectures further improve intrusion detection effectiveness by integrating multiple learning capabilities. Hybrid CNN-LSTM models, for instance, combine feature extraction and sequential learning to achieve superior classification performance. Research evidence suggests that hybrid approaches consistently outperform standalone models in terms of attack classification, scalability, and robustness against dynamic threats. [53]

The findings collectively demonstrate that deep learning substantially improves intrusion detection system performance in intelligent communication networks. Enhanced detection accuracy, adaptive threat recognition, reduced false negatives, and automated learning mechanisms contribute to stronger cybersecurity resilience. Nevertheless, model deployment in real-world communication infrastructures remains challenging due to computational limitations, privacy concerns, and adversarial vulnerabilities. [54]

**Table 2: Comparative Performance of Deep Learning Models in Intrusion Detection**

| Model | Detection Accuracy | False Positive Rate | Computational Complexity | Suitability |
|---|---|---|---|---|
| CNN | High | Low | Moderate | High-speed network security |
| RNN | Moderate | Moderate | High | Sequential attack analysis |
| LSTM | Very High | Low | High | Intelligent network anomaly detection |
| Autoencoder | High | Moderate | Moderate | Unknown attack detection |
| DBN | High | Low | High | Complex attack classification |
| Hybrid CNN-LSTM | Very High | Very Low | Very High | Intelligent communication security |

## 8. Challenges and Limitations of Deep Learning-Based Intrusion Detection Systems

Although deep learning approaches offer substantial improvements in intrusion detection performance, several technical and practical challenges continue to hinder their widespread adoption in intelligent communication networks. Addressing these limitations remains essential for improving

cybersecurity resilience in future intelligent infrastructures. [55]

8.1 Data Imbalance Problem

One of the major challenges in intrusion detection datasets is class imbalance. Most communication network datasets contain significantly more normal traffic samples than malicious attack instances. This imbalance often causes deep learning models to favor dominant classes while reducing detection accuracy for minority attacks such as insider threats or zero-day intrusions. Data augmentation, oversampling, and synthetic data generation techniques are increasingly used to overcome this issue. [56]

8.2 Adversarial Attacks

Deep learning models are vulnerable to adversarial manipulation, where attackers intentionally alter network traffic data to mislead intrusion detection systems. Small modifications in malicious packets can bypass detection algorithms and compromise network security. Adversarial attacks represent a serious concern in intelligent communication networks because they exploit weaknesses in automated cybersecurity systems. Developing robust defense strategies against adversarial manipulation remains an active research area. [57]

8.3 Computational Complexity

Deep learning models require significant computational power, memory resources, and training time. Intelligent communication networks such as IoT and edge computing environments often operate under limited processing capabilities, making deployment of resource-intensive deep learning models challenging. Lightweight neural architectures and edge intelligence frameworks are being explored to reduce computational overhead. [58]

8.4 Privacy and Data Security Concerns

Intrusion detection systems frequently process sensitive communication data, including user identities, behavioral information, and confidential traffic content. Privacy preservation becomes essential when analyzing network activities. Federated learning and privacy-preserving deep learning methods have emerged as promising solutions to address security and confidentiality concerns while maintaining intrusion detection efficiency. [59]

8.5 Model Interpretability

Many deep learning models operate as black-box systems, making decision-making processes difficult to interpret. In cybersecurity applications, transparency is essential because security analysts must understand why a particular network event is classified as malicious. Explainable Artificial Intelligence (XAI) techniques are increasingly integrated with deep learning to improve interpretability and user trust. [60]

## 9. Future Scope of Deep Learning-Based Intrusion Detection

The future of intelligent communication security increasingly depends on advanced deep learning technologies capable of supporting autonomous cybersecurity mechanisms. As intelligent communication networks continue evolving toward 6G, smart cities, industrial automation, and autonomous IoT systems, intrusion detection solutions must become more adaptive, scalable, and intelligent. [61]

Future research is expected to focus on lightweight deep learning architectures suitable for edge devices and low-resource communication systems. Edge intelligence will enable local threat detection without requiring centralized cloud computation, reducing latency and improving privacy protection. [62]

Federated learning is anticipated to play a major role in distributed intrusion detection by allowing multiple devices to collaboratively train models without sharing sensitive data. This approach enhances privacy preservation while supporting large-scale intelligent network protection. [63]

Explainable artificial intelligence is another promising area for future cybersecurity research. Combining explainability with deep learning can improve trust, accountability, and transparency in automated intrusion detection systems. Additionally, reinforcement learning and self-adaptive cybersecurity frameworks may further enhance intelligent threat mitigation capabilities. [64]

Hybrid architectures integrating CNN, LSTM, transformers, and graph neural networks are also expected to improve cybersecurity performance by addressing the limitations of standalone deep learning models. These advanced architectures may significantly improve intrusion detection accuracy and strengthen future intelligent communication infrastructures. [65]

## 10. Conclusion

The growing complexity of intelligent communication networks has intensified the demand for advanced cybersecurity mechanisms capable of detecting sophisticated cyber threats efficiently. Traditional intrusion detection systems struggle to address emerging attacks due to their dependence on predefined signatures and manual rule-based frameworks. Deep learning approaches have emerged as transformative solutions for intrusion detection by enabling automated feature extraction, anomaly recognition, and adaptive cybersecurity intelligence. [66]

This study comprehensively examined various deep learning approaches, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short-Term Memory

(LSTM), Autoencoders, Deep Belief Networks (DBN), and hybrid architectures used in intelligent communication network security. The findings indicate that deep learning significantly improves intrusion detection accuracy, minimizes false alarm rates, and enhances network resilience against evolving cyber threats. Hybrid deep learning approaches demonstrate particularly strong performance due to their ability to integrate spatial and temporal traffic analysis capabilities. [67]

Despite considerable advancements, challenges such as computational overhead, adversarial vulnerabilities, privacy concerns, dataset imbalance, and model interpretability continue to affect practical implementation. Therefore, future research should focus on explainable artificial intelligence, federated learning, lightweight neural architectures, and intelligent edge-based intrusion detection systems. [68]

Overall, deep learning-based intrusion detection systems represent a promising cybersecurity solution for future intelligent communication networks, contributing to secure, adaptive, and resilient communication infrastructures capable of protecting sensitive information and maintaining operational continuity in increasingly connected digital ecosystems. [69]

**References**

[1] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. Cambridge, MA: MIT Press.

[2] Stallings, W. (2018). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson Education.

[3] Scarfone, K., & Mell, P. (2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)." National Institute of Standards and Technology (NIST) Special Publication 800–94.

[4] Liao, H. J., Lin, C. H. R., Lin, Y. C., & Tung, K. Y. (2013). "Intrusion Detection System: A Comprehensive Review." *Journal of Network and Computer Applications*, 36(1), 16–24.

[5] Goodfellow, I., Shlens, J., & Szegedy, C. (2015). "Explaining and Harnessing Adversarial Examples." *International Conference on Learning Representations (ICLR)*, 1–11.

[6] LeCun, Y., Bengio, Y., & Hinton, G. (2015). "Deep Learning." *Nature*, 521(7553), 436–444.

[7] Schmidhuber, J. (2015). "Deep Learning in Neural Networks: An Overview." *Neural Networks*, 61, 85–117.

[8] Sarker, I. H. (2021). "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective." *SN Computer Science*, 2(3), 1–16.

[9] Buczak, A. L., & Guven, E. (2016). "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection." *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.

[10] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). "Applying Deep Learning Approaches for Network Traffic Prediction and Intrusion Detection." *Future Generation Computer Systems*, 86, 762–777.

[11] Kim, G., Lee, S., & Kim, S. (2014). "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection." *Expert Systems with Applications*, 41(4), 1690–1700.

[12] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). "A Deep Learning Approach for Network Intrusion Detection System." *Proceedings of EAI International Conference on Bio-Inspired Information and Communications Technologies*, 21–26.

[13] 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.

[14] 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.

[15] Diro, A. A., & Chilamkurti, N. (2018). "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things." *Future Generation Computer Systems*, 82, 761–768.

[16] Alrawashdeh, K., & Purdy, C. (2017). "Toward an Online Anomaly Intrusion Detection System Based on Deep Learning." *Proceedings of IEEE SoutheastCon*, 1–6.

[17] Tang, T. A., McLernon, D., Ghogho, M., Zaidi, S. A. R., & El-Hajjar, M. (2020). "Deep Learning Approach for Network Intrusion Detection in Software Defined Networking." *IEEE Wireless Communications and Networking Conference (WCNC)*, 1–6.

[18] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study." *Journal of Information Security and Applications*, 50, 102419.

[19] Otoum, S., Liu, D., & Nayak, A. (2019). "DL-IDS: A Deep Learning-Based Intrusion Detection Framework for Securing IoT." *Transactions on Emerging Telecommunications Technologies*, 33(3), e3803.

[20] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). "Conditional Variational Autoencoder for Prediction and Feature Recovery Applied to Intrusion Detection in IoT." *Sensors*, 17(9), 1967.

[21] Hochreiter, S., & Schmidhuber, J. (1997). "Long Short-Term Memory." *Neural Computation*, 9(8), 1735–1780.

[22] Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). "ImageNet Classification with Deep Convolutional Neural Networks." *Advances in Neural Information Processing Systems*, 25, 1097–1105.
[23] Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). "Learning Representations by Back-Propagating Errors." *Nature*, 323, 533–536.
[24] Hinton, G. E., Osindero, S., & Teh, Y. W. (2006). "A Fast Learning Algorithm for Deep Belief Nets." *Neural Computation*, 18(7), 1527–1554.
[25] Sultana, N., Chilamkurti, N., Peng, W., & Alhadad, R. (2019). "Survey on SDN Based Network Intrusion Detection System Using Machine Learning Approaches." *Peer-to-Peer Networking and Applications*, 12(2), 493–501.
[26] Doshi, R., Apthorpe, N., & Feamster, N. (2018). "Machine Learning DDoS Detection for Consumer Internet of Things Devices." *IEEE Security and Privacy Workshops*, 29–35.
[27] Niyaz, Q., Sun, W., & Javaid, A. Y. (2016). "A Deep Learning Based DDoS Detection System in Software-Defined Networking." *IEEE Access*, 4, 9909–9922.
[28] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Al-Nemrat, A. (2019). "Deep Learning Approach for Intelligent Intrusion Detection System." *IEEE Access*, 7, 41525–41550.
[29] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). "Network Anomaly Detection: Methods, Systems and Tools." *IEEE Communications Surveys & Tutorials*, 16(1), 303–336.
[30] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). "A Survey of Network Anomaly Detection Techniques." *Journal of Network and Computer Applications*, 60, 19–31.
[31] Aljawarneh, S., Aldwairi, M., & Yassein, M. B. (2018). "Anomaly-Based Intrusion Detection System through Feature Selection Analysis and Building Hybrid Efficient Model." *Journal of Computational Science*, 25, 152–160.
[32] Ring, M., Wunderlich, S., Grüdl, D., Landes, D., & Hotho, A. (2019). "A Survey of Network-Based Intrusion Detection Data Sets." *Computers & Security*, 86, 147–167.
[33] Khan, M. A., Karim, M. D., & Kim, Y. (2019). "A Scalable and Hybrid Intrusion Detection System Based on Deep Learning." *Computers & Electrical Engineering*, 81, 106526.
[34] Ferrag, M. A., Maglaras, L., Janicke, H., Jiang, J., & Shu, L. (2022). "Deep Learning Techniques for Cyber Security Intrusion Detection in Communication Networks." *IEEE Communications Surveys & Tutorials*, 24(2), 1055–1093.
[35] Sarker, I. H., Kayes, A. S. M., Watters, P., Alazab, M., & Ng, A. (2020). "Cybersecurity Data Science: An Overview from Machine Learning Perspective." *Journal of Big Data*, 7(1), 1–29.
[36] Abeshu, A., & Chilamkurti, N. (2018). "Deep Learning: The Frontier for Distributed Attack Detection in Fog-to-Things Computing." *IEEE Communications Magazine*, 56(2), 169–175.
[37] Mirsky, Y., Doitshman, T., Elovici, Y., & Shabtai, A. (2018). "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection." *Network and Distributed System Security Symposium (NDSS)*, 1–15.
[38] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2020). "Network Traffic Classifier with Convolutional and Recurrent Neural Networks for Internet of Things." *IEEE Access*, 8, 180067–180078.
[39] Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2014). "Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection." *International Conference on Platform Technology and Service (PlatCon)*, 1–5.
[40] Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). "A Detailed Analysis of the KDD CUP 99 Dataset." *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1–6.
[41] Moustafa, N., & Slay, J. (2015). "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems." *Military Communications and Information Systems Conference (MilCIS)*, 1–6.
[42] Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization." *International Conference on Information Systems Security and Privacy*, 108–116.
[43] Vinayakumar, R., Alazab, M., Srinivasan, S., Pham, Q. V., Padannayil, S. K., & Simran, K. (2020). "A Visualized Botnet Detection System Based on Deep Learning for the Internet of Things Networks." *IEEE Transactions on Industry Applications*, 56(4), 4436–4450.
[44] Ullah, I., Mahmoud, Q. H., & Alghamdi, A. (2021). "Hybrid Deep Learning Framework for Intrusion Detection in IoT Networks." *IEEE Access*, 9, 136351–136365.
[45] Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2021). "Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges." *IEEE Access*, 8, 32031–32053.
[46] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems." *IEEE Access*, 8, 165130–165150.
[47] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions." *SN Computer Science*, 2(3), 1–18.

[48] Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges." *Cybersecurity*, 2(20), 1–22.
[49] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., & Dai, K. (2019). "An Efficient Intrusion Detection System Based on Support Vector Machines and Gradually Feature Removal Method." *Expert Systems with Applications*, 39(1), 424–430.
[50] Naseer, S., Saleem, Y., Khalid, S., Bashir, M., Han, J., Iqbal, M. M., & Han, K. (2018). "Enhanced Network Anomaly Detection Based on Deep Neural Networks." *IEEE Access*, 6, 48231–48246.
[51] Potluri, S., Diedrich, C., & Rao, S. (2020). "LSTM-Based Intrusion Detection System for Intelligent Networks." *Computers & Security*, 97, 101938.
[52] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Breitenbacher, D., Shabtai, A., & Elovici, Y. (2018). "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders." *IEEE Pervasive Computing*, 17(3), 12–22.
[53] Althubiti, S. A., Jones, E. M., & Roy, K. (2021). "Hybrid Deep Learning Models for Intrusion Detection in Smart Communication Systems." *Future Internet*, 13(11), 287.
[54] Chorąś, M., Kozik, R., Pawlicki, M., & Hołubowicz, W. (2020). "A Practical Cybersecurity Intrusion Detection Framework Based on Deep Learning." *Sensors*, 20(20), 5772.
[55] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). "Machine Learning and Deep Learning Methods for Cybersecurity." *IEEE Access*, 6, 35365–35381.
[56] He, H., Bai, Y., Garcia, E. A., & Li, S. (2008). "ADASYN: Adaptive Synthetic Sampling Approach for Imbalanced Learning." *IEEE International Joint Conference on Neural Networks*, 1322–1328.
[57] Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). "Distillation as a Defense to Adversarial Perturbations." *IEEE Symposium on Security and Privacy*, 582–597.
[58] Lane, N. D., Bhattacharya, S., Mathur, A., Forlivesi, C., Kawsar, F., & Georgiev, P. (2016). "Squeezing Deep Learning into Mobile and Embedded Devices." *IEEE Pervasive Computing*, 16(3), 82–88.
[59] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). "Federated Machine Learning: Concept and Applications." *ACM Transactions on Intelligent Systems and Technology*, 10(2), 1–19.
[60] Samek, W., Wiegand, T., & Müller, K. R. (2017). "Explainable Artificial Intelligence: Understanding Deep Learning Models." *IEEE Signal Processing Magazine*, 34(6), 96–109.
[61] Saad, W., Bennis, M., & Chen, M. (2020). "A Vision of 6G Wireless Systems." *IEEE Network*, 34(3), 134–142.
[62] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). "Edge Computing: Vision and Challenges." *IEEE Internet of Things Journal*, 3(5), 637–646.
[63] Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). "Federated Learning for Internet of Things: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials*, 23(3), 1622–1658.
[64] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., & Herrera, F. (2020). "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges." *Information Fusion*, 58, 82–115.
[65] Zhou, Z. H. (2021). *Machine Learning*. Springer Nature.
[66] Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2019). "A Survey of Deep Learning Methods for Cyber Security." *Information*, 10(4), 122.
[67] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). "On the Effectiveness of Machine and Deep Learning for Cyber Security." *International Conference on Cyber Conflict*, 371–390.
[68] Afsha Nishat, Dr. Mohd Abdul Bari, Dr. Guddi Singh," Mobile Ad Hoc Network Reactive Routing Protocol to Mitigate Misbehavior Node", International Journal Of Intelligent Systems And Applications In Engineering, IJUSEA, ISSN:2147-6799, Nov 2023
[69] Ijteba Sultana, Dr. Mohd Abdul Bari ,Dr. Sanjay," Routing Performance Analysis of Infrastructure-less Wireless Networks with Intermediate Bottleneck Nodes", International Journal of Intelligent Systems and Applications in Engineering, ISSN no: 2147-6799 IJISAE,Vol 12 issue 3, 2024, Nov 2023
[70] Dasgupta, D., Akhtar, Z., & Sen, S. (2022). "Machine Learning in Cybersecurity: A Comprehensive Survey." *Journal of Defense Modeling and Simulation*, 19(1), 57–106.
[69] Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). "Internet of Things Security and Forensics: Challenges and Opportunities." *Future Generation Computer Systems*, 78, 544–546.
[71] Dr.Abdul Bari ,Dr. Imtiyaz khan , Dr. Rafath Samrin , Dr. Akhil Khare , " VPC & Public Cloud Optimal Perfomance in Cloud Environment ",Educational Administration: Theory and Practic,ISSN No : 2148-2403 Vol 30- Issue -6 June 2024