# A Survey Paper on Automated Intrusion Detection using Deep Learning Techniques

B. Manivannan[1], K. Abarna[2], D. Radhika[3]
[1]*Assistant Professor, Department of Computer Science and Engineering Vivekanandha College of Engineering for Women, Tamilnadu, India*
[2]*PG Scholar, Department of Computer Science and Engineering,Vivekanandha College of Engineering for Women, Tamilnadu, India*
[3] *Assistant Professor,Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tamilnadu, India*

**Abstract: The rapid evolution of cyber threats necessitates the development of robust and adaptive intrusion detection systems (IDS) to safeguard critical networks and systems. Deep learning (DL) has emerged as a powerful tool in automating intrusion detection, offering superior capabilities in feature extraction, anomaly detection, and real-time threat identification. This survey paper comprehensively reviews the state-of-the-art research on automated intrusion detection leveraging deep learning techniques. It explores various architectures, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), generative adversarial networks (GANs), and auto encoders, highlighting their strengths and limitations in addressing different intrusion detection challenges. The paper also examines hybrid approaches that combine DL with traditional methods to enhance detection accuracy and mitigate false positives. Emphasis is placed on the performance evaluation of these techniques using benchmark datasets, their adaptability to evolving threats, and their deployment in real-world scenarios. This reviews significant contributions from recent studies, focusing on the application of various deep learning models for automated intrusion detection.**

**Key Words: Intrusion Detection Systems (IDS), Deep Learning (DL), Cybersecurity, Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Generative Adversarial Networks (GAN).**

## I. INTRODUCTION

In today's connected world, protecting digital assets and critical systems from cyber threats is more important than ever. Cyberattacks, ranging from network breaches to advanced persistent threats, can cause significant financial losses, reputational harm, and operational disruptions. To address these challenges, Intrusion Detection Systems (IDS) play a crucial role in identifying unauthorized access and malicious activities within networks and systems.

Traditional IDS methods, such as signature-based detection and rule-based anomaly detection, are effective for identifying known threats but struggle with zero-day attacks and complex patterns. The increasing volume and complexity of modern network traffic and system logs make manual analysis and conventional detection techniques insufficient to address today's cybersecurity challenges.Deep learning, a subset of machine learning that uses multi-layered neural networks, offers significant advantages for intrusion detection. Techniques such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Generative Adversarial Networks (GANs) have shown great promise in automating and improving detection accuracy. CNNs are designed to process structured data, such as images or spatially organized information, by learning features through convolutional, pooling, and fully connected layers. RNNs, particularly Long Short-Term Memory (LSTM) networks, excel at analyzing sequential data and addressing long-term dependencies, making them highly effective for tasks such as time-series predictions. Additionally, Generative Adversarial Networks (GANs) generate realistic data by training two networks in competition with each other, enabling applications like data augmentation and intrusion detection simulation. By analyzing large amounts of network traffic, system logs, and other security data, deep learning models can identify complex patterns of malicious behavior that traditional methods often miss.

This survey paper provides a comprehensive review of recent advancements in the application of deep learning techniques for automated intrusion detection. Explore the architecture, methodologies, and evaluation metrics used across various studies,

highlighting their effectiveness and limitations. Through this survey, aim to shed light on the transformative role of deep learning in cybersecurity and identify key areas where further innovation is needed to stay ahead of rapidly evolving cyber threats.

## II. LITERATURE REVIEW

### DEEP LEARNING METHODS IN INTRUSION DETECTION SYSTEMS (IDS)

The rapidly evolving landscape of network security demands robust and adaptive Intrusion Detection Systems (IDS) capable of identifying a wide variety of cyber threats in real-time. With the increasing complexity of attacks and the massive scale of network traffic, traditional IDSs, which often rely on signature-based methods, have become insufficient. As a result, deep learning techniques, such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and hybrid models combining these methods, have gained significant attention in the field of intrusion detection. This literature review highlights key studies that leverage deep learning models for improving IDS performance, focusing on advanced frameworks, feature selection, and evaluation metrics.

[1] Vanlalruata Hnamte, several studies have proposed the use of deep convolutional neural networks (DCNNs) to enhance IDS performance by automatically extracting meaningful features from network traffic data. In particular, DCNN-based IDS has demonstrated superior detection accuracy, with studies achieving detection rates ranging from 99.79% to 100%. For example, research utilizing large-scale datasets such as ISCX-IDS 2012, DDoS (Kaggle), CICIDS2017, and CICIDS2018 highlights the effectiveness of DCNN in accurately distinguishing between benign and malicious traffic, with GPU acceleration further enhancing computational efficiency and enabling real-time threat detection. DCNNs excel in capturing spatial features from raw network data, making them a promising solution for modern IDSs. The combination of high accuracy and low false positive rates underscores the value of DCNNs in detecting emerging cyber threats.

[2] Sydney Mambwe Kasongo, While DCNNs excel at capturing spatial features, Recurrent Neural Networks (RNNs), particularly Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), are effective for analyzing sequential dependencies in network traffic. IDSs employing LSTMs have been shown to outperform traditional systems, especially in detecting new and sophisticated attacks. In one study, an LSTM-based IDS achieved an accuracy of 88.13% on the NSL-KDD dataset, demonstrating the potential of RNNs to handle time-series data efficiently. Another study integrated LSTM with XGBoost-based feature selection to optimize the model's ability to detect anomalies while reducing training time. This approach highlights the importance of feature selection to enhance model performance, particularly in the context of expanding feature dimensions.

[3] Lirim Ashiku,Recurrent neural networks are effective for analyzing spatial data and are frequently employed for feature extraction from network traffic. Studies employing datasets like UNSW-NB15 and KDD-Cup demonstrate the effectiveness of CNNs in intrusion detection. With detection accuracies of 94.4% and 95.6% for different dataset partitions, these models overcome the challenges of traditional machine learning techniques, showcasing the promise of deep learning in cybersecurity applications.

[4] Zhen Wang**,** Recent advancements in deep learning have explored the integration of attention mechanisms into CNNs to improve IDS accuracy by allowing the model to focus on the most relevant features of the input data. One study proposed an attention-based CNN model, which processed network traffic data by converting it into image format. By applying multiple attention mechanisms, the model achieved high classification accuracy (above 96%) and high processing speeds of over 500 samples per second on the CSE-CIC-IDS2018 dataset. The attention mechanism enables the model to prioritize important features, which can be crucial in the context of network traffic data, where noise and irrelevant features may compromise the detection performance.

[5]Arun Kumar Silivery, Deep learning techniques have also been applied to multi-attack classification, where the goal is to detect and classify various types of attacks simultaneously. For example, a study utilizing LSTM-RNN models optimized with advanced functions like adamax demonstrated

superior classification performance on the NSL-KDD dataset, successfully identifying multiple attack types with high accuracy and low false alarm rates. The ability to classify various attack types is essential for real-time network monitoring and response, particularly as new attack vectors emerge.

[6] Juan Fernando Canola Garcia, Given the widespread threat of Denial-of-Service (DoS) attacks, several studies have focused on leveraging deep learning models to detect and prevent such attacks. For instance, the Dique system, which utilizes a multi-layered Deep Feed Forward neural network, achieved an accuracy of 0.994 in detecting DoS attacks in real-time, trained on the CICDDoS2019 dataset. The system includes both detection and prevention modes, offering real-time monitoring and effective mitigation of DoS attacks. This study underscores the importance of deep learning in improving IDSs' capabilities to handle large datasets and provide immediate responses to emerging threats.

[7]Rachid Ben Said, a CNN-BiLSTM model designed for Software-Defined Networking (SDN) demonstrated high classification performance while addressing the challenges posed by DDoS attacks in SDN environments. The model's ability to handle both temporal and spatial features, combined with hybrid feature selection techniques, made it a powerful tool for securing SDN architectures. The use of BiLSTM allows for bidirectional processing of sequences, enhancing the model's understanding of past and future context in network traffic.

[8] Vanlalruata Hnamte, Innovative hybrid model, LSTM-AE (Auto-Encoder), integrates LSTMs with auto-encoders to improve anomaly detection in network traffic. This two-stage model achieved accuracy rates of 99.98% and 99.97% on the CICIDS2017 and CSE-CICIDS2018 datasets, respectively, highlighting the model's capacity to identify complex attacks while ensuring efficient anomaly detection. The incorporation of auto-encoders helps the system learn a compact representation of normal network behavior, improving the detection of anomalies.

[9]AsmaaHalbouni**,** the combination of CNNs and LSTMs in hybrid models has gained popularity due to the complementary strengths of these architectures. CNN-LSTM hybrid models are particularly effective in capturing both spatial and temporal features from network traffic data. For example, one study showed that the CNN-LSTM model achieved impressive accuracy across multiple datasets, including CIC-IDS2017, UNSW-NB15, and WSN-DS, with detection accuracies exceeding 99.95%. These hybrid models leverage CNNs for feature extraction and LSTMs for sequential data analysis, making them well-suited for complex, evolving attack patterns.

[10]Chakrawarti, the importance of feature representation in deep learning-based IDSs cannot be overstated. One study highlights the significant role of feature representation in improving the performance of IDSs, particularly when training data is limited. It emphasizes the potential of few-shot learning**,** a technique aimed at improving IDS performance when labeled data is scarce. Few-shot learning allows models to generalize from limited examples, making it a valuable approach for real-world deployment, where obtaining labeled datasets can be challenging. This approach is particularly useful in detecting novel or unknown attack patterns, where traditional methods may fall short.

III. PERFORMANCE METRICS

| Model | Dataset(s) | Accuracy | False Positive Rate (FPR) | Optimization |
|---|---|---|---|---|
| DCNN Framework | ISCX-IDS 2012, CICIDS2017/2018, DDoS (Kaggle), CICIDS2017 | 99.79% - 100% | Low | GPU acceleration for real-time detection, superior performance over traditional models. High scalability and adaptability |
| LSTM, GRU, Simple RNN (XGBoost-LSTM) | NSL-KDD, UNSW-NB15 | 88.13%-87.07% | Medium | Feature space reduced to 17 attributes via XGBoost. Feature selection reduces dimensions. |

| | | | | |
|---|---|---|---|---|
| CNN model | UNSW-NB15, NSL-KDD | 94.4%-95.6% | Low | Improved focus on relevant features via attention mechanisms. Pre-partitioned vs. user-defined datasets |
| Attention-CNN with Feature Selection | CSE-CIC-IDS2018 | >96% | Low | >500 samples/second processing speed, improved efficiency via attention mechanisms. Attention mechanisms improve focus. |
| RNN-LSTM Model(multi-attack classification) | NSL-KDD | High | Low | ROC-AUC This metric evaluates the model's ability to distinguish between classes. Superior multi-attack classification. |
| Deep Feedforward NN(Dique) | CICDDoS2019 | 99.4% | Low | Real-time detection/prevention with GUI for user interaction. |
| CNN-BiLSTM Hybrid Model | UNSW-NB15, NSL-KDD, InSDN | High (Exact N/A) | Low | Reduced data redundancy, optimized for SDN environments. Addresses SDN-specific threats effectively. |
| LSTM-AE Two-Stage Model | CICIDS2017, CSE-CICIDS2018 | 99.98%-99.97% | Low | Exceptional performance against evolving cyber threats. High adaptability for dynamic attacks. |
| CNN-LSTM Hybrid Model | CIC-IDS2017, UNSW-NB15, WSN-DS | 99.95%-99.98% | Low | Balanced datasets, high detection rates for both known and unknown threats. Comprehensive data preprocessing methods. |
| LSTM with FCNN(few shot learning) | NSL-KDD , KDDCup99 | 99% | Low | The model's ability to perform well on unseen data, evaluated using cross-validation techniques. Few-shot learning potential. |

## IV ANALYSIS

Deep Convolutional Neural Networks (DCNNs) and Convolutional Neural Networks (CNNs) excel in extracting spatial features, achieving high detection rates with low false positives. Recurrent Neural Networks (RNNs), particularly LSTM and GRU, effectively analyze sequential data, making them ideal for detecting complex attack patterns. Hybrid models, such as CNN-LSTM and LSTM-AE, combine spatial and temporal feature extraction, achieving near-perfect accuracy across diverse datasets. Innovations like attention mechanisms improve IDS focus on relevant features, while few-shot learning addresses challenges with limited labeled data, enabling detection of novel threats.

## V. CONCLUSION

Deep learning techniques have become essential for improving automated intrusion detection systems (IDS) in response to increasing cybersecurity threats. This survey highlights various approaches, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and hybrid models like CNN-LSTM and Attention-CNN. These methods have shown significant improvements in detection accuracy, false alarm rates, and adaptability to complex attacks. Many models, such as DCNN-based frameworks, achieve over 99% accuracy on datasets like CICIDS2017, UNSW-NB15, and NSL-KDD. Hybrid approaches and attention mechanisms further enhance performance by focusing on key features and combining the strengths of multiple models. Feature selection techniques like XGBoost also improve efficiency by reducing redundant data. However, challenges remain, such as managing large-scale data, handling imbalanced datasets, and preventing overfitting. Innovations like LSTM-AE and CNN-BiLSTM provide promising solutions for these issues, while regularly updating datasets and refining architectures will help keep pace with evolving threats. In summary, deep learning has transformed intrusion detection, offering highly effective tools to detect and prevent cyberattacks. Continued research and innovation will strengthen these systems, making them even more robust and scalable for real-world applications.

## VI. REFERENCE


[1] Vanlalruata Hnamte ,Jamal Hussain, Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach, Telematics and Informatics Reports, Volume 11, September 2023, https://doi.org/10.1016/j.teler.2023.100077.

[2] Sydney Mambwe Kasongo, A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework, Computer Communications, Volume 199, 1 February 2023, Pages 113-125,https://doi.org/10.1016/j.comcom.2022.12.010.

[3] Lirim Ashiku, Cihan Dagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, https://doi.org/10.1016/j.procs.2021.05.025.

[4] Zhen Wang and Fuad A. Ghaleb, An Attention-Based Convolutional Neural Network for Intrusion Detection Model, IEEEAccess (Volume:11), April 2023, 10.1109/ACCESS.2023.3271408, ,https://ieeexplore.ieee.org/document/10110980.

[5] Arun Kumar Silivery, Ram Mohan Rao Kovvur, Ramana Solleti, LK Suresh Kumar, Bhukya Madhu, A model for multi-attack classification to improve intrusion detection performance using deep learning approaches, Measurement: Sensors, Volume 30, December 2023, 100924,https://doi.org/10.1016/j.measen.2023.100924.

[6] Juan Fernando Canola Garcia, Gabriel Enrique Taborda Blandon, A Deep Learning-Based Intrusion Detection and Preventation System for Detecting and Preventing Denial-of-Service Attacks, IEEE Access (Volume: 10), August 2022,10.1109/ACCESS.2022.3196642, https://ieeexplore.ieee.org/document/9851436

[7] Rachid Ben Said, Zakaria Sabir, ImanAskerzade, CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking with Hybrid Feature Selection, IEEE Access (Volume: 11), December 2023,10.1109/ACCESS.2023.3340142,https://ieeexplore.ieee.org/document/10347226

[8] Vanlalruata Hnamte, Hong Nhung-Nguyen, Jamal Hussain, Yong Hwa-Kim, A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE, IEEE Access (Volume:11), April 2023,10.1109/ACCESS.2023.3266979,https://ieeexplore.ieee.org/document/10101759

[9] Asma a Halbouni, Teddy Surya Gunawan, Mohamed Had iHabaebi, Mura d Halbouni, Mira Kartiwi, Robiah Ahma d, CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System, IEEEAccess (Volume: 10), September2022, 10.1109/ACCESS.2022.3206425, https://ieeexplore.ieee.org/document/9889698

[10] Chakrawarti, A., &Shrivastava, S. (2023). Intrusion Detection System using Long Short-Term Memory and Fully Connected Neural Network on Kddcup99 and NSL-KDD Dataset. International Journal of Intelligent Systems and Applications in Engineering, volume 11(9s), https://ijisae.org/index.php/IJISAE/article/view/3211

[11] A.E. Cil, K. Yildiz, A. Buldu, Detection of ddos attacks with feed forward based deep neural network model, Expert Syst. Appl. 169(2021)114520, https://doi.org/10.1016/j.eswa.2020.114520

[12] M.S. ElSayed, N.-A. Le-Khac, M.A. Albahar, A. Jurcut, A novel hybrid model for intrusion detection systems in sdns based on cnn and a new regularization technique, J. Netw. Comput. Appl. 191 (2021) 103160, https://doi.org/10.1016/j.jnca.2021.103160.

[13] S. Alzughaibi, S.E. Khediri, A cloud intrusion detection systems based on dnn using backpropagation and pso on the cse-cic-ids2018 dataset, Appl. Sci. 13 (4) (2023), doi:10.3390/app13042276.

[14] A. El-Ghamry, A. Darwish, A.E. Hassanien, An optimized cnn-based intrusion detection system for reducing risks in smart farming, Internet of Things 22 (2023) 100709,doi:10.1016/j.iot.2023.100709.

[15] S.N. Mighan, M. Kahani, A novel scalable intrusion detection system based on deep learning, Int. J. Inf. Secur. 20 (3) (2021) 387–403,doi:10.1007/s10207-020-00508-5