*I. J. Computer Network and Information Security,* **2026, 1, 131-141**
Published Online on February 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.01.09

# A Comparative Analysis of Deep Learning Architecture for Early Detection of DoS/DDoS Patterns in Network Traffic Using Intrusion Detection Systems

**Andreas Handojo***
Informatics Department, Petra Christian University, Surabaya, Indonesia
E-mail: handojo@petra.ac.id
ORCID iD: https://orcid.org/0000-0003-0365-2496
*Corresponding author

**Marvel Wilbert Odelio**
Informatics Department, Petra Christian University, Surabaya, Indonesia
E-mail: C14220223@john.petra.ac.id

**Nico Alexandre Kurniawan**
Informatics Department, Petra Christian University, Surabaya, Indonesia
E-mail: C14220091@john.petra.ac.id

**Dillan Engelbert Hendrarto**
Informatics Department, Petra Christian University, Surabaya, Indonesia
E-mail: C14220344@john.petra.ac.id

**Matthew Timothy Handoyo**
Business Management Department, National Tsing Hua University, Hsinchu, Taiwan, China
E-mail: s113006437@m113.nthu.edu.tw

Received: 02 September 2025; Revised: 18 October 2025; Accepted: 24 November 2025; Published: 08 February 2026

**Abstract:** Advanced intrusion detection systems are required due to the quick uptake of cloud computing and the growing complexity of cyber threats, especially Denial of Service and Distributed Denial of Service attacks. Deep learning architectures are becoming more popular because traditional IDS techniques frequently falter in dynamic, large-scale settings. Using datasets including CICIDS2017, NSL-KDD, and UNSW-NB15, this paper assesses the effectiveness of well-known DL architectures for intrusion detection, including Convolutional Neural Network, Recurrent Neural Networks, Long Short-Term Memory, and others. Key performance indicators such as accuracy, precision, and false positive rates are examined to compare the efficacy of these models. The findings show that some designs, like ResNet and Self-Organizing Map, perform well in structured environments but poorly on complicated datasets like KDDTest-21. Another important data gap highlighting the need for more research in this area is that most models do not automatically adjust to unexpected threats. This work aids in the creation of intelligent, scalable systems for changing network environments by evaluating the efficacy of DL-based IDS solutions.

**Index Terms:** Intrusion Detection System, Deep Learning, Denial of Service, Convolutional Neural Network, Long Short-Term Memory.

## 1. Introduction

The rapid expansion of cloud computing and the exponential increase in data storage and processing needs have made security a paramount concern in the digital world. With more businesses and organizations shifting to cloud platforms, the exposure to potential cyber threats has risen significantly [1]. Traditional cybersecurity measures, such as

signature-based and anomaly-based intrusion detection systems (IDS), have demonstrated limitations in managing the vast volume of data and countering increasingly sophisticated attack patterns, particularly in the context of Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These systems often struggle to adapt to new, unknown threats, especially in dynamic, large-scale environments like cloud infrastructures. As a result, there is a growing need for more advanced, intelligent systems capable of identifying and mitigating intrusions more effectively [1].

As illustrated in Fig. 1, DDoS attacks accounted for a significant portion (15%) of security incidents within McAfee's network in 2017. This statistic underscores the urgency of developing robust systems for the early detection of such attacks to minimize their impact. This figure highlights the urgency of strengthening IDS, given that DDoS attacks constitute a significant portion of real-world incidents, emphasizing the importance of proactive and adaptive detection methods. Strengthening early detection is crucial for mitigating the operational and financial consequences of DDoS attacks, particularly in cloud-based environments, where attacks can rapidly escalate and spread.

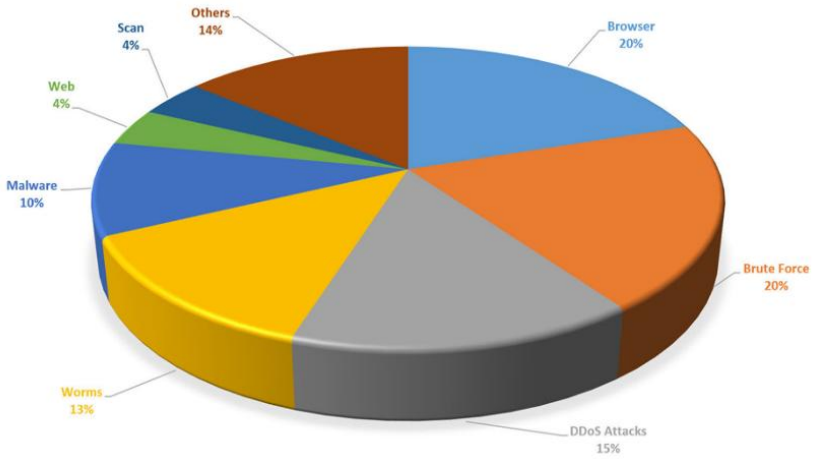



Fig.1. Security attacks in McAfee network in 2017 [2]

Deep learning (DL), a subset of Machine Learning (ML), has shown remarkable promise in the field of cybersecurity due to its ability to automatically learn complex patterns from vast amounts of data without the need for manual feature engineering. Unlike traditional methods, DL architecture can adapt to new attack behaviors by learning from historical data and improving its detection capabilities over time. Various DL architectures, such as Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), and Deep Belief Network (DBN), have been applied in IDS to enhance their performance in detecting both known and unknown attacks [3]. Despite the promising potential of DL in intrusion detection, the effectiveness of different architectures can vary based on factors such as the attack types, the dataset used for training, and the specific architecture of the model. For instance, CNN excel at recognizing spatial patterns in data, making them particularly effective for identifying certain types of attacks, while RNN and LSTM are more suited for processing sequential data, such as time-series traffic logs, to detect unusual patterns over time [3].

This paper aims to provide a comprehensive comparative analysis of several popular DL architectures in the context of intrusion detection. Specifically, this research evaluates the performance of CNN, RNN, LSTM, and other DL architectures using key metrics such as detection accuracy, false positive rates, and detection rate. Through this comparison, this research aims to identify the strengths and weaknesses of each approach in the context of cloud and network security. Additionally, this research addresses a minor issue prevalent in many IDS research papers: the tendency to compare non-optimized baseline models with proposed approaches to emphasize their effectiveness. By ensuring a fair and unbiased evaluation of all models, this analysis seeks to provide a realistic representation of their capabilities and limitations. The comparative analysis presented in this research will provide valuable insights for researchers, security professionals, and organizations in selecting the most effective DL model for real-time intrusion detection. By highlighting the practical performance of these architectures in different scenarios, this paper will contribute to the ongoing effort to improve the security of cloud computing environments and serve as a reference for future advancements in AI-driven IDS.

## 2. Literature Review

### *2.1. DoS and DDoS*

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are among the most common and damaging cyber threats in network security. A DoS attack involves overwhelming a target system or network with traffic, rendering its services unavailable to legitimate users. In a DDoS attack, this flooding is amplified by using

multiple compromised devices (often called a botnet) to execute the attack, making it harder to trace and mitigate [4]. DDoS attacks can take various forms, including:

- Flood attacks overwhelm a network's bandwidth by sending large amounts of traffic, often exploiting communication protocols like TCP, UDP, or ICMP. These attacks saturate network resources, rendering legitimate traffic unable to pass through.
- Application Layer Attacks are more targeted, aiming at specific application services such as HTTP requests or DNS queries. By exhausting server resources like memory and CPU, these attacks disrupt service functionality without necessarily generating significant traffic volume, making them harder to detect.
- Amplification and Reflection Attacks leverage vulnerable third-party servers to magnify the attack's impact. Attackers send requests with a spoofed source address (the victim's address) to these servers, which respond with amplified traffic aimed at the victim. Examples include DNS amplification and NTP reflection, where small queries generate disproportionately large responses.

The diversity of DDoS techniques necessitates robust, multi-layered mitigation strategies, including advanced filtering, rate limiting, and employing specialized DDoS protection services. As attack sophistication grows, proactive defenses capable of detecting and mitigating emerging threats are critical for maintaining network security and availability.

### *2.2. Deep Learning*

Deep learning (DL) is a specialized subset of machine learning (ML) that leverages multi-layered neural networks to simulate the decision-making processes of the human brain. These networks, known as deep neural networks (DNN), consist of multiple layers of interconnected nodes, or artificial neurons, which collaborate to process and analyze complex datasets. One of the primary advantages of DL is its ability to automatically extract and learn intricate patterns and features from raw data without requiring extensive manual feature engineering. This characteristic makes DL particularly effective for tasks involving unstructured data, such as image recognition, speech processing, and natural language understanding [5, 6].

This advantage of DL has led to its widespread use in a variety of industries. In healthcare, DL models have been employed to improve medical diagnoses by analyzing medical images, such as X-rays and MRIs. In the financial sector, DL helps in fraud detection by identifying irregular patterns in transaction data. Additionally, DL has transformed real-time translation systems, enabling more accurate and efficient translation between languages. The continual development and application of DL in these fields have led to significant breakthroughs, reshaping industries, and enhancing both business and societal operations [5, 6].

### *2.3. Convolutional Neural Network*

Convolutional Neural Networks (CNN) are widely recognized as an effective DL architecture for classifying multi-dimensional data, such as images, into predefined categories. Their application in IDS leverages their ability to extract complex spatial patterns from network traffic data, enabling accurate detection of malicious activities. For instance, in the context of IDS, CNN has been enhanced with density and coverage metrics to classify not only known attacks but also previously unseen threats. These metrics help define thresholds for identifying outliers, which represent potential unknown attacks. Such a system allows for dynamic updating through incremental learning, where labeled unknown attacks are integrated into the model, improving its ability to adapt to evolving threat landscapes.

Datasets like CICIDS2017 and play a crucial role in training and validating these CNN-based models. CICIDS2017 provides a comprehensive representation of normal and malicious traffic, including a variety of attack scenarios, while CICDDoS2019 focuses specifically on Distributed Denial of Service (DDoS) attacks. These datasets, along with others, offer a robust foundation for testing the efficacy of CNN-based IDS in detecting sophisticated and real-world cyber threats. Research studies have demonstrated the capability of CNN to handle these datasets effectively, showcasing their potential in modern cybersecurity applications [7-9]

### *2.4. Long Short-term Memory*

Recurrent Neural Networks (RNN) are DL models designed to process sequential data by using outputs from previous steps to influence current inputs and outputs, enabling them to capture temporal dependencies. However, they struggle with long-term dependencies due to issues like gradients exploding or vanishing during backpropagation. To address these challenges, Long Short-Term Memory (LSTM) networks were introduced as an advanced form of RNN. LSTM use specialized input, forget, and output gates to regulate information flow, allowing the network to retain or discard data as needed. This makes LSTM capable of capturing both short-term and long-term dependencies, ideal for tasks like time-series analysis, natural language processing, and anomaly detection.

In practice, researchers have implemented an IDS using an RNN-LSTM model to classify network data as either positive (indicating the presence of an intrusion) or negative (indicating no intrusion). The system was trained and evaluated using two well-known datasets, KDD Test+ and KDD Test-21, which are subsets of the KDD Cup 1999 dataset. By leveraging the LSTM architecture's ability to learn temporal patterns and dependencies in the data, this IDS

demonstrated effectiveness in distinguishing between normal and malicious activities within a network environment. [10].

### *2.5. Gated Recurrent Unit*

In the research of network anomaly detection and mitigation, Gated Recurrent Units (GRU) have emerged as an efficient alternative to LSTM networks due to their simpler architecture and fewer trainable parameters. This work uses GRUs to forecast various traffic features such as bits per second, packets per second, and entropy values for source and destination IPs and ports. The results of these predictions are subsequently fed into a fuzzy logic system to provide qualitative assessments of potential network anomalies. This approach is particularly effective in software-defined networks (SDN), which centralize control for easier traffic monitoring and management. By utilizing both GRUs and fuzzy logic, the system can detect and mitigate network anomalies like DDoS attacks, as demonstrated using datasets such as CIC-DDoS2019. The system's ability to forecast network conditions and detect deviations effectively makes it a promising tool for enhancing the security and reliability of SDN environments [11].

### *2.6. Deep Belief Network*

Deep Belief Network (DBN) are a type of DL architecture composed of stacked Restricted Boltzmann Machines (RBM). Each RBM consists of a visible layer, which accepts input data, and a hidden layer, which processes and transforms this data into meaningful representations. The stacked arrangement allows DBN to learn hierarchical, layer-wise features, enabling the model to capture both low-level and high-level abstractions in complex datasets. By training one layer at a time, DBN can effectively initialize weights in a manner that enhances their performance during fine-tuning with labeled data [12].

In the context of IDS, DBN have shown considerable promise due to their ability to model the intricate patterns in network traffic data. A notable implementation of a DBN-based IDS utilized the CICIDS2017 dataset for training and evaluation. This dataset is widely recognized in cybersecurity research as a benchmark for intrusion detection, providing a comprehensive mix of legitimate traffic and various types of attacks, including DoS, DDoS, and infiltration. To address the class imbalance inherent in such datasets, researchers applied advanced balancing techniques, ensuring the underrepresented attack categories were sufficiently modeled. The DBN-based approach demonstrated significant improvements in detecting these minority classes compared to traditional Multi-Layer Perceptron (MLP) and other state-of-the-art techniques [12].

### *2.7. Self-organizing Map*

Self-Organizing Map (SOM) is a DL architecture that serves as an unsupervised method for dimensionality reduction, transforming high-dimensional input data into a low-dimensional, discretized map that represents the underlying structure of the data. In the context of network intrusion detection, SOM can be used to map the features of various types of cyberattacks, facilitating the detection of abnormal behavior in network traffic. A key advantage of SOM in this area is its ability to visualize and classify attacks, which is crucial in handling large and complex datasets.

Studies have utilized datasets such as CICDDoS2019, which includes labeled network traffic data representing different types of attacks, to train SOMs and evaluate their effectiveness in intrusion detection. In recent research, SOM has been integrated into the training of models that aim to improve detection accuracy, especially in scenarios involving underrepresented attack types. This method, when paired with DL models like DBN, demonstrates an effective approach to tackling challenges posed by imbalanced datasets in intrusion detection, providing promising results in classifying and detecting sophisticated attacks in real-time scenarios [13].

### *2.8. Self-adaptive Evolutionary Extreme Learning Machine*

Extreme Learning Machine (ELM) are a type of feedforward neural network with a single hidden layer that achieves rapid training by initializing neuron weights randomly and using the Moore-Penrose pseudo-inverse to compute output weights, instead of traditional backpropagation. To enhance the performance of ELMs, Self-Adaptive Evolutionary ELM (SaE-ELM) integrates genetic algorithms to optimize initial weight selection, improving model robustness and classification accuracy.

Researchers have implemented SaE-ELM for IDS, using datasets such as NSL-KDD, ISCX IDS 2012, UNSW-NB15, and CICIDS2017 for validation. These datasets cover a wide range of attack types, providing a comprehensive benchmark for evaluating IDS performance. The combination of ELM’s speed and genetic algorithms' optimization allows SaE-ELMs to adapt to evolving attack patterns and classify both known and unknown threats effectively [14].

### *2.9. CNN-LSTM*

CNN-LSTM is a hybrid DL architecture that combines the spatial feature extraction capabilities of Convolutional Neural Networks (CNN) with the temporal sequence processing strength of Long Short-Term Memory (LSTM). This fusion is particularly effective in IDS, as CNN can efficiently analyze multidimensional input like network traffic, while LSTM adds the ability to learn and retain patterns over time, enhancing detection accuracy. For instance, researchers have applied CNN-LSTM models to datasets such as CICIDS-2017 to identify and mitigate DDoS attacks in SDN environments. SDN, with its centralized control and programmability, offers significant network management

advantages but is also vulnerable to DDoS attacks targeting controllers and switches.

The CNN-LSTM-based IDS leverages CNN's capability to extract high-level traffic features and LSTM's sequential memory to detect anomalies, achieving high accuracy rates in both binary and multiclass DDoS classification. These models outperform traditional IDS approaches by utilizing advanced evaluation metrics, such as precision-recall curves and ROC curves, and adopting innovative optimization techniques, making them a robust solution against evolving cyber threats [15].

### *2.10. Multilayer Perceptron*

Multilayer Perceptron is a DL architecture that consists of an input layer, one or more hidden layers, and an output layer where each neighboring layer's neurons are fully connected. The paper specified that hyperparameter tuning was utilized to optimize the system's number of neurons, learning rates, batch sizes, dropout rates, and optimization algorithms, such as Adam and RMSprop. The system was then trained and validated using an unspecified dataset and managed to almost reach the same performance as the other architectures that were listed [16]. Additionally, this study includes details on hyperparameter optimization to ensure reproducibility and fairness. Learning rates were explored between 0.001–0.01, batch sizes ranged from 32–128, and dropout rates were set between 0.2–0.5. A combination of grid search and manual fine-tuning was employed to select the most effective configurations for each model, ensuring that performance comparisons were based on optimized settings rather than arbitrary defaults.

### *2.11. Residual Neural Networks*

Residual Neural Networks is a DL architecture designed to overcome the vanishing gradient problem, a common challenge in training deep neural networks. By introducing skip connections, ResNet enables layers to pass information directly to subsequent layers, effectively bypassing certain computations. This approach not only facilitates the flow of gradients during backpropagation but also allows the network to learn identity mappings, making it more efficient in modeling complex data patterns.

The paper's model has incorporated an attention mechanism to focus on the most significant features in network traffic data, improving its ability to identify patterns indicative of attacks. The training process involves two stages: initial pre-training on raw data and subsequent fine-tuning using Synthetic Minority Oversampling Technique (SMOTE)-augmented data. This dual-phase training addresses class imbalance and enhances the model's predictive stability by incorporating a regularization term in the loss function, which penalizes large deviations between predictions from the pre-training and fine-tuning phases.

The research utilized the CICIDS2017 dataset, a comprehensive collection of network flow data featuring 225,745 entries and 83 attributes. This dataset captures a wide range of metrics, including packet sizes, flow durations, and flag counts, offering a robust foundation for analyzing DDoS attack patterns. The authors employed extensive preprocessing, including handling missing data, encoding categorical features, and applying feature scaling to ensure uniformity in data representation. The dataset was divided into training and testing sets to facilitate an objective evaluation of the model's performance.

The findings of the research underscore the efficacy of the proposed ResNet-based approach. By leveraging attention mechanisms and addressing class imbalances through SMOTE, the model demonstrated superior accuracy and robustness in detecting DDoS attacks compared to traditional methods. These results highlight the potential of integrating advanced DL architectures with data augmentation techniques for enhancing cybersecurity measures [17].

### *2.12. Sparse Autoencoder*

An autoencoder is a DL architecture that learns to encode input data into a compressed representation and then reconstructs the original input from this representation. Sparse Autoencoder (SAE) is a type of autoencoder that incorporates sparsity constraints to ensure that only a few neurons are activated at a time, focusing on extracting the most relevant features from high-dimensional data. The Enhanced Deep Sparse Autoencoder (EDSA) developed in this paper includes two hidden layers with sigmoid activation functions, enabling dimensionality reduction and effective feature selection. This design helps address issues like redundancy and overfitting, which are common challenges in intrusion detection.

The paper used the CICDDoS2019 dataset, which contains real-world network traffic data, including both benign traffic and various types of DDoS attacks. Features such as source and destination IPs, port numbers, protocols, and timestamps were preprocessed using min-max normalization and mapped to integers. The dataset was split into training and testing sets in a 75:25 ratio. The proposed EDSA model demonstrated high performance. Compared to other models shown in the paper, the EDSA showed superior results across multiple metrics, including precision, detection rate, and specificity. The research concluded that this approach significantly enhances intrusion detection by minimizing classification errors and reducing false alarms. Future work may include integrating clustering techniques and adding more layers to further optimize feature extraction and classification [2].

## 3. Network Intrusion Datasets

The use of network intrusion datasets has become essential for training and testing DL models in IDS. These

datasets provide labeled network traffic data that includes both normal behavior and various types of attacks, making them suitable for evaluating the performance of models in distinguishing between legitimate traffic and attacks like DoS (Denial of Service) and DDoS (Distributed Denial of Service). Such dataset types include:

- CICIDS2017: This dataset, developed by the Canadian Institute for Cybersecurity, contains detailed network traffic data, including various attack scenarios. It offers features for both machine learning and DL-based models, providing a realistic simulation of network environments under attack. It includes packet-level data and flow records, useful for analyzing how well models can handle large-scale real-world attacks [18, 19].
- NSL-KDD: An updated version of the KDD Cup 1999 dataset, NSL-KDD aims to address some of the issues in the original dataset, like redundant records, and provides a more balanced and structured format for machine learning models to assess performance [19].
- UNSW-NB15: This dataset includes a hybrid of real and synthetic traffic, with attack types ranging from DoS and DDoS to probing and more. It was created with modern attack patterns in mind and offers a comprehensive dataset for evaluating IDS models, particularly those incorporating DL techniques [19].
- CAIDA: This dataset contains anonymized traces of network traffic designed to mimic DDoS attack scenarios. Despite its limited diversity and absence of labels, CAIDA provides valuable insights into high-bandwidth traffic anomalies, helping researchers understand the mechanics of DDoS attacks [20].
- ADFA-LD and ADFA-WD: Created by researchers at the Australian Defense Force Academy, these datasets focus on host-based intrusion detection using system-call traces. They simulate attacks on both Linux (ADFA-LD) and Windows (ADFA-WD) systems, featuring a mix of standard and zero-day attack samples [20].
- AWID: The Aegean Wi-Fi Intrusion Dataset is a specialized resource for analyzing wireless network traffic. It includes labeled records of 802.11 Wi-Fi activity, organized into categories such as Injection, Flooding, and Impersonation. AWID provides both high-level and detailed data, making it versatile for testing machine learning models [20].
- CIC-DDoS2019: This dataset captures a variety of DDoS attack types based on protocols like NTP, DNS, and UDP. It includes extensive labeled records and 88 features, offering a rich resource for assessing the performance of IDS in handling modern, protocol-specific attacks [20].
- BoT-IoT: The BoT-IoT dataset is designed to emulate realistic IoT network scenarios. It includes a diverse array of attack types such as DoS, DDoS, and keylogging, as well as legitimate traffic. With its vast record count and varied attack landscape, it is a crucial dataset for evaluating IDS models in IoT environments [20].

To evaluate the performance of intrusion detection models using these datasets, metrics such as accuracy, precision, recall, and F1-score are often used. These metrics help to quantify a model's effectiveness in identifying and mitigating both known and unknown attack patterns.

Each dataset has unique characteristics (Table 1) that make it suitable for specific scenarios in IDS evaluation. For instance, the KDD 99 dataset is among the largest and most widely used datasets for intrusion detection, but it suffers from issues like redundant features and an imbalanced class distribution, which can hinder machine learning classification. Its modified version, NSL-KDD, addresses some of these issues by reducing duplicate records and balancing the dataset, making it more effective for modern IDS testing. However, it lacks representations of contemporary network attacks [20].

While multiple benchmark datasets such as CICIDS2017, CICDDoS2019, NSL-KDD, UNSW-NB15, and KDDTest-21 were employed in this study, each dataset presents inherent limitations that influence the results. For instance, NSL-KDD and KDDTest-21 contain attack types that are now outdated, which may inflate performance metrics but reduce generalizability to modern threats. CICIDS2017 and CICDDoS2019, although more recent, suffer from class imbalance where benign traffic dominates, potentially biasing models toward higher accuracy while underperforming on minority attack classes. UNSW-NB15 offers a richer set of contemporary attacks, yet inconsistencies in labeling and synthetic traffic generation may limit realism. These dataset properties directly affect evaluation outcomes: models such as CNN tend to excel on well-balanced datasets, while LSTM architectures better handle sequential traffic but are sensitive to imbalance. Consequently, comparative results should be interpreted with caution, as dataset biases and outdated patterns may artificially favor certain architectures, underscoring the need for ongoing validation with evolving real-world traffic.

On the other hand, datasets like CIC-DDoS2019 and BoT-IoT provide more recent intrusion scenarios, capturing modern and complex network attacks, including various types of DDoS and IoT-based threats [20]. These datasets are essential for evaluating the capabilities of IDS models in detecting evolving threats and are widely used in scientific studies for benchmarking current IDS solutions.

Datasets such as CAIDA, ADFA-LD, ADFA-WD, AWID, UNSW-NB15, and CICIDS2017 each have specific strengths and limitations. While some focus on host-based intrusion detection with system-call traces (e.g., ADFA datasets), others offer comprehensive representations of network traffic with diverse attack patterns [20]. As the landscape of cyber threats continues to evolve, these datasets must be updated periodically to include novel attack types and features, ensuring that IDS models remain relevant and effective in addressing emerging challenges. These comprehensive datasets, combined with robust evaluation metrics, allow researchers to measure the real-world applicability and robustness of IDS.

Table 1. Comparison of well-known IDS dataset [20]

| No | Dataset name | Year | Feature | Attack types | Labeled/ Unlabeled | Number of instances |
|---|---|---|---|---|---|---|
| 1 | DARPA | 1998 | No features | Dos, U2R, R2L, Probe | Unlabeled | - |
| 2 | KDD '99 | 1999 | 41 | Dos, U2R, R2L, Probe, Normal | Labeled | 4,900,000 |
| 3 | CAIDA | 2007 | 20 | DDoS, Normal | Unlabeled | - |
| 4 | NSL-KDD | 2009 | 41 | Dos, U2R, R2L, Probe, Normal | Labeled | 125,973 training 22,544 testing |
| 5 | ADFA-LD and ADFA-WD | 2014 | 26 | Stealth, Webshell, Zero-day, Dydra, Meterpreter, Adduser | Labeled | 13,675 traces |
| 6 | AWID | 2015 | 155 | Injection, Flooding, Impersonating, Normal | Labeled | 162,375,247 training 48,524,866 testing |
| 7 | UNSW-NB15 | 2015 | 49 | Analysis, Backdoors, DoS, Exploits, Generic, Fuzzers, Reconnaissance, Shell code, Worms | Labeled | 2,540,044 |
| 8 | CICIDS | 2017 | 80 | Brute force, Infiltration, DoS, DDoS, Heartbleed, Botnet, Web attack | Labeled | - |
| 9 | CIC-DDoS2019 | 2019 | 88 | Benign, Various DDoS attacks | Labeled | Hundred's thousands of records |
| 10 | BoT-IoT | 2018 | 49 | DoS, DDoS, Keylogging, Data exfiltration attacks, Service scan | Labeled | 72.000.000 |

## 4. IDS Metric

The evaluation of IDS often relies on a set of standard performance metrics that provide a comprehensive understanding of a model's effectiveness in distinguishing between legitimate traffic and potential threats. These metrics-accuracy, precision, recall, and F1-score—are particularly crucial in assessing the balance between detecting malicious activity and minimizing false alarms in network security systems. Here are the detailed explanations.

- Accuracy: Measures the proportion of correctly classified instances out of the total. While useful as a general measure, accuracy can be misleading for imbalanced datasets where one class dominates, as it does not differentiate between types of errors [21].
- Precision: Indicates the proportion of true positives among all predicted positives, answering the question, "Of all instances predicted as positive, how many are actually positive?" Precision is crucial when false positives carry significant costs, such as in financial fraud detection [21].
- Recall: Also called the true positive rate, recall measures the proportion of actual positives correctly identified. It is vital in scenarios where missing positive cases (false negatives) has severe consequences, such as in medical diagnostics or network intrusion detection [21].
- F1-Score: A harmonic mean of precision and recall, balancing these two metrics to provide a single measure of a model's performance. F1-score is especially valuable for imbalanced datasets, as it penalizes models that perform poorly in either precision or recall [21].

These metrics are fundamental in evaluating IDS performance, as they capture the model's ability to distinguish legitimate traffic from malicious attacks while accounting for the trade-offs between different error types.

## 5. Classification and Comparison Result

The comparative analysis of DL models across different datasets (Table 2) reveals significant variations in performance, influenced by both the model architecture and the dataset characteristics. Models trained on the KDDTest-21 dataset consistently scored lower across metrics such as accuracy, precision, recall, and F1-score. For instance, the Long Short-Term Memory (LSTM) model achieved an accuracy of 88.3% with a recall of 88.6% and an F1-score of 93.3%, while the SAL-ELM model lagged with an accuracy of 73%. This disparity may suggest that KDDTest-21 poses unique challenges, potentially due to the complexity of the dataset or its inclusion of harder-to-differentiate attack patterns. These findings highlight the importance of dataset selection in benchmarking IDS models, as well as the need for models robust enough to handle more challenging data.

In contrast, the CICIDS2017 dataset saw some of the highest-performing models (Fig. 2). The chart not only presents accuracy and F1-score but also illustrates the dependency of IDS performance on dataset complexity and relevance to current attack patterns. The ResNet architecture demonstrated near-perfect scores, achieving 99.9% accuracy, precision, recall, and F1-score, outperforming other architectures on this dataset. Similarly, SAL-ELM also attained perfect scores on CICIDS2017, indicating that the dataset is well-suited for these advanced models. The

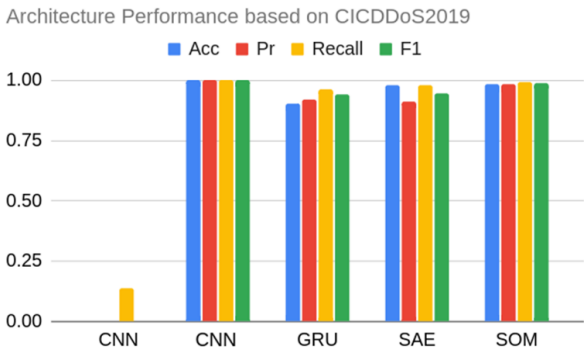
effectiveness of these models on CICIDS2017 suggests they may contain patterns or features that are more easily captured by DL architectures, highlighting the interplay between data structure and model design.

Table 2. Comparison of architecture performance

| Journal | Type | Dataset | Acc | Pr | Recall | F1 | Details |
|---|---|---|---|---|---|---|---|
| [7] | CNN | CICDDoS2019 LDAP (Before incremental training) | 0.002 | 0.000 | 0.138 | 0.000 | Done against untrained data |
| | CNN | CICDDoS2019 LDAP (Post incremental training) | 1.000 | 1.000 | 1.000 | 1.000 | Done against untrained data after it was labeled by an employee and put into incremental training |
| [10] | LSTM | KDDTest-21 | 0.883 | 0.987 | 0.886 | 0.933 | - |
| [11] | GRU | CICDDoS2019 | 0.904 | 0.922 | 0.965 | 0.943 | - |
| [12] | DBN | CICIDS2017 | 0.998 | 0.887 | 0.997 | 0.940 | - |
| [13] | SOM | CICDDoS2019 | 0.986 | 0.983 | 0.993 | 0.988 | - |
| [14] | SAL-ELM | KDDTest-21 | 0.730 | 0.902 | 0.612 | 0.730 | - |
| | SAL-ELM | CICIDS2017 | 0.999 | 1.000 | 1.000 | 1.000 | - |
| [15] | CNN-LSTM | CICIDS2017 | 0.989 | 0.978 | 0.997 | 0.987 | - |
| [16] | MP | Unknown | 0.987 | 0.984 | 0.981 | 0.982 | - |
| [17] | ResNet | CICIDS2017 | 0.999 | 0.999 | 0.999 | 0.999 | - |
| [22] | SAE | CICDDoS2019 | 0.980 | 0.910 | 0.981 | 0.944 | - |

For the CICDDoS2019 dataset, several models performed exceptionally well, reflecting its relevance for contemporary intrusion detection scenarios. The SOM achieved an impressive F1-score of 98.8%, closely followed by the SAE with an F1-score of 94.4%. The GRU model also excelled, achieving a high recall of 96.5% and an F1-score of 94.3%, indicating strong potential for sequence-based learning in detecting DDoS patterns. The effectiveness of SAE in this context is consistent with prior work on deep autoencoder-based methods for DDoS detection [22], which emphasized the ability of autoencoders to reconstruct traffic features and capture anomalies. These results underscore the suitability of CICDDoS2019 for training modern IDS models and the robustness of the SAE and SOM architectures for anomaly detection. Beyond accuracy, we evaluated computational cost and latency. ResNet and CNN-LSTM models, while highly accurate, required substantially longer training and inference times, which may limit deployment in real-time IDS scenarios. Conversely, GRU and SAE models offered a favorable trade-off between accuracy and runtime efficiency, making them attractive for edge environments.

A notable exception in the analysis is the performance of the CNN on the CICDDoS2019 LDAP subset. Before incremental training, the CNN scored extremely low, with an accuracy of 0.2% and an F1-score of 0. This highlights the challenges of detecting unknown attacks in untrained data. However, after human intervention to label attacks and apply incremental training, CNN achieved perfect scores across all metrics. This result emphasizes the lack of DL models designed to autonomously detect unknown attacks. Even in this case, human intervention was required to label the unknown attacks, indicating a significant gap in the current literature and practice. Autonomous systems capable of identifying previously unseen attacks remain a critical area for future research. From an interpretability standpoint, integrating explainable AI tools such as SHAP and LIME could provide valuable insights into which network features drive decisions, thereby enhancing analyst trust and facilitating adoption in operational IDS environments. Furthermore, while deep learning models can achieve high accuracy, they are often perceived as “black boxes.” Explainable AI can bridge this gap by providing transparent reasoning behind predictions, ultimately improving the practicality and trustworthiness of IDS deployments.



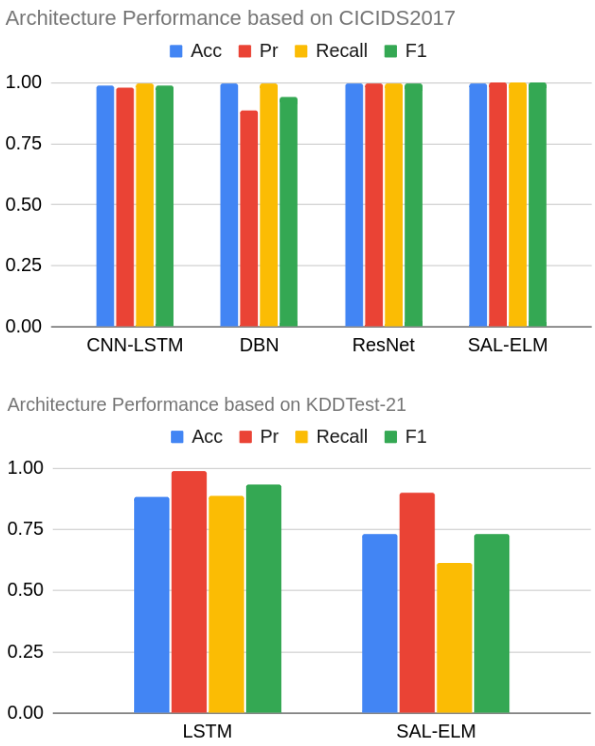



Fig.2. Visualization of various DL architecture performance based on the dataset they were tested on

## 6. Conclusions

The rapid growth of cloud computing and the increasing reliance on data storage and processing have elevated the importance of robust cybersecurity measures, especially in mitigating sophisticated threats like DoS and DDoS attacks. Traditional IDS, such as signature-based and anomaly-based methods, often fall short in adapting to unknown threats or managing vast volumes of data. The advent of DL has introduced promising alternatives due to its capacity for automatic feature extraction and adaptability to evolving attack patterns. DL architectures, including CNN, RNN, LSTM, and DBN, have shown a potential to enhance IDS performance. However, the effectiveness of these architectures varies significantly based on the dataset and application scenarios.

The related literature highlights the strengths and limitations of these DL models. CNN excel in recognizing spatial patterns, making them ideal for datasets like CICIDS2017, where traffic features are spatially represented. LSTM, with their capability to process sequential data, are better suited for time-series traffic logs but struggle with datasets that present complex or highly imbalanced patterns, such as KDDTest-21. DBN and SOM demonstrate effectiveness in learning hierarchical and dimensionality-reduced representations, particularly in datasets like CICIDS2017 and CICDDoS2019, which encompass diverse attack types.

The comparative analysis in this research underscores the variability in performance across datasets. ResNet and SAL-ELM models achieved near-perfect scores on CICIDS2017, while CNN excelled on CICDDoS2019. Conversely, models trained on KDDTest-21, such as LSTM and SAL-ELM, exhibited lower accuracy and F1-score, possibly reflecting the dataset's complexity and the inclusion of harder-to-differentiate attack patterns. Notably, the CNN model's incremental training on CICDDoS2019 demonstrated the potential of combining human-labeled unknown attacks with adaptive learning to enhance detection, highlighting a critical gap in the development of autonomous models for unknown threat detection.

In conclusion, while deep learning models offer significant advancements for intrusion detection, their success heavily depends on the dataset's nature and the model's design. Datasets like CICIDS2017 and CICDDoS2019 provide robust platforms for testing IDS models, but the challenge of autonomously identifying unknown attacks remains largely unaddressed. This research emphasizes the need for future research to focus on creating models capable of detecting novel threats without human intervention, ensuring adaptability and resilience against ever-evolving cyber threats. Achieving this may involve developing new, specialized network intrusion datasets tailored to train against unknown attacks or devising novel approaches to implementing DL architecture for IDS.

Future work should explicitly consider computational cost, latency, and scalability in edge/cloud IDS deployments. In addition, the integration of explainable AI techniques such as SHAP or LIME could enhance analyst trust, while federated learning across distributed environments may support adaptive IDS for evolving threats. Another critical direction is addressing the limitation of CNN-based models, which often require incremental retraining to handle

unseen attacks. Bridging this gap is essential to achieve more autonomous and resilient IDS solutions.

## References


[1] D. S. Berman, A. L. Buczak, J. S. Chavis and C. L. Corbett, "A Survey of Deep Learning Methods for Cyber Security," *Information*, vol. 10, no. 4, Art. no. 4, Apr. 2019, doi: 10.3390/info10040122.

[2] J. Lansky et al., "Deep Learning-Based Intrusion Detection Systems: A Systematic Review," *IEEE Access*, vol. 9, pp. 101574–101599, 2021, doi: 10.1109/ACCESS.2021.3097247.

[3] I. H. Sarker, "Deep Cybersecurity: A Comprehensive Overview from Neural Network and Deep Learning Perspective," *SN Comput. Sci.,* vol. 2, no. 3, p. 154, Mar. 2021, doi: 10.1007/s42979-021-00535-6.

[4] "What is a denial-of-service (DoS) attack?" Accessed: Nov. 27, 2024. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[5] "AI vs. Machine Learning vs. Deep Learning vs. Neural Networks | IBM." Accessed: Nov. 27, 2024. [Online]. Available: https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks

[6] A. B. Nassif, I. Shahin, I. Attili, M. Azzeh and K. Shaalan, "Speech Recognition Using Deep Neural Networks: A Systematic Review," *IEEE Access*, vol. 7, pp. 19143–19165, 2019, doi: 10.1109/ACCESS.2019.2896880.

[7] C.S. Shieh, T.T. Nguyen, M.F. Horng, "Detection of Unknown DDoS Attack Using Convolutional Neural Networks Featuring Geometrical Metric,"*Mathematics,* 2023, 11(9), 2145, doi: 10.3390/math11092145

[8] A. H. Halbouni, T. S. Gunawan, M. Halbouni, F. A. A. Assaig, M. R. Effendi and N. Ismail, "CNN-IDS: Convolutional Neural Network for Network Intrusion Detection System," *International Conference on Wireless and Telematics,* 2022, pp. 1–4. doi: 10.1109/ICWT55831.2022.9935478.

[9] L. Yang and A. Shami, "A Transfer Learning and Optimized CNNBased Intrusion Detection System for Internet of Vehicles," *IEEE International Conference on Communications*, 2022, pp. 2774–2779. doi: 10.1109/ICC45855.2022.9838780.

[10] M. Ibrahim and R. Elhafiz, "Modeling an intrusion detection using recurrent neural networks," *J. Eng. Res.*, vol. 11, no. 1, p. 100013, Mar. 2023, doi: 10.1016/j.jer.2023.100013.

[11] D. M. Brandão Lent, M. P. Novaes, L. F. Carvalho, J. Lloret, J. J. P. C. Rodrigues and M. L. Proença, "A Gated Recurrent Unit Deep Learning Model to Detect and Mitigate Distributed Denial of Service and Portscan Attacks," *IEEE Access*, vol. 10, pp. 73229-73242, 2022, doi: 10.1109/ACCESS.2022.3190008.

[12] O. Belarbi, A. Khan, P. Carnelli and T. Spyridopoulos, "An Intrusion Detection System Based on Deep Belief Networks. In: Su, C., Sakurai, K., Liu, F. *Lecture Notes in Computer Science*, 2022, vol 13580. Springer, Cham. https://doi.org/10.1007/978-3-031-17551-0_25

[13] M. Rafiee and A. Shirmarz, "Self-Organization Map (SOM) Algorithm for DDoS Attack Detection in Distributed Software Defined Network (D-SDN)," *J. Inf. Syst. Telecommun*, vol. 2, no. 38, p. 120, Apr. 2022, doi: 10.52547/jist.15644.10.38.120.

[14] G. S. Kushwah and V. Ranga, "Optimized extreme learning machine for detecting DDoS attacks in cloud computing," *Comput. Secur.*, vol. 105, p. 102260, Jun. 2021, doi: 10.1016/j.cose.2021.102260.

[15] D. M. Rajan and D. J. Aravindhar, "Detection and Mitigation of DDOS Attack in SDN Environment Using Hybrid CNN-LSTM," *Migration Letters*, 2023, Vol. 20, No. S13, doi: 10.59670/ml.v20iS13.6472.

[16] A. Sanmorino, L. Marnisah and H. D. Kesuma, "Detection of DDoS Attacks using Fine-Tuned Multi-Layer Perceptron Models," *Eng. Technol. Appl. Sci. Res.*, vol. 14, no. 5, Art. no. 5, Oct. 2024, doi: 10.48084/etasr.8362.

[17] A. Alfatemi, M. Rahouti, R. Amin, S. ALJamal, K.Xiong, Y.Xin, "Advancing DDoS Attack Detection: A Synergistic Approach Using Deep Residual Neural Networks and Synthetic Oversampling." Accessed: Nov. 28, 2024. *arXiv*, 2024. doi: 10.48550/arXiv.2401.03116

[18] "IDS 2017 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." Accessed: Nov. 27, 2024. [Online]. Available: https://www.unb.ca/cic/datasets/ids-2017.html

[19] N. Moustafa and J. Slay, "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *Military Communications and Information Systems Conference*, 2015, pp. 1–6. doi: 10.1109/MilCIS.2015.7348942.

[20] M. Ozkan-Okay, R. Samet, Ö. Aslan and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021, doi: 10.1109/ACCESS.2021.3129336.

[21] A. Kumar, "Accuracy, Precision, Recall & F1-Score - Python Examples," Analytics Yogi. Accessed: Nov. 27, 2024. [Online]. Available: https://vitalflux.com/accuracy-precision-recall-f1-score-python-example/

[22] S. Sindian and S. Sindian, "An Enhanced Deep Autoencoder-based Approach for DDoS Attack Detection." *WSEAS Transactions on Systems and Control*, Vol 15, 2020, pp. 716-724, doi: 10.37394/23203.2020.15.72

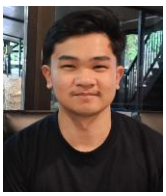

### Authors' Profiles

**Andreas Handojo** received his Doctor of Industrial Engineering degree in Supply Chain and Logistics Management; he also received his Master's degree in Management of Technology from the Institute of Technology Sepuluh Nopember, Indonesia. He achieved his Bachelor's degree in Electrical Engineering at Petra Christian University. He works as an Associate Professor at the Informatics Department at Petra Christian University, Indonesia. He has responsibility as Head of Field Study Software Engineering. His research interests are machine learning related to engineering and industrial application. He can be contacted at email: handojo@petra.ac.id

**Marvel Wilbert Odelio** student in the Informatics Department at Petra Christian University, Surabaya, Indonesia

**Nico Alexandre Kurniawan** student in the Informatics Department at Petra Christian University, Surabaya, Indonesia.

**Dillan Engelbert Hendrarto** student in the Informatics Department at Petra Christian University, Surabaya, Indonesia.



**Matthew Timothy Handoyo** student in Business Management Department, National Tsing Hua University, Hsinchu, Taiwan.

**How to cite this paper:** Andreas Handojo, Marvel Wilbert Odelio, Nico Alexandre Kurniawan, Dillan Engelbert Hendrarto, Matthew Timothy Handoyo, "A Comparative Analysis of Deep Learning Architecture for Early Detection of DoS/DDoS Patterns in Network Traffic Using Intrusion Detection Systems", International Journal of Computer Network and Information Security(IJCNIS), Vol.18, No.1, pp.131-141, 2026. DOI:10.5815/ijcnis.2026.01.09