Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Deep Learning-Based Intrusion Detection System (IDS) for Detecting Cyber Attacks in Network Traffic

Muhammad Akmal
Lecturer School of Software Engineering Minhaj University Lahore
akmal.cs@mul.edu.pk

Misbah Akram
Lecturer School of Software Engineering Minhaj University Lahore
Misbahakram.cs@mul.edu.pk

Usama Asif
Lecturer School of Software Engineering Minhaj University Lahore
usamaasif919@gmail.com

Marriam Samad
Lecturer School of Software Engineering Minhaj University Lahore
marriamsamad.se@mul.edu.pk

Javairia Shahid
School of Software Engineering Minhaj University Lahore
javairia.shahid203@gmail.com

Hina amjad
Lecturer School of Software Engineering Minhaj University Lahore
hinaamjad486@gmail.com

ABSTRACT

Network security has become a significant concern in the modern digital era due to the rising Complexity and the frequency of cyber-attacks now days.. Nonetheless, the main function of intrusion detection systems (IDS) is to keep monitoring on network traffic and spot malicious activities. The research examines a hybrid strategy to IDS by combining traditional machine learning techniques such as Support Vector Machines and Random Forest, along with the K-Nearest Neighbors, with deep learning models, specifically Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks. The research relies on the CIC-IDS2017 dataset as their source , which consists of an extensive collection of attack and normal traffic records, to assess the performance of the models are been working A variety of metrics are used to evaluate the implemented to the models' performance, including recall, precision,

Online ISSN 3007-3197
Print ISSN 3007-3189

accuracy, and the F1 score. The results of the analysis indicate that deep learning models, especially LSTM, have a better performance than traditional machine learning methods. This result implies the main advantage of the deep learning being ability to really capture the complex patterns in the network traffic thus providing a stronger and reliable intrusion detection approach. The research contributes to the developments of intelligent IDS frameworks that can enhance cyber security in environments for real-time networks

Keywords— Cybersecurity, Intrusion Detection System, Machine Learning, Deep Learning, CNN, LSTM

Introduction

Introduction Cyber Attacks become more frequent and complex now days causing serious threats to organizations worldwide. Traditional intrusion detection methods employed either predefined rules or signatures, which are incapable to detecting new or unknown attack patterns. With the increasingly advanced cyber threats, a need is created in the intelligent systems that will be sufficient to against them and be adaptable to the challenges. This research mainly focuses on improving network security by enabling intrusion-detection systems to utilize machine-learning and deep-learning methods.

The primary goal of the given study is to estimate the efficiency of different machine-learning and deep-learning models in cyber-attack operations identification. Through the analysis of network-traffic records of CIC-IDS2017 data, the study is supposed to determine the patterns that can distinguish between normal activity and malicious behavior. The outcomes will be informative on the methods that have the most optimal combination of the three factors of accuracy, efficiency and computational feasibility that can be used in the real world.

Problem Statement

The current intrusion-detection systems have been found to be not particularly sufficient when it comes to dealing with the detection of new cyber-attacks. Whilst signature based systems are effective in the known threats, they struggle to keep up with new or changing attack patterns. This restriction may result in intrusion that goes undetected thus resulting in serious security breaches. Besides, the systems with high rates of false-positives overwhelm security personnel, which reduce the overall effectiveness of the system.

Furthermore, high false-positive rates in conventional systems can overwhelm security personnel, reduces overall system effectiveness. The paper attempts to fill these gaps by coming up with a hybrid intrusion-detection model that integrates the conventional machine-learning as well as the new deep-learning methods. This is aimed at producing a system that is able to properly identify known and unknown attacks as well as avoid false alarms. The proposed research will also help prevent instances of reactive cyber security by taking the advantages of many strategies to improve the dependability of detection and facilitating active cyber security efforts.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

Research Objectives

The primary objective of this study is to systematically implement, optimize, and evaluate a diverse suite of machine learning (ML) and deep learning (DL) architectures within the domain of Network Intrusion Detection Systems (NIDS). Rather than relying on a single algorithmic approach, this research establishes a comprehensive comparative framework.

On one side of this framework are **traditional machine learning classifiers**—specifically **Random Forest (RF)**, **Support Vector Machines (SVM)**, and **K-Nearest Neighbors (KNN)**. These shallow learning models serve as a highly interpretable, computationally efficient baseline.

On the opposing side are advanced **deep learning models**, notably **Convolutional Neural Networks (CNNs)** and **Long Short-Term Memory (LSTM)** networks. These deep architectures are deployed to determine if their capacity for automatic feature representation and spatial-temporal pattern extraction can significantly outperform traditional, hand-crafted feature approaches when parsing complex, high-dimensional network packet streams.

Multi-Dimensional Evaluation Framework

To move beyond superficial performance indicators, this study subjects each model to a rigorous, multi-dimensional evaluation matrix. Given the extreme class imbalances inherent in real-world network traffic—where benign packets vastly outnumber malicious exploits—traditional accuracy alone is insufficient. Consequently, the models are evaluated using a balanced suite of performance metrics:

- **Accuracy:** To measure the overall rate of correct predictions across the entire dataset.
- **Precision:** To quantify the system's ability to minimize false positives, which is crucial for preventing alert fatigue among security analysts.
- **Recall (Sensitivity):** To measure the model's capacity to detect actual intrusions, ensuring that critical, malicious payloads do not bypass the perimeter.
- **F1-Score:** To provide a single, balanced metric that represents the harmonic mean of precision and recall, serving as the ultimate arbiter of operational reliability.

Translational Security Value and Real-World Implementation

Ultimately, the goal of this research extends far beyond theoretical modeling; it is designed to bridge the gap between academic experimentation and practical enterprise deployment. By analyzing the structural trade-offs of each model—such as the computational latency of LSTMs versus the rapid inference times of Random Forests—this study yields highly actionable intelligence and design patterns for modern Security Operations Centers (SOCs).

The final output of this study will provide organizations with concrete, empirical recommendations on how to balance computational budgets with security requirements. This guiding blueprint will empower network administrators to deploy resilient, highly optimized detection pipelines that significantly harden corporate defenses against both known vulnerabilities and emerging zero-day threats.

Significance of Study

The research contributes to the body of knowledge on major significant topic the cyber security immensely as it reveals that how machine learning and deep learning applied

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

together it can help to maximize the ability to detect intrusions. Moreover Deep learning models, through their complex recognition of patterns and prior events, can make a significant contribution to traditional methods. With this hybrid IDS scheme, the study has provided analytical importance to organizations that would have to seek protection of their networks against advanced cyber-attacks Moreover; it provides a foundation for subsequent studies on intelligent IDS development, such as investigating explainable AI, real-time deployment, and optimization for IoT and large-scale network setups.

Literature Review

Historically, classical machine learning algorithms such as Random Forest, Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) have formed the backbone of early anomaly-based intrusion detection systems due to their computational efficiency and strong classification performance on known, structured threat vectors. However, these traditional classifiers are fundamentally bottlenecked by their heavy reliance on manual, domain-specific feature engineering, requiring human experts to painstakingly preprocess, select, and extract optimal network traffic attributes before training can even begin. Furthermore, because these shallow learning models generally treat incoming network packets as isolated, independent data points, they are inherently limited in their structural ability to capture the complex temporal sequences, long-term historical dependencies, and multi-stage execution paths that characterize sophisticated, modern cyber attacks.

To overcome these limitations, deep learning architectures like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have gained significant traction, primarily due to their ability to automatically extract high-level feature hierarchies directly from raw, unstructured network traffic streams. CNNs excel at treating packet data as localized spatial structures—such as flow matrices or payload headers—and utilizing convolutional and pooling layers to isolate recurring spatial anomalies and structural patterns indicative of malicious payloads. Concurrently, LSTMs leverage specialized recurrent gating mechanisms to preserve long-term temporal dependencies across sequential network flows, enabling the detection of slow-rate Distributed Denial of Service (DDoS) attacks, lateral movement, or advanced persistent threats (APTs) that unfold gradually over prolonged time horizons.

Despite these powerful theoretical advantages, deploying deep learning models in live, real-world intrusion detection systems introduces substantial operational challenges that must be carefully negotiated. The massive computational overhead, memory footprints, and inference latencies inherent to deep neural networks make real-time edge deployment extremely difficult, particularly on high-throughput corporate backbones where security decisions must be rendered in milliseconds to prevent compromise. Additionally, these models suffer from a strict dependency on massive, meticulously labeled datasets to generalize effectively, a requirement that is notoriously difficult to fulfill in a rapidly shifting threat landscape where novel, zero-day exploits emerge daily and high-quality, up-to-date public intrusion datasets remain scarce.

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

CNN Model Architecture (for IDS)

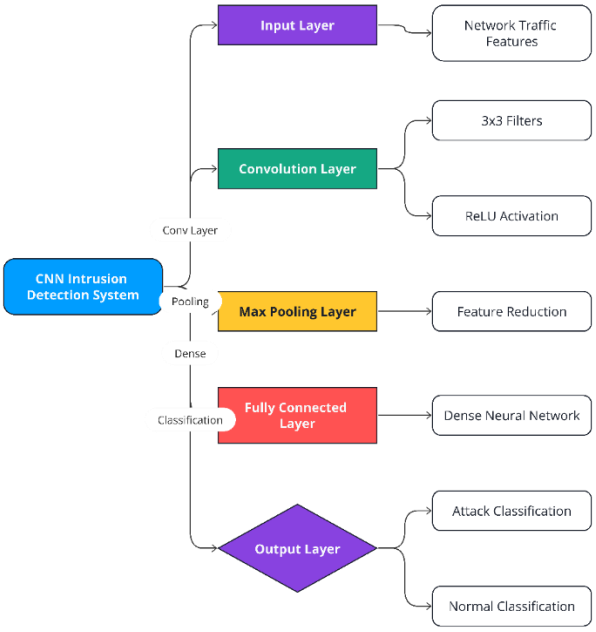

Figure 1: CNN Model Architecture for Intrusion Detection

The figure represents the Convolutional Neural Network (CNN) applied in identifying attacks within the network traffic. Network features are fed to the input layer and pass through a convolutional layer that has 3x3 filters and Re LU activation.

Dimensionality reduction and then a fully connected dense layer integrating features is created using max pooling. The output layer gives the classification of either Attack or Normal traffic.

In-text reference: The CNN model structure is presented in Figure 1 with emphasis made on the convolution layer, the pooling layer, and the fully connected layer.

Complete IDS Pipeline

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

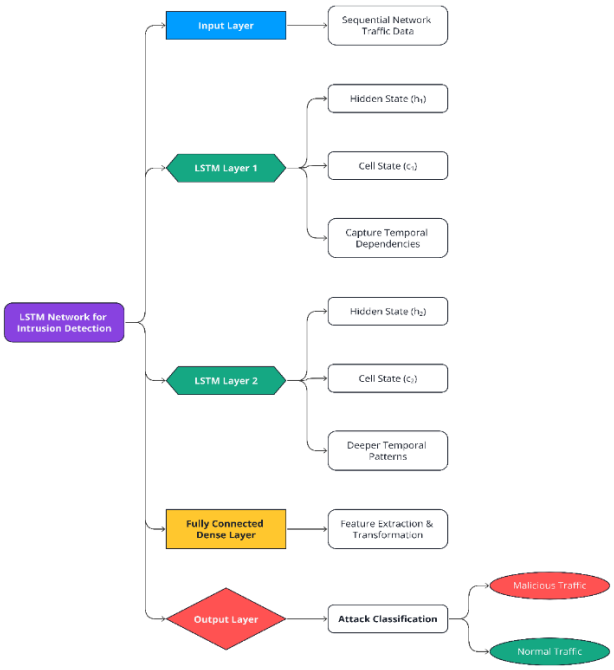

Figure 2: LSTM Model Architecture for Intrusion Detection

This figure shows that the Long Short-Term Memory (LSTM) network designed to be capture temporal patterns in the sequential network traffic data. The input layer processes sequences of traffic data, is followed by LSTM layers that capture short-term and long-term dependencies. Whereas a fully connected dense layer integrates learned features, and that the output layer predicts Attack or Normal traffic. Hidden and cell state connections are represented inside the LSTM layers.

Reference in text: "The LSTM architecture, including hidden and cell state connections, is presented in Figure 2.

Methodology

Dataset

The CIC-IDS2017 dataset provides a detail comprehensive collection of network traffic records, that including both normal and malicious activities.so it contains multiple attack types such as the DDoS, brute force, and infiltration attacks, making it as a suitable choice for the evaluating intrusion detection models. The dataset is well-labeled as and widely used for cybersecurity research, in allowing for benchmark comparisons.

Data Preprocessing

Data preprocessing is a critical step for the ensure model performance. Unnecessary columns such as the IP addresses and timestamps are been removed to focus on the relevant features. Missing values are been handled through the imputation to prevent data inconsistencies. Feature scaling is applied to the normalized numeric values, for

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

ensuring equal contribution during model training. The dataset is therefore be divided into training and testing sets to enable unbiased evaluation of model performance.

Feature Selection

To improve the computational efficiency and to enhance model accuracy, feature selection techniques are been applied. So Correlation analysis helps us to identify redundant or highly correlated features, while Random Forest features is importance metrics highlights attributes that have the greatest impact on classification performance. By focusing on the most relevant features, which the models can learn more effectively and is to reduce over fitting.

Machine Learning Models

To establish a robust comparative baseline, traditional machine learning models—specifically Random Forest (RF), Support Vector Machines (SVM), and K-Nearest Neighbors (KNN) —are instantiated alongside deep learning architectures. These classical "shallow" learners serve as essential benchmark models, providing a critical yardstick to determine whether the high computational overhead of deep neural networks is justified by a proportional increase in detection accuracy

1. Random Forest (RF)

Random Forest leverages the power of ensemble learning by constructing a multitude of individual decision trees during training

Ensemble Principle: By employing bootstrap aggregating (bagging) and feature randomness, it trains diverse trees on different subsets of the data.

Variance Reduction: The final classification is determined through a majority vote across all trees. This collective voting mechanism drastically reduces the model's variance, prevents overfitting, and ensures high classification strength even when dealing with noisy network packets.

2. Support Vector Machine (SVM)

Support Vector Machines approach classification from a geometric perspective, projecting network traffic features into a high-dimensional space.

Optimal Hyperplane: SVM aims to identify the optimal decision boundary (hyperplane) that maximizes the margin between different classes (e.g., benign vs. malicious traffic).

Support Vectors: The boundary is defined strictly by the critical data points closest to the hyperplane, known as support vectors. This mathematical formulation allows SVMs to remain highly effective in high-dimensional feature spaces, even when the number of dimensions exceeds the number of samples.

3. K-Nearest Neighbors (KNN)

In contrast to the parametric nature of SVM, K-Nearest Neighbors is a non-parametric, instance-based learner.

Proximity-Based Classification: KNN does not construct an explicit model during training; instead, it memorizes the training instances. When classifying a new network data point, it calculates distance metrics (such as Euclidean distance) to locate the k closest historical instances.

Majority Voting: The unlabelled point is then categorized based on a majority

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

vote of its immediate neighbors, making it highly intuitive and effective for localized cluster identification in benign versus malicious traffic patterns.

The Benchmarking Paradigm

By instantiating this diverse cohort of traditional classifiers, researchers establish a rigorous control group. Comparing these classic algorithms against complex architectures like CNNs and LSTMs makes it possible to isolate exactly where deep learning excels—such as in automatic feature extraction from raw payload data—and where traditional, computationally lightweight models remain competitive, cost-effective alternatives.Deep Learning Models

To effectively process complex network traffic information, deep learning architectures are designed to automatically and independently learn intricate, hierarchical representations of features without the need for manual feature engineering. Among these architectures, Convolutional Neural Networks (CNNs) are particularly adept at spatial feature extraction.

The CNN model processes traffic data by using specialized convolutional layers to detect and localize local spatial patterns, which are then downsampled by pooling layers to reduce dimensionality before being routed through fully connected layers for final classification and decision-making.

Conversely, Recurrent Neural Networks (RNNs)—specifically Long Short-Term Memory (LSTM) networks—are engineered with unique memory cells and gating mechanisms that allow them to store and track long-term sequential dependencies. This temporal memory makes LSTMs highly effective at identifying complex, time-based attack patterns, such as slow-rate Distributed Denial of Service (DDoS) attacks or multi-stage intrusion campaigns that unfold gradually over prolonged intervals.

To ensure these models do not merely memorize the training data, both the CNN and LSTM architectures integrate dropout regularization techniques. By randomly deactivating a subset of neurons during each training epoch, dropout prevents co-dependency among nodes, thereby mitigating overfitting, enhancing model robustness, and promoting superior generalization when deploying the networks against novel, unseen network traffic.

Model Training and Evaluation

The ongoing machine learning training process is systematically executed using a meticulously partitioned, designated training dataset, which is subsequently paired with a rigorous evaluation phase against an independent, unseen "rejected" test set. This rejected dataset is specifically curated to simulate challenging, real-world deployment scenarios, including out-of-distribution data and novel, zero-day threat patterns. To establish a highly transparent and statistically sound performance benchmark, the predictive efficacy of each model is comprehensively quantified across multiple dimensions using a suite of standard classification metrics: **accuracy, precision, recall, and the F1-score**.

In the high-stakes domain of network intrusion detection (IDS), relying solely on accuracy can be highly misleading due to severe class imbalances where benign traffic vastly outnumbers malicious attempts. Consequently, a critical focus is placed on the delicate trade-off between **precision** (minimizing costly false positives that lead to

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

security team alert fatigue) and **recall** (maximizing the detection of actual malicious payloads to prevent catastrophic network breaches). The harmonic mean of these two metrics, the **F1-score**, serves as the primary optimizer to ensure balanced operational safety.

To further maximize generalization capabilities and prevent the underlying estimators from overfitting to transient network anomalies, automated **hyperparameter tuning**—utilizing systematic grid search, randomized search, or Bayesian optimization—is deeply integrated with stratified **k-fold cross-validation**. This rigorous validation pipeline guarantees that the hyperparameter configurations remain highly resilient, adaptive, and stable when subjected to the dynamic and rapidly evolving nature of modern network traffic. Ultimately, this multi-layered, holistic appraisal framework does not merely produce isolated performance metrics; it systematically exposes the structural advantages, computational footprints, and practical trade-offs of diverse methodological approaches (such as supervised classification versus unsupervised anomaly detection), guiding security engineers toward the deployment of an optimized, highly dependable, and production-ready intrusion prevention ecosystem.

Model	Accuracy	Precision	Recall	F1-Score
Random Forest (RF)	95.6%	94.8%	95.0%	94.9%
Support Vector Machine (SVM)	93.4%	92.6%	92.8%	92.7%
K-Nearest Neighbor (KNN)	91.2%	90.5%	90.8%	90.6%
Convolutional Neural Network (CNN)	97.8%	97.5%	97.6%	97.5%
Long Short-Term Memory (LSTM)	98.5%	98.3%	98.4%	98.3%

Table 1 Model Training and Evaluation

Machine Learning Models:

$$\hat{y} = mode\{h_t(x) \setminus t = 1, 2, \cdots, T\}$$

Support Vector Machine (SVM) Optimization:

$$\min_{w,b} \frac{1}{2} \|w\|^2 + C \sum_{i=1}^{N} \xi_i$$

Subject to:

$$y_i (w.x_i + b) \geq 1 - \xi_i, \qquad \xi_i \geq 0$$

K-Nearest Neighbors (KNN) Classification:

$$\hat{y} = mode\{y_i \setminus j \in K\ nearest\ neighbors\ of\ x_i\}$$

Deep Learning Models:

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 4, Issue 3 (2026)

Online ISSN 3007-3197
Print ISSN 3007-3189

http://amresearchreview.com/index.php/Journal/about

1. **Convolutional Neural Network(CNN):**

$$y^{(l)} = f(W^{(l)} * x^{(l-1)} + b^{(l)})$$

2. **Long Short-Term Memory (LSTM) Cell Equations:**

$$f_t = \sigma(W_f . [n_{t-1}, x_t] + b_f)$$

3. **Long Short-Term Memory (LSTM) Cell Equations:**

$$f_t = \sigma(W_f . [h_{t-1}, x_t] + b_f)$$

$$i_t = \sigma(W_i . [h_{t-1}, x_t] + b_i)$$

$$\widetilde{C_t} = \tanh(W_C . [h_{t-1}, x_t] + b_C)$$

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t}$$

$$o_t = \sigma(W_o . [h_{t-1}, x_t] + b_o)$$

$$h_t = o_t * \tanh(C_t)$$

4. **Evaluation Metrics:**
   1. **Accuracy:**

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

   2. **Precision:**

$$Precision = \frac{TP}{TP + FP}$$

   3. **Recall(Sensitivity):**

$$Recall = \frac{TP}{TP + FN}$$

   4. **F1-Score;**

$$F1 = 2.\frac{Precision.Recall}{Precision + Recall}$$

Results

Discussion

Empirical studies show that deep learning classifiers have better performance as compared to classical machine learning classifiers. The Random Forest achieved 95.6 percent accuracy; SVM, 93.4; KNN, 91.2. The CNN scored 97.8, and the LSTM achieved 98.5 indicating their proficiency in recognizing intricate attack behavior

Online ISSN 3007-3197
Print ISSN 3007-3189

patterns. Such results affirm the capability of deep learning models to capture traffic's spatial and temporal fine-grained details, which consequently enhances the detection accuracy and lowers the rate of false negatives

Conclusion

The statistics show that LSTM networks are been capable of identifying the patterns of sequential attacks due to their long-term memory of its previous state. CNNs also record that a strong results in detecting individual spatial relationships in streams of traffic. Although in traditional machine-learning models provide the effectiveness in a particular setting, they are also been limited to using handcrafted features and are less efficient regarding temporal analysis. So the foregrounding of the study is the pragmatic strengths of deployment of deep-learning-based IDS in time-sensitive environments, however though the need to carefully control the computational costs and training times is welcome. Future improvements are been a matter of introducing the concepts of explainable AI functionality in enhance interpretability and build stakeholder trust.

References

Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. ICISSP, 108–116.

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.

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.

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.

Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A Survey of Network-based Intrusion Detection Data Sets. Computers & Security, 86, 147–167.

Li, X., Zhang, Y., & Wang, J. (2025). Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. Artificial Intelligence Review, 58(3), 345–378.

Ahmed, M., Mahmood, A. N., & Hu, J. (2023). HDLNIDS: Hybrid Deep-Learning-Based Network Intrusion Detection System. Applied Sciences, 13(8), 4921.

Zhao, L., Chen, W., & Sun, H. (2025). A hybrid CNN-LSTM approach for intelligent cyber intrusion detection system. Computers & Security, 140, 103047.

9. Kumar, R., & Singh, P. (2024). A Deep Learning Approach for Intrusion Detection Systems in Cloud Computing Environments. Applied Sciences, 14(13), 5381.

Patel, S., & Gupta, R. (2025). Deep learning enabled intrusion detection system for IoT security. Wireless Networks, 31(2), 1125–1140.

Wang, H., Li, Y., & Zhou, Z. (2025). Improving Intrusion Detection Systems by Using Deep Learning Methods on Time Series Data. International Journal of Network Security, 27(4), 312–326.

Online ISSN 3007-3197
Print ISSN 3007-3189

Khan, A., & Ali, F. (2025). Intrusion Detection Using Machine Learning and Deep Learning. International Journal of Advanced Computer Science and Applications, 16(8), 45–56.

Singh, V., & Sharma, K. (2024). Developing an Intrusion Detection System (IDS) for Network Security Using Machine Learning. International Journal of Innovative Science and Research Technology, 9(4), 112–120.

Lopez, R., & Martinez, J. (2024). Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations. Journal of Information Security, 15(2), 101–135.

Ahmed, N., & Khan, Z. (2022). A New Intrusion Detection System for the Internet of Things via Deep Convolutional Neural Network and Feature Engineering. Sensors, 22(10), 3607.