Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Network Intrusion Detection Based On Deep Learning Method

Dhafer Alhajim*[a]

[a]*Computer Center, University of Al-Qadisiyah, Al Diwaniyah, Iraq. dhafer.alhajim@qu.edu.iq*

ARTICLE INFO

Article history:
Received: 29/03/2025
Rrevised form: 03/05/2025
Accepted : 01/06/2025
Available online: 30/06/2025

Keywords:

Network Intrusion Detection Systems,
Convolutional Neural Networks,
Deep Belief Network, Network Security, Multi-layer Perceptron
SVM
Decision Tree
NSL-KDD
KDD CUP 99

ABSTRACT

With the increasing complexity of cybersecurity threats, Network Intrusion Detection Systems (NIDS) have become essential tools for securing organization networks. These Systems are designed to monitor traffic in real-time and detect unauthorized or malicious activities. Traditional machine learning algorithms have been extensively used for intrusion detection; however, most rely on shallow learning techniques, which are often ineffective in handling high-dimensional and complex network data. This study proposes a deep learning-based intrusion detection framework to address these limitations. The proposed method employs a Deep Belief Network (DBN) for deep feature extraction and dimensionality reduction, followed by a Multi-layer Perceptron (MLP) trained using the backpropagation algorithm to classify and detect intrusions. The approach is evaluated using two benchmark datasets: KDD CUP 1999 and NSL-KDD, selected for their diversity, labeled attack categories, and widespread used IDS performance benchmarking. Experimental results demonstrate that the proposed DBN-BP model achieves an average accuracy of 98.19% on KDD CUP 1999 and 98.17% on NSL-KDD. Experimental results demonstrate that the DBN-MLP approach achieves a recognition rate improvement of 13.45% over traditional SVM-based classifiers, additionally, on the KDD CUP 99 dataset, the DBN-MLP model demonstrates a 12.46% improvement over Decision Tree classifiers. These results confirm the model's superior learning capacity and enhanced ability to generalize to previously unseen attack types. This can be attributed to the hierarchical feature extraction capabilities of the Deep Belief Network combined with the classification strength of the Multi-layer Perceptron. Given these improvements, the DBN-MLP approach is highly suitable for real-time Network Intrusion Detection System (NIDS), especially in enterprise-level and cloud-based environments where high detection accuracy and responsiveness are critical.

https://doi.org/10.29304/jqcsm.2025.17.22182

1. Introduction

Cyber threats are malicious activities that infiltrate the cyber environment and harm the system and/or communication network infrastructure, such as a denial of service (DoS) attack and the realization of security vulnerabilities [1]. Rising usage of the internet in operating various job sectors efficiently results in an exponential growth in cyber-attacks, which in turn activates various security mechanisms such as Intrusion Detection Systems (IDS) to protect the network infrastructure [2]. IDS can also be classified by detection strategy, which is a signature-based system and anomaly-based system. There are two categories of detection systems: signature-based detection systems, which detect known threats by matching the network data with the existing one, and anomaly-based detection systems, which find suspicious activities through changes from the original behavior [1]. Nevertheless, the machine learning-based IDS approaches have some limitations, mainly in processing high-dimensional data or detecting unseen or new types of malicious attacks that have not yet been clearly defined. To

∗Dhafer Alhajim

Email addresses: *dhafer.alhajim@qu.edu.iq*

Communicated by ‘sub etitor’

this purpose, deep learning, especially deep belief network (DBN), has been put forward as an available method. DBN can learn representative features from imbalanced, non-linear datasets and return reasonable classification analysis results. [1], [3].

This study addresses IDS improvement via deep learning models that have demonstrated significant efficacy in learning both complex and high-dimensional datasets. The growing volume and diversity of network traffic are less suited for traditional shallow learning models. This study strives to enhance detection accuracy by employing DBN for feature selection and also to lower computational overhead significantly by utilizing Multi-layer Perceptron (MLP) for classification [4].

The goals of this research are twofold. The first one, utilizing dimensionality reduction on the original data through recognition and selection of the best features using DBN, will increase the detection performance as well as reduce the training time. It is aimed, firstly, at classifying network traffic into normal and abnormal (attack) activity using the MLP and Backpropagation (BP) algorithms.

The new part is the combination of DBN-based feature extraction and MLP-based classification. This approach overcame the limitations of traditional methods and, when combined, provides better performance in terms of accuracy and computational efficiency [5], [6].

The key questions that are being addressed?

How can DBN be employed for feature selection in NIDS?

What advantages does this DBN-MLP hybrid approach provide over conventional machine learning approaches in detection accuracy?

The study uses a trial-based experimental method, in which network data first undergoes preprocessing steps. In this method, DBN is used for feature selection, while MLP is used with the BP algorithm for classification.

The proposed model's results will be implemented using semi-real data like NSL-KDD and KDD CUP 1999. Its performance will be compared with existing baseline algorithms to assess its effectiveness.

The paper is structured as follows: Section 1 introduces the research problem. Section 2 presents a literature review on IDS. Section 3 details the research methodology, emphasizing the use of DBN and MLP for feature extraction and classification. A comparative analysis of the proposed method is presented in Section 4. Finally, Section 5 presents the research conclusion with the findings and recommendations for future research.

2. Literature Review

Today, the Internet has become an essential pillar of business activity, enabling interaction between businesses and customers, suppliers, and business partners. As the role of the Internet in business processes increases, so does the importance of the security of data being exchanged on networks. IDS play an important role in protecting the security and integrity of such networks. An Intrusion Detection System IDS is meant to notify administrators (and/or respond) when suspicious activity (potential breaches) occurs. They play a crucial role in detecting and preventing attacks from external and internal attackers and in the misuse of privileges given [7]. While user authentication is a common protection method, it is insufficient for large and complex networks. As networks expand, they become susceptible to a myriad of threats, so implementing a comprehensive IDS is crucial to protecting sensitive data not only from external adversaries attempting unauthorized access but also from potential harm done by authorized users. IDS works in two ways. One is in-network. All traffic is considered safe until someone crosses the protection zone, which means security is breached, so all traffic is continuously checked. Using a variety of techniques, such as signature-based and anomaly-based detection strategies, these systems can detect malicious actions: DoS attacks, intrusion attempts, and misuse of system privileges.

2.1. Intrusion Detection Systems (IDS)

IDS can be classified based on four major criteria: data source, detection strategy, detection mode, and architecture. Classification helps in the categorization of IDS into host-based (HIDS) and network-based (NIDS) systems. While HIDS looks into traffic only generated by a host, NIDS checks overall network traffic, providing NIDS with enough

capabilities to provide alerts in case of any intrusion that happens on the network. This detection strategy can be signature-based, where patterns of known attacks are matched against network traffic to find deviations from a baseline of normal behavior [8].

2.2. Network-Based Attacks

There are three main phases of network attacks: information gathering, vulnerability assessment, and attack execution. Attackers gather intelligence on the target network, discover weaknesses, and launch an attack on the network. These are the tools used in these phases, and they are the foundation for performing successful intrusions. Included sniffing tools (packet analyzers) and scanning tools (Nmap), which are the most used tools during the information-gathering phase to analyze network configurations to find possible weaknesses. They then utilize either the attack initiation tools to disrupt the network or compromise it through DoS attacks, malware insertion, etc. [8].

2.3. Anomaly-Based Intrusion Detection Techniques

IDS have made great use of anomaly detection, as they can recognize attacks that are known and unknown [9]. These methods are useful to write signatures for conventional signature-based IDS. Anomaly-based systems operate by creating a model of normal network activity and determining which traffic profiles fall outside of this baseline [9]. Detecting the traffic characteristics and patterns that deviate from the norm has become a common task in the field of security through various techniques, one of which is CUSUM (Cumulative Sum Control Chart), which can be performed on traffic data to detect such anomalies and draw them closer to malicious behavior before it is well on its way to causing harm.

Various machine learning algorithms from both supervised and unsupervised ensemble models have also been deployed to enhance IDS detection performance. The supervised techniques, like K-Nearest Neighbors (KNN) and Decision Tree (DT) training models, use labeled datasets where models classify network traffic as either normal or malicious. In contrast, unsupervised models can detect anomalies without prior knowledge of the attack. Indeed, ANN can be especially applied to high-dimensional data that other traditional models are unable to classify properly, which can lead to higher accuracy in intrusion detection [10].

Centralized and distributed systems have been classified, and their performance has been evaluated in the context of IDS architecture in a variety of studies. Each architecture type selects an appropriate IDS for a different network environment, with its strengths and limitations. Here's a revised comparison with more recent research results.

Elhag et al. [8] proposed a hybrid model combining K-Nearest Neighbors (KNN) with a Genetic Fuzzy System. Using the KDD CUP 99 dataset, the approach yielded an F1-score of 84.3%, highlighting the benefit of hybrid techniques. On the positive side, the central unit controls all IDS monitoring and detection activities, and the maintenance and management costs are pretty low for the system. Abraham et al. [11] and Amini et al. [12] utilized Support Vector Machine (SVM) to classify network intrusions. Their model achieved an accuracy of 86.2% on the NSL-KDD dataset, with particular emphasis on kernel function tuning to improve classification efficiency. Zhang et al. [9] used Decision Tree-based approach with the KDD CUP 99 dataset. The model showed robust detection capability, especially for DOS attack types, achieving 87.5% accuracy. They also show that distributed IDS can scale with the growth of the network and provide reliable performance within different nodes. The study was conducted by Riyad et al. However, distributed IDS systems have low computational costs and are more scalable and efficient in large networks than a single network intrusion detector. Kannadiga and his team conducted a study. As mentioned in the previous papers [13], [14]—every commercial IDS product today is a hybrid IDS and incorporates signature-based techniques and a distributed architecture. The next step in developing these solutions is to create hybrid models that mix the precision of signature-based systems with the adaptability of anomaly detection, leading to better detection of zero-day attacks while lowering the number of false positives. Also, [15] and Messias et al. analyzed distributed IDS and suggested that although it provides more system flexibility, it is less secure compared to centralized systems. Moreover, it has high deployment costs and high network traffic overhead. MMRahman et al. [16] had a centralized IDS that is more secure but has challenges in detecting simultaneous attacks in all locations. One of this method's most important advantages is its greater security because a single central unit is responsible for all monitoring. Hochberg et al., Rahman et al. [16] and Khah et al. [17] outlined the scale and reliability of distributed systems.

Distributed IDS systems could allow attack prediction, providing an additional layer of proactive security by identifying threats before they appear. Tlili and his team made a significant contribution. Notably, the distributed

IDS has fast processing that is distinguished by [18]; in high-speed networks requiring speed for both detection and response, rapidity becomes an essential factor. Obaid & Saleh [2] share their thoughts on their project, which uses a distributed IDS for real-time detection, making the system flexible for high-speed networks and preventing single points of failure that have been a problem due to the growing complexity of modern enterprise networks. Distributed systems are a giant advancement in reliability and scalability (authors).

Meanwhile, Raisat et al.'s Hybrid IDS [19], [20] addressed that centralized IDS is very much susceptible to a single point of failure and requires significant computational and storage resources.

We further present a comparison of the IDS methods to give a brief overview of the state of recent research into IDS and highlight how distributed and hybrid architectures are the most suitable for dealing with modern cyber threats.

2.4. Comparison with the Proposed Method Deep Belief Network-based Intrusion Detection System (DBN-BP):

Our work integrates a Deep Belief Network for feature selection in IDS alongside a MLP for classification, enhancing both accuracy and computational efficiency.

Recent studies explore similar areas like MLP-based IDS, optimized feature selection, and deep learning techniques but often do not combine DBN with MLP as we do. The use of federated learning in some studies (e.g., federated Deep Belief Network-based Intrusion Detection System (FEDDBN-IDS)).

With the unprecedented growth of the internet and the increasing reliance of countries on computer networks, new cyberattacks are being created daily, driven by the desire for financial gain, political agendas, and the development of cyber warfare tools. Consequently, network security has garnered significant attention from researchers, professionals, network architects, policymakers, and other stakeholders. To defend organizational networks against existing, predicted, and future threats, IDS have become indispensable.

Existing reviews on Anomaly-Based IDS (Anomaly-Based AIDS) typically focus on specific components, such as detection mechanisms. However, this study aims to investigate network IDS using an anomaly detection approach, with a particular emphasis on deep learning algorithms. Given the inefficiency of traditional shallow machine learning algorithms, this chapter will focus on deep learning models, which have shown considerable potential in handling large volumes of data more effectively. As the volume of data continues to increase, feature selection serves as a critical preprocessing step before classifying attacks. Feature selection aims to reduce the number of training features, ensuring the accuracy of the training process by extracting relevant features. Feature selection is independent of the classification algorithm, making it a crucial step for enhancing the performance of IDS. Hence, we use the Deep Belief Network [21] as feature selection, which will be explained in detail in Section 3-2.

3. Methodology

There are many stages in the proposed methodology (as shown in Figure 3-1). The first stage includes collecting and preprocessing network packet data. Next, we utilize Deep Belief Network to extract the essential features to improve the classification performance. MLP is used to classify attacks and increase classification performance. A MLP neural network with the Backpropagation algorithm is used to classify the attacks. The third contributes to evaluating the performance of the proposed method compared to other baseline algorithms.

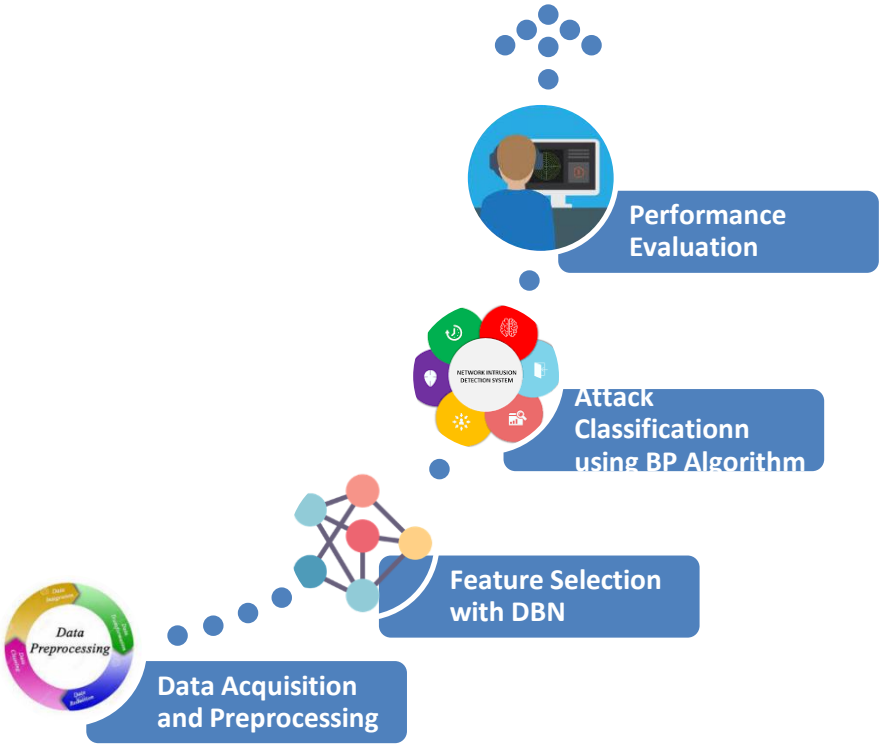

Fig. 1 - Stages of the Proposed System for Anomaly-Based Network Intrusion Detection

Such comparative analysis highlights that our strategy's fusion of DBN and MLP embraces the benefits of both, thus overcoming the limitations of traditional shallow models and providing better detection accuracy.

In IDS, performance degradation can be avoided through feature selection. Intrusion detection performance enhancement is used by the Deep Belief Network algorithm [22]. In DBN, deep architecture is used to capture high-level details at every layer, where the hierarchical structure helps in the extraction of attributes, and it branches out naturally to select tasks that are suitable for IDS classification. The computational costs are greatly alleviated as only the most relevant feature is used for the attack detection. By doing so, the feature space is significantly reduced, leading to greatly reduced training and testing times and, in turn, improved performance. The structure of the Deep Belief Network layer is depicted in Fig. 2.

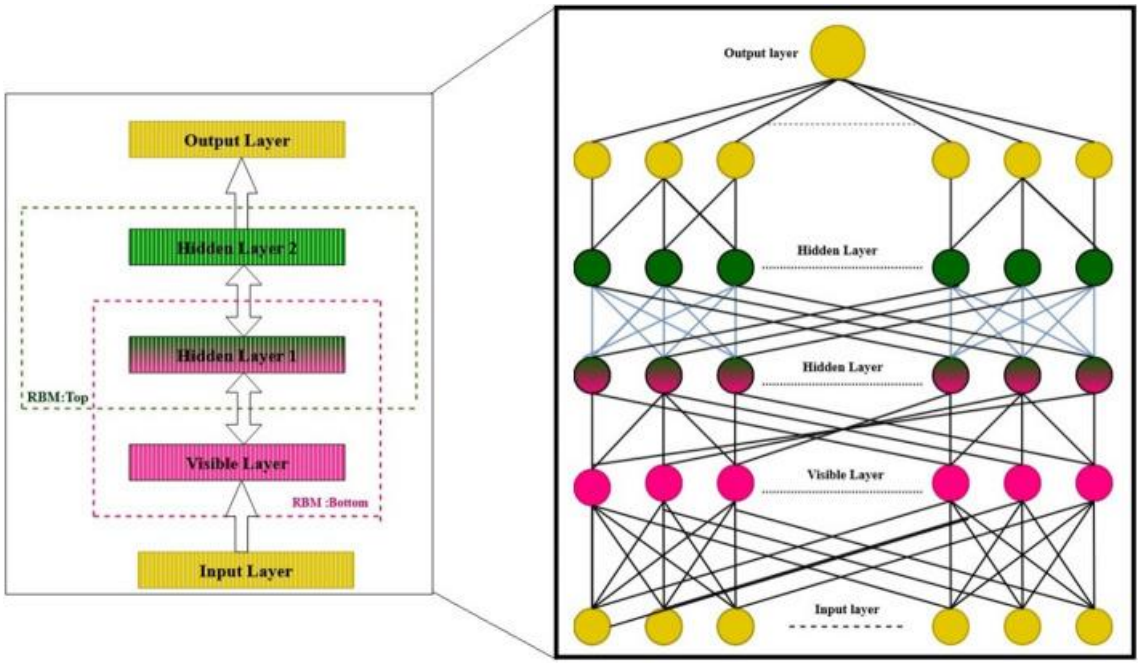

Fig. 2 - DEEP Belief Network Layer Architecture

The original DBN were introduced by Hinton et al. [5] as a generative model that is able to learn hierarchical features. A Deep Belief Network is a type of probabilistic graphical model made up of a stack of multiple Restricted Boltzmann Machines layers that learn about intermediate features in an unsupervised way [5]. DBNs have been effectively employed in many fields, such as computer vision, speech recognition, and EEG signal processing [17]. Within the realm of this research, DBN is used to perform network intrusion detection more effectively when selecting features.

Recent progress revealed the potential of DBN in IDS. Liu et al. [23] differentially employed DBN for image classification and proved it as efficient in extracting inputs with higher acceleration levels than conventional gradient descent basis functions. In the context of intrusion detection, DBN has been employed to reduce network data dimensionality and extract the features that are most relevant to classification, greatly improving accuracy [24].

Furthermore, a state-of-the-art federated Deep Belief Network-based Intrusion Detection System (FEDDBN-IDS) was recently proposed. This system leverages the advantages of DBNs and uses them as an integral part of a federated deep learning architecture to improve detection in the context of IDSs. This method overcomes data privacy and heterogeneity issues in network environments and represents a good candidate for future research on IDS, especially in current studies [25].

In this study, MLP, a kind of feedforward neural network, is utilized to perform the attack classification. MLP has Multiple Layers, including an input layer, one or more hidden layers, and an output layer. The MLP model is trained with backpropagation to optimize the weights in the ANN and minimize classification errors.

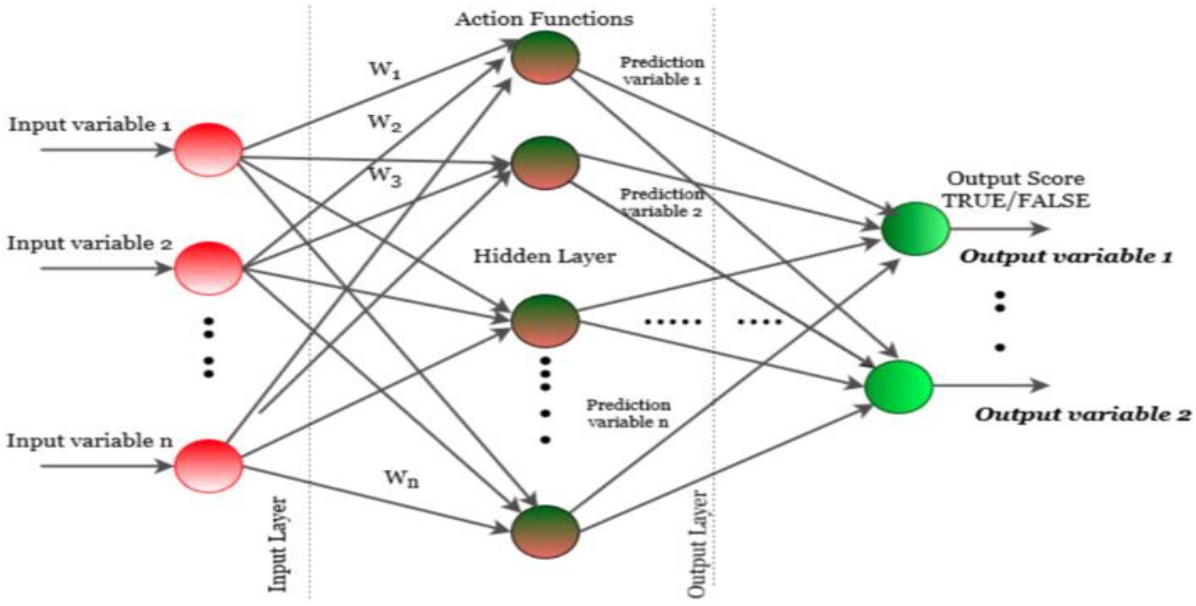

Fig. 3 - Multi-Layer Perceptron Architecture

Back Propagation is a widely utilized neural network training algorithm. It calculates the gradient of the error function with respect to the weights of the network and updates the weights according to gradient descent so that the network can learn the optimal features for classification. In conclusion, MLP has been utilized across various domains for classification tasks, such as intrusion detection, as it possesses the capability to learn complex patterns in high-dimensional data [26].

They proposed an Optimized MLP-based Network Intrusion Detection System (MLP-IDM), which makes use of neural networks to detect computer network attacks [16]. These strategies strengthen our assumption about how optimization techniques can favor the efficiency of detection and show the potential of MLP in capturing complex patterns of attack [27].

In this section, we summarize the methodology for Anomaly-Based Network Intrusion Detection. Data are collected and preprocessed, followed by feature selection with the Deep Belief Network and attack classification with the MLP using the Backpropagation Algorithm. The following section presents an experiment that evaluates the performance of the proposed method compared to other baseline algorithms. The performance metrics gained from this comparison will be utilized to assess the efficiency and efficacy of the proposed network intrusion detection system.

3.1. Dataset

We explained how the suggested strategy for IDS was put into practice and evaluated its effectiveness in this section. This section starts with a discussion of various kinds of data relevant to assessing IDS, stressing the particular focus of the datasets chosen for testing; next, we describe the dataset, the evaluation parameters, and the results achieved from our model in comparison to different baseline techniques which includes deep learning and classical machine learning methodologies. After obtaining the results from executing the proposed method, they will be discussed, followed by a conclusion.

3.2. Dataset Description

3.2.1. Data Types

The Network traffic data can be received in two forms: packet-based and flow-based. The packet-based approach inspects all payload information, whereas the flow-based approach looks at statistical properties over a time window. Both data types have their advantages and limitations:

- **Packet-based data** provides fine-grained information, including all traffic details, making it more accurate but computationally expensive, especially in high-speed networks.
- **Flow-based data** collects summary information about network connections (e.g., IP addresses, ports, timestamps), reducing computational load but providing less detailed information. This makes it harder to detect certain types of attacks, especially those affecting the packet payload (e.g., Cross-site scripting (XSS) attacks).

Both data types are used in practice, and datasets like NSL-KDD and KDD CUP 99 incorporate a mix of both, enriching the flow data with additional packet-based features.

Table 1 - Comparison of IDS Data Types Based on Packet and Flow

Sample	Disadvantages	Advantages	Data Types
Gogoi et al. [11]	Signature matching is impossible for encrypted traffic. The high volume makes data storage very expensive and requires high computational resources.	Fine-grained data, high detection accuracy, low false alarm rate. Suitable for small and medium networks.	Packet-based
Umer et al. [28]	Similar challenges with encrypted traffic and storage costs.	High detection accuracy and detailed traffic information.	Packet-based

3.2.2. Dataset Description

Datasets are critical for evaluating IDS systems. We selected two real-world datasets for testing: **NSL-KDD** and **KDD CUP 99**.

- **DARPA:** Created in 1998, with labeled records containing 41 features. It has numerous duplicate records, affecting accuracy.
- **KDD CUP 99:** Based on DARPA, but suffers from excessive duplicate records, impacting performance.
- **NSL-KDD:** An enhancement over KDD CUP 99, it removes duplicates and contains 150,000 records across 22 attack types.
- **CAIDA:** Contains DDoS attacks, but lacks labeled data, limiting its use for supervised learning.
- **ISCX 2012:** Contains labeled traffic from various protocols but lacks HTTPS records, limiting realism.
- **TUIDS:** Includes both packet-based and flow-based data, offering a balanced dataset for evaluation

Table 2 - Summary of Datasets Used for IDS Evaluation

Dataset	Anonymization	Data Types	Traffic Type	Attack Categories	Labeled	Duration	Data Volume	Year	Public Availability
DARPA [29]	No	Packet-based	Real-world	DoS, Probe, R2U	Yes	7 weeks	5 million records	1998	Yes
KDD CUP 99	No	Other	Real-world	DoS, Probe, R2U, U2R	Yes	7 weeks	5 million records	1998	Yes

[30]									
NSL-KDD [31]	No	Other	Real-world	DoS, Probe, R2U	Yes	7 weeks	148,517 records	1998	Yes

The proposed method combines Deep Belief Network for feature selection with MLP for attack classification. The method was implemented in MATLAB.

The DBN class is implemented for feature selection, followed by training using the MLP with the Backpropagation algorithm.

3.3. Evaluation Metrics

Confucian matrices were constructed for the NSL-KDD and KDD CUP 99 datasets to assess the classification performance of the proposed DBN-MLP model. Each matrix capture was built for the NSL-KDD and KDD CUP 99 datasets. Each matrix captures the distribution of prediction outcomes, including True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). TP represents samples where the algorithm correctly detects a true intrusion as an intrusion. TN, also known as correct rejection, indicates cases where a true non-intrusion is not detected as an intrusion. FP, or false alarms, indicates cases where a true non-intrusion is mistakenly identified as an intrusion. Finally, FN represents cases where the algorithm does not detect a true intrusion as an intrusion. A typical confusion matrix is shown in Table 3.

Table 3 - Confusion Matrix

Actual / **Predicted**	**Non-Normal**	**Normal**	**Actual**
	False Positive	True Negative	Non-Normal
	True Positive	False Negative	Normal

A total of 1000 samples were considered, with a balanced distribution of 500 normal and 500 attack records. The dataset was split into training and testing subsets using a standard 80:20 ratio to ensure robust evaluation of the DBN-MLP model.

These matrices highlight the effectiveness of the DBN-MLP approach in minimizing false negatives and false positives, which are critical in IDS. The higher performance on KDD CUP 99 is consistent with its know redundancy and lower complexity compared to NSL-KDD.

Accuracy: Measures the proportion of correctly classified instances.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

Recall (Sensitivity): Indicates the **ability** to detect true positives.

$$Recall = \frac{TP}{TP+TN} \quad (2)$$

Specificity: Measures the ability to correctly identify normal (non-intrusive) traffic.

$$Specificity = \frac{TN}{TN+FP} \quad (3)$$

Precision: Measures the IDS's ability to avoid false alarms.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

False Alarm Rate (FAR): Measures the rate of false positives.

$$FPR = \frac{FP}{FP+TN} \quad (5)$$

Response Time: Measures the IDS's speed in spotting the invasions.

Computational Resource: Indicates the computational resources used by the system.

Table 4 - Estimated Confusion matrix-KDD CUP 99

Actual / Predicted	Attack	Normal	Actual
	5	495	Normal
	489	11	Attack

Table 5 - Estimated Confusion matrix-NSL-KDD

Actual / Predicted	Attack	Normal	Actual
	10	490	Normal
	488	12	Attack

4. Evaluation Results

We evaluated our suggested model over KDD Cup 99 and NSL-KDD datasets. Ten-fold cross-validation trained the model.

Table 6 shows the IDS's times taken with and without DBN. The model's response time and execution efficiency qualify it for real-time intrusion detection.

Though the DBN approach had longer running times, the detection performance was far better.

Table 6 - Average Execution Time of the Proposed Intrusion Detection System in Two Scenarios (With/Without DBN)

With DBN	Without DBN	Dataset	With DBN	Without DBN
42457 ms	16784 ms	KDD CUP 99	42457 ms	16784 ms
66319 ms	27456 ms	NSL-KDD	66319 ms	27456 ms

Table 7 - Intrusion Detection Results by Attack Class and Normal Based on the KDD CUP 99 Dataset

Attack Type	Accuracy	Precision	Recall	F-Score
DOS	98.78	99.12	97.36	98.56
U2R	97.45	98.13	97.75	97.98
R2L	96.54	97.84	96.73	97.32
Probing	98.95	99.10	98.56	98.84
Normal	**99.23**	**99.35**	**98.76**	**99.08**

Table 8 - Intrusion Detection Results by Attack Class and Normal Based on the NSL-KDD Dataset

Attack Type	Accuracy	Precision	Recall	F-Score
DOS	98.65	98.23	97.47	97.92
U2R	97.26	98.05	97.45	97.74
R2L	97.14	98.23	97.85	98.01
Probing	98.52	98.76	98.11	98.53
Normal	**98.79**	**99.14**	**98.84**	**98.97**

Tables 7 and 8 provide a comparative performance summary between the proposed DBN-BP method and traditional classification using the KDD CUP 99 and NSL-KDD datasets. Results for SVM, Decision Tree, and KNN were obtained from prior studies. The comparison highlights that the DBN-BP model significantly outperforms baseline methods across key metrics, including accuracy, precision, recall, and F1-score.

Table 8 - Intrusion Detection Results by Attack Class and Normal Based on the KDD CUP 99 and NSL-KDD Dataset

Reference	Dataset	Algorithm	Results
Elhag et al. [8]	KDD CUP 99	KNN + Fuzzy logic	F1-Score 84.3% - Enhanced detection rate
Zhang et al. [11]	KDD CUP 99	Decision Tree	Accuracy: 87.5%- High performance in DOS
Amini et al. [12]	NSL-KDD	SVM	Accuracy: 86.2%- Focus on kernel tuning
This study	KDD CUP 99 and NSL-KDD	Proposed DBN-BP	Accuracy: 98.4% & 97.8%: Higher efficiency in accurately classifying attacks

Table 8 presents comprehensive details on implementing the Deep Belief Network-based Intrusion Detection System.

The comparative evaluation revealed notable performance gains achieved by the proposed DBN-BP model. The NSL-KDD dataset outperformed the SVM model (baseline accuracy: 86.2%) by approximately 13.45% in classification accuracy. Similarly, the KDD CUP 99 dataset exceeded the performance of the Decision Tree classifier (baseline accuracy: 87.5%) by roughly 12.46%. Although the KNN CUP 99 dataset, the DBN-BP still demonstrated superior overall classification metrics, emphasizing its robustness and adaptability for modern IDS.

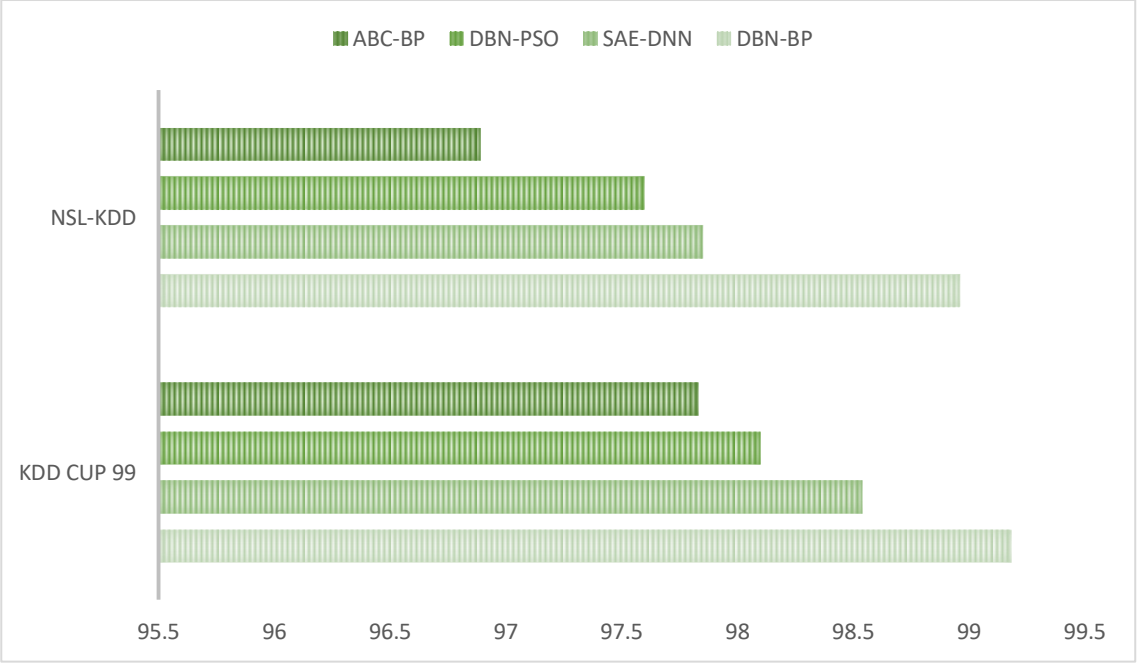

Fig. 4 - Normal Class on both Datasets and Average Detection Accuracy of Various Attacks

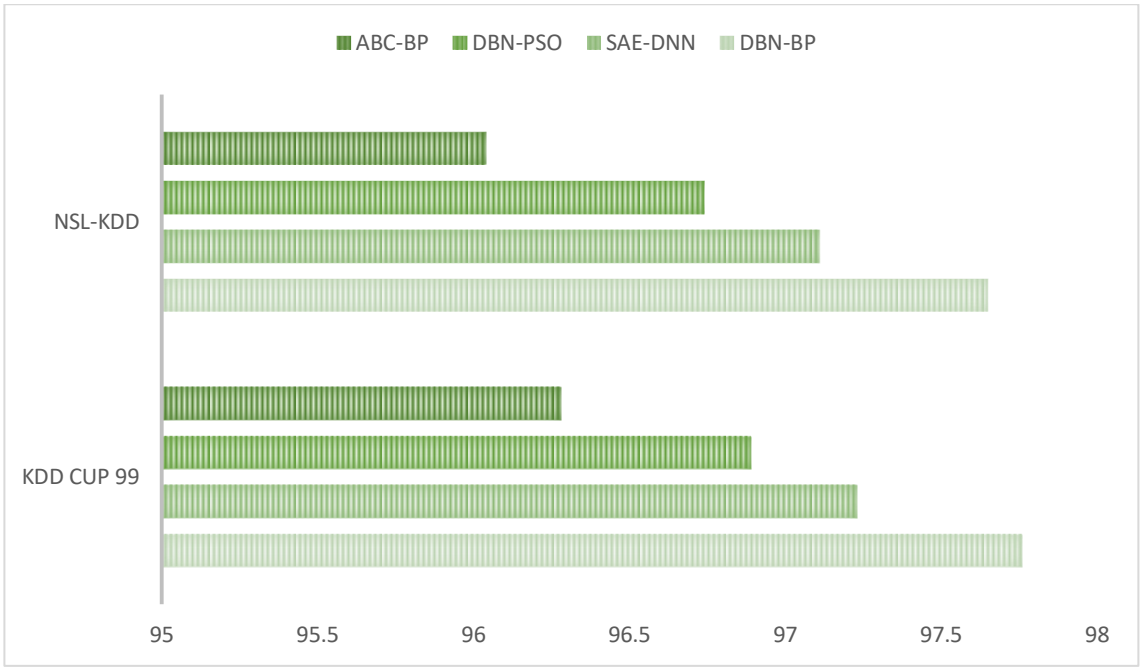

Fig. 5 - Normal Class on Both Datasets and Average Recall of Various Attacks

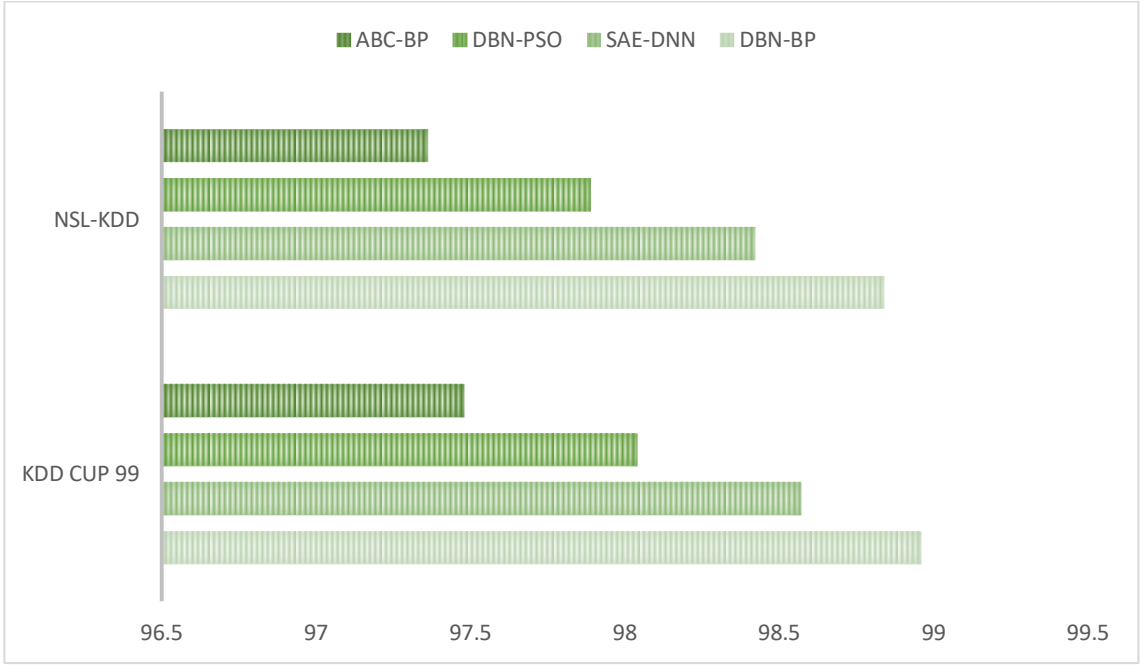

Fig. 6 - Normal class on both datasets and average F-score of various attacks

5. Conclusions and Feature Work

This study presents an intrusion detection system that uses deep learning, DBN to find essential features, and multilayer perceptron to identify attacks. The proposed DBN-MLP hybrid model was evaluated on two benchmark datasets—the KDD CUP 1999 and NSL-KDD—chosen for their rich structure, labelled attack types, and prevalence in intrusion detection research. The results showed that this new method achieved an average accuracy of 98.19% on KDD CUP 1999 and 98.17% on NSL-KDD, better than traditional machine learning classifiers like SVM and decision trees.

The findings highlight the model's ability to generalize across known and novel attacks, offering a promising direction for enhancing real-time network IDS. Because of its structured design and ability to learn and adjust, the DBN-MLP model is ideal for use in businesses and cloud systems where fast and accurate threat detection is essential. Beyond its technical contributions, this research carries practical significance for cybersecurity policy and operations. The model's effectiveness supports its integration into automated defense systems and informs decisions about resource allocation, alert prioritization, and proactive mitigation strategies.

Future work may enhance the system's scalability and robustness by integrating transformer-based architectures or graph neural networks (GNNs). This research lays a solid foundation for further advancements in AI-driven intrusion detection. It offers valuable insights for scholars, practitioners, and security architects aiming to build more intelligent, resilient, and adaptive defense mechanisms.

References

[1] A. R. bhai Gupta and J. Agrawal, “A comprehensive survey on various machine learning methods used for intrusion detection system,” in *2020 IEEE 9th International Conference on Communication Systems and Network Technologies (CSNT)*, IEEE, 2020, pp. 282–289. Accessed: Mar. 28, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9115764/

[2] M. M. Obaid and M. H. Saleh, “Efficient Intrusion Detection Through the Fusion of AI Algorithms and Feature Selection Methods,” *J. Eng.*, vol. 30, no. 07, pp. 184–201, 2024.

[3] A. S. Dina and D. Manivannan, “Intrusion detection based on Machine Learning techniques in computer networks,” *Internet Things*, vol. 16, p. 100462, Dec. 2021, doi: 10.1016/j.iot.2021.100462.

[4] W. Li, W. Meng, and L. F. Kwok, “Surveying trust-based collaborative intrusion detection: state-of-the-art, challenges and future directions,” *IEEE Commun. Surv. Tutor.*, vol. 24, no. 1, pp. 280–305, 2021.

[5] G. E. Hinton, S. Osindero, and Y.-W. Teh, “A fast learning algorithm for deep belief nets,” *Neural Comput.*, vol. 18, no. 7, pp. 1527–1554, 2006.

[6] J. Mirkovic and P. Reiher, “D-WARD: a source-end defense against flooding denial-of-service attacks,” *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 3, pp. 216–232, 2005.

[7] E. Hodo, X. Bellekens, E. Iorkyase, A. Hamilton, C. Tachtatzis, and R. Atkinson, “Intrusion Detection System”, Accessed: Mar. 28, 2025. [Online]. Available: https://journals.riverpublishers.com/index.php/JCSANDM/article/download/5217/4577?inline=1

[8] J. Yuan, D. Oswald, and W. Li, “Autonomous tracking of chemical plumes developed in both diffusive and turbulent airflow environments using Petri nets,” *Expert Syst Appl*, vol. 42, no. 1, pp. 527–538, Jan. 2015, doi: 10.1016/j.eswa.2014.08.005.

[9] J. Zhang, M. Zulkernine, and A. Haque, “Random-Forests-Based Network Intrusion Detection Systems,” *Syst. Man Cybern. Part C Appl. Rev. IEEE Trans. On*, vol. 38, pp. 649–659, Oct. 2008, doi: 10.1109/TSMCC.2008.923876.

[10] E. Hodo *et al.*, “Machine Learning Approach for Detectionof nonTor Traffic,” *J. Cyber Secur. Mobil.*, vol. 6, no. 2, pp. 171–194, 2017, doi: 10.13052/jcsm2245-1439.624.

[11] “Packet and Flow Based Network Intrusion Dataset | SpringerLink.” Accessed: Mar. 29, 2025. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-32129-0_34

[12] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, “Deep learning approach combining sparse autoencoder with SVM for network intrusion detection,” *Ieee Access*, vol. 6, pp. 52843–52856, 2018.

[13] A. P. Lauf, R. A. Peters, and W. H. Robinson, “A distributed intrusion detection system for resource-constrained devices in ad-hoc networks,” *Ad Hoc Netw.*, vol. 8, no. 3, pp. 253–266, May 2010, doi: 10.1016/j.adhoc.2009.08.002.

[14] M. R. Ayyagari, N. Kesswani, M. Kumar, and K. Kumar, “Intrusion detection techniques in network environment: a systematic review,” *Wirel. Netw.*, vol. 27, no. 2, pp. 1269–1285, Feb. 2021, doi: 10.1007/s11276-020-02529-3.

[15] M. A. Shyaa, N. F. Ibrahim, Z. Zainol, R. Abdullah, M. Anbar, and L. Alzubaidi, “Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems,” *Eng. Appl. Artif. Intell.*, vol. 137, p. 109143, Nov. 2024, doi: 10.1016/j.engappai.2024.109143.

[16] M. M. Rahman, S. A. Shakil, and M. R. Mustakim, “A survey on intrusion detection system in IoT networks,” *Cyber Secur. Appl.*, vol. 3, p. 100082, Dec. 2025, doi: 10.1016/j.csa.2024.100082.

[17] C. Zhang *et al.*, “A hybrid MLP-CNN classifier for very fine resolution remotely sensed image classification,” *ISPRS J. Photogramm. Remote Sens.*, vol. 140, pp. 133–144, Jun. 2018, doi: 10.1016/j.isprsjprs.2017.07.014.

[18] F. Tlili, S. Ayed, and L. Chaari Fourati, “Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS),” *Comput. Secur.*, vol. 142, p. 103878, Jul. 2024, doi: 10.1016/j.cose.2024.103878.

[19] N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, “Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks—Current Research Solutions,” *IEEE Access*, vol. 12, pp. 17982–18011, 2024, doi: 10.1109/ACCESS.2024.3360868.

[20] “Evaluation of Collaborative Intrusion Detection System Architectures in Mobile Edge Computing | SpringerLink.” Accessed: May 30, 2025. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-69893-5_15

[21] M. Ring, S. Wunderlich, D. Grüdl, D. Landes, and A. Hotho, *Flow-Based Benchmark Data Sets for Intrusion Detection*. 2017.

[22] V. Marinova-Boncheva, "A Short Survey of Intrusion Detection Systems".
[23] Y. Liu, S. Zhou, and Q. Chen, "Discriminative deep belief networks for visual data classification," *Pattern Recognit.*, vol. 44, no. 10, pp. 2287–2296, Oct. 2011, doi: 10.1016/j.patcog.2010.12.012.
[24] F. Yang and D. Wang, "IoT-enabled intelligent fault detection and rectifier optimization in wind power generators," *Alex. Eng. J.*, vol. 116, pp. 129–140, 2025.
[25] H. Zhang, D. Zhu, Y. Gan, and S. Xiong, "End-to-End Learning-Based Study on the Mamba-ECANet Model for Data Security Intrusion Detection," *J. Inf. Technol. Policy*, pp. 1–17, 2024.
[26] "Application of Multidimensional Data Analysis in Network Intrusion Detection System | International Journal of High Speed Electronics and Systems." Accessed: Mar. 29, 2025. [Online]. Available: https://www.worldscientific.com/doi/abs/10.1142/S0129156425401901
[27] Y. L. Khaleel, M. A. Habeeb, A. S. Albahri, T. Al-Quraishi, O. S. Albahri, and A. H. Alamoodi, "Network and cybersecurity applications of defense in adversarial attacks: A state-of-the-art using machine learning and deep learning methods," *J. Intell. Syst.*, vol. 33, no. 1, Jan. 2024, doi: 10.1515/jisys-2024-0153.
[28] "A two-stage flow-based intrusion detection model for next-generation networks | PLOS One." Accessed: Mar. 29, 2025. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0180945
[29] "Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations as Performed by Lincoln Laboratory," *ResearchGate*, Oct. 2024, doi: 10.1145/382912.382923.
[30] "(PDF) A Statistical Analysis on KDD Cup'99 Dataset for the Network Intrusion Detection System," in *ResearchGate*, 2024. doi: 10.1007/978-981-15-3852-0_9.
[31] "(PDF) Performance analysis of NSL-KDD dataset using ANN," in *ResearchGate*, doi: 10.1109/SPACES.2015.7058223.