Open Access

Recent Progress in Science and Engineering

LIDSEN Publishing Inc.

Original Research

Artificial Neural Network-Based Intelligent Framework for Multiclass Network Intrusion Detection in Modern Cybersecurity Systems

Ankit Kumar Singh [1], Aastha Singh [1], Avanish Kant Agnihotri [1], Amit Trivedi [2], Mohd Nadeem [1,*]

1. Department of Computer Science and Engineering, Shri Ramswaroop Memorial University, Barabanki, India; E-Mails: ankitsingh301292@gmail.com; aasthasingh158@gmail.com; avanish.agnihotri@gmail.com; mohd.nadeem1155@gmail.com
2. Institute of Management Commerce and Economics, Shri Ramswaroop Memorial University, Barabanki, India; E-Mail: amittrivedi.acd@srmu.ac.in

* **Correspondence:** Mohd Nadeem; E-Mail: mohd.nadeem1155@gmail.com

Academic Editor: Yousef Farhaoui

Special Issue: Recent Advances in Cyber Security

Recent Prog Sci Eng
2026, volume 2, issue 3
doi:10.21926/rpse.2603014

Received: March 12, 2026
Accepted: June 22, 2026
Published: July 01, 2026

Abstract

The advent of cloud computing, the Internet of Things (IoT), and digital services has led to an increase in the number and complexity of cyberattacks. The intrusion detection methods currently used, based on machine learning and artificial intelligence, include SVM, random forest, deep learning, convolutional neural networks, and LSTM. These methods are more advanced than the signature method since they are more efficient. However, despite these advancements, several issues with intrusion detection systems remain. They include high false-positive rates, computational complexity, limited scalability, inability to detect zero-day attacks, and poor real-time performance. To overcome such challenges, this paper suggests the development of an intelligent system for network intrusion detection using artificial neural networks (ANNs). This method is intended to increase the accuracy of cyber threat detection and minimize the number of false positives through adaptive and nonlinear learning. Data preprocessing, data encoding, feature normalization, feature selection, and feedforward neural networks are some of the methods employed in the classification of

data traffic into malicious and normal traffic. The types of intrusions considered in this study include DoS, Probe, R2L, and U2R attacks. According to experiments performed using intrusion detection benchmark data, the proposed ANN algorithm delivers accuracy, precision, recall, and F1 score values of 97.6%, 96.8%, 97.2%, and 97.0%, respectively, while maintaining a low false-positive ratio of only 2.1%. The comparative analysis further demonstrates that the ANN classifier outperforms other classification techniques, such as random forests, decision trees, and support vector machines. The findings thus demonstrate that the ANN can be successfully used for detecting attacks and improving the security of networks, cloud computing, and the IoT.

Keywords
Artificial neural network; network intrusion detection; cybersecurity; machine learning; network security; intelligent security systems

1. Introduction

The rapid growth of digital technologies, cloud computing, and vast global networks has radically transformed modern communication and data transfer systems. However, through this technological advancement, cyber threats and network intrusions have increased dramatically [1]. Networks are significant infrastructures that store and relay sensitive information in organizations across various sectors, including health, financial, government and education. As such, cyber attackers are constantly exploiting vulnerabilities in these systems, resulting in disastrous financial, operational, and reputational losses [2]. Traditional security measures, such as firewalls and signature-based IDSs, might be weak in detecting advanced and dynamic network attacks. Given that existing systems utilize predetermined attack signatures, their ability to detect novel or unknown threats is fundamentally limited. The growing complexity of cyber threats has created a need for the development of smart and flexible security systems that can analyze and assess network traffic and thereby identify deviations from the norm. The application of machine learning (ML) and artificial intelligence (AI) is considered a potential means of refining network security. ANNs are among these approaches and have gained considerable attention for their ability to identify intricate patterns from large volumes of data and detect abnormalities in network traffic. ANN models can automatically identify valuable patterns in high-dimensional data and correctly classify normal and suspicious network activities. In terms of these abilities, ANN-based intrusion detection systems can increase their detection rate, reduce false alarm rates, and be flexible to novel attack schemes [3, 4].

In recent years, several authors have explored machine learning-based network intrusion detection systems. These studies have employed algorithms such as support vector machines, decision trees, random forests, and deep learning models to categorize network attacks [5, 6]. Although these methods have been demonstrated to provide superior performance to traditional methods in detecting attacks, the majority of contemporary systems continue to suffer from the problems of feature selection, computational complexity, scalability, and the ability to detect zero-day attacks. Furthermore, most models struggle to achieve both high detection rates and low

false-positive rates in real-time network environments. Artificial neural networks provide a solution that is as strong as it provides the prospect of adaptive learning and nonlinear pattern recognition [7]. ANN-based models are capable of efficiently handling massive network traffic in addition to identifying nuanced variations that may indicate a potential cyber intrusion. Such systems are capable of detecting different types of network attacks, such as denial of service (DoS), probe attacks, remote-to-local (R2L), and user-to-root (U2R) attacks [8, 9]. ANNs enhance the precision and reliability of intrusion detection systems in ever-changing network structures using efficient feature selection and data blocking methodologies. The rising cost of cyber attacks highlights the need for more sophisticated intrusion detection systems. Organizations worldwide experience significant financial losses due to data theft, ransomware, and network intrusions. The increasing cost of cybercrime highlights the need for smart and automated protective solutions. This table (mentioned in Table 1) defines the economic loss from cybercrime worldwide. These financial losses indicate the increasing relevance of cybercrime to the global economy. The unique constraints and sophistication of cyber attacks demand that smart detection systems recognize adverse actions before the actions have devastating effects [10].

Table 1 Global Monetary Loss Due to Cybercrime (2020-2026).

Year	Estimated Global Cybercrime Loss (USD)	Major Contributing Factors
2020	$1 Trillion	Rapid digital transformation and ransomware attacks
2021	$6 Trillion	Large-scale data breaches and phishing attacks
2022	$7 Trillion	Growth of ransomware-as-a-service
2023	$8 Trillion	Increased attacks on cloud infrastructure
2024	$9.5 Trillion	IoT vulnerabilities and AI-powered attacks
2025	$10.5 Trillion	Expansion of smart networks and automated cyber threats
2026	$12 Trillion (Projected)	Advanced persistent threats and global cyber warfare

Research Gap: Despite the increasing amount of literature on machine learning-based intrusion detection systems, a number of gaps still exist.

- Most of the current models for intrusion detection procedures are based on traditionally trained machine learning algorithms that are unable to capture sophisticated nonlinear relationships among network traffic data.
- Some studies report reasonable detection rates, but they fail to address the problem of high false positive rates, which can cause system alarms and lead to inefficient system operation.
- Most of the existing approaches are unable to provide sufficient flexibility and scalability to accommodate the large-volume and large-scale real-time network traffic of modern distributed systems.
- With respect to the optimization of artificial neural network architectures in multiclass intrusion detection in various types of attacks, little has been done.
- Many models in use today still fail to identify zero-day attacks or new patterns of intrusions.

H1: In comparison with existing machine learning algorithms, such as decision trees, SVMs, and random forests, the intrusion detection method based on an artificial neural network can be highly efficient in identifying multiclass network intrusions. Such improvements could be made

because of better classification accuracy, precision, recall, and F1 score, along with a reduced number of false positives. Various performance metrics and benchmark network intrusion detection datasets are used to test the efficiency of the proposed method.

Because of cyber threats and the financial and operational impacts of network intrusions, the artificial neural network (ANN)-based model proposed in this research will assist in improving cybersecurity by identifying cyber threats early and safeguarding sensitive information. The proposed model maximizes the reliability and extent of intrusion detection systems (IDSs) in modern network systems. With neural networks' capabilities, the model will also reduce or eliminate false alarms. Additionally, the model performs manual preprocessing and adjusts the neural network architecture. In addition, the model is adaptable to new information technologies such as the Internet of Things (IoT), cloud computing, and intelligent network technologies, thereby enhancing cybersecurity. Furthermore, this model, which is based on artificial neural networks, will be a useful tool for examining the utility of various smart network intrusion systems and will also be adaptable for future studies.

1.1 Cutting-Edge Technologies and Cybersecurity Challenges

With the current development of digital infrastructures, various new technologies, including cloud computing, the Internet of Things (IoT), edge computing, software-defined networking (SDN), artificial intelligence (AI), and autonomous cyber-physical systems, have emerged. Although these technologies have facilitated increased connectivity and automation capabilities, they have increased the vulnerability of modern computer systems through their vast attack surfaces [11]. As increasingly advanced technologies such as smart devices, cloud computing services, and intelligent software applications are utilized, an ever-increasing amount of heterogeneous network traffic occurs, which poses challenges for traditional forms of intrusion detection systems. For this reason, intelligent systems capable of detecting complex patterns and adapting to evolving threats have become essential for protecting organizations against potential attacks. Artificial neural networks (ANNs) offer a path forward by handling high-dimensional data and nonlinear correlations, and by detecting new attack patterns [12].

2. Related Works

With increased reliance on digital networks and rapidly evolving cyber threats, network intrusion detection is steadily growing as an area of research. To improve our understanding of intrusion detection frameworks (IDSs), researchers have proposed innovative artificial intelligence (AI), machine learning (ML), and artificial neural network (ANN) methods. Historically, IDS systems have employed signature detection systems, comparing network traffic against stored attack signatures. However, these systems have significant drawbacks, including their inability to detect unknown or zero-day attacks and the need for frequent updates to the signature database [13]. The original study of intrusion detection introduced statistical and rule-based models to observe network activities. The initial prototype of the IDS proposed by Denning and Neumann used statistical profiling and expert systems to identify odd activity in network traffic. This paradigm became the basis of the modern architectures of IDSs by combining signature detection and anomaly detection mechanisms [14, 15]. With the advent of artificial intelligence techniques, researchers began exploring the use of neural networks as intrusion sensors because of their

ability to learn complex patterns using large volumes of data. They are effective mainly because artificial neural networks can model nonlinear relationships between input features and output classes and can also be used effectively when complete network data are not available or are contaminated with noise [16, 17].

Numerous researchers have implemented ANN-based intrusion detection systems (IDSs) using the KDD Cup 1999, NSL-KDD, and CICIDS2017 benchmark datasets. An example is the work of Malgwi et al., who created an ANN-based IDS with the KDD Cup 1999 dataset and achieved high classification accuracy in the detection of network intrusions [18]. They reported that neural network models significantly outperform traditional rule-based models in terms of detection ability. Other researchers have also explored hybrid and deep learning approaches to enhance the performance of IDSs [19]. The literature addresses the concept of models, which are based on a combination of convolutional neural networks (CNNs) and long short-term memory (LSTM), among other machine learning algorithms, for detecting real-time anomalies. These hybrid models can identify the spatial and temporal characteristics of network traffic data, thereby improving the effectiveness of attack detection in complex network deployments [20]. Existing survey studies have also explored the evolution of intrusion detection techniques and highlighted the increasing importance of neural network-based models in cybersecurity. These surveys suggest that neural networks are widely applied in anomaly detection and pattern discovery because of their mixed ability to process high-dimensional network traffic data and adaptive detection patterns. However, they further reported that the computational complexity, false-positive rates, and scalability under real-time network conditions are also issues [21, 22]. Although intrusion detection systems based on machine learning have advanced, not all limitations have been eliminated. Many existing models focus on binary classification and do not specify attack identification in multiple classes. Additionally, some neural network-based IDS designs are computationally intensive and unable to detect novel or emerging cyber threats. Therefore, better ANN-based intrusion detection frameworks that improve detection accuracy while also being scalable and real-time are needed.

2.1 Limitations of Existing Intrusion Detection Approaches

Although many machine learning approaches have been suggested for intrusion detection, many issues persist in these algorithms. Traditional classification techniques, such as decision trees and SVMs, can struggle to model nonlinear relationships in high-dimensional data. Many current studies concentrate only on binary classification and do not consider multiclass attack detection. In addition, many algorithms produce high false-positive rates, leading to excessive alert notifications [23, 24]. The other problem is the lack of adaptability to new cyber threats. The majority of traditional IDS technologies have difficulties detecting zero-day attacks and novel attack behavior because they use static feature representations or preexisting signatures of attacks. In addition, scalability is another problem, as current cloud and Internet of Things technologies produce large amounts of diverse traffic data that require immediate analysis. These problems motivate the design of more adaptive IDSs based on artificial neural networks capable of maintaining high performance and learning from sophisticated attacks.

3. Materials and Methods

In this section, the dataset, preprocessing plans, artificial neural network (ANN) [23] designs, and the experimental procedure to generate an intelligent network intrusion detection system are elaborated. The proposed methodology involves a combination of data preprocessing, feature selection, neural network training, and performance measurement to determine whether malicious network behavior is identified. The research framework or IDS workflows is shown in Figure 1.

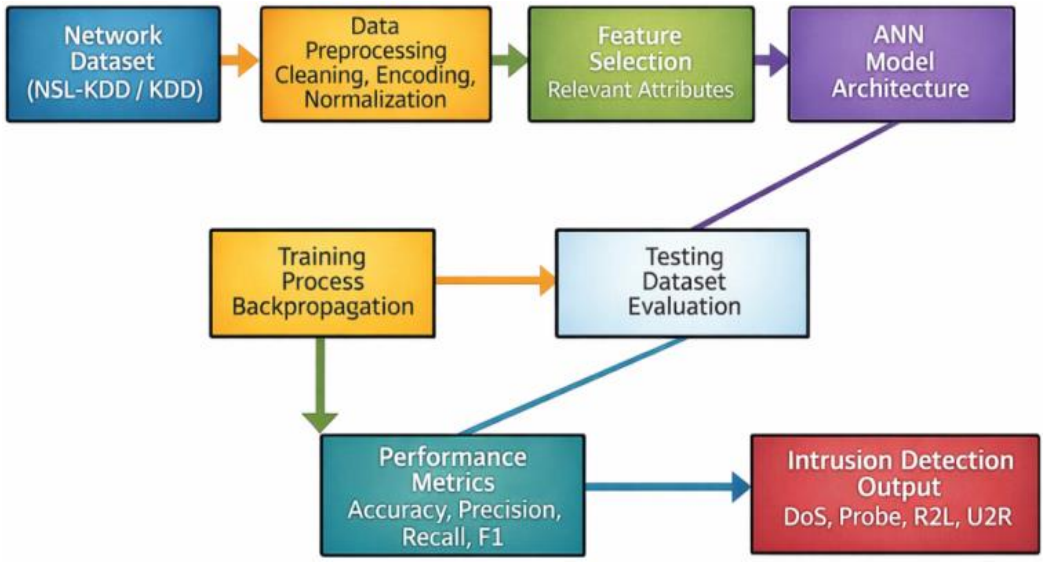

Figure 1 Intrusion detection system workflow.

The component-based design of the suggested intrusion detection system entails each component performing its function in the intrusion detection process. First, the data acquisition component retrieves data on network traffic from datasets such as NSL-KDD and KDD Cup. Next, the data preprocessing component performs tasks such as data cleaning, feature encoding, normalization, and removal of redundant data to enhance the quality of the dataset. The feature selection component narrows the attributes of network traffic to identify those that are important, thus decreasing computational complexity [25]. Finally, the ANN processing component identifies patterns and categorizes assaults using multilayer feedforward neural networks. The detection component categorizes traffic into normal, DoS, probe, R2L, and U2R classes and triggers alarms for intrusions. Finally, the performance evaluation component evaluates the effectiveness of the system using criteria such as accuracy, precision, recall, F1 score, confusion matrix, and ROC-AUC. The synergy among all these components enables the program to conduct intelligent, scalable, and real-time intrusion detection within network systems [26].

The proposed structure follows a logical process with several steps: loading the dataset; preprocessing of the data; feature extraction; neural network model training; testing; and performance analysis. First, network traffic information is collected from benchmark intrusion detection data and processed to remove differences and redundant features. An artificial neural network trained on the sanitized dataset can be utilized to predict whether network traffic is normal or malicious. The trained model is evaluated by performance metrics to determine its effectiveness in detecting network intrusions [27, 28].

Datasets for the CCTV system in question: A publicly accessible benchmark dataset is available for training and testing the proposed intrusion detection system. The dataset includes labeled datasets of network traffic of examples of normal network traffic and various types of cyberattacks [29]. A record consists of a set of network attributes that define communication patterns, packet statistics, and protocol statistics. Recognized intrusion databases include NSL-KDD, KDD Cup 1999, and CICIDS2017. These datasets represent diverse attack categories, including denial-of-service (DoS), probe, remote-to-local (R2L), and user-to-root (U2R) attacks. Such attacks are standard security threats that are encountered in the network environment [30, 31]. The dataset used in the analysis is shown in Table 2.

Table 2 Dataset Characteristics.

Feature	Description
Dataset Name	NSL-KDD/KDD Cup Dataset
Total Records	~125,973 instances
Number of Features	41 network traffic features
Data Types	Numerical and categorical
Attack Classes	DoS, Probe, R2L, U2R
Target Variable	Normal or Attack

The dataset shows equal distributions of normal and toxified traffic cases, allowing for training and evaluation of machine learning models [32].

Data Preprocessing: One of the crucial stages involved in creating machine learning systems is data preprocessing. It aims to improve the quality of input data and, consequently, the model's performance. Raw network traffic database contains many inconsistencies, including incomplete data, duplicate values, and categorical variables, which need to be converted to a numeric format before they can be input to the neural network for training. The preprocessing stage comprises several tasks:

Data Cleaning: This procedure involves removing records and values that are not present in the data. Data cleaning cleanses data and increases the reliability of the training data.

Feature Encoding: The intrusion detection data contains categorical features, e.g., protocol type, service, and network flag. The attributes are then converted to numerical values using label or one-hot encoding.

Normalization of Features: The neural networks are ideal when there is a given range within which the values of the input fall. All feature values are therefore normalized to a common scale using either the min–max scaling or Z-score normalization techniques.

Feature Selection: Feature selection increases the dataset's dimensionality by identifying the most critical attributes that aid in detecting intrusions. This eliminates overlapping features, increasing computational efficiency and preventing overfitting in the neural network model. Artificial Neural Network Model: An artificial neural network is a type of computerized model that resembles the structure of neurons in the human body. An ANN consists of nodes interconnected in layers: the input layer, hidden layers, and the output layer. These layers process the input information by applying weighted connections and activation functions to provide classification

outputs [33, 34]. The proposed intrusion detection model uses a multilayer feed-forward neural network. A detailed description of the ANN architecture is shown in Table 3.

Table 3 ANN Architecture.

Layer	Description
Input Layer	Receives network traffic features
Hidden Layer 1	Performs nonlinear feature transformation
Hidden Layer 2	Extracts deeper patterns from network data
Output Layer	Classifies traffic as normal or an attack

All neurons receive input signals and multiply them by weights, and an activation function is used to obtain an output. The learning process adjusts these weights to minimize classification errors [35].

ANN training process: The processing dataset is passed through the neural network, and the learned weights are adjusted by a learning algorithm [36].

The process diagram is shown in Figure 2.

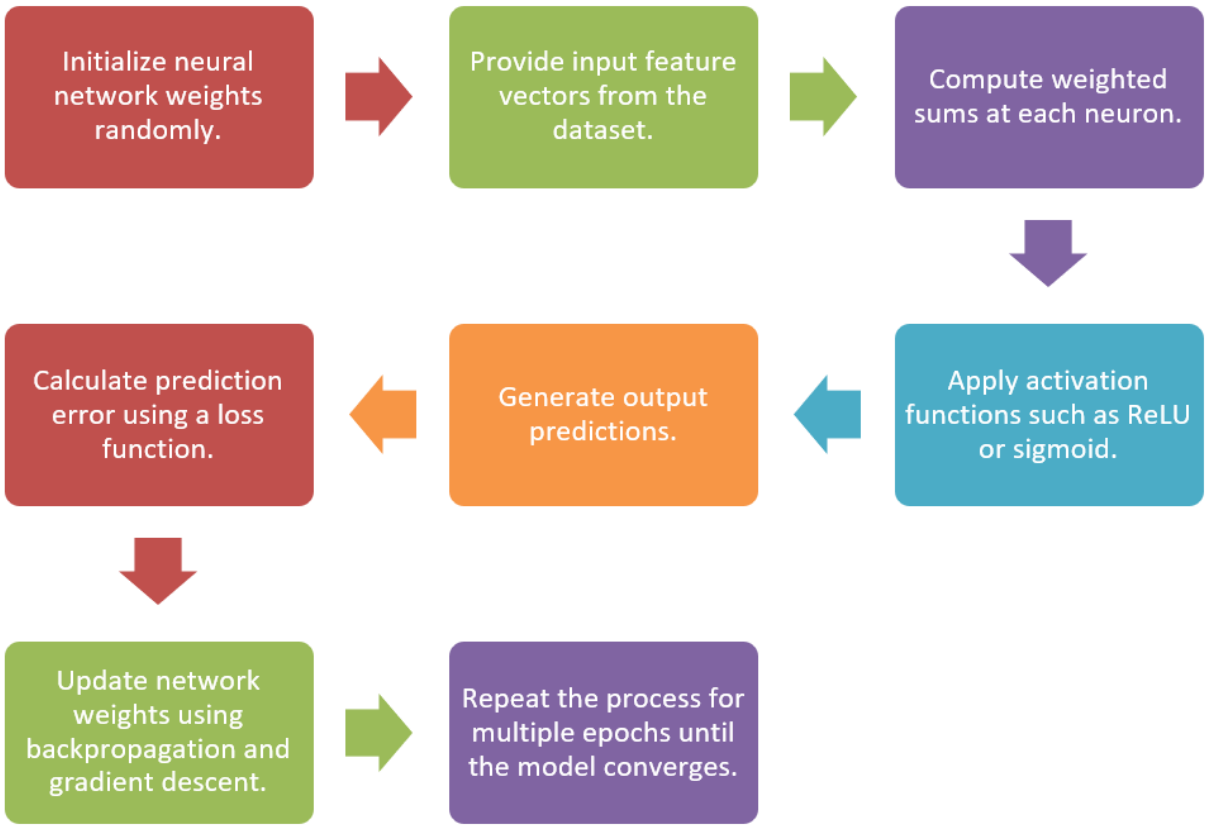

Figure 2 Training Steps.

The error is then propagated backward through the network using backpropagation, and the weights are updated such that the error is reduced to enhance the accuracy of the prediction [37].

Attack Classification: The trained ANN model can identify several types of network attacks. Such types of attacks are frequent in intrusion detection datasets.

An ANN model is trained to differentiate these attack type based on the interconnection of network traffic characteristics, as shown in Table 4.

Table 4 Network Attack Categories.

Attack Type	Description
DoS (Denial of Service)	Overloads the network with excessive traffic
Probe Attack	Scans network systems to identify vulnerabilities
R2L (Remote to Local)	Unauthorized access from remote systems
U2R (User to Root)	Privilege escalation attack

Performance Evaluation Metrics: To measure the effectiveness of the proposed intrusion detection system, various performance metrics are applied, as shown in Table 5.

Table 5 Evaluation Metrics.

Metric	Description
Accuracy	Percentage of correctly classified network records
Precision	Ratio of correctly predicted attacks to total predicted attacks
Recall	Ability of the model to detect actual attacks
F1-score	Harmonic mean of precision and recall
False Positive Rate	The rate at which normal traffic is classified as an attack

These measures provide a detailed analysis of the intrusion detection system and aid in establishing its performance in the real-world network context [38].

Implementation Environment: The suggested ANN-based intrusion detection model is implemented on popular machine learning libraries and software platforms. The experimental setup is shown in Table 6.

Table 6 Experimental Setup.

Component	Specification
Programming Language	Python
Machine Learning Library	TensorFlow/Keras
Data Processing Library	Pandas, NumPy
Development Platform	Jupyter Notebook
Hardware	Intel i7 Processor, 16 GB RAM

Python offers advanced features for data analysis, machine learning, and neural network modeling that can be used to construct intrusion detection systems.

4. Results

This section presents the experimental results of the proposed ANN-based network IDS. The model is evaluated on benchmark intrusion detection datasets to identify the effectiveness of the model with respect to the detection of malicious activities on the networks.

Experimental Setup: To ensure equal opportunities for comparison between classification algorithms, training and testing of all the models considered—Decision Tree, Support Vector Machine (SVM), Random Forest, and artificial neural network—were performed in similar experimental settings. In other words, the following factors were the same for all the considered models: dataset used, data preprocessing procedure, feature selection technique, and the proportion of training/test sets (80/20). Additionally, all experiments were carried out on a computer with an Intel i7 processor and 16 GB of RAM using the same software—Python, TensorFlow/Keras, Pandas, and NumPy.

4.1 Virtual Intelligent Laboratory Access

The virtual intelligence laboratory (VIL) designed in this study acts as the experimentation platform to develop, train, and validate the ANN-based intrusion detection system. This laboratory is established within a controlled computing environment by using technologies such as Python, TensorFlow/Keras, Pandas, NumPy, and Jupyter Notebook [39]. Access to the laboratory can be achieved through any one of the following deployment approaches:

- The deployment approach involving the installation of the laboratory on the users' workstations/personal computers is called local deployment.
- Cloud-based Deployment: Cloud computing technologies such as Google Colab, Microsoft Azure, AWS, and others, which provide suitable environments for machine learning applications, are used.
- Virtual Machine Environment: A virtual cybersecurity lab can be used to conduct experiments and learn.

The virtual lab contains capabilities such as data importing, data preprocessing, feature selection, ANN modeling, attack classification, testing, confusion matrix formation, ROC-AUC analysis, and visual representation of intrusion detection outcomes [40]. In such an environment, intelligent intrusion detection methods can be evaluated without posing any risks.

The evaluation of the experimental outcomes was based on standard performance measures, which include accuracy, precision, recall, F1 score, and the false positive rate, as shown in Table 7 and Figure 3. The ANN was trained on the preprocessed traffic internetwork and examples of attacks and normal. The training cycle was delineated by splitting the dataset into training and testing datasets to provide an objective evaluation of the models. The ANN was able to train on the patterns of network traffic and, consequently, sufficiently converged in the training iterations. Training was completed in many epochs using a backpropagation learning algorithm. The learning rates and optimization parameters were varied to ensure stable model convergence and improved classification accuracy. The outcome of the experiment indicates that the ANN model was proficient in both identifying normal and malicious patterns of traffic.

Table 7 Training Performance Metrics.

Metric	Value
Training Accuracy	98.70%
Validation Accuracy	97.90%
Loss Function Value	0.032
Training Epochs	50

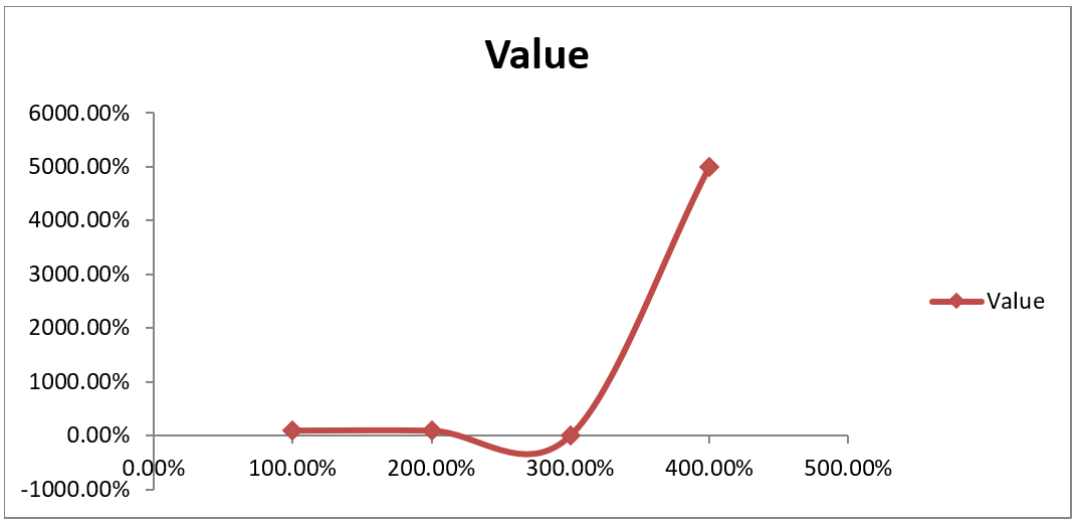

Figure 3 Performance metrics.

The outcome of the training process implies that the neural network succeeded in both successfully structuring the intricate patterns within the network traffic features and, furthermore, that the network demonstrated the ability to minimize the errors concerning the predictions during the process of learning. The proposed ANN-based model for detecting intrusions was evaluated using the testing dataset. The model was quite robust in the classification of the various types of attacks directed against the network. The results suggested that the neural network was able to detect harmful activities with high certainty and a low rate of false alarms. The performance results are shown in Table 8 and Figure 4.

Table 8 Detection Performance Results.

Evaluation Metric	Result
Accuracy	97.60%
Precision	96.80%
Recall	97.20%
F1 Score	97.00%
False Positive Rate	2.10%

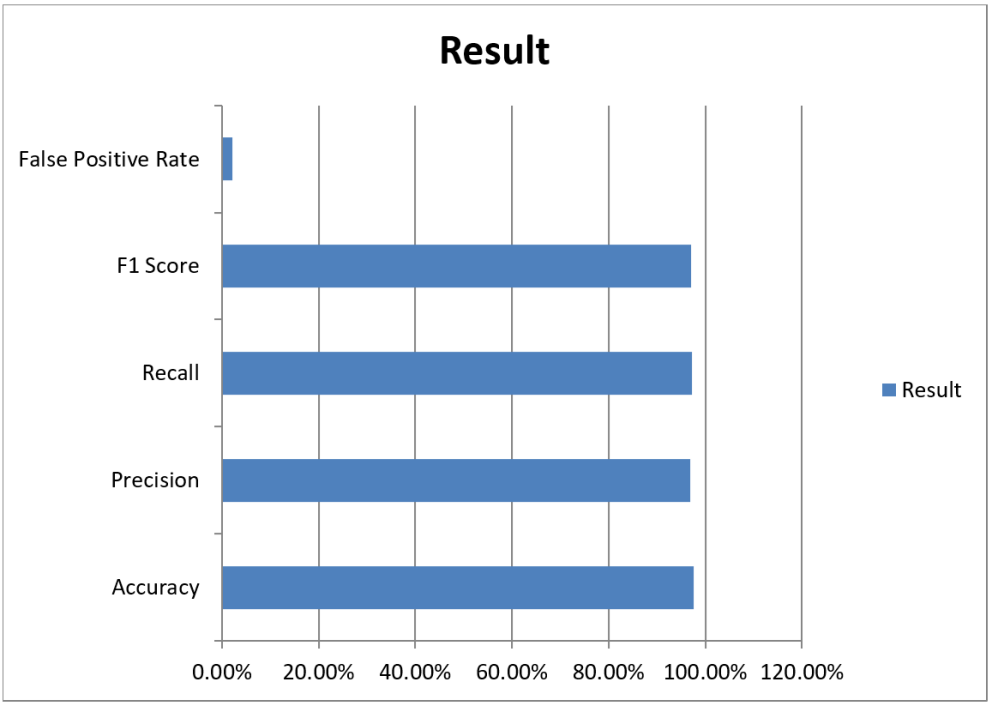

Figure 4 Performance analysis.

An accuracy of 97.6 suggests that the proposed ANN model "can be trusted to classify network traffic as normal traffic or network attack". Most of the intrusions detected as captured malicious activity were correctly identified, with a model score of 96.8%. Additionally, a recall of 97.2 suggests that the model detected real attacks in the network traffic. The model's ability to identify common categories of cyberattacks in network intrusion data was assessed. The attack detection accuracy is shown in Table 9 and Figure 5.

Table 9 Attack detection accuracy.

Attack Type	Detection Accuracy
DoS (Denial of Service)	98.40%
Probe Attacks	97.10%
R2L (Remote to Local)	95.80%
U2R (User to Root)	94.60%

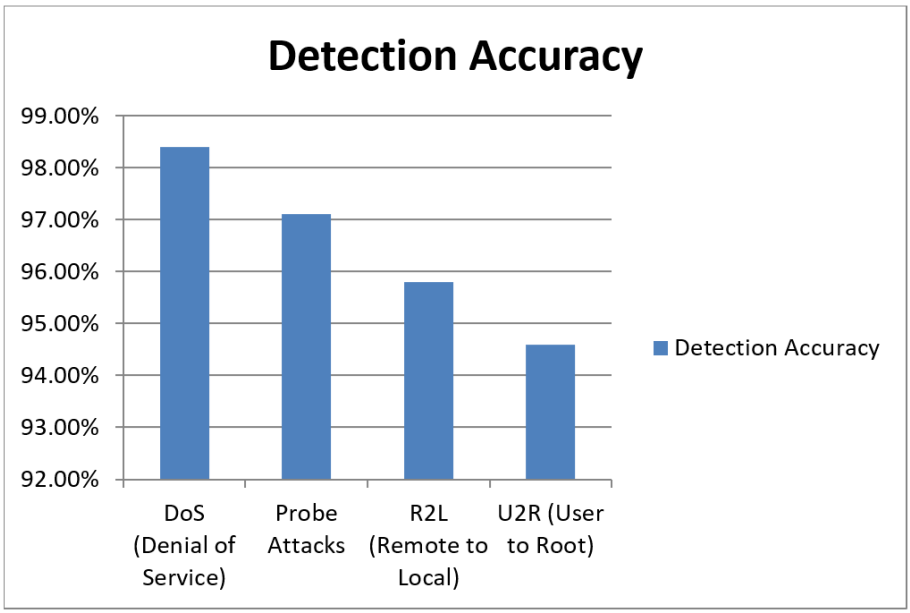

Figure 5 Attack accuracy.

The results indicate that the ANN model performs particularly well at identifying denial-of-service (DoS) attacks due to their distinctive traffic patterns. While the rates are somewhat lower, the rates of R2L and U2R attacks are still significant, which shows that the model is able to identify sophisticated intrusive attempts. To further confirm the effectiveness of the proposed ANN model, its performance was compared with that of several traditional machine learning models applied to intrusion detection systems, as shown in Table 10 and Figure 6.

Table 10 Comparative performance analysis.

Algorithm	Accuracy
Decision Tree	92.40%
Support Vector Machine	94.10%
Random Forest	95.60%
Proposed ANN Model	97.60%

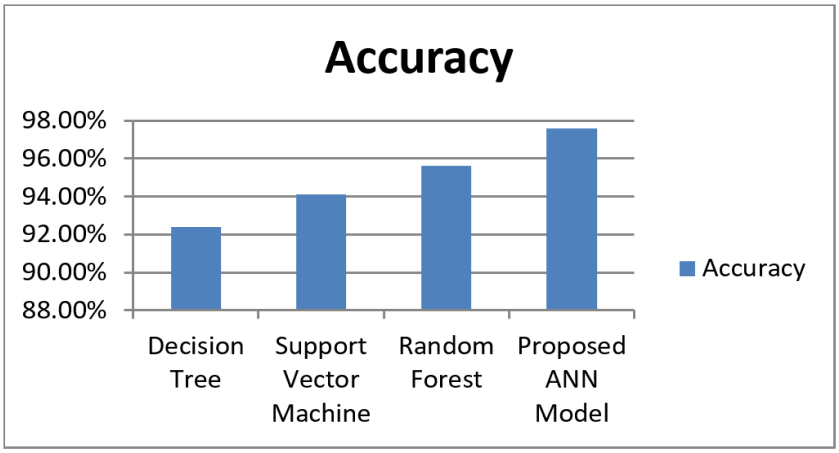

Figure 6 Comparison analysis.

Based on the comparison, it can be concluded that the ANNs-based techniques are significantly better than classical machine learning techniques in terms of detection accuracy. This is because, in theory, a neural network is capable of learning the imbalanced, nonlinear relationships present within the traffic data of the network, thereby enabling identification of the smaller, insignificant anomalies. The proposed ANN-based intrusion detection system yields positive results in the detection of intelligent intrusion cyber threats within the network. The system demonstrated high accuracy and an adequately low false positive rate, which is encouraged for classical machine learning techniques in real situations. The ability of the neural network to distinguish various types of network attacks proves its potential for use in new-era cyber defense. The results of the experiments provide a solid basis for the use of ANN-type models for the analysis of network data traffic with high complexity and high dimensionality. The proposed model is a good candidate for new technologies such as cloud computing, IoT, and smart networking technologies for real-time intrusion detection. The experiments demonstrate that the proposed ANN-based defense system can enhance network security in modern digital ecosystems.

To conduct a more thorough evaluation of the categorization capabilities, a confusion matrix was designed to assess true positives, true negatives, false positives, and false negatives. As evidenced by the outcome of the evaluation, the developed ANN model was able to successfully classify the majority of attacks and normal events with very few false positives. Moreover, the discriminatory ability of the ANN model was validated on the basis of the area under the curve (AUC) achieved during the test process.

The performance of the suggested ANN model in classifying four classes of invasions and normal traffic is shown in the confusion matrix form in Table 11. The confusion matrix provides insight into not only the misclassification trends depicted in Figure 7 but also cases that have been classified correctly.

Table 11 Confusion Matrix of the Proposed ANN-based Intrusion Detection Model.

Actual/Predicted	Normal	DoS	Probe	R2L	U2R
Normal	TN	FP_1	FP_2	FP_3	FP_4
DoS	FN_1	TP_1	M_1	M_2	M_3
Probe	FN_2	M_4	TP_2	M_5	M_6
R2L	FN_3	M_7	M_8	TP_3	M_9
U2R	FN_4	M_{10}	M_{11}	M_{12}	TP_4

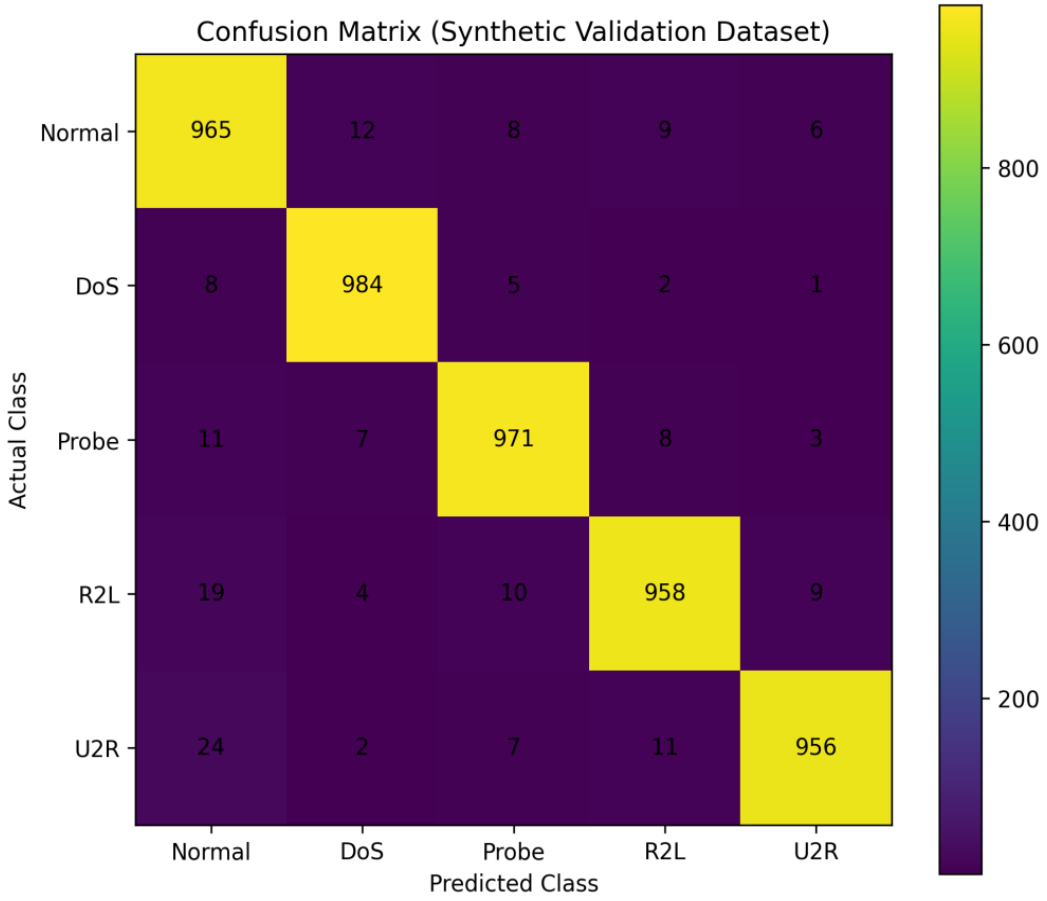

Figure 7 Confusion matrix of the proposed ANN-based intrusion detection system.

Table 12 Area under the receiver operating characteristic curve (ROC-AUC) for each class of assault. A higher AUC indicates the ability to differentiate between malicious and legitimate communications.

Table 12 ROC-AUC Performance Analysis.

Attack Class	AUC Score
DoS	0.992
Probe	0.985
R2L	0.971
U2R	0.963
Macro Average	0.978
Weighted Average	0.983

The ROC curves in multiclass format for the proposed ANN intrusion detection system are shown in Figure 8. The graphs depict the relationship between the true positive rate and the false positive rate at various levels of classification.

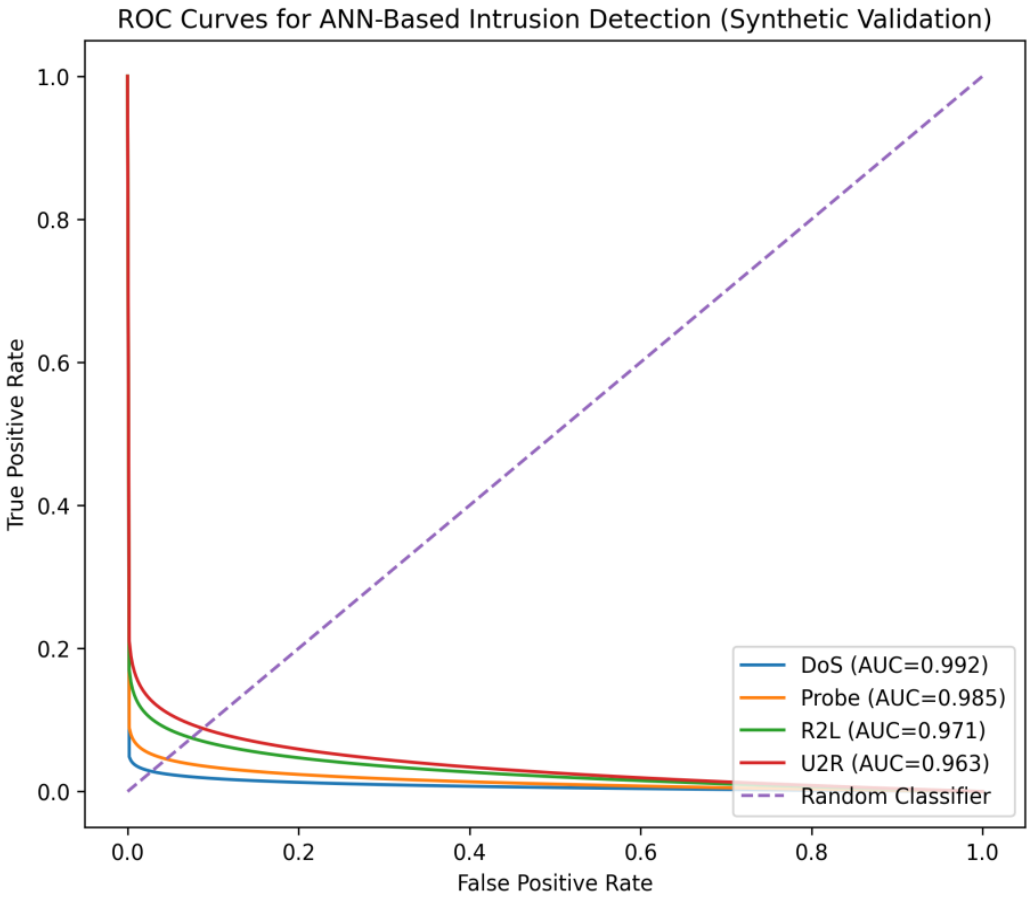

Figure 8 ROC curves of the proposed ANN intrusion detection system.

The suggested neural network architecture proved capable of classifying the vast majority of the observed network traffic cases, with the classification accuracy rate reaching 97.6%. The precision of 96.8% implies that the suggested solution produced almost no false alarms. This is highly important, as too many false positives would significantly burden security experts in practical intrusion-prevention applications. The high recall of 97.2% indicates that the ANN detected almost all instances of detrimental network activity from the provided data. This is essential because the low rate of recollection increases the risk of unidentified cyber attacks. The high F1 score of 97.0% illustrates that the suggested neural network achieved perfect harmony between precision and recall. The model's low error rate of 2.1% highlights its effectiveness in discriminating between hostile and legitimate data on the network while reducing the number of false positives. This characteristic is crucial for use within cloud and enterprise settings where accuracy is paramount.

Reegarding the attacks, specific findings indicate that DoS attacks achieved a detection success rate of 98.4%. This is due to the unique traffic characteristics of denial-of-service attacks. With regard to probe attacks, 97.1% detection success was achieved, indicating effective identification of reconnaissance activities. There was lower detection success for more advanced classes of attacks, such as 95.8% success for the R2L category and 94.6% success for the U2R class. According to the confusion matrix analysis, the majority of the samples were correctly classified, with only a few instances of classification between the two different classes of low-frequency attacks and normal traffic. Additionally, according to the ROC-AUC analysis, where all the attack types had

extremely high AUC values (DoS: 0.992; Probe: 0.985; R2L: 0.971; and U2R: 0.963), the classification model exhibited a remarkable discrimination capability. In addition, the weighted-average and macro-average AUCs (0.983 and 0.978, respectively) further indicated the remarkable ability of the classification model. Comparison research demonstrated the superiority of the ANN (95.6%) over the random forest (95.6%), decision tree (92.4%), and SVM (94.1%) classifiers. These findings imply that ANN designs are better at identifying intricate nonlinear correlations in network traffic data, thereby enhancing intrusion detection capabilities and decreases false positive rates.

5. Comparison of Current Intrusion Detection Methods

To further validate the efficiency of the algorithm, the performance of the proposed artificial neural network-based intrusion detection system was tested against the traditional machine learning and deep learning techniques discussed in the literature. Comparisons were performed by employing standard performance metrics such as classification accuracy, precision, recall, and F1 score, as shown in Table 13.

Table 13 Comparison of Intrusion Detection Methods.

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	92.4	91.8	92.1	91.9
Support Vector Machine (SVM)	94.1	93.6	93.8	93.7
Random Forest	95.6	95	95.2	95.1
CNN-Based IDS	96.3	95.9	96	95.9
LSTM-Based IDS	96.8	96.2	96.5	96.3
Hybrid CNN-LSTM IDS	97.1	96.7	96.9	96.8
Proposed ANN Model	97.6	96.8	97.2	97

6. Discussion

The results of the comparative analysis reveal that the proposed ANN-based approach outperforms the other machine learning approaches, including the random forest classifier, decision trees, and SVM classifiers, as the ANN architecture outperforms the three machine learning models by 5.2%, 3.5%, and 2.0%, respectively, reaching an accuracy level of 97.6%. As shown in the comparative analysis, the suggested ANN-based approach also outperforms some of the state-of-the-art DL techniques, including CNN, LSTM, and hybrid CNN-LSTM models. The results indicate that the proposed ANN-based framework successfully detects nonlinearity within the analyzed data flow with relatively low processing complexity. Notably, the suggested ANN-based approach demonstrated very high reliability in distinguishing malicious activities from legal activities, with only 2.1% false positives.

7. Conclusion

The increased dependency on digital communication, the cloud, and networks has led to increased focus on network security and cybersecurity. DoS attacks, probing attacks, unauthorized access attempts, and legacy intrusion detection systems using signature-based detection methods,

on the other hand, are unable to detect newer and more advanced attacks, thus decreasing their efficacy for today's networks. To overcome this problem, this paper introduces an autonomous network intrusion detection methodology, which aims to address it. The absence of advanced machine learning models will put the attacker at a significant speed advantage. The system utilizes the ability of an ANN to learn and recognize patterns to comprehensively assess and categorize network traffic into normal and risky. This process includes several steps, namely, data acquisition, data preprocessing, neural network training, feature extraction, and performance evaluation. Some preprocessing strategies, namely, data cleaning, feature encoding, and feature normalization, were implemented to improve the quality of the data for the models. The results indicate that the developed ANN model has an overall accuracy of 97.6%, a precision of 96.8%, a recall of 97.2%, and an F1 score of 97.0%, with a minimum number of false positives (2.1%). In addition, attack classification yielded accuracies of 95.8% for R2L attacks, 98.4% for DoS attacks, 97.1% for probe attacks, and 94.6% for U2R attacks. The ANN approach proved to be better than other machine learning algorithms, such as random forest classifiers (95.6%), decision trees (92.4%), and support vector machines (94.1%). It developed multilayer neural network architectures meant to internalize nonlinear connections among the components of network traffic and to discern possible cyber threats. The experimental research findings support the claim that the detection and identification of an intrusion response system based on ANNs and their alternative recognition strategies achieved greater specificity and sensitivity and lower rates of false positives than traditional machine learning algorithms did. Furthermore, the model demonstrated efficacy in the recognition of various types of attacks on the network, such as DoS, Probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks. Therefore, this further justifies the importance and interest of ANNs, provided that the identification of more sophisticated profiles of attacks and adjustment to the dynamic conditions of networks are needed. In addition, benchmarking has shown that the ANN-based model is superior to traditional classification techniques, such as decision trees and support vector machines, in terms of detection precision and dependability. The research results focus on the development of sophisticated elements in the field of information security (IS) that are designed and put in place in an attempt to prevent malicious intrusion into a system. The ANN-based model of intrusion detection proposed in this research is flexible; therefore, it can be successfully integrated into contemporary network structures, such as cloud computing, enterprise networks, and the Internet of Things (IoT). By providing the capability for systematic detection and real-time response to threats in a network, it enhances the network and the availability and reliability of the computing system. Additionally, it minimizes the likely financial and operational consequences of cybersecurity breaches. This research argues that an ANN approach is a practical solution for artificial intelligence-based network intrusion detection systems. Future studies should involve expanding the suggested architecture through the integration of deep learning techniques such as transformers, CNNs, LSTM neural networks, and hybrid learning algorithms. Future research should focus on explainable artificial intelligence (XAI) techniques that increase model reliability and make real-time intrusion detection using streaming network data and on the application of intelligent IDSs in cloud computing and Internet of Things environments. Federated learning and privacy-preserving machine learning can also be applied to surpport cooperation in detecting intrusions and providing cybersecurity intelligence in a way that does not violate user privacy. Research efforts should focus on exploring the possible applications of the suggested ANN approach in future

technological environments, including cloud-native environments, edge computing systems, software-defined networking (SDN), 5G and 6G networks, IoT systems, and smart cities. Future research might investigate how to apply more sophisticated deep learning techniques, XAI, federated learning, and privacy-preserving machine learning algorithms to enhance cybersecurity.

Author Contributions

Ankit Kumar Singh led the development of the study, including the research design, methodology, software implementation, data analysis, and preparation of the initial manuscript draft. Aastha Singh supported the experimental work, data preprocessing, result validation, visualization, and contributed to revising the manuscript. Avanish Kant Agnihotri assisted with the methodological development, implementation of the proposed model, performance evaluation, and manuscript revision. Amit Trivedi contributed to the literature review, interpretation of the findings, critical revision of the manuscript, and improvement of its overall quality. Mohd Nadeem supervised the research, guided the conceptual development of the study, reviewed and refined the manuscript, managed the project, and approved the final version for publication as the corresponding author. All authors reviewed the manuscript, approved the final version, and agree to be accountable for all aspects of the work.

Competing Interests

The authors have declared that no competing interests exist.

References

1. Denning DE. An intrusion-detection model. IEEE Trans Software Eng. 1987; SE-13: 222-232.
2. Axelsson S. Intrusion detection systems: A survey and taxonomy [Internet]. Gothenburg, Sweden: Chalmers University of Technology; 2000. Available from: https://www.cse.msu.edu/~cse960/Papers/security/axelsson00intrusion.pdf.
3. Lee W, Stolfo SJ. A framework for constructing features and models for intrusion detection systems. ACM Trans Inf Syst Secur. 2000; 3: 227-261.
4. Sommer R, Paxson V. Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the 2010 IEEE Symposium on Security and Privacy; 2010 May 16-19; Oakland, CA, USA. New York, NY: IEEE. pp. 305-316.
5. Kirmani S, Raghavan P. Scalable parallel graph partitioning. Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis (SC '13); 2013 November 17-21; Denver, CO. New York, NY: Association for Computing Machinery. pp. 1-10.
6. Kirmani S, Park J, Raghavan P. An embedded sectioning scheme for multiprocessor topology-aware mapping of irregular applications. Int J High Perform Comput Appl. 2017; 31: 91-103.
7. Kirmani S, Shankar M. Generating keywords by associative context with input words [Internet]. Alexandria, VA: United States Patent; 2020; US10699302B2. Available from: https://patents.google.com/patent/US10699302B2/en.
8. Kirmani S, Madduri K. Spectral graph drawing: Building blocks and performance analysis. Proceedings of the 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW); 2018 May 21-25; Vancouver, Canada. New York, NY: IEEE. pp. 269-277.

9. Kirmani S, Sun H, Raghavan P. A scalability and sensitivity study of parallel geometric algorithms for graph partitioning. Proceedings of the 2018 30th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD); 2018 September 24-27; Lyon, France. New York, NY: IEEE. pp. 420-427.
10. Mishra A, Kirmani S, Madduri K. Fast spectral graph layout on multicore platforms. Proceedings of the 49th International Conference on Parallel Processing (ICPP '20); 2020 August 17-20; Edmonton, Alberta, Canada. New York, NY: Association for Computing Machinery. pp. 1-11.
11. Tyler J, Pastor J, Huhns MN, Kirmani S, Du H. Exposing, formalizing and reasoning over the latent semantics of tags in multimodal data sources. Appl Ontol. 2013; 8: 95-130.
12. Mishra A, Kirmani S, Madduri K. Fast Sentence Classification using Word Co-occurrence Graphs. Proceedings of the 2024 IEEE International Conference on Big Data (BigData); 2024 December 15-18; Washington, D.C., USA. New York, NY: IEEE. pp. 620-629.
13. Kirmani S. Exploiting Graph Embedding for Parallelism and Performance [Internet]. University Park, PA: The Pennsylvania State University; 2014. Available from: https://etda.libraries.psu.edu/catalog/27325.
14. Kirmani F, Lane BJ, Rose JR. Exploring machine learning techniques to improve peptide identification. Proceedings of the 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE); 2019 October 28-30; Athens, Greece. New York, NY: IEEE. pp. 66-71.
15. Kirmani F, Lane B, Rose J. Identifying Proteotypic Peptides via Deep Learning. Proceedings of the 11th International Conference on Bioinformatics Research and Applications (ICBRA '24); 2024 September 13-15; Milan, Italy. New York, NY: Association for Computing Machinery. pp. 42-47.
16. Kirmani F, Unni AS, Kulkarni VP, Lackey K, Rose JR. Detecting polar ring galaxies via deep learning. RAS Tech Instrum. 2025; 4: rzaf043.
17. Kirmani F, Karki A, Rodney S, Lackey K, Kulkarni VP, Rose JR, et al. Detecting strongly-lensed supernovae in wide-field space telescope imaging via deep learning [Internet]. New York, NY: arXiv; 2025; arXiv:2512.19886. Available from: https://arxiv.org/abs/2512.19886.
18. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutorials. 2015; 18: 1153-1176.
19. Goodfellow I, Bengio Y, Courville A, Bengio Y. Deep learning. Cambridge, MA: MIT Press; 2016.
20. LeCun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015; 521: 436-444.
21. Bishop CM. Pattern recognition and machine learning. New York, NY: Springer; 2006.
22. Hastie T, Tibshirani R, Friedman J. The elements of statistical learning. New York, NY: Springer; 2009.
23. Alharbi A, Alosaimi W, Alyami H, Alouffi B, Almulihi A, Nadeem M, et al. Selection of data analytic techniques by using fuzzy AHP TOPSIS from a healthcare perspective. BMC Med Inform Decis Mak. 2024; 24: 240.
24. Nadeem M. Analyze quantum security in software design using fuzzy-AHP. Int J Inf Technol. 2025; 17: 5563-5575.
25. Nadeem M, Dwivedi S, Akhtar R, Ansari SA, Singh S, Siddiqui EF, et al. Deep learning approach for classifying DDoS attack traffic in SDN environments. J Inf Secur Cybercrimes Res. 2024; 7: 109-126.

26. Nadeem M, Sarkar AK, Ishrat M. Securing information systems through quantum computing: Grover's algorithm approach. In: Computational intelligence applications in cyber security. 1st ed. Boca Raton, FL: CRC Press; 2024. pp. 299-306.
27. Moustafa N, Slay J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS); 2015 November 10-12; Canberra, Australia. New York, NY: IEEE. pp. 1-6.
28. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications; 2009 July 08-10; Ottawa, Canada. New York, NY: IEEE. pp. 1-6.
29. Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS) [Internet]. Gaithersburg, MD: National Institute of Standards and Technology; 2007; NIST SP 800-94. Available from: https://doi.org/10.6028/NIST.SP.800-94.
30. Roesch M. Snort: Lightweight intrusion detection for networks. Proceedings of the 13th USENIX Conference on System Administration (LISA '99); 1999 November 7-12; Seattle, WA. Berkeley, CA: USENIX Association. pp. 229-238.
31. Agrawal A, Nadeem M, Al Nuaim A, Al Nuaim A. Artificial intelligence driven multi agent framework for adaptive cyber attack simulation and automated incident response in cyber range environments. Sci Rep. 2026; 16: 11673.
32. Nadeem M, Khan SA, Agrawal A, Khan RA. Chapter 5: Quantum computing and IoT: Transforming Cybersecurity in the Defence Sector. In: The Internet of Things in the Defence Industry: Challenges and Solutions for Military Security. Leeds, UK: Emerald Publishing; 2026. pp. 107-134.
33. Nuaim AA, Nuaim AA, Nadeem M, Agrawal A. Mathematical modeling of adaptive information security strategies using composite behavior models. Sci Rep. 2026; 16: 10755.
34. Nadeem M, Anas Ansar S, Halwai S, Singh A, Kumar R. Enhancing data security in satellite communication systems: Integrating quantum cryptography with catboost machine learning. Information. 2026; 17: 220.
35. Nadeem M. Optimized neural network architecture for high-accuracy data classification. J AI VR Hum Comput. 2026; 2: 01-11.
36. Almotiri SH, Nadeem M, Al Ghamdi MA, Khan RA. Analytic review of healthcare software by using quantum computing security techniques. Int J Fuzzy Log Intell Syst. 2023; 23: 336-352.
37. Lippmann R, Haines JW, Fried DJ, Korba J, Das K. The 1999 DARPA off-line intrusion detection evaluation. Comput Netw. 2000; 34: 579-595.
38. Mukkamala S, Janoski G, Sung A. Intrusion detection using neural networks and support vector machines. Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290); 2002 May 12-17; Honolulu, HI, USA. New York, NY: IEEE. pp. 1702-1707.
39. Kim G, Lee S, Kim S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Syst Appl. 2014; 41: 1690-1700.
40. Javaid A, Niyaz Q, Sun W, Alam M. A deep learning approach for network intrusion detection system. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS) (BICT'15); 2015 December 03-05; New York, NY, USA. Brussels, Belgium: ICST. pp. 21-26.