AI-Enabled Intelligent Intrusion Detection Framework Using Artificial Neural Networks for Secure and Sustainable Networked Systems

Brajesh Kumar[1], and Kashish Rajan[2]

[1]School of Computer Science and Engineering, Sandip University, Sijoul, Madhubani, India

[2]Department of Computer Science and Engineering, Shri Ramswaroop Memorial University, Barabanki, India

DOI: https://doi.org/10.47772/IJRISS.2026.100300102

Received: 11 March 2026; Accepted: 16 March 2026; Published: 27 March 2026

ABSTRACT

The explosion of cloud computing, online services, and interlinked digital services has contributed to increased susceptibility of modern networks to cyber-attacks. Traditional Intrusion Detection Systems (IDS) detect attacks by utilising signature-based detection methods, which often fail to recognise novel or previously unrecorded attack patterns. To counter these shortcomings, the research will describe a sophisticated Artificial Neural Network (ANN) application, designed to not only improve the effectiveness of cyber security systems, but also boost the overall rate of threat detection. Proposed detection systems will improve cyber security by employing the ability of neural networks to learn patterns, and will therefore be able to evaluate and categorise network activity as being acceptable, or as representing a threat. The complete system will consist of a number of steps including, but not limited to, the acquisition of datasets, and the application of preprocessing.feature encoding, feature normalization and selection to improve data quality and minimize redundancy. It is a multilayer feedforward neural network model that is trained and tested over benchmark intrusion detection datasets against a number of attack types that include Denial-of-Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks. As demonstrated through experimental analysis, the proposed ANN model will achieve high precision and recall in addition to low false positive rate at 97.6 percent. Additional comparative study can show that ANN-based methodology outperforms other traditional machine learning algorithms, such as Decision Trees, Support Vector Machines, and Random Forest classifiers. The results show that neural network-based solutions can be useful in detecting complex intrusion patterns and making real-time network security in modern computing and cloud-based systems, with Internet of Things (IoT) networks.

Keywords: Artificial Neural Network (ANN); Network Intrusion Detection; Cybersecurity; Intrusion Detection System (IDS); Machine Learning; Network Security; Anomaly Detection; Cyber Attack Detection; Intelligent Security Systems; Deep Learning in Security.

INTRODUCTION

The impact of the rapid growth of digital technologies, cloud-computing and vast global networks has transformed modern communication and data transfer systems radically. It is however through this technological advancement that the 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, finances, government and education. As such, cyber attackers are constantly capitalising on the vulnerabilities in these systems, which cause disastrous financial, operational and reputational losses [2]. The traditional security measures such as firewalls and signature-based Intrusion Detection System (IDS) might be weak to detect advanced and dynamic network attacks. Given that existing systems utilise predetermined attack signatures, there is a fundamental limitation in their capabilities regarding the detection of novel or unknown threats. The growing intricacy of cyber threats has created a need for the development of smart and flexible security systems that can analyse and assess network traffic and, therefore, identify deviations from the norm.

The application of machine learning (ML) and artificial intelligence (AI) is considered a potential means of refining network security.

Artificial Neural Networks (ANN) is among those approaches and have gained colossal levels of attention because of their ability to identify intricate patterns through high volumes of information and locate abnormalities in network traffic. ANN models have the ability to automatically recognize valuable patterns on high-dimensional data, and correctly classify normal and suspicious network activities. In these abilities, ANN-based intrusion detection systems could enhance their detection rate, reduce the 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 such algorithms as Support Vector Machines, Decision Trees, Random Forest, and Deep Learning models to categorize network attacks [5], [6]. Although these methods have been demonstrated to provide superior performance to the traditional methodologies in detecting attacks, the majority of contemporary systems continue to suffer problems of feature selection, computational complexity, scalability, and the ability to detect zero-day attacks. Furthermore, most models struggle with a high detection rate with a low false-positively rate in real-time network environments. The Artificial Neural Networks provide a solution that is as strong as it opens up the prospect of adaptive learning and nonlinear pattern recognition [7]. ANN-based models are capable of efficiently handling massive networks 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]. ANN enhances the precision and reliability of intrusion detection systems in ever-changing network structures using efficient feature selection and data blocking methodologies. The rising figure on the cost of cyberattacks shows the evident need for the evolution of more sophisticated intrusion detection systems. Organizations globally experience extensive financial losses due to data theft, ransomware, and network intrusion. The increasing cost of cybercrime highlights the necessity of smart and automated protective solutions. This table (mentioned in Table 1) defines the economic loss from cybercrime for the world. These financial losses indicate the increasing relevance of cybercrime to the global economy. The unique constraints and sophistication of cyberattacks demand smart detection systems to recognize the adverse actions before the actions produce their 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: Even with the rising amount of literature on machine learning-based intrusion detection systems, a number of gaps still exist.

Disadvantages:

• Most of the current models of the procedures of intrusion detection are based on the traditionally trained machine learning algorithms that are unable to capture sophisticated nonlinear relationships among the 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 operation of the system.

• Most of the existing approaches are unable to provide sufficient flexibility and scalability to accommodate the large volume and the large scale real-time networks traffic of today's modern distributed systems.

As far as the optimisations of the Artificial Neural Network architectures in multi-class intrusion detection in the various types of attacks are concerned, little has been done.

Many models in use today still fail to identify zero-day attacks or new patterns of intrusions.

Because of the 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 will do this while maximising the reliability and extent of Intrusion Detection Systems (IDS) in modern network systems. With the abilities of neural networks, the model will also cancel or otherwise critically diminish false alarm rates. Additionally, the model will perform manual preprocessing and optimised neural network architecture adjustments. In addition to the above, the model will also be adaptable to new information technologies such as the Internet of Things (IoT), cloud computing, and intelligent network technologies, thereby enhancing cybersecurity. Furthermore, to examine the utility of various models of smart network intrusion systems based on the Artificial Neural Network, this model will also be the adaptable option for future studies.

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 (IDS), researchers have proposed innovative artificial intelligence (AI), machine learning (ML), and artificial neural networks (ANN) methods. Historically, IDS systems have employed signature detection systems, comparing network traffic against stored attack signatures. However, these systems have significant drawbacks, such as their inability to capture unknown or zero-day attacks, and the need for regular updates to the signature database [11].

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 the network traffic. This paradigm became the basis of the modern architectures of IDS by combining signature detection and anomaly detection mechanisms [12], [13].

With the advent of the techniques of artificial intelligence, researchers began exploring the use of neural networks as intrusion sensors due to their capabilities 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 that they can also be used effectively when the complete network data are not available or are contaminated with noise [14], [15].

Numerous researchers have implemented ANN-based intrusion detection systems (IDS) 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. They showed that neural network models significantly outperformed the detection capabilities of traditional rule-based models.

Other researchers have also explored hybrid and deep learning approaches to enhance the performance of the IDS. The literature has addressed the concept of models, which have been based on combination of

Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) among other machine learning algorithms in detecting real-time anomalies. These hybrid models are capable of identifying spatial and temporal characteristics of network traffic data, which improves the effectiveness of detecting attacks in a complex network deployment [20].

Furthermore, the existing survey studies have also explored the evolution of intrusion detection techniques and highlighted the rising importance of neural network-based models in cybersecurity. These surveys drive home the point 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 observe that the computational complexity, false-positive rates, and scalability under real-time network conditions are also an issue [21], [22].

Although intrusion detection systems based on machine learning have come a long way, not all limitations are eliminated. Many existing models focus on binary classification and do not specify attack identification multi-classes. Additionally, some neural network-based IDS designs are both computationally expensive and incapable of detecting novel or emerging cyber threats. Therefore, there is a need to have better ANN-based intrusion detection frameworks that are capable not only of improving the accuracy of detection, but also of being scalable and real-time.

Materials and Methods

In this section, the dataset, pre-processing plans, Artificial Neural Network (ANN) [23] designs, and the experimental procedure to generate intelligent network intrusion detection system, are elaborated. The proposed methodology is a blend of data pre-processing, feature selection; neural network training and performance measurement to ascertain that malicious network behavior is identified.

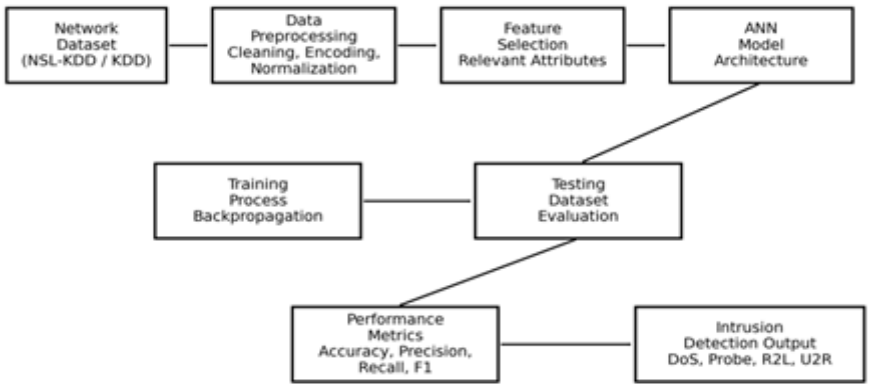
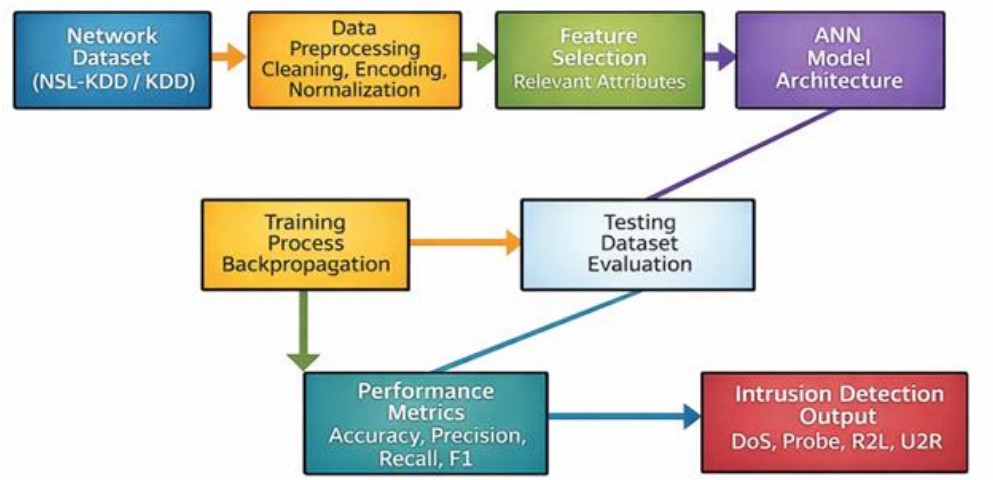


Figure 1: Research framework



Intrusion detection system workflow diagram

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. To begin with, network traffic information are collected on benchmark intrusion detection data and subjected to processing to remove differences and redundant features. An Artificial Neural Network model trained on the sanitized data set can be utilized to predict the network traffic as either normal or malicious. The trained model is evaluated by performance metrics to determine the effectiveness of the trained model in detecting network intrusions [24], [25].

Data sets of the CCTV system in question: There is a publicly accessible benchmark data set available to train and test the proposed intrusion detection system. The data set includes labeled data sets of network traffic of examples of normal network traffic and various types of cyberattacks. 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 data sets represent diverse categories of attacks such as Denial of Service (DoS), Probe attacks, Remote-to-Local (R2L), and User-to-Root (U2R). Such attacks are standard security threats that are encountered in the network environment [26], [27].

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 illustrates equal distribution of normal and toxified traffic cases, allowing for training and evaluation of the machine learning models [28].

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

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

Feature Encoding: There are categorical features in intrusion detection data, e.g. protocol type, service and network flag. The attributes are then transformed into numbers using encoding schemes of the label encoding 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. The entire feature values are therefore normalized to a common level of normalization by either the Min-Max scaling technique or the Z-score normalization technique.

Feature Selection: Feature selection works to enlarge the dimensions of the dataset, as it identifies the most captive attributes that will aid in the detection of intrusion. This eliminates any overlapping features that increase computation efficiency and prevents 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 human body. An ANN consists of nodes interconnected in layers; the input layer, hidden layers and the output layer. These layers operate on the input information by applying weighted connections and activation functions in order to provide classification outputs [29], [30].

The proposed intrusion detection model utilizes a multilayer feed forward neural network.

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 attack

All neurons receive the input signals and multiply them by weights respectively and an activation function is used to give an output. The learning process adjusts these weights such that the classification errors are minimised.

ANN training Process: The processing dataset is passed through the neural network and the learn weights are adjusted by a learning algorithm.

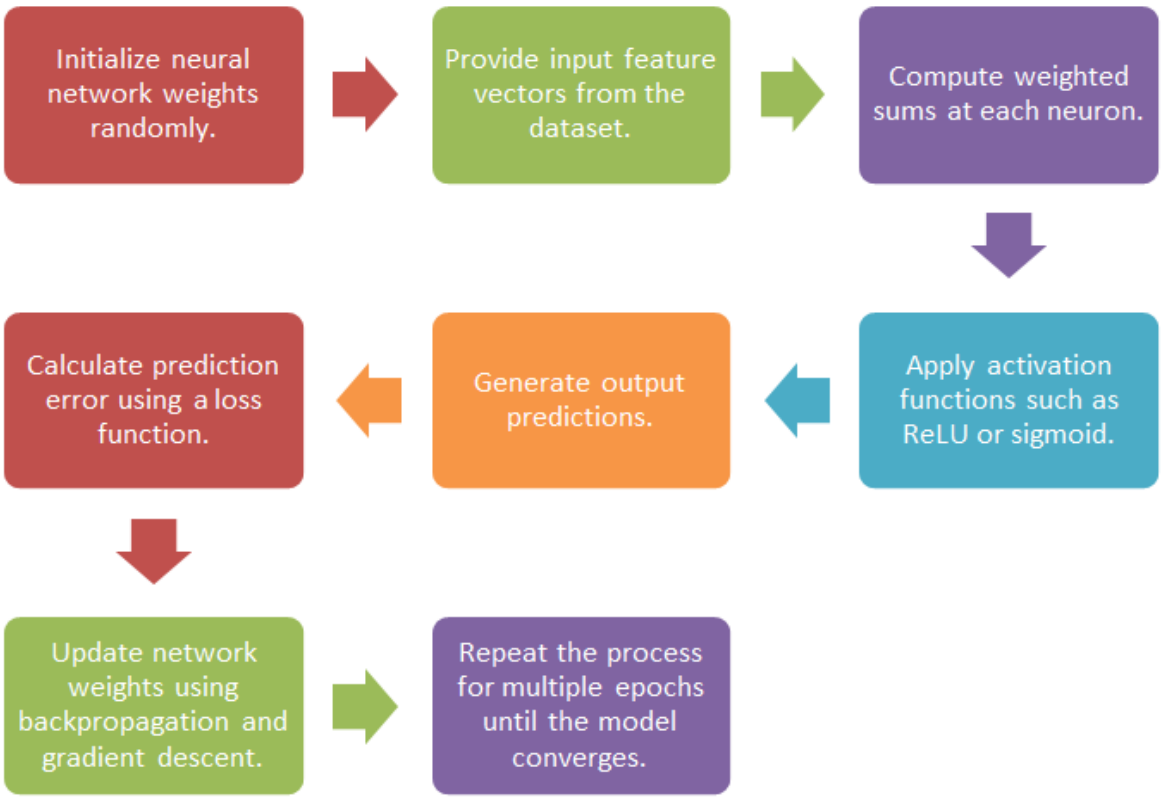
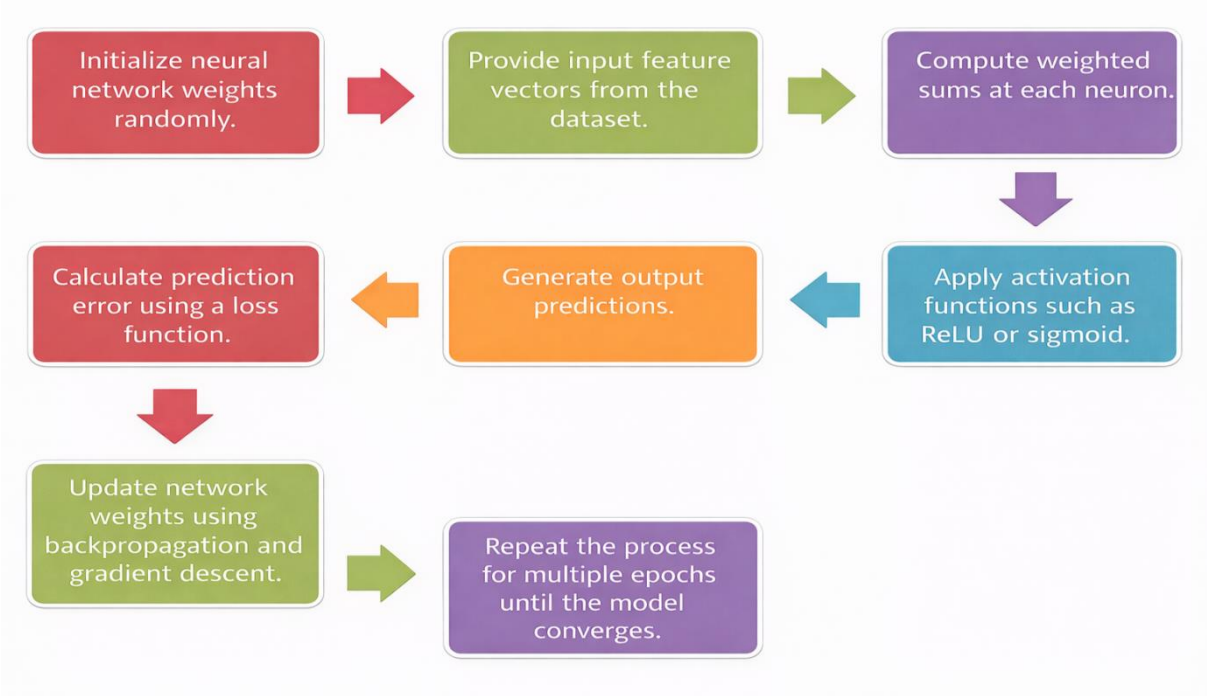


Figure 2: Training Steps



Neural networking flowchart process

The error is then propagated backwards through the network using backpropagation and the weights are updated in such a manner that the error is reduced to enhance the accuracy of the prediction.

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

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

ANN model is trained to differentiate these type of attacks based on the interconnection of network traffic characteristics.

Performance Evaluation Metrics: In order to measure the effectiveness of the proposed intrusion detection system, various performance metrics are applied.

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	Rate at which normal traffic is classified as an attack

These measures offer a detailed analysis of the intrusion detection system and aid in establishing its performance effectiveness within the real-world networks context [31].

Implementation Environment: The suggested ANN-based intrusion detection model is implemented on popular machine learning libraries and software platforms.

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, 16GB RAM

Python has advanced features in data analysis, machine learning, and neural network modeling that can be used to build intrusion detection systems.

RESULTS

This section details the experimentation outcomes of the proposed Network Intrusion Detection System (IDS) using the Artificial Neural Network (ANN). The model has been evaluated on benchmark intrusion detection datasets aimed at identifying the effectiveness of the model in regard to the detection of malicious activities on the networks. Evaluation of the experimentation outcomes was based on the standard measures of performance, which include accuracy, precision, recall, F1-score, and the false positive rate.

The performance of model training: The ANN was trained on the preprocessed traffic internetwork and examples of attacks and normal. The training cycle was delineated by the splitting of the dataset into the training and testing dataset 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 assure stable model convergence and improved classification accuracy. The outcome of the experiment indicates that the ANN model was proficient in both identifying normal and the 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

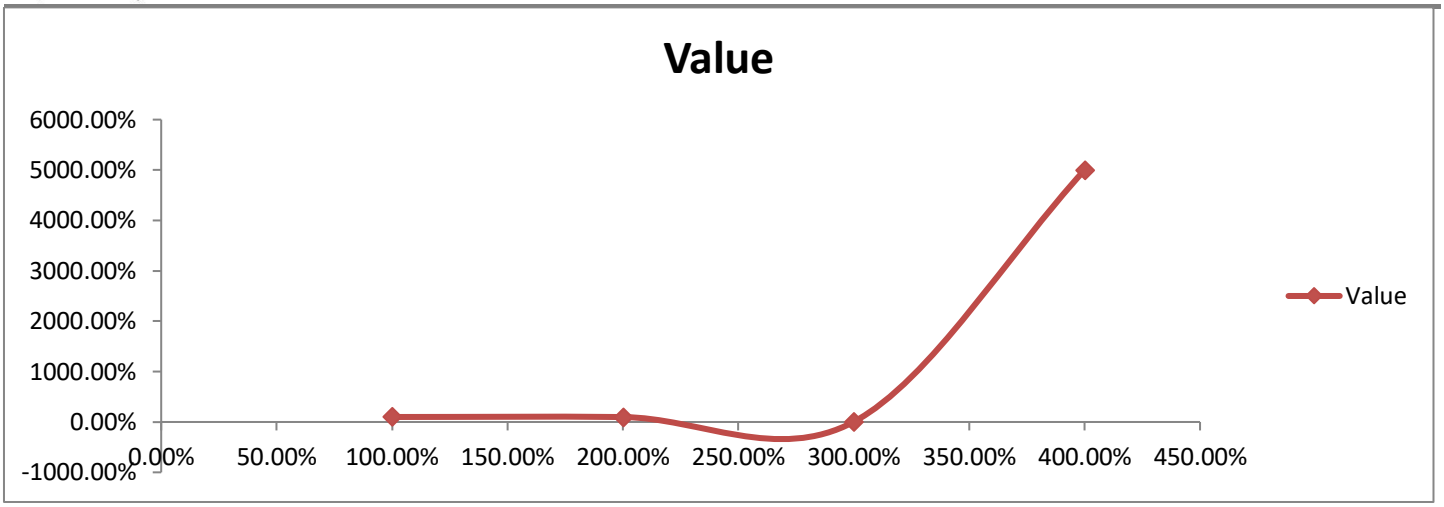


Figure 3: Performance metrics

Sharp growth in value chart

The outcome of the training process implies that the neural network succeeded in both successfully structuring the intricate patterns within the features of network traffic, and, furthermore, the network demonstrated an ability to minimize the errors concerning the predictions during the process of learning.

Evaluation of the Detection of Intrusions: The ANN-based model for detecting intrusions that has been proposed 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 [32].

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%

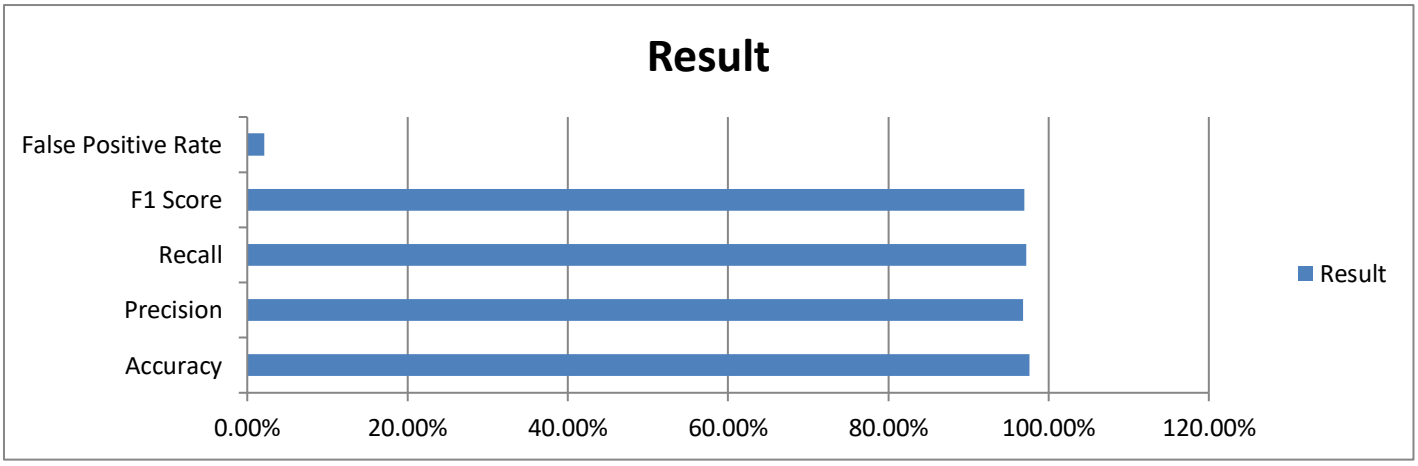


Figure 4: Performance analysis

An accuracy of 97.6 suggests the ANN model proposed "can be trusted to classify network traffic as normal traffic or network attack". Most detected intrusions as a captured malicious activity were correctly identified; the model scored 96.8%. Also, a recall of 97.2 suggests the model detected real attacks in the network traffic [33].

Attack Type Detection. The model was assessed on the ability to identify various categories of cyberattacks that are common in the data of intrusions in networks.

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%

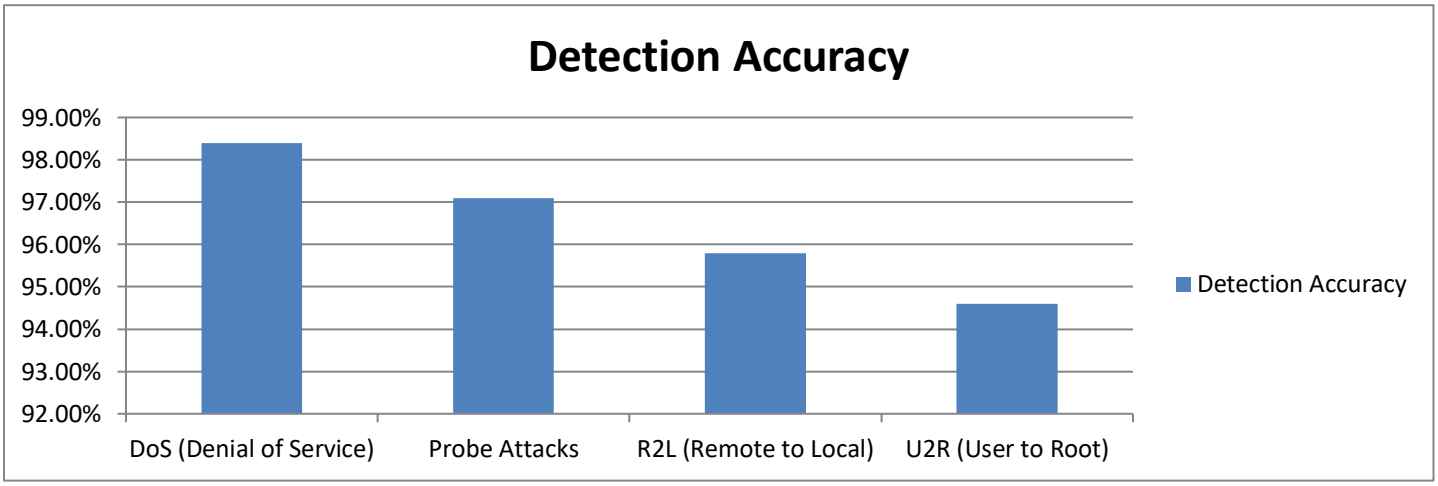


Figure 5: Attack accuracy

The results indicate that the ANN model works particularly well for identifying Denial of Service (DoS) attacks due to their unique traffic pattern. While the rates are somewhat lower, the rate of R2L and U2R attacks is still significant, which shows that the model is able to identify sophisticated intrusive attempts.

Performance Comparison: To further confirm the effectiveness of the proposed ANN model, the performance of the model was compared to that of a number of traditional machine learning models applied to intrusion detection systems.

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%**

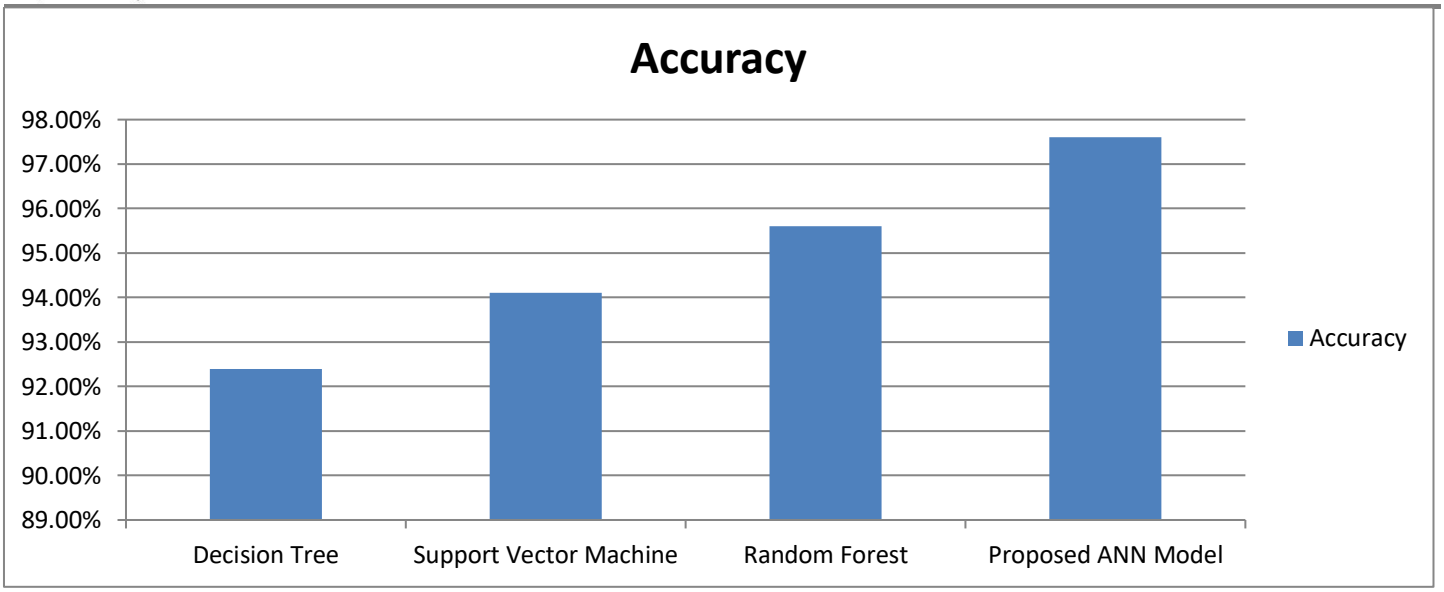


Figure 6: Comparison analysis

Based on the comparison, it can be concluded that the techniques that are based on Artificial Neural Networks (ANN) are significantly better than the classical machine learning techniques in regard to accuracy of detection. 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 [34],[35].

The proposed ANN-based intrusion detection system has yielded positive results in the detection of intelligent intrusion cyber threats within the network. The system demonstrated high accuracy and adequately low false positive rates, 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 defenses. The results of the experiments are a solid basis for the use of ANN-type models for the analysis of network data traffic of high complexity and high dimensionality. The proposed model is a good candidate for the new technologies such as cloud computing, Internet of Things (IoT), and smart networking technologies for real-time intrusion detection. The results of the experiments proved that the proposed ANN-based Idefense system is the proposed model that can solve the problem of enhancing network security in the modern digital ecosystems.

CONCLUSION

The increased dependency on digital communication, clouds, and networks has warranted increased focus on network security and cyber security. DoS attacks, probing attacks and unauthorised access attempts. However, legacy intrusion detection systems using signature detection methods, on the other hand, are unable to detect newer and more advanced attacks, thus, decreasing their efficacy for today's networks. To combat this, the current paper introduces what we call the autonomous network intrusion detection methodology, which attempts to blank. The absence of advanced machine learning models will put the attacker at a significant speed advantage. The system utilises the ability of ANN to learn and recognise patterns to comprehensively assess and categorise 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 pre-processing strategies, namely, data cleaning, feature encoding and feature normalisation were implemented to improve the quality of the data to the models.It developed multilayer neural network architectures meant to internalise nonlinear connections among the components of network traffic and to discern possible cyber threats.

The experimental research findings measurably 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 when compared to traditional machine learning algorithms. 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 ANN, provided that the identification of more sophisticated profiles of attacks and adjustment to the dynamic conditions of networks are required. In addition, the ANN-based model has been shown, through benchmarking, to be superior to traditional techniques of classification, like 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, and, therefore, it can be successfully integrated into the contemporary network structure, such as cloud computing, enterprise networks, and The Internet of Things (IoT). By providing the capability for the systematic detection and response to the threats in a network in real-time, it enhances a network and the computing system's availability and reliability. Additionally, it minimizes the likely financial and operational consequences of the breaches of cybersecurity. This research maintains that an ANN approach constitutes a practical solution for network intrusion detection systems that are based on artificial intelligence.In future research for a subsequent generation, the focus could be on integrating both deep learning models and hybrid machine learning approaches with real-time streaming data analysis for the further enhancement of network systems intrusion detection and/or cybersecurity hardening.

REFERENCES

1. D. E. Denning, “An intrusion-detection model,” IEEE Trans. Softw. Eng., vol. SE-13, no. 2, pp. 222–232, 1987.
2. S. Axelsson, “Intrusion detection systems: A survey and taxonomy,” Technical Report, Chalmers University of Technology, 2000.
3. W. Lee and S. J. Stolfo, “A framework for constructing features and models for intrusion detection systems,” ACM Trans. Inf. Syst. Secur., vol. 3, no. 4, pp. 227–261, 2000.
4. Shad Kirmani and Padma Raghavan. 2013. Scalable parallel graph partitioning. In Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis (SC '13). Association for Computing Machinery, New York, NY, USA, Article 51, 1–10. https://doi.org/10.1145/2503210.2503280
5. Kirmani S, Park J, Raghavan P. An embedded sectioning scheme for multiprocessor topology-aware mapping of irregular applications. The International Journal of High Performance Computing Applications. 2017;31(1):91-103. doi:10.1177/1094342015597082
6. S. Kirmani and M. Shankar, “Generating keywords by associative context with input words,” US Patent US10699302B2, Jun. 30, 2020. [Online]. Available: https://patents.google.com/patent/US10699302B2/en
7. S. Kirmani and K. Madduri, "Spectral Graph Drawing: Building Blocks and Performance Analysis," 2018 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW), Vancouver, BC, Canada, 2018, pp. 269-277, doi: 10.1109/IPDPSW.2018.00053
8. S. Kirmani, H. Sun and P. Raghavan, "A Scalability and Sensitivity Study of Parallel Geometric Algorithms for Graph Partitioning," 2018 30th International Symposium on Computer Architecture and High Performance Computing (SBAC-PAD), Lyon, France, 2018, pp. 420-427, doi: 10.1109/CAHPC.2018.8645916.
9. Ashirbad Mishra, Shad Kirmani, and Kamesh Madduri. 2020. Fast Spectral Graph Layout on Multicore Platforms. In Proceedings of the 49th International Conference on Parallel Processing (ICPP '20). Association for Computing Machinery, New York, NY, USA, Article 45, 1–11. https://doi.org/10.1145/3404397.3404471
10. Tyler J, Pastor J, Huhns MN, Kirmani S, Du H. Exposing, formalizing and reasoning over the latent semantics of tags in multimodal data sources. Applied Ontology. 2013;8(2):95-130. doi:10.3233/AO-130124
11. Mishra, S. Kirmani and K. Madduri, "Fast Sentence Classification using Word Co-occurrence Graphs*," 2024 IEEE International Conference on Big Data (BigData), Washington, DC, USA, 2024, pp. 620-629, doi: 10.1109/BigData62323.2024.10825869.

12. S. Kirmani, “Exploiting Graph Embedding for Parallelism and Performance,” Ph.D. dissertation, Dept. of Computer Science and Engineering, The Pennsylvania State University, University Park, PA, USA, 2014. Available: https://etda.libraries.psu.edu/catalog/27325
13. F. Kirmani, B. J. Lane and J. R. Rose, "Exploring Machine Learning Techniques to Improve Peptide Identification," 2019 IEEE 19th International Conference on Bioinformatics and Bioengineering (BIBE), Athens, Greece, 2019, pp. 66-71, doi: 10.1109/BIBE.2019.00021.
14. Fawad Kirmani, Bryan Lane, and John Rose. 2025. Identifying Proteotypic Peptides via Deep Learning. In Proceedings of the 11th International Conference on Bioinformatics Research and Applications (ICBRA '24). Association for Computing Machinery, New York, NY, USA, 42–47. https://doi.org/10.1145/3700666.3700691
15. Fawad Kirmani, Ananthavishnu S Unni, Varsha P Kulkarni, Kyle Lackey, John R Rose, Detecting polar ring galaxies via deep learning, RAS Techniques and Instruments, Volume 4, 2025, rzaf043, https://doi.org/10.1093/rasti/rzaf043
16. Kirmani, F., “Detecting Strongly-Lensed Supernovae in Wide-field Space Telescope Imaging via Deep Learning”, arXiv e-prints, Art. no. arXiv:2512.19886, 2025. doi:10.48550/arXiv.2512.19886.
17. M. Alenezi, M. Nadeem, A. Agrawal, R. Kumar, and R. A. Khan, “Fuzzy multi criteria decision analysis method for assessing security design tactics for web applications,” Int. J. Intell. Eng. Syst., vol. 13, no. 5, 2020, doi: 10.22266/ijies2020.1031.17.
18. M. Ahmad et al., “Healthcare device security assessment through computational methodology,” Comput. Syst. Sci. Eng., vol. 41, no. 2, 2022, doi: 10.32604/csse.2022.020097.
19. H. Alyami et al., “The evaluation of software security through quantum computing techniques: A durability perspective,” Appl. Sci., vol. 11, no. 24, 2021, doi: 10.3390/app112411784.
20. W. Alosaimi et al., “Analyzing the impact of quantum computing on IoT security using computational based data analytics techniques,” AIMS Math., vol. 9, no. 3, pp. 7017–7039, 2024, doi: 10.3934/math.2024342.
21. Alharbi et al., “Managing Software Security Risks through an Integrated Computational Method,” Intell. Autom. Soft Comput., vol. 28, no. 1, p. 179, Mar. 2021, doi: 10.32604/IASC.2021.016646.
22. S. H. Almotiri, M. Nadeem, M. A. Al Ghamdi, and R. A. Khan, “Analytic Review of Healthcare Software by Using Quantum Computing Security Techniques,” Int. J. Fuzzy Log. Intell. Syst., vol. 23, no. 3, pp. 336–352, Sep. 2023, doi: 10.5391/IJFIS.2023.23.3.336.
23. M. Nadeem, M. Ahmad, M. Ahmad, P. C. Pathak, S. Gupta, and H. Pandey, “Evaluating the Factors of CGTMSE Scheme in Bank by Using Fuzzy AHP,” in 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), 2023, vol. 6, pp. 56–61, doi: 10.1109/IC3I59117.2023.10397669.
24. F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar, and R. A. Khan, “Integrity Assessment of Medical Devices for Improving Hospital Services,” Comput. Mater. Contin., vol. 67, no. 3, p. 3619, Mar. 2021, doi: 10.32604/CMC.2021.014869.
25. P. C. Pathak, M. Nadeem, and S. A. Ansar, “Security assessment of operating system by using decision making algorithms,” Int. J. Inf. Technol., 2024, doi: 10.1007/s41870-023-01706-9.
26. Masood Ahmad, F. Al-Amri, “Healthcare Device Security Assessment through Computational Methodology,” Comput. Syst. Sci. Eng., vol. 41, no. 2, pp. 811–828, 2022, doi: 10.32604/csse.2022.020097.
27. H. Alyami et al., “Analyzing the data of software security life-span: Quantum computing era,” Intell. Autom. Soft Comput., vol. 31, no. 2, 2022, doi: 10.32604/iasc.2022.020780.
28. F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar, and R. A. Khan, “Integrity Assessment of Medical Devices for Improving Hospital Services,” Comput. Mater. Contin., vol. 67, no. 3, 2021, doi: 10.32604/cmc.2021.014869.
29. F. Alassery, A. Alzahrani, A. I. Khan, A. Khan, M. Nadeem, and M. T. J. Ansari, “Quantitative Evaluation of Mental-Health in Type-2 Diabetes Patients Through Computational Model,” Intell. Autom. Soft Comput., vol. 32, no. 3, 2022, doi: 10.32604/IASC.2022.023314.
30. M. Nadeem, “Deep Learning Approach for Classifying DDoS Attack Traffic in SDN Environments”, JISCR, vol. 7, no. 2, pp. 109-126, Dec. 2024.

31. Mohd Nadeem, Amal Krishna Sarkar, Mohammed Ishrat, "Securing information systems through quantum computing Grover's algorithm approach", Computational Intelligence Applications in Cyber Security, 1st Edition, 2024.
32. Mohd Nadeem, Prabhash Chandra Pathak, Masood Ahmad, Nafees Akhter Farooqui, "Identification of security factors in cloud computing Defence security perspective", Computational Intelligence Applications in Cyber Security, 1st Edition, 2024.
33. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in Military Communications and Information Systems Conf., 2015.
34. M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 dataset," in IEEE Symp. Computational Intelligence for Security and Defense Applications, 2009.
35. K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems," NIST Special Publication 800-94, 2007.
36. M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. USENIX Conf. System Administration, 1999.