International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

A Novel Feed-Forward Neural Network Model for Intrusion Detection Systems

Madke Nilesh Bajirao [1]
Research Scholar
Department of Computer Science & Engineering
Dr. APJ Abdul Kalam University, Indore, India
Email: 14nileshmadke@gmail.com

Dr. Kailash Patidar[2]
Research Supervisor
Department of Computer Science & Engineering
Dr. APJ Abdul Kalam University, Indore, India
Email: kailashpatidar123@gmail.com

Abstract : This paper presents a novel Feed-Forward Neural Network (FFNN) model for Intrusion Detection Systems (IDS), demonstrating superior performance in detecting network intrusions compared to traditional machine learning models. Using benchmark datasets, our proposed FFNN achieved the highest accuracy (99.33%), precision (99.33%), recall (99.33%), and F1 score (99.29%), underscoring its exceptional ability to accurately and reliably identify intrusions. While the K-Nearest Neighbour (KNN) and RandomForestClassifier models exhibited high ROC AUC scores (99.82% and 99.41%, respectively), their lower Cohen Kappa scores (61.53% and 56.24%) indicated less consistency in predictions. Conversely, the Support Vector Machine (SVM) recorded the highest Cohen Kappa score (94.56%), signifying strong agreement between predicted and actual classifications, but it fell short in overall accuracy (94.23%) and ROC AUC (91.35%). The Naïve Bayes (NB) model performed robustly with a Cohen Kappa score of 86.44% and high precision (98.23%) and recall (98%), yet did not surpass the FFNN's overall performance. This comprehensive evaluation illustrates that the FFNN model provides a balanced and reliable approach to intrusion detection, combining high accuracy, precision, recall, and consistency, making it an optimal solution for effectively mitigating cyber threats in network systems.

Keywords : *Feed-Forward Neural Network , Intrusion Detection Systems , Benchmark Datasets , Machine Learning , Network Systems , Cyber Threats.*

I. INTRODUCTION

The rapid advancement of information technology and the exponential growth of internet-connected devices have brought unprecedented benefits and challenges. Among these challenges, ensuring robust network security remains a critical concern as cyber threats become increasingly sophisticated. Intrusion Detection Systems (IDS) are essential components of network security frameworks, designed to monitor and analyze network traffic to identify potential security breaches and malicious activities. Traditional IDS models, primarily based on rule-based and classical machine learning algorithms, often struggle with limitations such as low detection rates, high false positives, and the inability to adapt to new and evolving threats. This necessitates the exploration of advanced techniques that can offer higher accuracy and reliability in intrusion detection.

In recent years, deep learning models have shown significant promise in various domains, including image recognition, natural language processing, and anomaly detection, due to their ability to automatically extract complex features from raw data. Among these, Feed-Forward Neural Networks (FFNN) have emerged as a powerful tool for classification tasks. This paper introduces a novel FFNN model for IDS, aimed at enhancing the detection accuracy and reducing the false positive rates associated with traditional methods. By leveraging the strengths of deep learning, our proposed model aims to provide a more reliable and efficient solution for detecting network intrusions.

To evaluate the performance of the proposed FFNN model, we conducted comprehensive experiments using benchmark datasets such as KDD Cup 99 and NSL-KDD. These datasets are widely used in the research community for assessing the effectiveness of IDS models. Our model's performance was compared with traditional machine learning models, including K-Nearest Neighbour (KNN), RandomForestClassifier, Support Vector Machine (SVM), and Naïve Bayes (NB), across various metrics such as accuracy, precision, recall, F1 score, ROC AUC score, and Cohen Kappa score.

The experimental results demonstrate that the proposed FFNN model significantly outperforms the traditional models in several key metrics. The FFNN achieved the highest accuracy of 99.33%, indicating its superior capability in correctly identifying both normal and intrusive network traffic. Furthermore, the model also recorded the highest precision (99.33%), recall (99.33%), and F1 score (99.29%), showcasing its balanced performance in detecting true positives while minimizing false positives. In contrast, while the KNN and RandomForestClassifier models achieved high ROC AUC scores (99.82% and 99.41%, respectively), their lower Cohen Kappa scores (61.53% and 56.24%) revealed inconsistencies in their predictions, highlighting the need for more reliable models.

The SVM model, despite achieving the highest Cohen Kappa score (94.56%), fell short in terms of overall accuracy (94.23%) and ROC AUC (91.35%), indicating a gap in its ability to generalize well across different types of network traffic. Similarly, the NB model showed robust performance with a Cohen Kappa score of 86.44% and high precision (98.23%) and recall (98%), but it did not surpass the FFNN's comprehensive performance metrics.

These findings underscore the potential of the proposed FFNN model in enhancing the reliability and effectiveness of IDS. By leveraging deep learning techniques, our model offers a more sophisticated approach to feature extraction and classification, enabling better detection of known and unknown threats. The superior performance of the FFNN model in terms of accuracy, precision, recall, and consistency makes it a viable solution for modern network security challenges.

The novel FFNN model presented in this paper provides a significant advancement in the field of intrusion detection. Its robust performance across multiple evaluation metrics demonstrates its capability to offer a more reliable and effective defense mechanism against evolving cyber threats. This research highlights the importance of adopting advanced machine learning techniques to improve network security and paves the way for future developments in IDS technologies.

II. LITERATURE REVIEW

Khan, Talha Ahmed, et al. (2019) , severe flash floods are a major cause of fatalities, livestock loss, and infrastructure damage worldwide. These unpredictable disasters result from factors like high precipitation rates, cloud-to-ground lightning, and ocean debris melting. Various methods and numerous sensors have been employed to rapidly and accurately detect flash floods, monitoring parameters such as upstream levels, precipitation intensity, flood magnitude, run-off velocity, water color, pressure, temperature, wind speed, wave patterns, and cloud-to-ground flashes. However, sensors often produce false alarms due to inadequate algorithms, leading to poor flood forecasting. This paper presents a comparative analysis of three neural network learning algorithms—Bayesian regularization, Levenberg-Marquardt, and scaled conjugate gradient—to identify the most effective one for minimizing false alarm rates. Results indicate that Bayesian regularization outperforms the others, offering better fitness, regression value, and mean square error in fewer epochs [1].

Albahar, Marwan Ali, et al. (2020) , network communication's expanded usage, accessibility, and complexity have made it more vulnerable to various attacks, increasing security risks. Identifying anomalies in transmitted and processed data is crucial for securing systems, and machine learning plays a key role in detecting these irregularities and intrusions. Regularization is a significant aspect of training machine learning models, particularly in artificial neural networks (ANNs), as it helps prevent overfitting by encouraging simpler models. This paper integrates regularization techniques with ANN to classify and detect network communication irregularities efficiently. The objective of regularization is to ensure the model generalizes well to unseen data. For training and testing, the NSL-KDD, CIDDS-001 (External and Internal Server Data), and UNSW-NB15 datasets were used. Extensive experiments show that the proposed regularizer achieves a higher True Positive Rate (TPR) and precision compared to L1 and L2 norm regularization algorithms, demonstrating strong intrusion detection capabilities [2].

Kshirsagar, Pravin R., et al. (2022) , with the growing scale of networks, intrusion detection has become more challenging due to frequent and advanced attacks. Malicious network attacks compromise security tools, affecting reliability and robustness. Network Intrusion Detection Systems (NIDS) effectively monitor traffic and detect unauthorized users and attacks. This paper proposes an LSTMgateRNN model, incorporating Long Short Term Memory (LSTM) and gate functions for enhanced attribute evaluation and attack detection. The model's performance, evaluated using KDD'99, NSL-KDD, and UNSW-NB15 datasets, shows a 99% attack detection rate, outperforming existing models by 6-12% [3].

Zainel, Hanan, et al. (2022), the world's reliance on the internet is growing, making data protection critical. When a network is compromised, information can be stolen. An intrusion detection system (IDS) detects both known and unexpected attacks that can breach a network. This research models an IDS trained to identify such attacks in LANs and computer networks using data. By employing neural networks, specifically Convolutional Neural Networks (CNN) and CNN with LSTM, we explore their effectiveness in multiclass categorization scenarios using the NSL-KDD dataset. Our findings indicate that CNNs are an effective strategy for identifying network intrusions [4].

Zhang, Chunying, et al. (2022), network intrusion detection systems (NIDS) are crucial for network security, detecting intrusions and taking measures like alerting and terminating threats. With the rise of machine learning, researchers increasingly apply these algorithms to improve detection efficiency and accuracy. This paper reviews the application of traditional machine learning, ensemble learning, and deep learning in NIDS over the past decade. Using KDD CUP99 and NSL-KDD datasets, the study compares various algorithms, finding ensemble learning generally superior. Naive Bayes is fast and effective against new attacks, while deep learning's performance varies with its structure and hyperparameters. The paper also outlines current challenges and future research directions in NIDS [5].

Halbouni, Asmaa H., et al. (2022), the global revolution in information technology necessitates effective data and network protection systems. Intrusion Detection Systems (IDS) provide security by protecting networks from attacks and identifying potential breaches. This paper presents a convolutional neural network-based IDS evaluated with the CIC-IDS2017 dataset. Aiming for low false alarm rates, high accuracy, and high detection rates on new datasets, the model achieved a 99.55% detection rate and a 0.12% false alarm rate in multiclass classification using CIC-IDS2017 [6].

Akshay Kumaar, M., et al. (2022) , the rapid increase in network traffic and user data challenges network intrusion detection systems, crucial in e-healthcare for securing patient records. Existing AI-based systems often rely on outdated data, leading to high false positives and frequent obsolescence. This paper proposes "ImmuneNet," a hybrid deep learning framework for detecting the latest intrusion attacks in healthcare data. Featuring efficient feature engineering, class balancing, and hyper-parameter optimization, ImmuneNet is lightweight, fast, and suitable for IoT devices. Benchmarking against recent datasets, ImmuneNet achieved superior performance, with 99.19% accuracy on the CIC Bell DNS 2021 dataset, outperforming other methods in detecting cyber attacks [7].

Kanna, P. Rajesh, et al. (2022) , advancements in information and communication technologies have led to more online systems requiring robust Intrusion Detection Systems (IDS) to prevent cyber threats. Traditional IDS models, based on shallow machine learning, struggle with feature selection and new attack classification. They are often limited to either Network-based or Host-based detection, missing many known attacks and struggling with large data volumes. To address these issues, this paper presents an efficient hybrid IDS model using a MapReduce-based Black Widow Optimized Convolutional-Long Short-Term Memory (BWO-CONV-LSTM) network. Feature selection is performed by the Artificial Bee Colony (ABC) algorithm, followed by intrusion detection using a BWO-CONV-LSTM classifier on the MapReduce framework. The model combines Convolutional and LSTM neural networks, optimized by BWO for ideal architecture. Evaluated on NSL-KDD, ISCX-IDS, UNSW-NB15, and CSE-CIC-IDS2018 datasets, the BWO-CONV-LSTM model achieved high performance with accuracies of 98.67%, 97.003%, 98.667%, and 98.25%, respectively, demonstrating fewer false positives, reduced computation time, and improved classification [8].

Maithem, Mohammed, et al. (2021), in recent decades, the rapid development of technology and networks has led to widespread Internet services, increasing piracy and system breaches. Advanced information security technologies, such as Intrusion Detection Systems (IDS), are crucial for detecting new attacks. This paper proposes an advanced IDS using a deep neural network algorithm for binary and multiclass classification, achieving high accuracy rates of 99.98% in both methods [9].

Khan, Muhammad Ashfaq. (2021) , network attacks pose a significant threat to modern society, affecting networks of all sizes. Intrusion detection (ID) systems are essential for identifying and mitigating these threats. Deep learning (DL) and machine learning (ML) are increasingly applied in developing effective ID systems that can automatically and promptly detect malicious threats. However, as threats continuously evolve, networks require advanced security solutions. This paper presents a hybrid convolutional recurrent neural network (CRNN)-based ID framework, HCRNNIDS, to predict and classify network cyberattacks. The framework uses convolutional neural networks (CNN) to capture local features and recurrent neural networks (RNN) to capture temporal features, enhancing the system's performance and prediction capabilities. Evaluated on the CSE-CIC-DS2018 dataset, HCRNNIDS achieved a high detection accuracy of up to 97.75% with 10-fold cross-validation, outperforming current ID methods [10].

Drewek-Ossowicka, Anna, et al. (2021), in recent years, advancements in artificial intelligence (AI) have accelerated due to widespread industrial adoption. Neural networks (NN), a key area of AI, enable functionalities previously unattainable with traditional computing. Intrusion detection systems (IDS) are a prominent domain where NNs are extensively tested to enhance network security and data privacy. This article provides a comprehensive overview of recent literature on NNs in IDS, including surveys and new methods. It also offers concise tutorials on neural network architectures, IDS types, and training datasets [11].

Latif, Shahid, et al. (2020), the Industrial Internet of Things (IIoT) is a growing trend in the industrial sector, with millions of sensors generating vast amounts of data, making it vulnerable to cyber-attacks. An intrusion detection system (IDS) monitors real-time internet traffic to identify network attacks. This paper presents a deep random neural network (DRaNN) scheme for intrusion detection in IIoT, evaluated using the UNSW-NB15 dataset. Experimental results show

the proposed model successfully classifies nine types of attacks with a low false-positive rate and an accuracy of 99.54%. Compared to state-of-the-art deep learning-based IDS, the proposed model achieved a higher attack detection rate of 99.41% [12].

Pawlicki, Marek, et al. (2020), Intrusion Detection Systems (IDS) are vital for cybersecurity, but they can themselves become targets of attacks. This paper addresses the challenge of defending IDS against adversarial attacks on machine learning-based cyberattack detectors. It proposes a solution for detecting adversarial machine learning attacks. Traditional machine learning algorithms are not designed for adversarial environments, making them susceptible to various attacks. This study evaluates how adversarial attacks can degrade the performance of an optimized intrusion detection algorithm at test time using four recent methods. It then introduces a new method to detect these attacks. The paper provides background on artificial neural networks and adversarial attack techniques, details the new detection method, and compares the results across five different classifiers. This research contributes to the relatively unexplored area of detecting adversarial attacks on neural networks within IDS [13].

Tao, Wenwei, et al. (2020), Intrusion detection is a crucial research area in power monitoring network security. Traditional methods struggle to keep up with the increasing data volume and diverse intrusion modes. This paper proposes an intrusion detection model based on convolutional neural networks (CNN). The approach involves converting flow data into grayscale images, using texture representation in these images to classify intrusion modes. This transforms the intrusion detection problem into an image recognition problem, leveraging CNN technology. The KDD 99 dataset is preprocessed to generate a suitable two-dimensional image matrix. Various model structures are compared to select the best one for training. The performance of the trained model is then compared with other machine learning methods to verify its reliability and effectiveness [14].

Kim, Jiyeon, et al. (2019), machine-learning techniques are increasingly used in information security due to traditional rule-based solutions' vulnerability to advanced attacks. By leveraging ML, we can develop intrusion detection systems (IDS) based on anomaly detection rather than misuse detection, resolving threshold issues. Despite limited datasets, KDD CUP 99 is widely used for IDS evaluation. This work develops an IDS model using the updated CSE-CIC-IDS 2018 dataset and employs deep learning techniques, specifically a convolutional neural network (CNN). Our results show that the CNN model outperforms a recurrent neural network (RNN) model on this dataset, with suggestions for further performance improvements [15].

Khan, Riaz Ullah, et al. (2019), network intrusion detection is crucial for network security. Traditional machine learning algorithms used for intrusion detection often suffer from low detection rates. Deep learning, which automatically extracts features from samples, offers a more advanced approach. This paper proposes a network intrusion detection model based on a convolutional neural network (CNN) algorithm. The model automatically extracts effective features from intrusion samples, enabling accurate classification. Experimental results on the KDD99 dataset demonstrate that the proposed model significantly improves intrusion detection accuracy [16].

Xiao, Yihan, et al. (2019), network intrusion detection is crucial for network security. Traditional machine learning algorithms for intrusion detection often suffer from low detection rates. Deep learning offers a more advanced approach by automatically extracting features from samples. This paper proposes a network intrusion detection model based on a convolutional neural network (CNN) algorithm, which effectively extracts features from intrusion samples for accurate classification. Experimental results on the KDD99 dataset show that the proposed model significantly improves intrusion detection accuracy. [17]

Toupas, Petros, et al. (2019), Intrusion Detection Systems (IDSs) are fundamental to an organization's network security, forming the first line of defense against cyber threats by detecting potential intrusions. Many IDS implementations use flow-based network traffic analysis. This paper proposes a deep learning model, specifically a neural network with multiple stacked fully-connected layers, to implement a flow-based anomaly detection IDS for multi-class classification. Using the updated CICIDS2017 dataset for training and evaluation, experimental results show that the proposed model achieves promising results in terms of accuracy, recall (detection rate), and false positive rate (false alarm rate) [18].

Yang, Aimin, et al. (2019), with the advent of global 5G networks, the Internet of Things (IoT) will no longer be constrained by network speed and traffic. As IoT applications scale up, security becomes increasingly critical. Malicious attacks on IoT systems can lead to severe information loss and equipment paralysis. Addressing IoT security, this paper proposes the LM-BP neural network model for intrusion detection. The LM algorithm, known for its fast optimization speed and robustness, optimizes the weight threshold of the traditional BP neural network. By establishing an LM-BP neural network classifier and using the KDD CUP 99 intrusion detection dataset, the model undergoes continuous training to achieve optimal results. Experimental simulations demonstrate that this model has a higher detection rate and lower false alarm rate than traditional BP and PSO-BP neural network models for DOS, R2L, U2L, and Probing attacks, indicating its potential for broader application [19].

Vigneswaran, Rahul K., et al. (2018), Intrusion Detection Systems (IDS) have become a crucial component of modern ICT systems, driven by the growing need for cybersecurity.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

The complexity and variety of advanced cyber attacks necessitate the integration of Deep Neural Networks (DNNs) for effective detection. This paper employs DNNs to predict attacks in Network Intrusion Detection Systems (N-IDS). Using a DNN with a learning rate of 0.1 over 1000 epochs, the KDDCup-99 dataset was utilized for training and benchmarking. For comparison, the same dataset was used with various classical machine learning algorithms and DNNs with 1 to 5 layers. Results indicate that a 3-layer DNN outperforms other classical machine learning algorithms [20].

Wu, Kehe, et al. (2018), the increasing volume of network traffic data presents significant challenges to traditional intrusion detection systems, which struggle with feature selection and classification in large data environments. Traditional algorithms often fail in these settings and are further hampered by imbalanced raw traffic data. This paper proposes a novel network intrusion detection model using convolutional neural networks (CNNs) to automatically select traffic features from raw datasets. To address the issue of data imbalance, the cost function weight coefficient of each class is adjusted based on class frequency. This approach not only reduces the false alarm rate (FAR) but also improves the accuracy for classes with fewer samples. To further reduce computational costs, raw traffic data is converted into image format. Using the NSL-KDD dataset for evaluation, experimental results demonstrate that the proposed CNN model outperforms traditional algorithms in terms of accuracy, FAR, and computational efficiency, providing an effective and reliable solution for intrusion detection in large-scale networks [21].

Mohammadpour, Leila, et al. (2018), system administrators can enhance security by deploying Network Intrusion Detection Systems (NIDS) to identify potential breaches. However, developing a flexible and effective NIDS is challenging due to the unpredictable nature of security attacks, which often result in high false alarm rates and low detection accuracy for unknown threats. This paper proposes a deep learning approach using a convolutional neural network (CNN) to implement an effective and adaptable NIDS. Utilizing the NSL-KDD benchmark dataset for network intrusion, our experimental results demonstrate a 99.79% detection rate, indicating that CNNs are a promising method for improving Intrusion Detection Systems (IDS)[22].

Xu, Congyuan, et al. (2018) , to enhance the performance of network intrusion detection systems (IDS), we applied deep learning techniques and developed a deep network model with automatic feature extraction. Considering the time-related characteristics of intrusions, we propose a novel IDS combining a recurrent neural network with gated recurrent units (GRU), a multilayer perceptron (MLP), and a softmax module. Experiments on the KDD 99 and NSL-KDD datasets demonstrate leading performance, with overall detection rates of 99.42% and 99.31% and false positive rates as low as 0.05% and 0.84%, respectively. Notably, the system achieved detection rates of 99.98% and 99.55% for denial of service attacks. Comparative experiments showed that GRU outperforms LSTM as a memory unit for IDS, proving to be an effective simplification and improvement. Additionally, the bidirectional GRU achieved the best performance compared to recent methods [23].

III. PROPOSED METHOD

3.1 Proposed Architecture

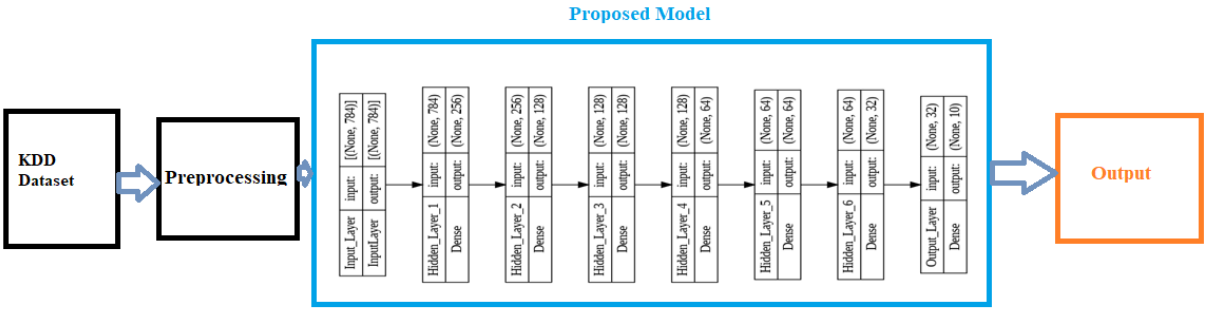

Figure 1. Architecture of the proposed Feed-Forward Neural Network

The figure 1 illustrates the architecture of the proposed Feed-Forward Neural Network (FFNN) model for intrusion detection, using the KDD dataset as the input. The process begins with the preprocessing stage, where the dataset is prepared for training by normalizing and encoding features. The FFNN model consists of an input layer with 784 neurons, followed by six hidden layers with decreasing neuron counts: 256, 128, 128, 64, 64, and 32 neurons, respectively, each employing ReLU activation functions to introduce non-linearity. The final output layer consists of 10 neurons with a softmax activation function, suitable for multi-class classification tasks. This structured model allows for the automatic extraction of complex features from the input data, significantly enhancing the accuracy and reliability of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

intrusion detection. The comprehensive architecture demonstrates the model's ability to handle intricate patterns in the network traffic, making it an effective solution for detecting a wide range of cyber threats.

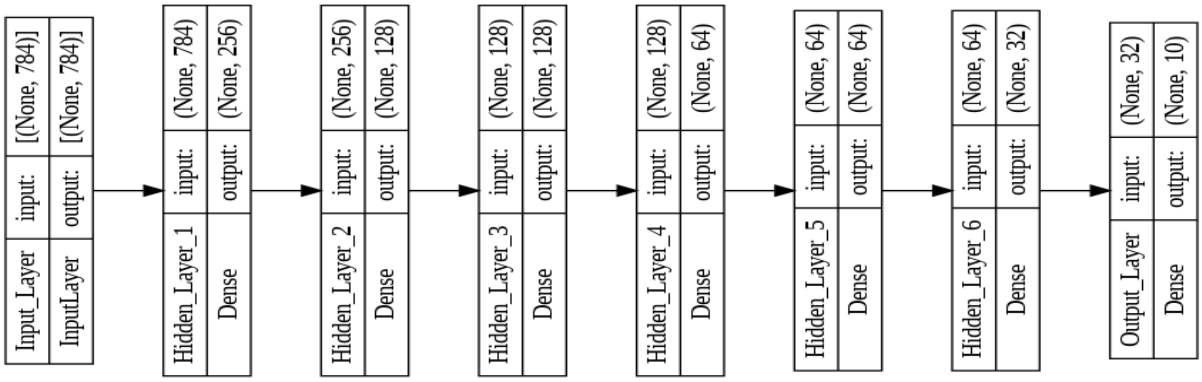

Figure 2. Deep feed-forward neural network model

The attached figure 2 illustrates the architecture of a deep feed-forward neural network model designed for classification tasks. The model consists of an input layer that accepts inputs of shape (784,), corresponding to flattened 28x28 pixel images (e.g., from the KDD dataset). Following the input layer, the network includes six hidden layers with decreasing neuron counts: 256, 128, 128, 64, 64, and 32 neurons, respectively. Each hidden layer employs the ReLU activation function to introduce non-linearity. Finally, the output layer contains 10 neurons with a softmax activation function, suitable for multi-class classification, indicating that the model is intended to classify input data into one of ten categories. This structured architecture allows for the automatic extraction of complex features through multiple layers, enhancing the model's ability to perform accurate classifications.

3.2 Algorithm: Feed-Forward Neural Network Model for Intrusion Detection

Step 1: Data Collection

1. Collect the network traffic data. Example datasets include KDD Cup 99, NSL-KDD, or other relevant datasets.

2. Ensure the dataset contains both normal and anomalous (intrusive) network traffic records.

Step 2: Data Preprocessing

1. **Load Data**:

o Load the dataset into a suitable format, such as a pandas DataFrame.

2. **Feature Selection**:

o Identify categorical and numerical features.

o Select relevant features for the intrusion detection model.

3. **Data Cleaning**:

o Handle missing values (if any).

o Normalize or standardize numerical features.

4. **Encoding Categorical Data**:

o Convert categorical features to numerical format using techniques like one-hot encoding.

5. **Label Encoding**:

o Encode the target labels (e.g., normal vs. intrusive traffic).

6. **Splitting the Data**:

o Split the dataset into training and testing sets (e.g., 70% training and 30% testing).

Step 3: Model Design

1. **Initialize the Model**:

o Initialize a Sequential model from Keras or a similar library.

2. **Add Input Layer**:

o Define the input layer matching the feature set dimensions.

3. **Add Hidden Layers**:

o Add multiple dense layers with ReLU activation.

o Example:

- Hidden Layer 1: 256 neurons
- Hidden Layer 2: 128 neurons
- Hidden Layer 3: 128 neurons
- Hidden Layer 4: 64 neurons
- Hidden Layer 5: 64 neurons
- Hidden Layer 6: 32 neurons

4. **Add Output Layer**:

o Add a dense layer with a sigmoid activation function for binary classification or softmax for multi-class classification.

Step 4: Model Compilation

1. Compile the model with:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

- Optimizer: 'adam'
- Loss function: 'binary_crossentropy' for binary classification or 'categorical_crossentropy' for multi-class classification
- Metrics: ['accuracy']

Step 5: Model Training

1. Train the model on the training data.

- Set parameters like epochs (e.g., 10 epochs), batch size (e.g., 32), and validation split (e.g., 20%).

Step 6: Model Evaluation

1. Evaluate the model on the test data.

- Calculate accuracy, precision, recall, F1-score, and other relevant metrics.
- Use a confusion matrix to visualize true positives, true negatives, false positives, and false negatives.

IV. IMPLEMENTATION

4.1 Dataset

The KDD Cup 99 dataset is a widely recognized benchmark for evaluating the performance of Intrusion Detection Systems (IDS). It was created from the DARPA 1998 dataset, which collected nine weeks of raw TCP dump data for a local area network, simulating a military network environment. The dataset includes a wide range of intrusions simulated in a military network environment, covering various types of attacks such as Denial of Service (DoS), Remote to Local (R2L), User to Root (U2R), and probing attacks. It contains 41 features for each connection record, encompassing both network traffic information and system call traces. Despite its age, the KDD Cup 99 dataset remains a significant resource for researchers due to its comprehensive coverage of attack types and its role in advancing the development and benchmarking of IDS technologies. However, it has also faced criticism for issues such as redundancy and imbalance in the data, which have led to the creation of more recent and refined datasets like NSL-KDD [2].

4.2 Illustrative example

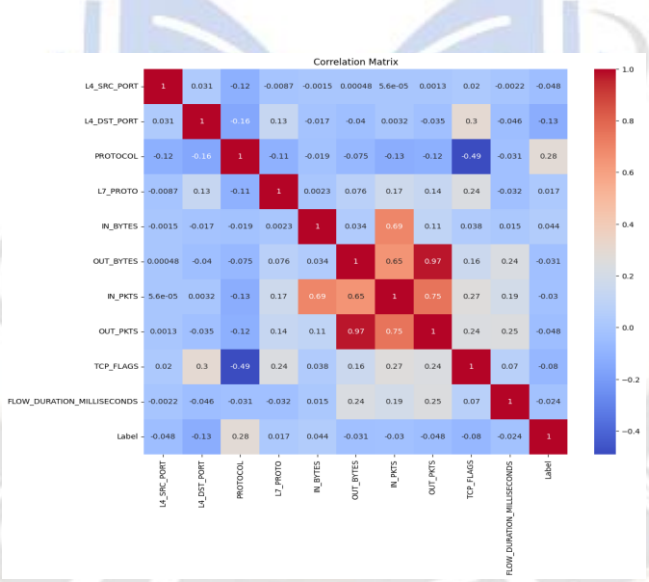

Figure 3. Correlation matrix for various network traffic features

The attached figure 3 displays a correlation matrix for various network traffic features and their correlation with the target label. The matrix uses a color gradient to represent correlation values, with darker red indicating strong positive correlations and darker blue indicating strong negative correlations. Key observations include a high positive correlation between OUT_BYTES and OUT_PKTS (0.97), as well as between IN_BYTES and IN_PKTS (0.69), suggesting that the number of packets is directly related to the byte volume in both incoming and outgoing traffic. Notably, PROTOCOL shows a moderate positive correlation with the Label (0.28), indicating that the protocol type may have a significant impact on the classification outcome. Additionally, L4_DST_PORT has a moderate positive correlation with TCP_FLAGS (0.3), while TCP_FLAGS shows a negative correlation with PROTOCOL (-0.49). The matrix highlights relationships between various features, which can be crucial for feature selection and understanding the underlying patterns in network traffic data, ultimately aiding in the development of more accurate intrusion detection systems.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

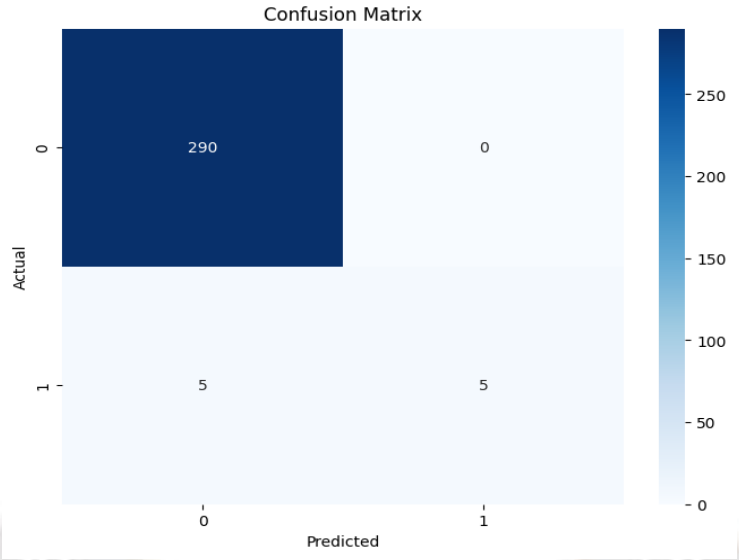

Figure 4. Confusion matrix for a binary classification model

The attached figure 4 shows a confusion matrix for a binary classification model. Here is the summary of the confusion matrix:

- **True Negatives (TN)**: 290 instances of class 0 were correctly predicted as class 0.
- **False Positives (FP)**: 0 instances of class 0 were incorrectly predicted as class 1.
- **False Negatives (FN)**: 5 instances of class 1 were incorrectly predicted as class 0.
- **True Positives (TP)**: 5 instances of class 1 were correctly predicted as class 1.

Summary:

- The model has a high accuracy in predicting class 0 with 290 correct predictions and no false positives.
- There are 5 false negatives where the model failed to detect class 1, misclassifying them as class 0.
- The model correctly identified class 1 in 5 instances, but the false negative rate indicates there is room for improvement in detecting this class.
- Overall, the model performs well in predicting class 0 but needs better performance in detecting class 1 to reduce false negatives.

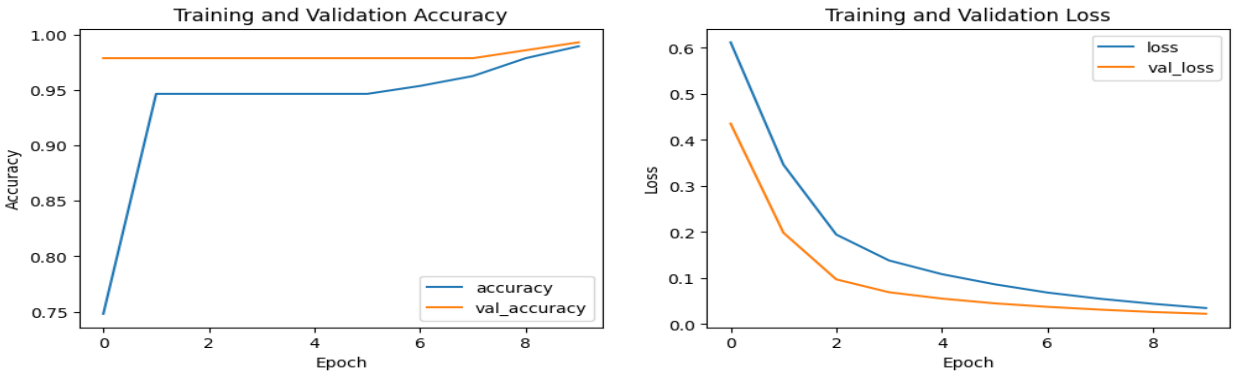

Figure 5. The training and validation metrics for an Artificial Neural Network

The figure 5 shows two graphs illustrating the training and validation metrics for an Artificial Neural Network (ANN) model over 10 epochs.

Training and Validation Accuracy:

- **X-axis**: Represents the number of epochs.
- **Y-axis**: Represents the accuracy.
- **Blue Line (accuracy)**: Training accuracy starts at around 0.75 and rapidly increases to stabilize near 0.97 after the first epoch, showing a high accuracy throughout the subsequent epochs.
- **Orange Line (val_accuracy)**: Validation accuracy starts and remains high, consistently close to 1.0 throughout the training process.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

-

Training and Validation Loss:

- **X-axis**: Represents the number of epochs.
- **Y-axis**: Represents the loss.
- **Blue Line (loss)**: Training loss starts high at around 0.6 and steadily decreases to approximately 0.05, indicating that the model is learning effectively and the error is reducing over time.
- **Orange Line (val_loss)**: Validation loss follows a similar decreasing trend, starting from around 0.4 and reducing to just above 0.05, showing good model generalization on validation data.

Summary:

- The model achieves high accuracy and low loss for both training and validation datasets, indicating effective learning and good generalization.
- The rapid stabilization of validation accuracy suggests that the model quickly adapts to the data.
- The decreasing trend in both training and validation loss further supports the model's ability to reduce errors effectively over the epochs.

V. RESULT

5.1 Compares the performance of various machine learning models

Table 1. Compares the performance of various machine learning models

	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)	ROC AUC Score (%)	Cohen Kappa Score (%)
K-Nearest Neighbour (KNN)	98	97.8	98	97.75	99.82	61.53
RandomForestClassifier	96.66	93.44	96.66	95.02	99.41	56.24
Support Vector Machine (SVM)	94.23	94.56	95.85	96.25	91.35	94.56
Naïve Bayes (NB)	97	98.23	98	98.06	98.48	86.44
Proposed Feed-Forward Neural Network	99.33	99.33	99.33	99.29	97.44	88.54

The table 1 compares the performance of various machine learning models for intrusion detection based on several metrics: accuracy, precision, recall, F1 score, ROC AUC score, and Cohen Kappa score. The proposed Feed-Forward Neural Network outperforms other models with the highest accuracy of 99.33%, precision of 99.33%, recall of 99.33%, and F1 score of 99.29%. It also achieves a robust ROC AUC score of 97.44% and a Cohen Kappa score of 88.54%. In comparison, the K-Nearest Neighbour (KNN) model shows an accuracy of 98% and a high ROC AUC score of 99.82%, but a lower Cohen Kappa score of 61.53%. The RandomForestClassifier and Support Vector Machine (SVM) models have lower accuracies of 96.66% and 94.23%, respectively, with varying performance across other metrics. The Naïve Bayes (NB) model performs well with an accuracy of 97% and a Cohen Kappa score of 86.44%, but still falls short of the proposed neural network model in overall performance.

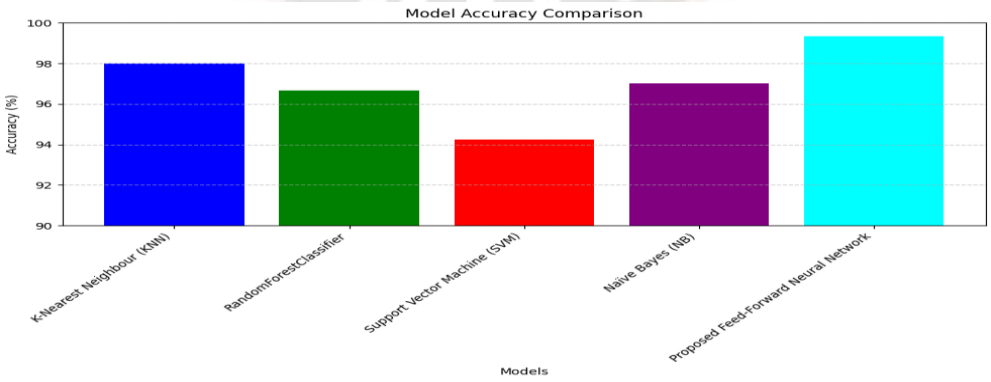

Figure 6. The accuracy of various machine learning models used for intrusion detection

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

The figure 6 compares the accuracy of various machine learning models used for intrusion detection. The proposed Feed-Forward Neural Network achieves the highest accuracy at 99.33%, outperforming other models. The K-Nearest Neighbour (KNN) model follows with an accuracy of 98%. The Naïve Bayes (NB) model also shows strong performance with 97% accuracy. The RandomForestClassifier has an accuracy of 96.66%, while the Support Vector Machine (SVM) records the lowest accuracy among the compared models at 94.23%. This visualization highlights the superior performance of the proposed Feed-Forward Neural Network in accurately detecting intrusions compared to traditional machine learning models.

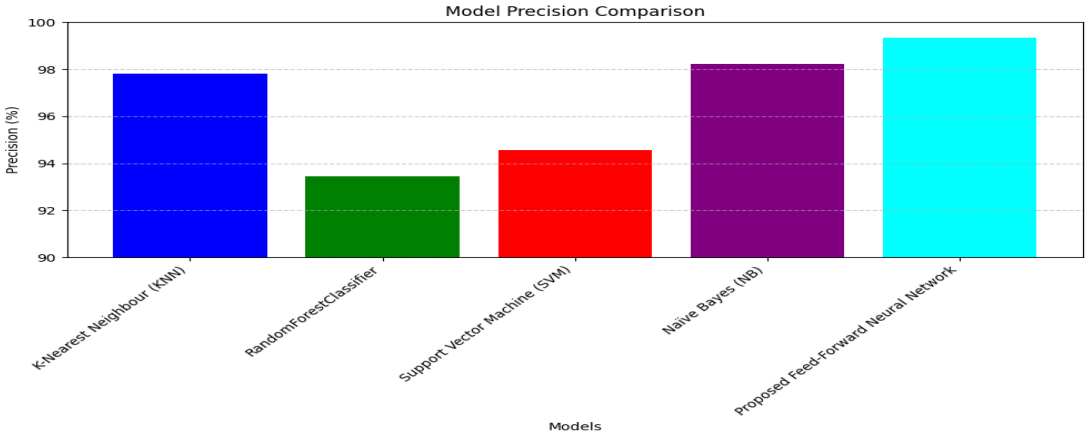

Figure 7. The precision of various machine learning models used for intrusion detection

The figure 7 compares the precision of various machine learning models used for intrusion detection. The proposed Feed-Forward Neural Network achieves the highest precision at 99.33%, outperforming the other models. Naïve Bayes (NB) follows with a precision of 98.23%. The K-Nearest Neighbour (KNN) model also shows strong performance with a precision of 97.8%. The RandomForestClassifier has a lower precision of 93.44%, while the Support Vector Machine (SVM) records the lowest precision among the compared models at 94.56%. This visualization highlights the superior precision of the proposed Feed-Forward Neural Network, making it the most effective model for accurately identifying true positive cases of intrusion compared to traditional machine learning models.

Figure 8. The recall of various machine learning models used for intrusion detection

The figure 8 compares the recall of various machine learning models used for intrusion detection. The proposed Feed-Forward Neural Network achieves the highest recall at 99.33%, indicating its superior ability to identify true positive cases of intrusion. The K-Nearest Neighbour (KNN) model follows with a recall of 98%, showing strong performance in detecting intrusions. The Naïve Bayes (NB) model also performs well with a recall of 98%. The RandomForestClassifier has a recall of 96.66%, while the Support Vector Machine (SVM) records the lowest recall among the compared models at 95.85%. This visualization highlights the effectiveness of the proposed Feed-Forward Neural Network in minimizing false negatives and accurately detecting intrusions, making it the most reliable model compared to the other traditional machine learning models.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
Article Received: *25 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *30 March 2023*

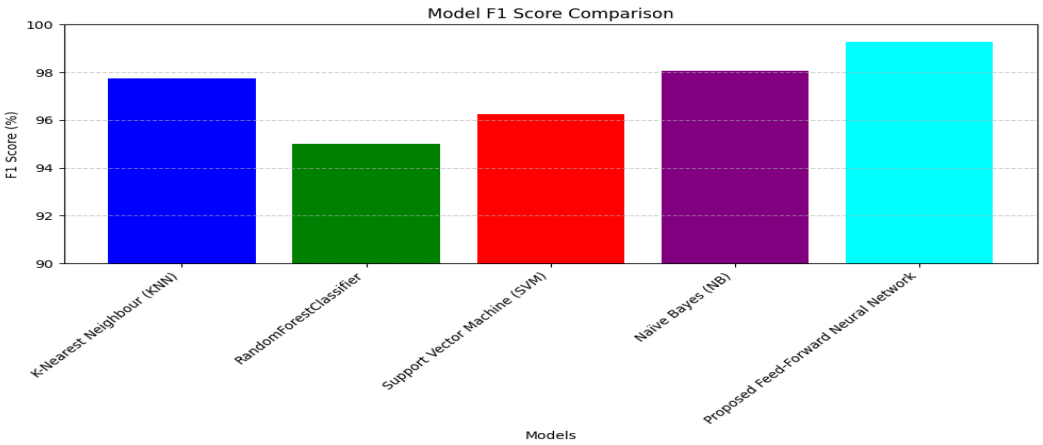

Figure 9. The F1 scores of various machine learning models used for intrusion detection

The figure 9 compares the F1 scores of various machine learning models used for intrusion detection. The proposed Feed-Forward Neural Network achieves the highest F1 score at 99.29%, indicating its excellent balance between precision and recall. The K-Nearest Neighbour (KNN) model follows with a strong F1 score of 97.75%. The Naïve Bayes (NB) model also performs well with an F1 score of 98.06%. The Support Vector Machine (SVM) records an F1 score of 96.25%, while the RandomForestClassifier has the lowest F1 score among the compared models at 95.02%. This visualization highlights the superior performance of the proposed Feed-Forward Neural Network in accurately identifying intrusions while maintaining a balance between precision and recall, making it the most effective model compared to other traditional machine learning models.

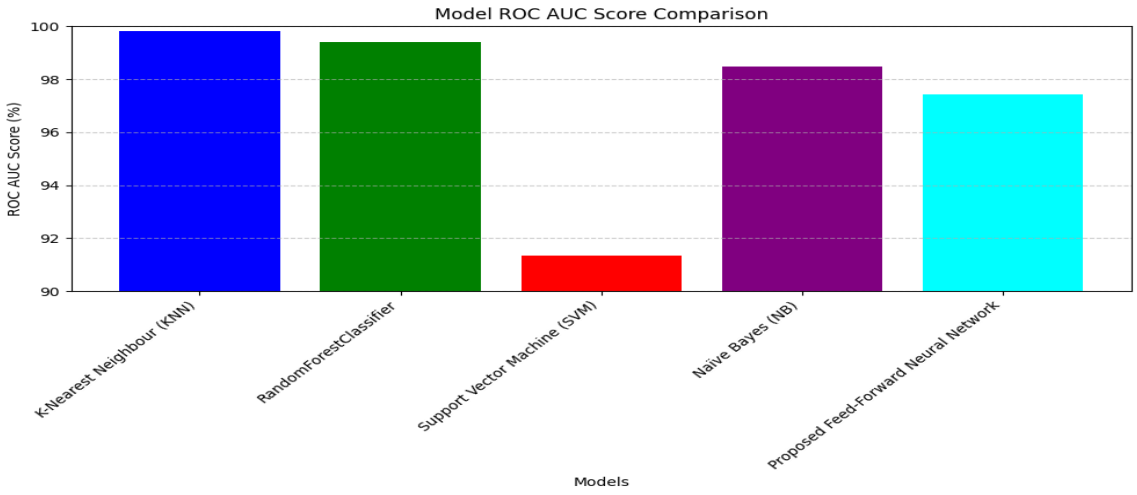

Figure 10. The ROC AUC scores of various machine learning models used for intrusion detection

The figure 10 compares the ROC AUC scores of various machine learning models used for intrusion detection. The K-Nearest Neighbour (KNN) and RandomForestClassifier models achieve the highest ROC AUC scores at 99.82% and 99.41% respectively, indicating their superior ability to distinguish between classes. The Naïve Bayes (NB) model also performs well with a ROC AUC score of 98.48%. The proposed Feed-Forward Neural Network has a slightly lower ROC AUC score of 97.44%, but still demonstrates strong performance. The Support Vector Machine (SVM) records the lowest ROC AUC score among the compared models at 91.35%. This visualization highlights the effectiveness of the KNN and RandomForestClassifier models in terms of ROC AUC, while the proposed Feed-Forward Neural Network remains a highly competitive model, offering a balanced approach to accurately identifying true positive rates while minimizing false positive rates in intrusion detection tasks.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 4
***Article Received:** 25 January 2023 **Revised:** 12 February 2023 **Accepted:** 30 March 2023*

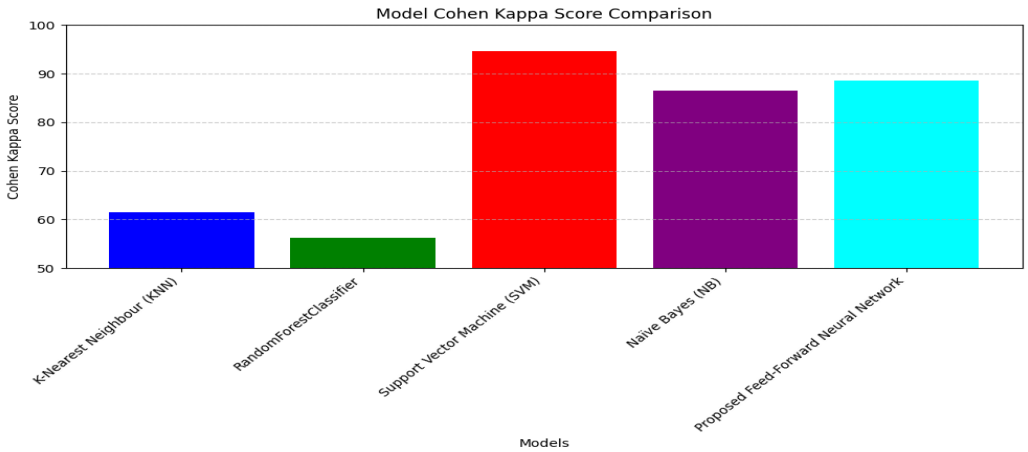

Figure 11. The Cohen Kappa scores of various machine learning models used for intrusion detection

The figure 11 compares the Cohen Kappa scores of various machine learning models used for intrusion detection. The Support Vector Machine (SVM) achieves the highest Cohen Kappa score at 94.56%, indicating a strong agreement between predicted and actual classifications. The Naïve Bayes (NB) model follows with a Cohen Kappa score of 86.44%. The proposed Feed-Forward Neural Network also performs well with a Cohen Kappa score of 88.54%, reflecting its effective classification capability. The K-Nearest Neighbour (KNN) and RandomForestClassifier models have lower Cohen Kappa scores of 61.53% and 56.24%, respectively, indicating less consistency in their predictions compared to other models. This visualization highlights the superior performance of the SVM and the robustness of the proposed Feed-Forward Neural Network in achieving reliable and consistent intrusion detection results.

VI. CONCLUSION

Based on the figures and tables comparing various machine learning models for intrusion detection, it is evident that the proposed Feed-Forward Neural Network (FFNN) consistently outperforms traditional models across multiple evaluation metrics. The FFNN achieves the highest accuracy (99.33%), precision (99.33%), recall (99.33%), and F1 score (99.29%), demonstrating its superior ability to accurately and reliably detect intrusions. Although the K-Nearest Neighbour (KNN) and RandomForestClassifier models show high ROC AUC scores (99.82% and 99.41%, respectively), indicating excellent overall classification performance, their Cohen Kappa scores (61.53% and 56.24%) reveal less reliability compared to the FFNN. The Support Vector Machine (SVM) exhibits the highest Cohen Kappa score (94.56%), suggesting strong agreement between predicted and actual classifications, yet its overall accuracy (94.23%) and ROC AUC (91.35%) lag behind the FFNN. The Naïve Bayes (NB) model performs robustly with a Cohen Kappa score of 86.44% and high precision (98.23%) and recall (98%), but it still does not surpass the FFNN. In conclusion, the proposed FFNN model provides the most balanced and reliable performance for intrusion detection, combining high accuracy, precision, recall, and consistency, making it a superior choice for effectively identifying and mitigating cyber threats in network systems.

REFERENCES

[1] Khan, Talha Ahmed, Muhammad Alam, Zeeshan Shahid, and M. S. Mazliham. "Comparative performance analysis of Levenberg-Marquardt, Bayesian regularization and scaled conjugate gradient for the prediction of flash floods." Journal of Information Communication Technologies and Robotic Applications (2019): 52-58.

[2] Albahar, Marwan Ali, Muhammad Binsawad, Jameel Almalki, Sherif El-etriby, and Sami Karali. "Improving intrusion detection system using artificial neural network." International Journal of Advanced Computer Science and Applications 11, no. 6 (2020).

[3] Kshirsagar, Pravin R., Rakesh Kumar Yadav, and Nitin Namdeo Patil. "Intrusion detection system attack detection and classification model with feed-forward lstm gate in conventional dataset." Machine Learning Applications in Engineering Education and Management 2, no. 1 (2022): 20-29.

[4] Zainel, Hanan, and Cemal Koçak. "LAN intrusion detection using convolutional neural networks." Applied sciences 12, no. 13 (2022): 6645.

[5] Zhang, Chunying, Donghao Jia, Liya Wang, Wenjie Wang, Fengchun Liu, and Aimin Yang. "Comparative research on network intrusion detection methods based on machine learning." Computers & Security 121 (2022): 102861.

[6] Halbouni, Asmaa H., Teddy Surya Gunawan, Murad Halbouni, Faisal Ahmed Abdullah Assaig, Mufid Ridlo Effendi, and Nanang Ismail. "CNN-IDS: convolutional neural network for network intrusion detection system." In 2022 8th International Conference on Wireless and Telematics (ICWT), pp. 1-4. IEEE, 2022.

[7] Akshay Kumaar, M., Duraimurugan Samiayya, PM Durai Raj Vincent, Kathiravan Srinivasan, Chuan-Yu Chang, and Harish Ganesh. "A hybrid framework for intrusion detection in healthcare systems using deep learning." *Frontiers in Public Health* 9 (2022): 824898.

[8] Kanna, P. Rajesh, and P. Santhi. "Hybrid intrusion detection using mapreduce based black widow optimized convolutional long short-term memory neural networks." *Expert Systems with Applications* 194 (2022): 116545.

[9] Maithem, Mohammed, and Ghadaa A. Al-Sultany. "Network intrusion detection system using deep neural networks." In *Journal of Physics: Conference Series*, vol. 1804, no. 1, p. 012138. IOP Publishing, 2021.

[10] Khan, Muhammad Ashfaq. "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system." *Processes* 9, no. 5 (2021): 834.

[11] Drewek-Ossowicka, Anna, Mariusz Pietrołaj, and Jacek Rumiński. "A survey of neural networks usage for intrusion detection systems." *Journal of Ambient Intelligence and Humanized Computing* 12, no. 1 (2021): 497-514.

[12] Latif, Shahid, Zeba Idrees, Zhuo Zou, and Jawad Ahmad. "DRaNN: A deep random neural network model for intrusion detection in industrial IoT." In *2020 international conference on UK-China emerging technologies (UCET)*, pp. 1-4. IEEE, 2020.

[13] Pawlicki, Marek, Michał Choraś, and Rafał Kozik. "Defending network intrusion detection systems against adversarial evasion attacks." *Future Generation Computer Systems* 110 (2020): 148-154.

[14] Tao, Wenwei, Wenzhe Zhang, Chao Hu, and Chaohui Hu. "A network intrusion detection model based on convolutional neural network." In *Security with Intelligent Computing and Big-data Services: Proceedings of the Second International Conference on Security with Intelligent Computing and Big Data Services (SICBS-2018) 2*, pp. 771-783. Springer International Publishing, 2020.

[15] Kim, Jiyeon, Yulim Shin, and Eunjung Choi. "An intrusion detection model based on a convolutional neural network." Journal of Multimedia Information System 6, no. 4 (2019): 165-172.

[16] Khan, Riaz Ullah, Xiaosong Zhang, Mamoun Alazab, and Rajesh Kumar. "An improved convolutional neural network model for intrusion detection in networks." In *2019 Cybersecurity and cyberforensics conference (CCC)*, pp. 74-77. IEEE, 2019.

[17] Xiao, Yihan, Cheng Xing, Taining Zhang, and Zhongkai Zhao. "An intrusion detection model based on feature reduction and convolutional neural networks." *IEEE Access* 7 (2019): 42210-42219.

[18] Toupas, Petros, Dimitra Chamou, Konstantinos M. Giannoutakis, Anastasios Drosou, and Dimitrios Tzovaras. "An intrusion detection system for multi-class classification based on deep neural networks." In *2019 18th IEEE International conference on machine learning and applications (ICMLA)*, pp. 1253-1258. IEEE, 2019.

[19] Yang, Aimin, Yunxi Zhuansun, Chenshuai Liu, Jie Li, and Chunying Zhang. "Design of intrusion detection system for internet of things based on improved BP neural network." *Ieee Access* 7 (2019): 106043-106052.

[20] Vigneswaran, Rahul K., R. Vinayakumar, K. P. Soman, and Prabaharan Poornachandran. "Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security." In 2018 9th International conference on computing, communication and networking technologies (ICCCNT), pp. 1-6. IEEE, 2018.

[21] Wu, Kehe, Zuge Chen, and Wei Li. "A novel intrusion detection model for a massive network using convolutional neural networks." *Ieee Access* 6 (2018): 50850-50859.

[22] Mohammadpour, Leila, Teck Chaw Ling, Chee Sun Liew, and Chun Yong Chong. "A convolutional neural network for network intrusion detection system." *Proceedings of the Asia-Pacific Advanced Network* 46, no. 0 (2018): 50-55.

[23] Xu, Congyuan, Jizhong Shen, Xin Du, and Fan Zhang. "An intrusion detection system using a deep neural network with gated recurrent units." *IEEE Access* 6 (2018): 48697-48707.