IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

Distributed Denial of Service Attack Detection using Machine Learning

Namrata Sunil bodhale

Department of Computer Science Engineering, International Center of Excellence In Engineering and Management (ICEEM), Maharashtra, India

Abstract: The rapid growth of 5G communication and Internet of Things (IoT) devices has significantly increased the risk of Distributed Denial of Service (DDoS) attacks in modern networks. These attacks attempt to interrupt network services by flooding systems with excessive traffic, thereby affecting availability, reliability, and performance. Traditional detection mechanisms are often unable to identify evolving attack patterns efficiently, especially in high-speed 5G environments.

This research presents a machine learning-based framework for detecting DDoS attacks in 5G-enabled IoT networks. The proposed system utilizes Artificial Neural Networks (ANN) with Bayesian Regularization and backpropagation techniques to classify malicious and normal traffic. The model performs preprocessing, feature selection, training, and validation using network traffic datasets. The proposed framework improves detection accuracy while reducing false-positive rates. Experimental analysis demonstrates that machine learning methods can effectively identify abnormal traffic behavior and support real-time network protection mechanisms.

Keywords: DDoS Attack, Machine Learning, Artificial Neural Network, 5G Networks, IoT Security, Bayesian Regularization.

I. INTRODUCTION

The evolution of fifth-generation (5G) communication networks and Internet of Things (IoT) technologies has transformed modern digital communication systems. High-speed data transfer, low latency, and large-scale device connectivity have enabled smart healthcare, intelligent transportation, industrial automation, and cloud-based services. However, the increasing interconnectivity of devices has also created new cybersecurity challenges. One of the most dangerous threats in such environments is the Distributed Denial of Service (DDoS) attack.

A DDoS attack occurs when multiple compromised devices simultaneously send enormous amounts of traffic toward a target server or network. The objective is to exhaust system resources, making services unavailable to legitimate users. Modern DDoS attacks are becoming more sophisticated due to the availability of botnets, IoT malware, and automated attack tools.

In 5G-enabled systems, the attack surface increases significantly because millions of smart devices communicate continuously over high-speed networks. Conventional security systems often struggle to detect complex attack patterns in real time. Therefore, intelligent detection systems capable of learning traffic behavior are required.

Machine Learning (ML) has emerged as an effective solution for network intrusion detection because it can analyze large datasets, identify hidden patterns, and classify abnormal traffic efficiently. Artificial Neural Networks (ANNs), in particular, are widely used due to their ability to model nonlinear relationships within network traffic data.

This research focuses on designing a machine learning-based DDoS detection framework using ANN techniques. The proposed system aims to improve attack detection accuracy, reduce false alarms, and provide reliable protection for 5G and IoT infrastructures.

The evolution of fifth-generation (5G) communication networks and Internet of Things (IoT) technologies has transformed modern digital communication systems. High-speed data transfer, low latency, and large-scale device connectivity have enabled smart healthcare, intelligent transportation, industrial automation, and cloud-based services. However, the increasing interconnectivity of devices has also created new cybersecurity challenges. One of the most dangerous threats in such environments is the Distributed Denial of Service (DDoS) attack.

A DDoS attack occurs when multiple compromised devices simultaneously send enormous amounts of traffic toward a target server or network. The objective is to exhaust system resources, making services unavailable to legitimate users. Modern DDoS attacks are becoming more sophisticated due to the availability of botnets, IoT malware, and automated attack tools.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155133

In 5G-enabled systems, the attack surface increases significantly because millions of smart devices communicate continuously over high-speed networks. Conventional security systems often struggle to detect complex attack patterns in real time. Therefore, intelligent detection systems capable of learning traffic behavior are required.

Machine Learning (ML) has emerged as an effective solution for network intrusion detection because it can analyze large datasets, identify hidden patterns, and classify abnormal traffic efficiently. Artificial Neural Networks (ANNs), in particular, are widely used due to their ability to model nonlinear relationships within network traffic data.

This research focuses on designing a machine learning-based DDoS detection framework using ANN techniques. The proposed system aims to improve attack detection accuracy, reduce false alarms, and provide reliable protection for 5G and IoT infrastructures.

II. RELATED WORK

Several researchers have explored the application of machine learning and deep learning techniques for detecting DDoS attacks in modern communication networks.

Sura Abdulmunem Mohammed Al-Juboori et al. proposed machine learning models for identifying Denial of Service and Man-in-the-Middle attacks using Decision Tree, Random Forest, Gradient Boosting, and XGBoost algorithms. Their work achieved detection accuracy above 97%.

Mustafa S. Ibrahim Alsumaidaie et al. introduced an Intelligent Distributed Denial of Service Attack Detection approach that combined ensemble learning with supervised machine learning algorithms. Their system demonstrated detection accuracy between 92% and 100% on network datasets.

Marian Gusatu et al. focused on DDoS mitigation in Multi-access Edge Computing (MEC) environments for 5G networks. Their framework used AI-based anomaly detection mechanisms to isolate suspicious traffic and maintain service availability.

Yea-Sul Kim et al. emphasized feature selection methods for accelerating DDoS detection in 5G core networks. Their research highlighted that optimized feature extraction improves both detection speed and computational efficiency.

Recent studies also explored deep learning approaches such as Bidirectional Long Short-Term Memory (Bi-LSTM), Convolutional Neural Networks (CNN), and hybrid ANN models for intrusion detection in SDN-based 5G environments. Although these methods achieve high accuracy, they often require large computational resources and complex training procedures.

The literature indicates that ANN-based systems remain highly effective for network traffic classification because they provide faster convergence, adaptability, and improved anomaly recognition capabilities

III. LITERATURE SURVEY

The literature survey reveals that DDoS attacks continue to evolve rapidly with advancements in communication technologies. Existing studies mainly focus on supervised machine learning techniques such as Random Forest, Support Vector Machine, Decision Tree, and Neural Networks.

Most researchers agree that feature engineering and dataset preprocessing are critical for improving detection performance. Several studies achieved high detection accuracy but faced limitations such as:

- High false-positive rates
- Large computational overhead
- Inability to handle dynamic attack patterns
- Limited real-time detection capability
- Imbalanced datasets

In many traditional approaches, signature-based detection methods fail to recognize unknown attacks. Anomaly-based systems improve flexibility but may incorrectly classify legitimate traffic as malicious.

Artificial Neural Networks offer advantages because they can learn complex traffic relationships and adapt to changing network conditions. Bayesian Regularization further improves ANN performance by reducing overfitting and enhancing generalization capability.

The survey also highlights that integrating ANN with feature selection and preprocessing methods can significantly improve DDoS detection efficiency in 5G-enabled IoT systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

IV. PROPOSED SYSTEM

The proposed system introduces a machine learning framework for detecting DDoS attacks using Artificial Neural Networks with Bayesian Regularization.

The framework consists of four major stages:

1. Data Collection
2. Data Preprocessing
3. Feature Selection
4. ANN-based Classification

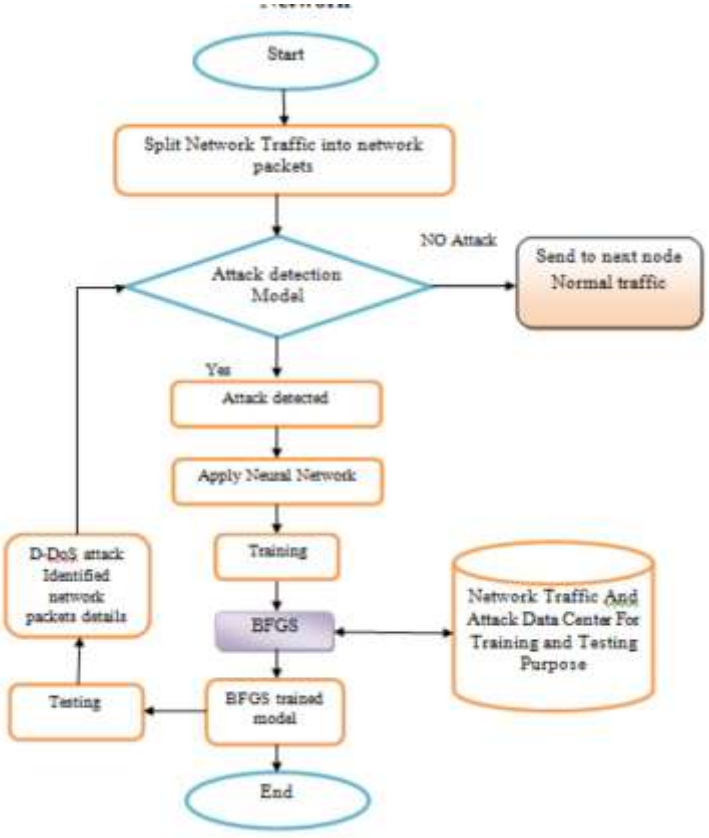
The collected network traffic dataset contains both normal and malicious traffic records. During preprocessing, irrelevant and missing data values are removed to improve dataset quality. Feature selection is then applied to identify important traffic parameters such as source IP, packet rate, protocol type, and destination port.

The ANN model contains three layers:

- Input Layer
- Hidden Layer
- Output Layer

The hidden layer processes network traffic features using activation functions, while the output layer classifies traffic as either normal or attack traffic. Backpropagation is used to adjust connection weights during training. Bayesian Regularization helps minimize overfitting and improves classification stability.

The proposed architecture supports real-time traffic monitoring and can effectively identify abnormal traffic behavior in large-scale 5G networks.



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.155133

V. METHODOLOGY AND VALIDATION

The methodology used in this research includes dataset preparation, neural network training, testing, and validation.

A. Data Preprocessing

Raw network traffic data contains noise, duplicate records, and missing values. Preprocessing techniques are applied to clean and normalize the dataset before training.

B. Feature Selection

Feature selection is performed to reduce unnecessary attributes and improve computational efficiency. Important traffic features are extracted to enhance classification accuracy.

C. ANN Training

The ANN model is trained using backpropagation with Bayesian Regularization. The learning process minimizes classification error by updating network weights iteratively.

D. Validation Metrics

The system performance is evaluated using the following parameters:

- Accuracy
- Precision
- Recall
- Sensitivity
- Specificity
- Confusion Matrix

The accuracy equation used for evaluation is:

Accuracy=TP+TN/(FP+FNTP+TN)

Where:

- TP = True Positive
- TN = True Negative
- FP = False Positive
- FN = False Negative

The confusion matrix is used to analyze classification performance between normal and attack traffic.

VI. RESULTS

The experimental analysis was performed using MATLAB-based ANN implementation. The proposed Bayesian Regularization Feed Forward Neural Network demonstrated improved classification performance compared to conventional approaches.

The model successfully identified abnormal traffic patterns with high accuracy and low error rates. Regression analysis and error histogram results confirmed stable training performance.

The major observations include:

- Improved DDoS detection accuracy
- Reduced false-positive rate
- Better generalization capability
- Efficient classification of attack traffic
- Faster convergence during training

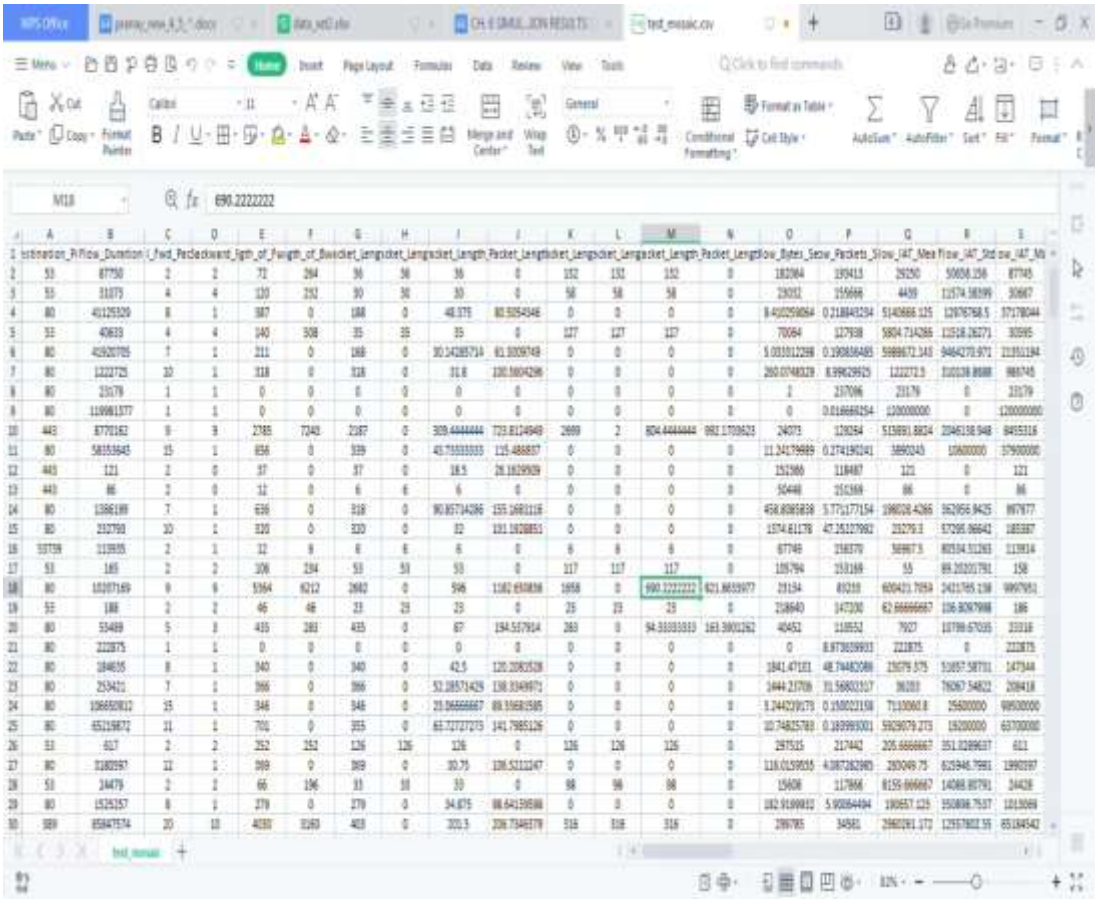
The ANN-based framework proved effective for detecting both high-volume and low-rate DDoS attacks in 5G-enabled IoT environments.

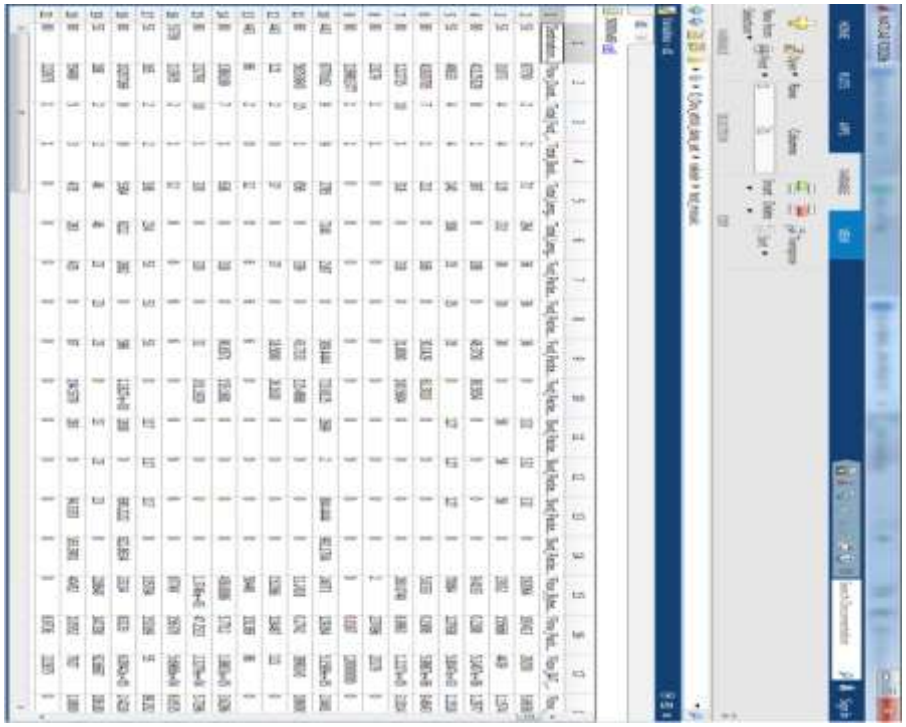
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133





IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

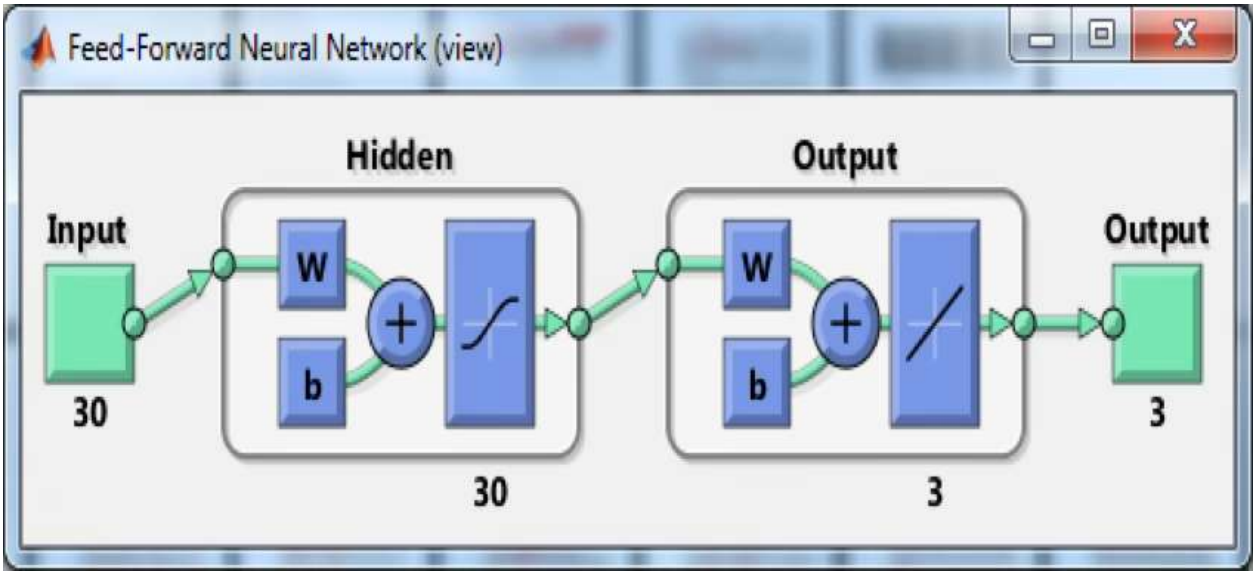


Fig. Bayesian regularization based Feed Forward Network

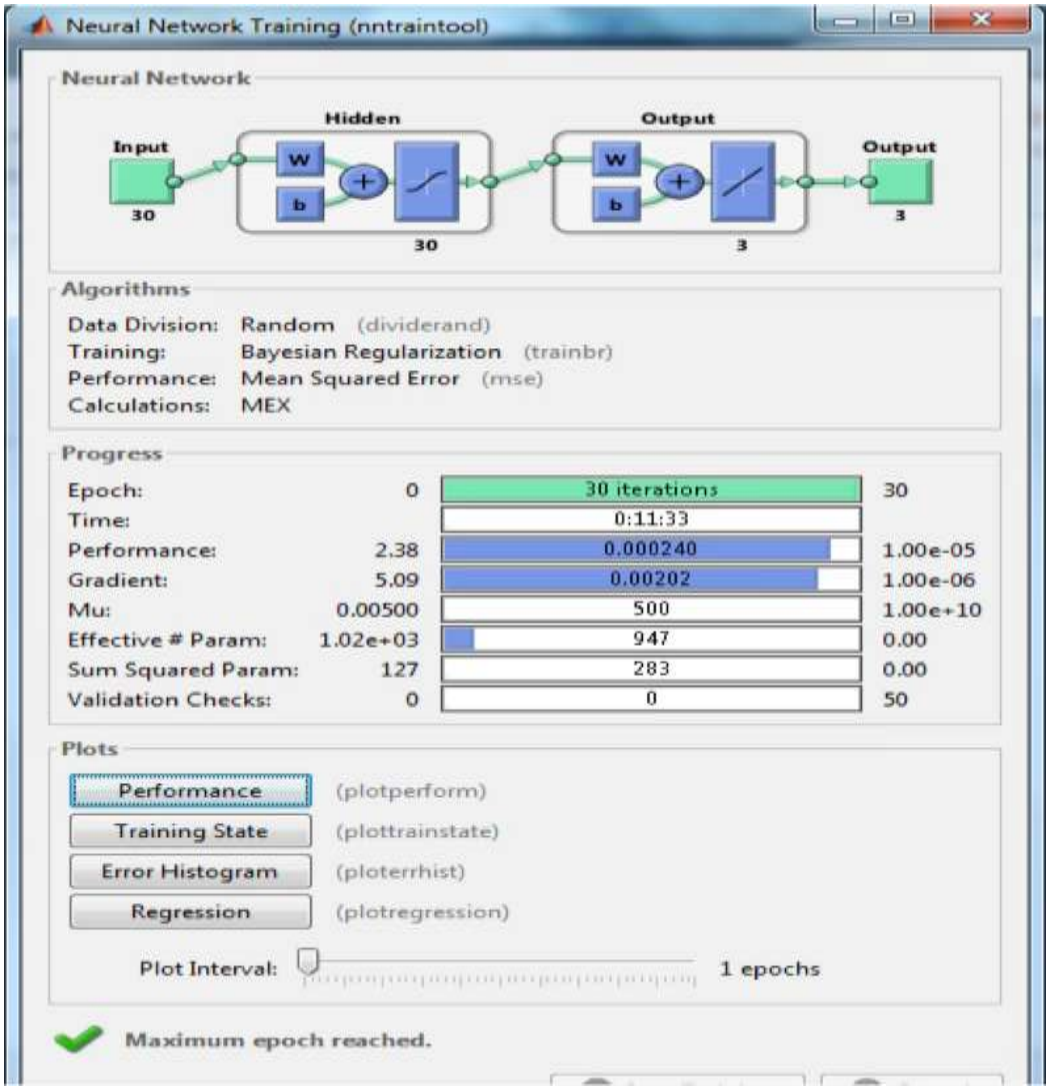


Fig: Training of proposed Bayesian regularization with Feed Forward and Cascaded Feed Forward

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

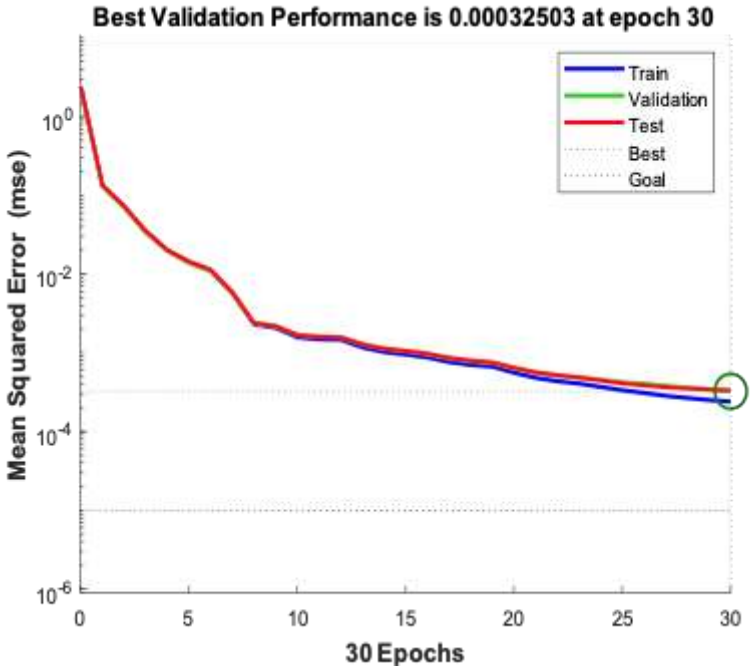


Fig: Shows the Training Outcome of Proposed Bayesian Regularization in Feed Forward Network

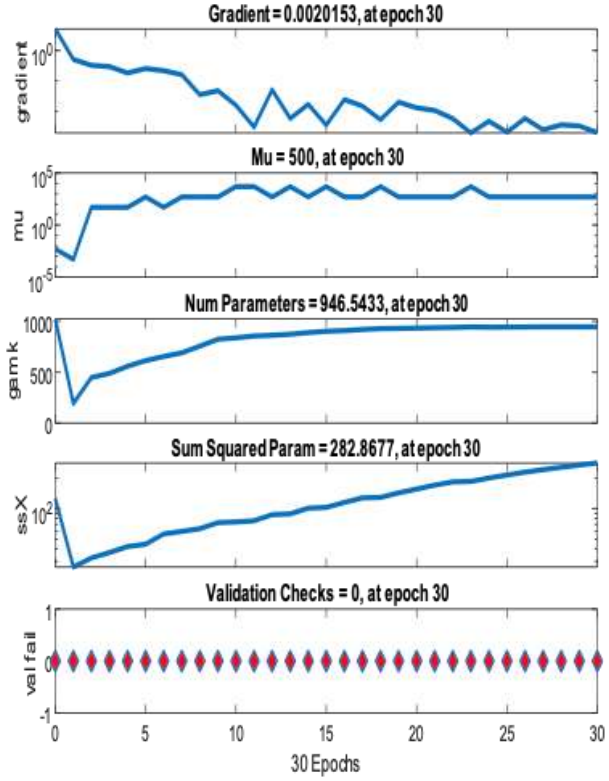


Fig: Shows The Gradient, Number Of Parameters, Sum Squared Parameter

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

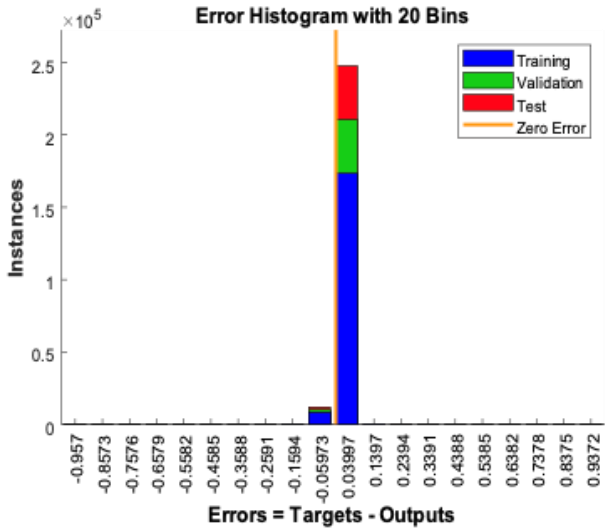


Fig: Shows the Error Histogram of proposed Bayesian Regularization for feed Forward Network

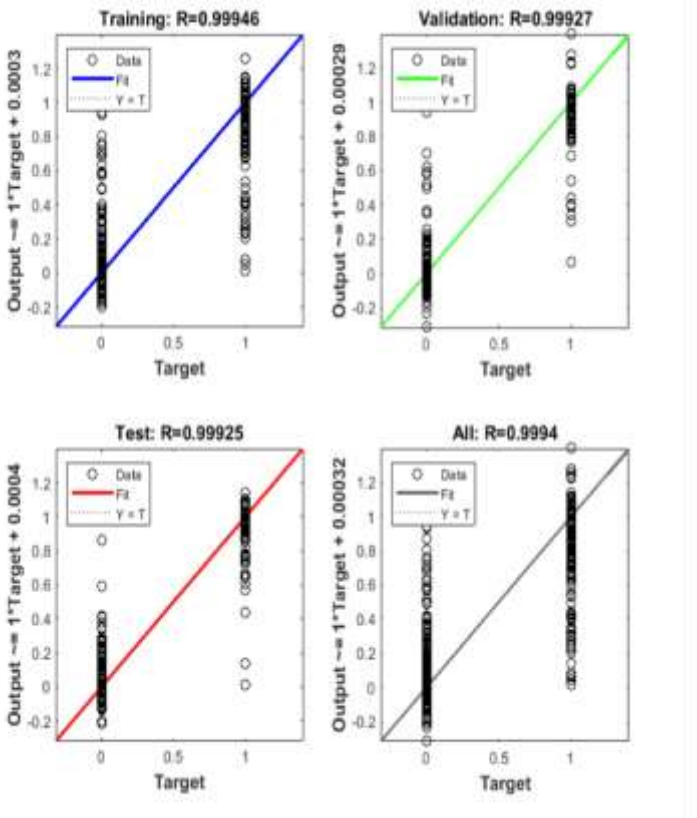


Fig: Shows the Regression Analysis of proposed Bayesian Regularization for feed Forward Network method

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

Table Shows the Resultant Parameters

S. No.	Parameter Name	Simulated Resultant value
01	Accuracy (Acc)	99.8557
02	True Positive (tp)	318 277 97
03	False Negative (fn)	0 1 0
04	False Positive (fp)	1 0 0
05	True Negative (tn)	374 415 596
06	Summation ∑TP	692
07	Summation ∑FN	1
08	Summation ∑FP	1
09	Summation ∑TN = 1385	1385

Confusion Matrix

mat = 318 0 0

1 277 0

0 0 97

Table Shows The Comparative Analysis Result Parameters

S.NO.	Result Parameters	Outcomes
01	Accuracy	99.9038
02	precision	99.8955
03	Selectivity	99.8955
04	Sensitivity	99.8801
05	Specificity	66.6734
06	Time Complexity	11 min. 33 second

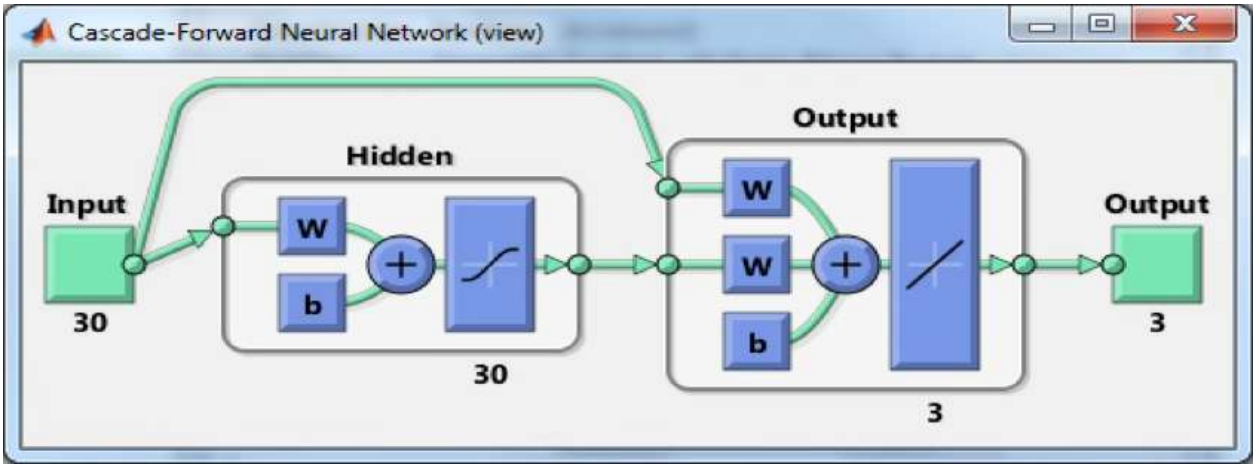
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155133

Table Shows: Algorithm Cascaded Forward of Bayesian regularization (CF-BR)



VII. CONCLUSION AND FUTURE SCOPE

This research presented a machine learning-based framework for detecting Distributed Denial of Service attacks in 5G-enabled IoT networks. The proposed ANN model with Bayesian Regularization effectively classified malicious and normal traffic using network traffic features.

The experimental results demonstrated that the proposed system achieves high detection accuracy while maintaining stable performance. Feature selection and preprocessing further improved computational efficiency and reduced classification errors.

The increasing adoption of IoT and 5G technologies makes intelligent security systems essential for future communication networks. Machine learning approaches provide adaptive and scalable solutions for handling evolving cyber threats.

Future work may include:

- Integration of deep learning techniques such as CNN and LSTM
- Real-time cloud-based deployment
- Hybrid AI-based intrusion detection systems
- Blockchain-supported network security
- Lightweight models for edge devices and IoT sensors

The proposed research can contribute toward building secure, scalable, and intelligent next-generation communication infrastructures.

REFERENCES

[1]. Sura Abdulmunem Mohammed Al-Juboori et al., “Machine Learning Techniques for Detecting Denial-of-Service and Man-in-the-Middle Attacks,” 2023.
[2]. Mustafa S. Ibrahim Alsumaidaie et al., “Sensible Identification of Distributed Denial of Service Attacks Using Machine Learning,” 2023.
[3]. Marian Gusatu et al., “Better DDoS Mitigation Security Solutions for 5G Multi-access Edge Computing,” 2022.
[4]. Yea-Sul Kim et al., “Techniques for Identifying IoT DDoS Attacks on 5G Core Networks,” 2022.
[5]. Mahmood A. Al-Shareeda et al., “MSR-DoS Scheme for 5G-enabled Vehicular Networks,” 2022.
[6]. Hao Wang et al., “Mitigation of Denial-of-Service Attacks Using G/M/1 in 5G Cellular Networks,” 2022.
[7]. Nashid Shahriar et al., “SliceSecure: DoS/DDoS Attack Detection on 5G Network Slices,” 2021.
[8]. VijeyThayananthan et al., “Machine Learning for SDN-based 5G Network Security,” 2021.
[9]. Sakib Shahriar Shafin et al., “AI-Powered Distributed Denial of Service Attack Identification,” 2021.
[10]. Amit V. Kachavimath et al., “Network Forensics: DDoS Attack Detection using Machine Learning,” 2020.
[11]. Ferhat Ozgur Catak et al., “Deep Learning Based DDoS Detection Framework,” 2019.
[12]. Adrien Bonguet et al., “DDoS Attacks in Cloud Computing: Detection and Mitigation,” 2017.

