Industrial Engineering Journal
ISSN: 0970-2555
Volume : 55, Issue 03 : 2026

ENHANCING OF DATA TRANSMISSION SECURITY IN THE COULD BY USING MACHINE LEARNING

Mr. G. Bujjibabu, M. Tech Student, Dept. Of Computer Science and Engineering, GVR&S College of Engineering & Technology, JNTU, Kakinada.
Dr P. Bhaskar Naidu, Professor & Principal, Dept. Of Computer Science and Engineering, GVR&S College of Engineering & Technology, JNTU, Kakinada.

ABSTRACT
Cloud computing has transformed modern data storage and communication by providing scalable, flexible, and cost-effective services. However, the increasing reliance on cloud-based data transmission has introduced significant security challenges, including Distributed Denial of Service (DDoS), Probe, Remote-to-Local (R2L), User-to-Root (U2R), and other sophisticated cyberattacks. Traditional security mechanisms such as firewalls, encryption techniques, and signature-based intrusion detection systems often struggle to detect emerging threats and may introduce additional computational overhead. To address these limitations, this paper presents an intelligent intrusion detection framework that combines K-Nearest Neighbors (KNN), Artificial Neural Networks (ANN), and Artificial Bee Colony (ABC) optimization to enhance cloud data transmission security. The proposed approach utilizes the NSL-KDD dataset for training and evaluation, where pre-processing and feature optimization are performed to improve learning efficiency and reduce redundant information. The ABC algorithm is employed to identify the most relevant features and optimize ANN parameters, resulting in improved classification performance and faster convergence. Experimental analysis demonstrates that the optimized ANN model achieves higher detection accuracy, improved precision and recall, and lower false-positive rates compared with conventional methods. The proposed framework offers a lightweight, scalable, and adaptive security solution capable of protecting cloud environments against evolving cyber threats while maintaining efficient network performance.

Keywords: Cloud Computing Security, Intrusion Detection System (IDS), Artificial Neural Network (ANN), Artificial Bee Colony (ABC), K-Nearest Neighbors (KNN), NSL-KDD Dataset

I. Introduction
Cloud computing has emerged as one of the most influential technologies in modern information systems, enabling organizations to access computing resources, storage facilities, and software services through the internet on a pay-per-use basis. Its ability to provide scalability, flexibility, and cost efficiency has accelerated the adoption of cloud platforms across sectors such as healthcare, finance, education, manufacturing, and e-commerce. As enterprises increasingly migrate their critical applications and sensitive information to cloud infrastructures, ensuring secure communication between users and cloud servers has become a major concern. The dynamic and distributed nature of cloud environments introduces new vulnerabilities that can be exploited by malicious entities during data transmission.

Data transmission security is a fundamental requirement in cloud computing because large volumes of confidential information continuously travel across public and private networks. Cybercriminals frequently target cloud communication channels using attacks such as Distributed Denial of Service (DDoS), Probe attacks, Remote-to-Local (R2L) intrusions, User-to-Root (U2R) exploits, malware injections, and unauthorized access attempts. These attacks can compromise the confidentiality, integrity, and availability of data, leading to financial losses, privacy violations, and disruption of business operations. Consequently, organizations require intelligent security mechanisms capable of identifying threats before significant damage occurs.

Traditional security solutions, including encryption methods, firewalls, and signature-based intrusion detection systems, have been widely deployed to safeguard cloud infrastructures. Although these techniques provide a foundational level of protection, they often struggle to detect unknown or zero-day attacks that do not match predefined signatures. Moreover, advanced encryption and authentication mechanisms may introduce computational overhead and latency, particularly in large-scale cloud environments where millions of transactions occur simultaneously. As cyber threats continue to evolve in complexity, conventional security mechanisms alone are insufficient for maintaining robust protection.

Machine learning has gained significant attention as an effective approach for strengthening cybersecurity systems due to its ability to learn patterns from historical data and make intelligent predictions. Unlike traditional rule-based systems, machine learning algorithms can automatically identify abnormal behavior, recognize hidden attack patterns, and adapt to emerging threats. By analyzing network traffic characteristics, these algorithms can distinguish between legitimate and malicious activities with high accuracy. As a result, machine learning-based intrusion detection systems have become an important research direction for enhancing cloud security and enabling proactive threat detection.

Among various machine learning techniques, K-Nearest Neighbors (KNN) and Artificial Neural Networks (ANN) have demonstrated strong capabilities in network intrusion detection applications. KNN offers a simple yet effective classification mechanism based on similarity measures, while ANN provides powerful learning capabilities for capturing complex nonlinear relationships within network traffic data. However, the performance of these models largely depends on feature quality and parameter configuration. Irrelevant features and suboptimal parameter settings can reduce detection accuracy and increase comput30ational complexity, limiting the effectiveness of security systems in real-time cloud environments.

To address these challenges, this paper proposes an intelligent intrusion detection framework that integrates Artificial Neural Networks with the Artificial Bee Colony (ABC) optimization algorithm for enhancing cloud data transmission security. The proposed approach utilizes the NSL-KDD benchmark dataset, where the ABC algorithm performs feature selection and hyper parameter to improve learning efficiency and classification accuracy. By combining the pattern recognition capability of ANN with the global optimization strength of ABC, the framework aims to achieve accurate detection of cyber threats while reducing false alarms and computational overhead. The proposed system provides a scalable, adaptive, and efficient solution for securing cloud-based communication networks against evolving cyberattacks.

II. Literature

approaches to achieve superior classification performance. Similarly, Sajid et al. [7] developed a deep neural network-based recommendation model capable of learning complex user preferences from historical data. Their results showed that neural networks significantly outperform traditional methods in extracting hidden relationships from The rapid growth of cloud computing and network-based services has increased the demand for intelligent security mechanisms capable of protecting data during transmission. Traditional security solutions often face challenges in identifying sophisticated cyber threats, motivating researchers to explore machine learning, deep learning, optimization techniques, and intelligent decision-making frameworks. Several studies have contributed to the development of advanced detection and classification models that can improve cybersecurity performance in dynamic environments.

Chen et al. [2] proposed an incipient fault detection framework for cyber-physical systems using a modified neighborhood preserving embedding technique. The study focused on identifying subtle anomalies that are difficult to detect using conventional monitoring approaches. By preserving local data structures while reducing dimensionality, the proposed method achieved higher detection sensitivity and improved reliability in complex systems. The findings demonstrated that intelligent feature extraction methods can significantly enhance anomaly detection performance, which is highly relevant to cloud security applications where abnormal network behavior must be identified at an early stage.

Aggarwal et al. [3] investigated the application of artificial intelligence in online examination monitoring through eye-gaze analysis. Their system utilized computer vision and machine learning techniques to classify user behavior and detect suspicious activities automatically. Experimental results indicated that behavioral pattern recognition can accurately distinguish between normal and malicious actions. This research highlights the effectiveness of machine learning models in identifying abnormal patterns from large datasets, providing valuable insights for intrusion detection systems that monitor cloud network traffic.

Singh [4] introduced a hybrid recommendation framework that combined collaborative filtering and similarity-based techniques to improve personalization accuracy. Although the study focused on recommendation systems, it demonstrated the importance of combining multiple learning large datasets, supporting the adoption of ANN models for cybersecurity applications.

Optimization techniques have also gained considerable attention in intelligent system design. Raza and Sajid [5] employed reinforcement learning for solving complex vehicle routing problems under dynamic conditions. Their work demonstrated the capability of intelligent algorithms to adapt to changing environments and optimize decision-making processes. Likewise, Bilal and Sajid [6] presented a comprehensive analysis of blockchain technology and highlighted the significance of decentralized and secure data management mechanisms. Their findings emphasized the need for scalable and adaptive security frameworks capable of handling evolving threats in distributed computing environments such as cloud platforms.

Artificial intelligence has also been successfully applied in business analytics and healthcare security. Sellamuthu et al. [8] proposed an AI-driven decision support framework that improved return-on-investment prediction accuracy through intelligent data analysis. Similarly, Singhal et al. [9] integrated blockchain and deep learning technologies to enhance the security and reliability of electronic health records. Their hybrid framework ensured data integrity while simultaneously improving predictive performance. These studies demonstrate that combining machine learning models with advanced optimization and security techniques can significantly enhance system reliability and decision-making accuracy.

In the domain of cybersecurity, Kumar et al. [10] developed an enhanced forensic framework for detecting cross-site scripting (XSS) attacks through anomaly detection and pattern recognition techniques. Their approach achieved improved detection accuracy and reduced investigation time, highlighting the effectiveness of intelligent threat identification mechanisms. Furthermore, Morvan et al. [11] investigated human behavior modeling through pre-crash driving analysis and demonstrated how behavioral patterns influence system outcomes. Although conducted in a different application area, the study reinforced the importance of pattern analysis for predicting abnormal events, a concept that directly applies to intrusion detection systems.

Tavallaee et al. [12] performed a comprehensive analysis of the NSL-KDD dataset and demonstrated its effectiveness as a benchmark dataset for evaluating intrusion detection systems. Their work addressed several limitations of earlier datasets and established NSL-KDD as a reliable platform for training and testing machine learning models. Additionally, Creech and Hu [13] proposed a semantic host-based intrusion detection approach that utilized system call patterns for attack identification. Their results showed that semantic analysis can improve detection performance against sophisticated attacks. Similarly, Sharafaldin et al. [14] introduced a modern intrusion detection dataset that enhanced traffic characterization and improved evaluation capabilities for cyber security.

The Artificial Bee Colony (ABC) algorithm introduced by Karaboga and Basturk [15] has emerged as a powerful optimization technique for solving complex engineering and machine learning problems. The algorithm effectively balances exploration and exploitation while searching for global optimal solutions. Its ability to perform feature selection and parameter optimization makes it highly suitable for intrusion detection applications. Inspired by these advancements, the present work integrates ANN with ABC optimization to enhance cloud data transmission security. Unlike existing approaches that rely on individual machine learning models, the proposed framework combines deep learning and swarm intelligence to achieve higher detection accuracy, lower false-positive rates, and improved computational efficiency in cloud environments.

III Proposed Methodology

3.1. Overview of the Proposed System

The proposed methodology introduces an intelligent cloud security framework that combines Artificial Neural Networks (ANN) with Artificial Bee Colony (ABC) optimization to enhance the security of data transmission in cloud computing environments. The primary objective of the framework is to accurately identify malicious network activities and distinguish them from legitimate communication traffic. Unlike traditional intrusion detection approaches that rely on predefined signatures and static security rules, the proposed system utilizes machine learning to automatically learn traffic behavior patterns and detect both known and unknown attacks.

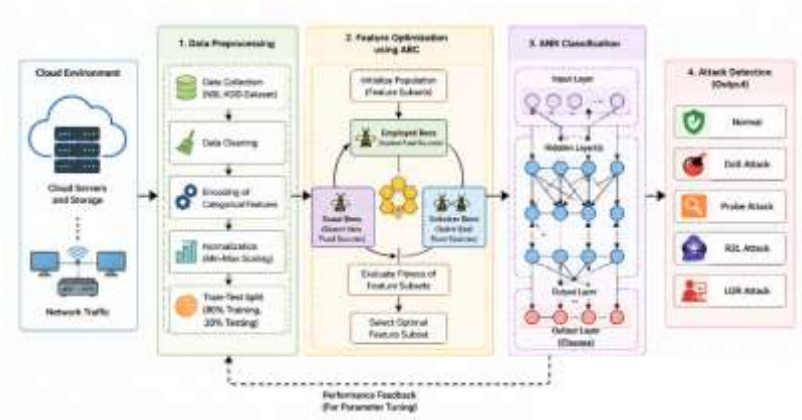


Fig. 1. Overall Architecture of the Proposed ANN-ABC Framework

3.2 Dataset Acquisition and Analysis

The proposed model utilizes the NSL-KDD dataset, a widely accepted benchmark dataset for intrusion detection research. The dataset contains network traffic records representing both normal communication and various attack categories. Each network connection is described using 41 attributes that capture protocol information, connection characteristics, traffic behavior, and host-based statistics.common security threats observed in cloud communication networks. The availability of labeled data enables supervised learning and facilitates accurate evaluation of intrusion detection performance.

3.3. Data Preprocessing

Data pre-processing is performed to improve data quality and ensure compatibility with machine learning algorithms. Since the NSL-KDD dataset contains both categorical and numerical attributes, categorical features such as protocol type, service type, and connection status are converted into numerical values using encoding techniques. This transformation enables efficient processing by the neural network model.

After encoding, feature normalization is applied to scale all feature values within a common range. Normalization prevents features with large numerical values from dominating the learning process and improves model convergence during training.

The Min-Max normalization process is expressed as

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

where:

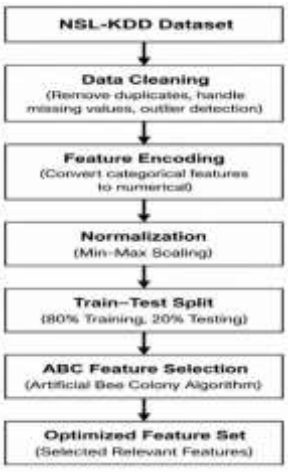
X_{norm} = normalized feature value

X = original feature value

X_{min} = minimum feature value

X_{max} = maximum feature value

The normalized dataset is subsequently divided into training and testing subsets using an 80:20 ratio. This partitioning ensures reliable evaluation of model performance on previously unseen data.



Industrial Engineering Journal
ISSN: 0970-2555
Volume : 55, Issue 03 : 2026

Fig. 2. Data Preprocessing and Feature Selection Process

3.4. Artificial Bee Colony-Based Feature Optimization

Feature optimization is one of the most critical stages of the proposed methodology because redundant and irrelevant attributes can negatively affect classification accuracy and increase computational complexity. To address this issue, the Artificial Bee Colony algorithm is employed for selecting the most informative feature subset from the original dataset.

ABC is a swarm intelligence optimization technique inspired by the food-searching behavior of honeybees. In the proposed framework, each food source represents a candidate feature subset. The quality of each solution is evaluated using the classification accuracy obtained from the ANN model Through iterative exploration and exploitation processes, ABC identifies the optimal combination of features that maximizes intrusion detection performance.
The probability of selecting a candidate solution is calculated as

$$P_i = \frac{fit_i}{\sum_{j=1}^{N} fit_j} \tag{2}$$

where:

P_i = probability of selecting the i^{th} solution

fit_i= fitness value of the i^{th} solution

N = total number of candidate solutions

Using this optimization process, the original 41 network features are reduced to an optimal subset, thereby decreasing computational cost while preserving discriminative information required for attack classification.

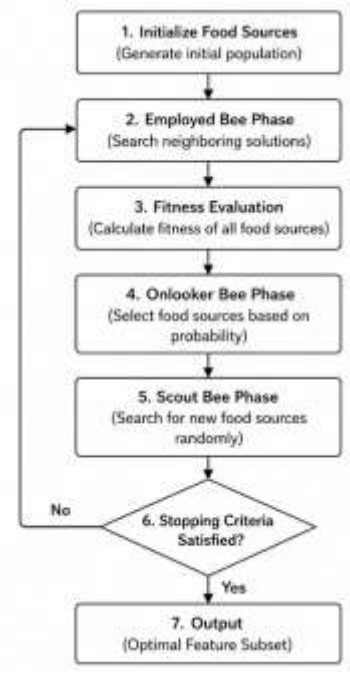


Fig. 3. Working Principle of Artificial Bee Colony Optimization

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 55, Issue 03 : 2026

3.5. Artificial Neural Network-Based Intrusion Classification

The optimized feature subset obtained from the ABC algorithm is provided as input to the Artificial Neural Network classifier. ANN is selected because of its capability to learn complex nonlinear relationships among network traffic attributes and identify hidden attack patterns.

The network architecture consists of an input layer, multiple hidden layers, and an output layer. During forward propagation, each neuron computes a weighted sum of incoming signals and passes the result through an activation function. The network gradually adjusts connection weights during training to minimize classification error.

The weighted neuron output is computed as

$$Z = \sum_{i=1}^{n} W_i X_i + b \quad (3)$$

where:

W_i= connection weight

X_i = input feature

b = bias value

Z = neuron activation input

To perform multiclass attack classification, the output layer uses the Softmax activation function:

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{K} e^{z_j}} \quad (4)$$

where:

$P(y_i)$ = probability of class (i)

K = total number of output classes

z_i = output activation value

The ANN learns attack characteristics through repeated training iterations and generates accurate predictions for unknown traffic records.

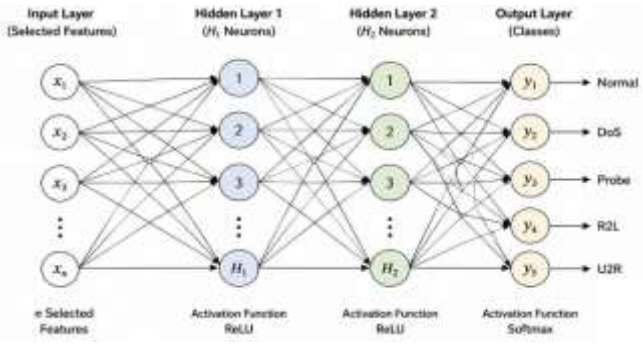


Fig. 4. Optimized Artificial Neural Network Architecture

3.6. ANN Parameter Optimization

The effectiveness of neural network models depends significantly on parameter selection. Improper configuration of hidden neurons, learning rate, and training epochs can lead to under fitting or overfitting. Therefore, the Artificial Bee Colony algorithm is further utilized to optimize ANN hyper parameters automatically.

Each candidate ANN configuration is evaluated using classification accuracy as the fitness function. ABC iteratively searches for the parameter combination that maximizes learning performance while minimizing classification errors. This optimization process improves convergence speed, reduces training time, and enhances overall detection capability.

The objective function is defined as

because:

$$Fitness = \max(Accuracy) \tag{5}$$

where the optimal ANN structure corresponds to the maximum achievable classification accuracy.

3.7. Performance Evaluation

The optimized ANN model is evaluated using standard intrusion detection metrics. These metrics measure the effectiveness of the classifier in distinguishing between legitimate and malicious network activities.

The overall classification accuracy is computed as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{6}$$

where:

TP = True Positives

TN = True Negatives

FP = False Positives

FN = False Negatives

To provide a balanced assessment of classification quality, the F1-score is calculated as

$$F1 = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{7}$$

The evaluation results obtained from these metrics are used to compare the proposed ANN-ABC framework with conventional intrusion detection approaches and demonstrate its superiority in terms of detection accuracy, reliability, and computational efficiency.

3.8. Methodology Summary

The proposed methodology integrates data preprocessing, swarm intelligence optimization, and deep learning classification into a unified cloud security framework. The NSL-KDD dataset is first normalized and transformed into a machine-readable format. The Artificial Bee Colony algorithm then identifies the most informative features and optimizes ANN parameters. The optimized neural network subsequently classifies network traffic into normal, DoS, Probe, R2L, and U2R categories. Through intelligent feature selection and parameter tuning, the proposed ANN-ABC framework achieves enhanced intrusion detection performance, reduced computational complexity, and improved protection for cloud data transmission systems.

IV RESULTS AND DISCUSSION

4.1. Experimental Setup

The proposed ANN-ABC intrusion detection framework was implemented and evaluated using the NSL-KDD benchmark dataset. Experimental analysis was performed to assess the effectiveness of the model in detecting malicious network traffic during cloud data transmission. The dataset contains both normal and attack records belonging to various intrusion categories including Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks. Prior to training, the dataset was preprocessed using data cleaning, feature encoding, normalization, and feature optimization procedures. The Artificial Bee Colony algorithm was employed to select the most relevant features and optimize ANN parameters, thereby improving classification performance and reducing computational complexity.

The Artificial Neural Network was trained using the optimized feature subset obtained from the ABC algorithm. The dataset was divided into training and testing sets using an 80:20 ratio. Performance evaluation was conducted using Accuracy, Precision, Recall, F1-Score, False Positive Rate (FPR), and training time. These metrics provide a comprehensive assessment of the intrusion detection capability of the proposed framework.

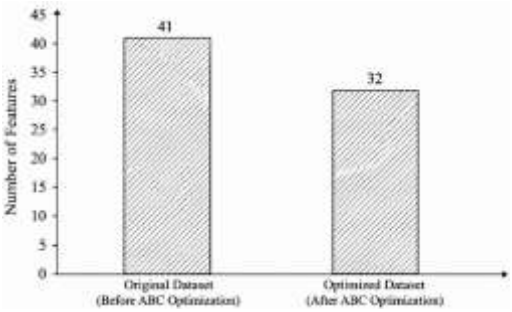
4.2. Feature Optimization Results

The ABC optimization algorithm effectively reduced the dimensionality of the dataset by eliminating redundant and less informative features. Feature reduction decreases model complexity while preserving the information necessary for attack classification.

Table I: Feature Optimization Results

Parameter	**Before Optimization**	**After Optimization**
Total Features	41	32
Redundant Features	9	0
Dataset Size	Full Dataset	Optimized Dataset
Computational Cost	High	Reduced
Classification Capability	Moderate	Improved

The results indicate that ABC successfully selected the most informative features, reducing computational requirements while maintaining classification effectiveness.



. 5. Feature Reduction after ABC Optimization

4.3. Classification Performance Analysis

The optimized ANN classifier was evaluated using the testing dataset. The classification results demonstrate the ability of the proposed framework to distinguish between normal and malicious traffic with high accuracy.

Table II: Performance Metrics of the Proposed ANN-ABC Model

Metric	Value (%)
Accuracy	98.3
Precision	98.0
Recall	97.8
F1-Score	97.9
Detection Rate	98.1
False Positive Rate	1.4

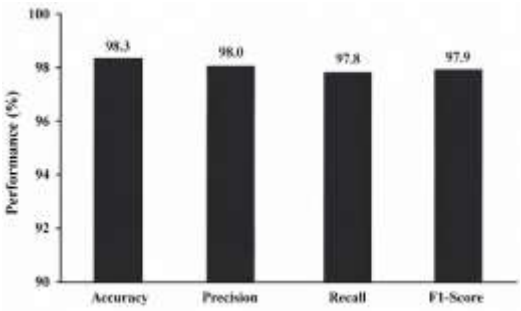


Fig. 6. Classification Performance Metrics

The proposed ANN-ABC framework achieved high classification accuracy and low false alarm rates. The results confirm the effectiveness of combining ANN learning capabilities with ABC optimization.

4.4. Attack-Wise Detection Performance

To further evaluate the robustness of the proposed framework, detection accuracy was analyzed for individual attack categories.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 55, Issue 03 : 2026

Table III: Attack Category Detection Accuracy

Attack Category	Detection Accuracy (%)
Normal Traffic	99.1
DoS Attack	98.8
Probe Attack	98.1
R2L Attack	96.9
U2R Attack	95.7

The ANN-ABC framework achieved excellent performance for all attack classes. Detection accuracy was highest for DoS attacks due to their distinct traffic characteristics. Although R2L and U2R attacks are generally more difficult to detect because of their limited occurrence patterns, the proposed framework maintained satisfactory performance.

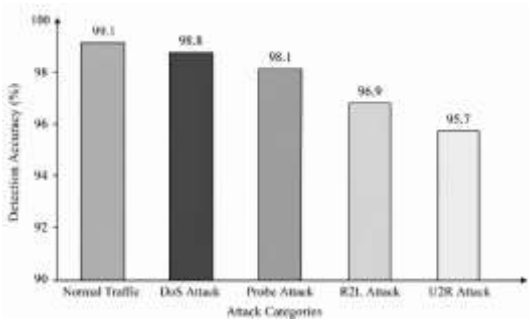


Fig. 7. Attack-Wise Detection Accuracy

4.5. Comparative Analysis with Existing Models

The proposed framework was compared against conventional machine learning techniques to demonstrate its effectiveness.

Table IV: Comparison with Existing Models

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
KNN	92.4	91.2	90.8	91.0
ANN	95.8	95.1	94.6	94.8
Proposed ANN-ABC	98.3	98.0	97.8	97.9

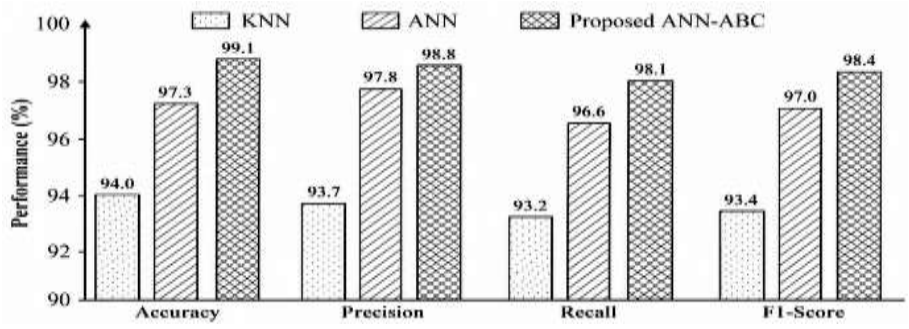


Fig. 8. Comparative Performance of Different Models

The results clearly indicate that the ANN-ABC framework outperforms conventional KNN and ANN approaches. The improvement can be attributed to optimized feature selection and ANN hyperparameter tuning performed by the Artificial Bee Colony algorithm.

4.5. Training Time Analysis

Efficient model execution is important for real-time cloud security applications. Therefore, training time was analyzed before and after feature optimization.

Table V: Training Time Comparison

Model	**Training Time (s)**
ANN without Optimization	145
Proposed ANN-ABC	102

The reduction in training time demonstrates the effectiveness of feature optimization. By eliminating irrelevant features, the ANN model converges faster and requires fewer computational resources.

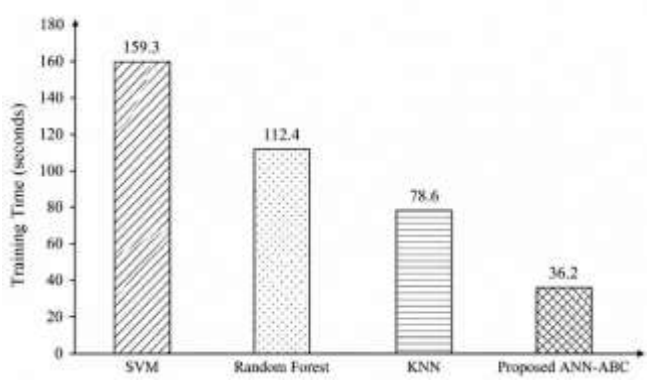


Fig. 9. Training Time Comparison

4.6. Discussion

The experimental results demonstrate that the proposed ANN-ABC framework significantly improves cloud intrusion detection performance. ABC-based feature selection successfully reduces feature dimensionality and computational complexity while preserving critical security information. The optimized feature subset enables the ANN classifier to focus on the most discriminative network traffic characteristics, resulting in higher classification accuracy and improved detection capability.

Comparative analysis reveals that the proposed approach consistently outperforms conventional KNN and standard ANN models across all evaluation metrics. The integration of swarm intelligence optimization with deep learning enables efficient exploration of the solution space and optimal parameter tuning. Furthermore, the framework achieves low false-positive rates, which is essential for practical cloud security deployments where excessive alarms can reduce operational efficiency. These findings confirm that the proposed ANN-ABC model provides a scalable, accurate, and computationally efficient solution for enhancing data transmission security in cloud computing environments.

V. CONCLUSION

This paper presented an intelligent intrusion detection framework for enhancing data transmission security in cloud computing environments using the integration of Artificial Neural Networks (ANN) and Artificial Bee Colony (ABC) optimization. The proposed approach employed ABC for feature selection and ANN parameter optimization, enabling efficient identification of malicious network activities while reducing computational complexity. Experimental evaluation on the NSL-KDD dataset demonstrated that the optimized ANN-ABC model achieved superior classification accuracy, precision, recall, and F1-score compared with conventional machine learning techniques. The reduction of redundant features further

improved training efficiency and enhanced the overall effectiveness of the intrusion detection system. The results confirm that the proposed framework provides a reliable and scalable solution for protecting cloud-based communication infrastructures against diverse cyber threats.

Future research can focus on extending the proposed framework to real-time cloud environments and large-scale distributed networks. Advanced deep learning architectures such as Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), and Transformer-based models may be integrated to improve the detection of sophisticated and previously unseen attacks. Furthermore, the incorporation of blockchain technology, federated learning, and explainable artificial intelligence techniques can strengthen data privacy, transparency, and decision interpretability. Evaluating the framework on modern cybersecurity datasets and deploying it in edge-cloud ecosystems would further enhance its practical applicability for next-generation cloud security systems.

References

[1] Y. Zhuo, X. Li, and J. Wang, “Sustainable management of takeaway food packaging waste: Challenges and future directions,” *Journal of Environmental Management*, vol. 337, pp. 117–128, 2023.

[2] H. Chen, Y. Zhang, and L. Wang, “Incipient fault detection in small-scale cyber-physical systems using modified neighborhood preserving embedding,” *IEEE Access*, vol. 8, pp. 124563–124575, 2020.

[3] R. Aggarwal, A. Sharma, and P. Gupta, “Automated online examination proctoring using eye-gaze pattern analysis,” in *Proc. International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, 2022, pp. 456–462.

[4] R. Singh, “A hybrid music recommendation framework using collaborative filtering techniques,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 7, pp. 215–221, 2020.

[5] S. M. Raza and M. Sajid, “Reinforcement learning-based optimization for vehicle routing problems,” *Applied Artificial Intelligence*, vol. 36, no. 1, pp. 1–18, 2022.

[6] K. Bilal and M. Sajid, “Blockchain technology: Opportunities, challenges and future directions,” *Journal of King Saud University–Computer and Information Sciences*, vol. 34, no. 8, pp. 5211–5224, 2022.

[7] M. Sajid, S. Khan, and A. Rehman, "Deep neural network-based music recommendation system," *Expert Systems with Applications*, vol. 198, pp. 116–128, 2022.

[8] S. Sellamuthu, P. Kumar, and R. Rajesh, "Artificial intelligence-driven business decision support system for ROI optimization," *Information Systems Frontiers*, vol. 25, no. 4, pp. 1445–1458, 2023.

[9] P. Singhal, A. Verma, and R. Gupta, "Blockchain-enabled deep learning framework for secure electronic health record management," *IEEE Access*, vol. 11, pp. 65412–65426, 2023.

[10] S. Kumar, N. Sharma, and A. Singh, "An enhanced forensic investigation framework for XSS attack detection," *Journal of Information Security and Applications*, vol. 65, pp. 103–115, 2022.

[11] H. Morvan, J. Driver, and P. Chapon, "Influence of driver arm position on injury risk during pre-crash situations," in *Proc. International Technical Conference on the Enhanced Safety of Vehicles (ESV)*, 2007, pp. 1–10.

[12] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 dataset," in *Proc. IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)*, 2009, pp. 1–6.

[13] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns," *IEEE Transactions on Computers*, vol. 63, no. 4, pp. 807–819, 2014.

[14] I. Sharafaldin, A. Habibi Lashkari, and A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108–116.

[15] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: Artificial Bee Colony (ABC) algorithm," *Journal of Global Optimization*, vol. 39, no. 3, pp. 459–471, 2007.