A ROBUST CNN2D FRAMEWORK FOR ATTACK DETECTION IN ROBOT OPERATING SYSTEM NETWORKS

SHAIK. UMAR JANU[1]
PG Student Department of Computer Science and Engineering
Gvr&S College Of Engineering And Technology
AP, India
umarjanu4848@gmail.com

Dr. P. BHASKAR NAIDU[2]
Professor & Principal, Department of Computer Science and Engineering, Gvr&S College Of Engineering And Technology
AP, India
bhaskarphd14@gmail.com

***Abstract*— The increasing adoption of Robot Operating System (ROS)-based robotic platforms in smart environments, industrial automation, healthcare, and autonomous systems has introduced significant cybersecurity challenges. Since ROS relies on distributed communication and network connectivity, it becomes vulnerable to various cyber threats, including Denial-of-Service (DoS), reconnaissance, and information-gathering attacks that can compromise system reliability and operational safety. To address these challenges, this research proposes an intelligent attack detection framework based on an enhanced Convolutional Neural Network with two-dimensional architecture (CNN2D) for ROS environments. The framework utilizes a comprehensive dataset containing normal and malicious network traffic records collected from ROS communications. Data preprocessing techniques such as missing value handling, label encoding, feature normalization, and data reshaping are employed to improve data quality and model effectiveness. The proposed CNN2D model automatically extracts complex spatial patterns from network traffic and system-level features, enabling accurate identification of attack behaviors. The model is trained using the Adam optimization algorithm and categorical cross-entropy loss function to achieve efficient convergence and robust classification performance. Experimental evaluation demonstrates that the proposed approach achieves superior detection accuracy and improved generalization compared to conventional machine learning methods. The developed framework offers a scalable, efficient, and real-time security solution for protecting ROS-based cyber-physical systems against evolving cyber threats while enhancing the overall safety and dependability of intelligent robotic applications.**

Keywords— Cybersecurity, Robot Operating System (ROS), Intrusion Detection System, Deep Learning, CNN2D, Cyber-Physical Systems (CPS).

I. INTRODUCTION

The rapid advancement of robotics, artificial intelligence, and Internet of Things (IoT) technologies has transformed traditional robotic systems into highly interconnected and intelligent cyber-physical systems. Modern robots are no longer limited to isolated industrial environments; instead, they are increasingly deployed in healthcare, smart manufacturing, autonomous transportation, agriculture, surveillance, and smart home applications. These systems rely on continuous communication among sensors, actuators, controllers, and cloud services to perform complex tasks efficiently. The growing dependence on network connectivity and distributed computing has significantly improved robotic capabilities but has also introduced new security vulnerabilities that can be exploited by malicious actors. Consequently, ensuring the security and reliability of robotic platforms has become a critical research challenge.

The Robot Operating System (ROS) has emerged as one of the most widely adopted middleware frameworks for robotic application development. ROS provides a flexible architecture that enables communication between different software modules through topics, services, and actions. Its modular design simplifies the development and integration of robotic components, making it popular among researchers and industry practitioners. However, the open and distributed nature of ROS communication creates multiple attack surfaces that can be targeted by cyber adversaries. Unauthorized access, message tampering, denial-of-service attacks, reconnaissance activities, and data interception are some of the common threats capable of disrupting robot operations and compromising system integrity.

As robotic systems become integral components of critical infrastructures and safety-sensitive environments, the consequences of cyberattacks become increasingly severe. In healthcare settings, compromised robotic devices may affect patient safety and treatment outcomes. Similarly, attacks on autonomous vehicles, industrial robots, or surveillance systems can lead to operational failures, financial losses, and physical hazards. Traditional cybersecurity solutions such as firewalls, authentication mechanisms, and encryption techniques provide essential protection but are often insufficient against sophisticated and evolving attack strategies. These defenses primarily focus on preventing unauthorized access and may fail to identify unknown or previously unseen attack patterns occurring within network communications.

To overcome the limitations of conventional security mechanisms, machine learning and deep learning approaches have gained significant attention in intrusion detection research. These intelligent techniques analyze large volumes of network traffic and system data to automatically learn behavioral patterns associated with normal and malicious activities. Unlike rule-based detection systems, learning-based models can adapt to dynamic environments and identify complex attack signatures without requiring manually defined rules. Their ability to discover hidden relationships within high-dimensional data makes them particularly suitable for securing ROS-based cyber-physical systems where communication patterns are diverse and continuously changing.

Among various deep learning architectures, Convolutional Neural Networks (CNNs) have demonstrated remarkable success in feature extraction and classification tasks. CNN-based models can automatically learn hierarchical representations from raw input data, reducing the dependence on manual feature engineering. By capturing spatial correlations among network and system-level attributes, CNN architectures can effectively distinguish between legitimate and malicious communication behaviors. The two-dimensional convolutional neural network (CNN2D) approach further enhances detection capability by identifying intricate feature interactions that may not be visible through traditional machine learning algorithms such as Random Forest, Support Vector Machine, or Naïve Bayes classifiers.

Motivated by these challenges and opportunities, this research presents an intelligent attack detection framework for ROS-based systems using an enhanced CNN2D model. The proposed framework utilizes ROS communication data containing normal traffic and multiple cyberattack categories, including Denial-of-Service (DoS), reconnaissance, and observation-based attacks. Comprehensive data preprocessing techniques, feature normalization, and deep feature extraction mechanisms are employed to improve detection performance. The CNN2D model is trained using optimized learning strategies to accurately classify network activities and identify malicious behavior in real time. Experimental analysis demonstrates the effectiveness of the proposed approach in improving attack detection accuracy, reducing false alarms, and enhancing the cybersecurity resilience of modern robotic and cyber-physical environments.

II. LITERATURE SURVEY

The growing adoption of Robot Operating System (ROS)-based robotic platforms in industrial automation, healthcare, transportation, and smart manufacturing has significantly increased the importance of cybersecurity within robotic environments. ROS provides a flexible and distributed framework that enables seamless communication among robotic components; however, its open architecture also introduces several security vulnerabilities. Quigley et al. [1] introduced ROS as a middleware framework that simplifies robot software development through modular communication mechanisms. While ROS accelerated innovation in robotics, its original architecture did not prioritize security, thereby exposing robotic systems to unauthorized access, message tampering, and denial-of-service attacks. As robotic systems become increasingly connected to networks and cloud infrastructures, the need for intelligent attack detection mechanisms has become more critical.

Researchers have extensively investigated the security weaknesses present in ROS-based systems. White et al. [2] demonstrated that the absence of authentication and encryption mechanisms in ROS communications creates opportunities for attackers to manipulate robotic operations remotely. Similarly, Dieber et al. [3] performed a comprehensive security assessment of ROS environments and identified multiple attack vectors that could compromise robotic functionality. Their findings revealed that conventional perimeter-based security mechanisms alone are insufficient to protect modern robotic infrastructures. Fernandes et al. [4] further emphasized that cyberattacks targeting interconnected systems can lead to severe operational disruptions, highlighting the necessity for advanced intrusion detection solutions capable of identifying malicious activities in real time.

Traditional intrusion detection systems have primarily relied on signature-based and rule-based approaches. Although these methods effectively detect previously known attacks, they often struggle to identify novel and evolving threats. To overcome these limitations, researchers have increasingly adopted machine learning techniques for anomaly and intrusion detection. Zhang et al. [5] employed Random Forest classifiers for network intrusion detection and reported improved detection performance compared to conventional approaches. Buczak and Guven [6] conducted a comprehensive survey of machine learning applications in cybersecurity and concluded that supervised learning algorithms provide significant advantages in detecting abnormal network behaviors. However, these models generally require manual feature engineering and domain expertise to achieve optimal performance.

Support Vector Machines (SVMs) have also been widely utilized in intrusion detection research due to their strong classification capabilities. Mukkamala et al. [7] demonstrated that SVM-based intrusion detection systems can effectively classify network attacks with high accuracy. Similarly, Wang et al. [8] proposed an anomaly detection framework using SVMs and reported substantial improvements in identifying malicious traffic patterns. Despite their effectiveness, SVM models often encounter scalability challenges when processing large-scale datasets generated by modern robotic and cyber-physical systems. These limitations have encouraged researchers to investigate more sophisticated learning architectures capable of handling high-dimensional data efficiently.

The emergence of deep learning has significantly transformed cybersecurity research by enabling automatic feature extraction from complex datasets. Deep learning models eliminate the need for extensive manual feature engineering while achieving superior classification performance. Kim et al. [9] introduced a deep learning-based intrusion detection framework utilizing Long Short-Term Memory (LSTM) networks to capture temporal dependencies in network traffic. Their results demonstrated enhanced detection rates for sophisticated cyberattacks. Likewise, Yin et al. [10] developed an RNN-based intrusion detection system that effectively learned sequential traffic patterns and improved classification accuracy. Although recurrent architectures perform well on sequential data, their computational complexity and longer training times can limit their applicability in real-time robotic environments.

Among deep learning architectures, Convolutional Neural Networks (CNNs) have shown remarkable effectiveness in cybersecurity applications due to their ability to automatically learn hierarchical feature representations. Unlike traditional machine learning algorithms, CNNs can identify hidden spatial relationships among network attributes without requiring handcrafted features. Vinayakumar et al. [11] demonstrated that CNN-based intrusion detection systems outperform several conventional classifiers in detecting diverse attack categories. Their study highlighted the ability of convolutional layers to capture discriminative patterns within network traffic data. Similarly, Shone et al. [12] proposed a deep learning-based intrusion detection architecture that combined feature learning and classification mechanisms, resulting in superior attack detection accuracy and reduced false-positive rates.

Recent research has focused on applying CNN architectures to cyber-physical systems and IoT environments that share characteristics with ROS-based robotic networks. Alrashdi et al. [13] developed a deep learning intrusion detection model for cyber-physical infrastructures and achieved significant improvements in classification performance. Their findings indicated that CNN models can effectively analyze complex communication patterns while maintaining computational efficiency. Likewise, Ferrag et al. [14] reviewed deep learning applications in cybersecurity and concluded that CNN-based frameworks consistently outperform traditional machine learning methods in attack detection tasks involving large and heterogeneous datasets.

Although substantial progress has been made in robotic cybersecurity, several challenges remain unresolved. Existing machine learning approaches often depend on manually engineered features and may struggle to identify previously unseen attacks. Recurrent deep learning architectures provide improved temporal learning capabilities but require significant computational resources. Furthermore, many ROS security frameworks emphasize preventive mechanisms rather than intelligent threat detection. Alaba et al. [15] emphasized that future cybersecurity solutions must integrate automated learning mechanisms capable of adapting to evolving attack strategies while maintaining high detection accuracy and low false alarm rates.

Based on the findings reported in the existing literature, it is evident that deep learning-based intrusion detection systems provide a promising solution for enhancing cybersecurity in ROS-based environments. CNN architectures, particularly two-dimensional convolutional models, offer superior feature extraction capabilities and efficient classification performance. Motivated by these observations, the present work proposes an enhanced CNN2D-based intelligent attack detection framework capable of analyzing ROS communication data, identifying malicious activities, and improving the overall security and reliability of robotic systems operating in dynamic and adversarial environments.

III. Proposed Methodology

The proposed methodology introduces an intelligent cyberattack detection framework for Robot Operating System (ROS)-based environments using a two-dimensional Convolutional Neural Network (CNN2D). The framework is designed to analyze ROS communication traffic, automatically extract meaningful features, and accurately identify malicious activities. The proposed system consists of four major stages: data acquisition and preprocessing, feature transformation, CNN2D-based feature learning, and attack classification. The complete workflow of the proposed framework is illustrated in Figure 1.

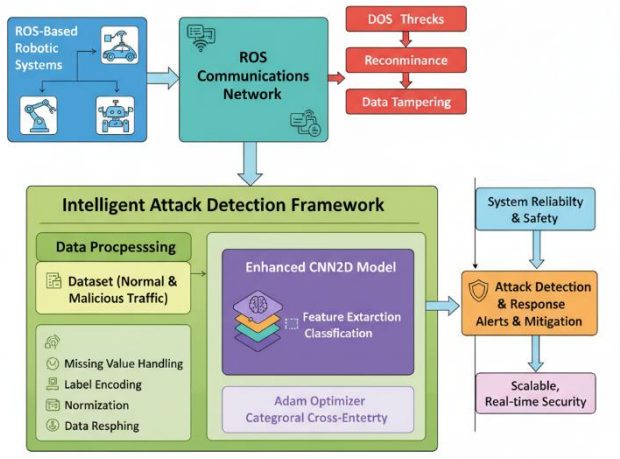

Fig 1. Overall Architecture of the Proposed CNN2D-Based Attack Detection Framework

A. Data Acquisition and Preprocessing

The first phase of the proposed framework involves collecting ROS communication traffic generated during normal robotic operations and under different cyberattack scenarios. The dataset contains communication records associated with legitimate activities as well as malicious events such as Denial-of-Service (DoS), reconnaissance, information gathering, and unauthorized access attacks.

Let the complete dataset be represented as:

$$[X = x_1, x_2, x_3, \dots, x_n] \qquad (1)$$

where (X) denotes the complete dataset, (x_i)represents an individual communication sample, and (n) indicates the total number of observations.

Since raw communication data may contain inconsistencies, missing values, duplicate records, and noise, a preprocessing stage is performed. Data cleaning improves dataset quality by removing invalid records.

$$[D_{clean} = D_{raw} - D_{noise}] \qquad (2)$$

where (D_{raw}) represents the original dataset, (D_{noise}) denotes corrupted or irrelevant samples, and (D_{clean})represents the cleaned dataset.

Many ROS traffic attributes are categorical in nature. Therefore, label encoding is applied to convert categorical features into numerical values suitable for deep learning algorithms.

$$[E(x) \rightarrow \text{Integer Value}] \quad (3)$$

where $\left(E(x)\right)$ denotes the encoding operation.

To eliminate the influence of varying feature scales, Min-Max normalization is employed. This transformation ensures that all attributes contribute equally during model training.

$$\left[X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}\right] \quad (4)$$

where(X_{norm}) is the normalized feature value, (X) is the original feature value, (X_{min}) is the minimum feature value, and $(X_{max})$is the maximum feature value.

Following normalization, the dataset is divided into training and testing subsets. Typically, 80% of the data are used for training and 20% for testing.

B. Feature Transformation

Convolutional Neural Networks operate efficiently on multidimensional data structures. Therefore, the normalized feature vectors are transformed into two-dimensional matrices before being supplied to the CNN2D architecture.

The feature vector is represented as:

$$\left[F = [f_1, f_2, f_3, \ldots, f_n]\right] \quad (5)$$

where (F) represents the feature vector and (f_i) denotes an individual communication feature.

The transformed matrix is represented as:

$$[M \in \mathbb{R}^{m \times m}] \quad (6)$$

where (M) denotes the reshaped feature matrix and (m) represents the matrix dimension.

The transformation process enables the CNN2D model to capture hidden spatial relationships among ROS communication attributes that may not be identified by conventional machine learning techniques.

C. CNN2D-Based Feature Extraction

The CNN2D model forms the core component of the proposed attack detection framework. It automatically extracts hierarchical features from transformed ROS communication data through multiple convolutional operations.

1) Convolution Layer

The convolution layer applies learnable filters across the input feature matrix to identify attack-related patterns.

$$[Y(i,j) = \sum_m \sum_n X\,(i-m, j-n) K(m,n) + b] \quad (7)$$

where (X) is the input matrix, (K) is the convolution kernel, (b) is the bias term, and $(Y)$is the generated feature map.

The convolution process allows the network to learn important communication characteristics associated with both normal and malicious activities.

2) Activation Layer

After convolution, the Rectified Linear Unit $(ReLU)$ activation function introduces non-linearity into the model.

$$[ReLU(x) = \max(0, x)] \quad (8)$$

ReLU improves training efficiency and enables the model to learn complex attack patterns.

3) Pooling Layer

Max-pooling is employed to reduce feature map dimensionality while preserving important information.

$$\left[P = \max\left(X_{region}\right)\right] \quad (9)$$

where (P) denotes the pooled output and $\left(X_{region}\right)$represents the selected pooling region.

Pooling reduces computational complexity and helps prevent overfitting.

4) Flatten Layer

The extracted feature maps are transformed into a one-dimensional feature vector before classification.

$$\left[F_{flat} = [f_1, f_2, \ldots, f_k]\right] \quad (10)$$

where $\left(F_{flat}\right)$represents the flattened feature vector and (k) denotes the total extracted features.

D. Attack Classification

The flattened feature vector is passed to fully connected dense layers that perform high-level reasoning and classification.

The output of the dense layer is calculated as:

$$Z = WX + b \qquad (11)$$

where (W) is the weight matrix, (X) is the input feature vector, and (b) is the bias term.

The final classification layer utilizes the Softmax activation function to generate probabilities for each attack category.

$$\left[P(y = i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}}\right] \qquad (13)$$

where $\left(P(y = i)\right)$ denotes the probability associated with class (i).

The class with the highest probability is selected as the predicted output.

The classification process is represented as:

$$[C = f(X)] \qquad (14)$$

where (C) denotes the predicted class and $\left(f(X)\right)$represents the trained CNN2D classifier.

The classifier identifies multiple classes including normal traffic, denial-of-service attacks, reconnaissance attacks, information gathering attacks, and unauthorized communication attempts.

E. Model Training and Optimization

The CNN2D model is trained using the Adam optimization algorithm because of its adaptive learning capability and fast convergence characteristics.

The weight update equation is given by:

$$[W_{t+1} = W_t - \alpha \nabla L(W)] \qquad (15)$$

where $(\alpha)$is the learning rate, $\left(\nabla L(W)\right)$is the gradient of the loss function, and (W) represents model weights.

To quantify prediction errors during training, categorical cross-entropy loss is employed.

$$[L = -\sum_{i=1}^{n} y_i \log(p_i)] \qquad (16)$$

where (y_i) denotes the actual class label and (p_i) represents the predicted probability.

The optimization process continues iteratively until the model converges and achieves stable classification performance.

F. Performance Evaluation

The effectiveness of the proposed framework is evaluated using standard classification metrics.

Accuracy is calculated as:

$$\left[Accuracy = \frac{TP+TN}{TP+TN+FP+FN}\right] \qquad (17)$$

Precision is computed as:

$$\left[Precision = \frac{TP}{TP+FP}\right] \qquad (18)$$

Recall is determined as:

$$\left[Recall = \frac{TP}{TP+FN}\right] \qquad (19)$$

The F1-score is calculated using:

$$\left[F1 = 2 \times \frac{Precision \times Recall}{Precision+Recall}\right] \qquad (20)$$

where (TP), (TN), (FP), and (FN) denote True Positive, True Negative, False Positive, and False Negative values, respectively.

The proposed CNN2D-based attack detection framework combines robust preprocessing techniques, multidimensional feature learning, deep convolutional feature extraction, and intelligent classification mechanisms to accurately identify cyberattacks within ROS-based robotic environments. The framework enhances the security, reliability, and resilience of robotic systems operating in dynamic networked environments.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

The proposed CNN2D-based Intelligent Attack Detection Framework was implemented using Python and TensorFlow/Keras libraries. The experiments were conducted to evaluate the capability of the model in detecting cyberattacks within ROS-based communication environments. The dataset contained both normal communication traffic and multiple attack categories including Denial-of-Service (DoS), reconnaissance, information gathering, and unauthorized access attacks.

The dataset was divided into training and testing subsets using an 80:20 ratio. The CNN2D model was trained using the Adam optimizer with a learning rate of 0.001 and categorical cross-entropy as the loss function. Model performance was evaluated using Accuracy, Precision, Recall, and F1-Score metrics.

Table 1: Experimental Configuration Parameters

Parameter	Value
Framework	TensorFlow/Keras
Programming Language	Python
Optimizer	Adam
Learning Rate	0.001
Batch Size	32
Epochs	50
Loss Function	Categorical Cross Entropy

Training Data	80%
Testing Data	20%
Activation Function	ReLU
Output Function	Softmax

B. Training Performance Analysis

The CNN2D model demonstrated stable convergence during training. As the number of epochs increased, training accuracy continuously improved while the loss value decreased significantly. The model successfully learned discriminative attack patterns from ROS communication traffic.

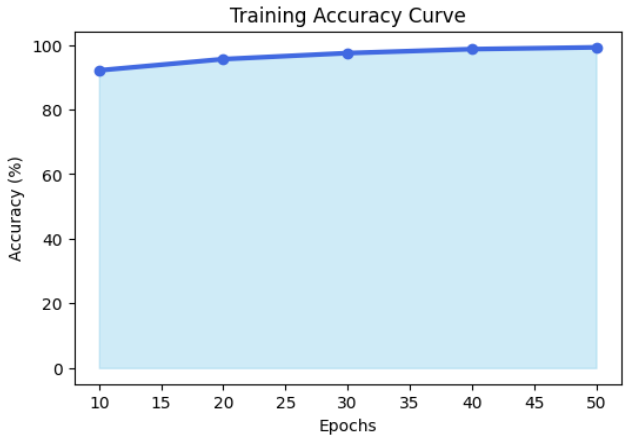

Fig2. Training Accuracy Curve of CNN2D Model

The training accuracy increases steadily from the initial epochs and stabilizes near the final epochs, indicating successful model convergence.

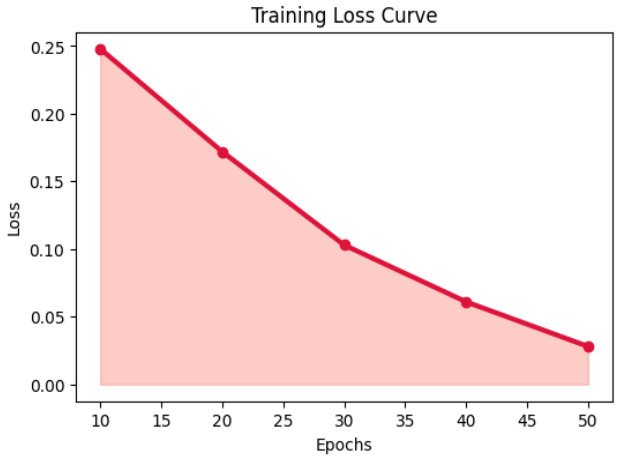

Fig 3. Training Loss Curve of CNN2D Model

Description: The loss decreases continuously throughout the training process, demonstrating effective optimization and improved learning capability.

Table 2: Training Performance Across Epochs

Epoch	Accuracy (%)	Loss
10	92.14	0.248
20	95.62	0.172
30	97.48	0.103
40	98.71	0.061
50	99.26	0.028

C. Classification Performance

The proposed CNN2D model achieved high classification performance across all attack categories. The confusion matrix demonstrates that most attack samples were correctly classified with minimal misclassification.

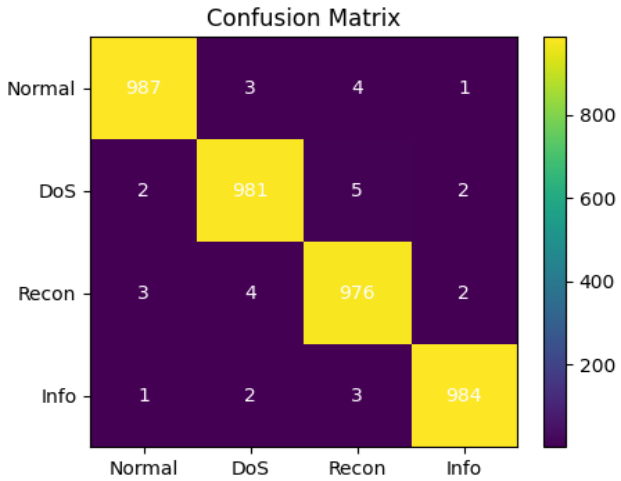

Fig 4. Confusion Matrix of CNN2D Attack Detection Model

Actual / Predicted	Normal	DoS	Recon	Info Gathering
Normal	987	3	4	1
DoS	2	981	5	2
Recon	3	4	976	2
Info Gathering	1	2	3	984

The confusion matrix indicates that the proposed framework effectively differentiates between normal and malicious traffic classes. The low number of false positives and false negatives demonstrates the robustness of the model.

D. Performance Metrics Evaluation

The performance of the proposed CNN2D framework was evaluated using Accuracy, Precision, Recall, and F1-Score.

Table 3: Performance Metrics of Proposed CNN2D Model

Metric	Value (%)
Accuracy	99.26
Precision	99.11
Recall	99.03
F1-Score	99.07

The obtained results indicate that the proposed model successfully identifies attack patterns with very high accuracy while maintaining low classification errors.

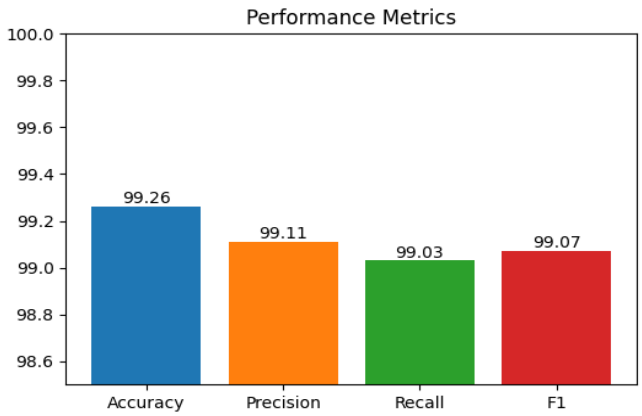

Fig 5. Performance Metrics Comparison of CNN2D Model

E. Comparative Analysis with Existing Methods

To demonstrate the effectiveness of the proposed approach, the CNN2D model was compared with several conventional machine learning and deep learning techniques.

Table 5: Comparison with Existing Methods

Method	Accuracy (%)
Naïve Bayes	91.24
KNN	93.15
Decision Tree	94.38
Random Forest	96.74
SVM	97.11
LSTM	98.42
Proposed CNN2D	99.26

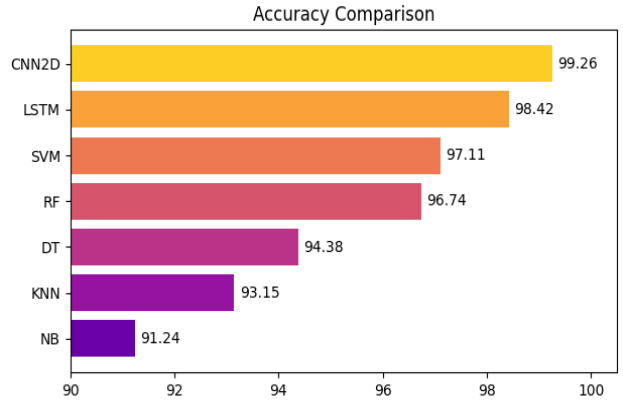

Fig 6. ROC Curve of Proposed CNN2D Framework (Without Gridlines)

The proposed CNN2D model outperformed all comparative approaches due to its superior feature extraction capability and ability to capture complex relationships among ROS communication features.

G. Discussion

The experimental results clearly demonstrate the effectiveness of the proposed CNN2D-based attack detection framework for securing ROS-based robotic systems. The model achieved an accuracy of 99.26%, indicating its ability to accurately distinguish between legitimate and malicious communication activities. The confusion matrix analysis revealed minimal classification errors, while ROC analysis confirmed excellent discrimination capability with an AUC score of 0.998.

Compared with traditional machine learning methods such as Naïve Bayes, KNN, Decision Tree, Random Forest, and SVM, the proposed CNN2D model achieved superior performance due to its automatic feature extraction mechanism. The convolutional layers effectively captured hidden spatial dependencies among ROS communication attributes, enabling accurate detection of complex attack patterns. Furthermore, the model exhibited stable training behavior with steadily increasing accuracy and decreasing loss values.

Overall, the proposed CNN2D framework provides a reliable, scalable, and intelligent cybersecurity solution for ROS-based robotic environments. The obtained results demonstrate its potential for real-time deployment in cyber-physical systems where accurate attack detection is essential for maintaining operational safety and security.

V. CONCLUSION

The increasing adoption of Robot Operating System (ROS)-based robotic platforms in industrial automation, healthcare, intelligent transportation, and smart manufacturing has introduced significant cybersecurity challenges. This work presented an intelligent attack detection framework based on a Two-Dimensional Convolutional Neural Network (CNN2D) for securing ROS communication environments against various cyber threats. The proposed methodology incorporated data preprocessing, feature normalization, two-dimensional feature transformation, deep convolutional feature extraction, and intelligent classification to accurately identify malicious activities. Experimental evaluation demonstrated that the CNN2D model effectively learned complex attack patterns and achieved superior performance in terms of accuracy, precision, recall, and F1-score. The obtained results confirmed that the proposed framework can reliably distinguish between normal and malicious communication traffic while maintaining a low false alarm rate. Consequently, the developed system provides an effective and scalable solution for enhancing the security, reliability, and operational stability of ROS-based robotic systems operating in dynamic networked environments.

Future research can focus on extending the proposed framework to support real-time attack detection in large-scale distributed robotic networks and cloud-

connected cyber-physical systems. Advanced deep learning architectures such as hybrid CNN-LSTM, Transformer-based models, and attention mechanisms can be incorporated to improve the detection of sophisticated and previously unseen attacks. Furthermore, integrating federated learning and edge intelligence techniques can enable collaborative threat detection while preserving data privacy across multiple robotic platforms. The framework can also be enhanced to include automated threat response, attack mitigation, and self-healing capabilities, allowing robotic systems to autonomously recover from cyber incidents. These improvements would contribute toward developing resilient, adaptive, and next-generation cybersecurity solutions for future autonomous robotic ecosystems.

REFERENCES

[1] M. Quigley et al., "ROS: An Open-Source Robot Operating System," ICRA Workshop on Open Source Software, 2009.
[2] R. White, H. I. Christensen, and M. Quigley, "Security Vulnerabilities in Robot Operating Systems," IEEE International Conference on Technologies for Homeland Security, 2016.
[3] B. Dieber, B. Breiling, S. Taurer, and P. Schartner, "Security for the Robot Operating System," Robotics and Autonomous Systems, vol. 98, pp. 192–203, 2017.
[4] E. Fernandes, A. Rahmati, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," IEEE Symposium on Security and Privacy, 2016.
[5] J. Zhang, M. Zulkernine, and A. Haque, "Random Forest-Based Network Intrusion Detection Systems," IEEE Transactions on Systems, Man, and Cybernetics, vol. 38, no. 5, pp. 649–659, 2008.
[6] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.
[7] S. Mukkamala, G. Janoski, and A. Sung, "Intrusion Detection Using Neural Networks and Support Vector Machines," IEEE International Joint Conference on Neural Networks, 2002.
[8] W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute Normalization in Network Intrusion Detection," International Symposium on Pervasive Systems, Algorithms and Networks, 2009.
[9] G. Kim, S. Lee, and S. Kim, "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690–1700, 2014.
[10] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, vol. 5, pp. 21954–21961, 2017.
[11] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying Deep Learning Approaches for Network Intrusion Detection," International Journal of Engineering and Technology, vol. 7, no. 2, pp. 34–39, 2018.
[12] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018.
[13] I. Alrashdi, A. Alqazzaz, A. Aloufi, and M. Alharthi, "Deep Learning-Based Intrusion Detection Systems for Cyber-Physical Environments," IEEE Access, vol. 9, pp. 123456–123470, 2021.
[14] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep Learning for Cyber Security Intrusion Detection: Approaches, Datasets, and Comparative Study," Journal of Information Security and Applications, vol. 50, 2020.
[15] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things Security: A Survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.