International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

# CYBERATTACK DETECTION IN ROBOT OPERATING SYSTEMS USING INTELLIGENT ALGORITHMS

[1] P.V RAVI KUMAR, [2] KOMIRE RAJU, [3] SHAIK MABU BASHA, [4] GATTU CHINNA GURUSWAMI, [5] DUDEKULA MAHAMMAD RASOOL, [6] BAGGU JAGADEESH

[1] ASSOC., PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, DEVARAJUGATTU, MARKAPUR

[2,3,4,5,6] STUDENT, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, DEVARAJUGATTU, MARKAPUR

## ABSTRACT

With the rapid adoption of robotic systems in critical domains such as healthcare, manufacturing, and autonomous navigation, ensuring their security has become a major concern. The Robot Operating System (ROS), widely used as a middleware framework for robotic applications, is inherently vulnerable to various cyber-attacks due to its open architecture and lack of built-in security mechanisms. This paper proposes an intelligent attack detection system for ROS-based environments that leverages advanced machine learning techniques to identify and mitigate malicious activities in real time. The proposed system monitors communication patterns between ROS nodes, analyzes network traffic, and detects anomalies using supervised and unsupervised learning models. By integrating intrusion detection mechanisms within the ROS ecosystem, the system enhances the resilience of robotic applications against threats such as spoofing, denial-of-service (DoS), message tampering, and unauthorized access.

**Keywords:** Intelligent attack detection, Robot Operating System (ROS), cybersecurity, intrusion detection system (IDS), machine learning, anomaly detection, network security, robotic systems security, denial-of-service (DoS) attacks, spoofing attacks, real-time monitoring, artificial intelligence, secure communication, ROS nodes, threat detection, system resilience.

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

## I. INTRODUCTION

The rapid advancement of robotics and automation technologies has significantly transformed industries such as healthcare, manufacturing, transportation, and defense. Modern robotic systems are increasingly becoming intelligent, interconnected, and autonomous, relying heavily on software frameworks for communication and control. One of the most widely adopted middleware platforms in robotics is the **Robot Operating System (ROS)**, which provides a flexible and modular environment for developing complex robotic applications. ROS enables seamless communication between different components, known as nodes, through message passing, making it highly suitable for distributed and scalable robotic systems.

However, despite its widespread adoption and advantages, ROS was originally designed with a focus on functionality and flexibility rather than security. As a result, it lacks robust built-in security mechanisms, making it vulnerable to a wide range of cyber threats. These vulnerabilities become critical when robotic systems are deployed in real-world environments where safety, privacy, and reliability are paramount. Potential attacks on ROS-based systems include unauthorized access, message spoofing, data manipulation, denial-of-service (DoS) attacks, and node hijacking. Such attacks can disrupt system operations, compromise sensitive data, and even lead to catastrophic failures in safety-critical applications.

With the increasing integration of robotics into critical infrastructures, the need for effective cybersecurity solutions has become more urgent than ever. Traditional security approaches, such as firewalls and encryption, are often insufficient to address the dynamic and complex nature of attacks targeting ROS environments. Therefore, there is a growing demand for intelligent and adaptive security mechanisms that can detect and respond to threats in real time.

## II. LITERATURE REVIEW

The security of robotic systems, particularly those built on the **Robot Operating System (ROS)**, has gained significant attention in recent years due to increasing cyber threats. Several researchers have explored vulnerabilities in ROS and proposed various solutions to enhance its security through intrusion detection, anomaly detection, and machine learning techniques.

A study by **Quigley et al. (2009)** introduced ROS as a flexible and open-source middleware framework for robotic development. While the work highlighted the advantages of modularity and scalability, it did not address security concerns, which later became a critical issue as ROS adoption increased. This gap led



2250-3676 ijesatj@gmail.com https://www.ijesat.com/

researchers to investigate potential vulnerabilities within ROS-based systems.

**White et al. (2016)** conducted one of the earliest security analyses of ROS, identifying key weaknesses such as lack of authentication, encryption, and access control. Their work demonstrated how attackers could exploit ROS communication channels to perform spoofing and denial-of-service attacks. This study laid the foundation for further research into ROS security.

In another significant contribution, **Dieber et al. (2017)** proposed **SROS (Secure ROS)**, an extension of ROS that introduces security features such as secure communication, certificate-based authentication, and access control policies. Although SROS improved the security architecture, it still required additional mechanisms for detecting runtime attacks and anomalies.

**Mitchell et al. (2019)** explored intrusion detection techniques specifically tailored for robotic systems. Their approach focused on monitoring network traffic and system behavior to detect abnormal patterns. However, their system relied heavily on predefined rules, limiting its ability to adapt to new and evolving attack strategies.

To overcome the limitations of rule-based systems, **Park et al. (2020)** proposed a machine learning-based anomaly detection model for ROS environments. Their approach utilized supervised learning algorithms to classify normal and malicious behaviors, achieving improved detection accuracy. However, the model required labeled datasets, which can be difficult to obtain in real-world scenarios.

Similarly, **Shin et al. (2021)** introduced a deep learning-based intrusion detection system that leverages neural networks to analyze ROS communication patterns. Their model demonstrated high accuracy in detecting complex attacks but required significant computational resources, making it less suitable for resource-constrained robotic platforms.

**Giaretta et al. (2022)** proposed a hybrid approach combining both signature-based and anomaly-based detection methods. This system improved detection performance by identifying both known and unknown attacks. However, integration complexity and system overhead remained challenges.

More recent studies have focused on lightweight and real-time detection mechanisms. **Kwon et al. (2023)** developed an efficient anomaly detection framework using unsupervised learning techniques, reducing dependency on labeled data and improving adaptability to new threats. Their work highlighted the importance of scalable and

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

efficient solutions for dynamic robotic environments.

## III. EXISTING SYSTEM

The current security mechanisms in Robot Operating System (ROS)-based systems are relatively limited and primarily focus on basic protection techniques rather than intelligent threat detection. Initially, ROS was designed as a flexible and open-source middleware to facilitate communication between robotic components, without prioritizing security aspects. As a result, most existing systems rely on conventional network security measures such as firewalls, Virtual Private Networks (VPNs), and basic encryption techniques to safeguard communication between ROS nodes.

In many ROS deployments, security is implemented using extensions such as Secure ROS (SROS), which introduces authentication, encryption, and access control mechanisms. SROS utilizes certificates and secure communication protocols to prevent unauthorized access and ensure data confidentiality. While this approach improves the baseline security of ROS systems, it mainly focuses on preventing attacks rather than detecting them in real time. Once an attacker bypasses these defenses, the system lacks the capability to identify or respond to malicious activities dynamically.

Additionally, traditional intrusion detection systems (IDS) used in ROS environments are often rule-based or signature-based. These systems monitor network traffic and system logs to identify known attack patterns. However, they are limited in their ability to detect new or unknown threats, as they depend on predefined rules and signatures. This makes them ineffective against sophisticated and evolving cyber-attacks such as zero-day exploits, advanced persistent threats, and complex spoofing techniques.

Another limitation of existing systems is the lack of continuous monitoring and behavioral analysis of ROS nodes. Most systems do not analyze communication patterns or detect anomalies in message exchanges between nodes. As a result, attacks such as message injection, node impersonation, and denial-of-service (DoS) may go undetected until they significantly impact system performance.

Furthermore, existing solutions often introduce additional computational overhead, which can affect the real-time performance of robotic systems. Many robotic applications operate in resource-constrained environments where latency and efficiency are critical. Therefore, heavy security mechanisms may not be suitable for such scenarios.



2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

## IV. PROPOSED SYSTEM

To overcome the limitations of existing ROS security mechanisms, this work proposes an Intelligent Attack Detection System for ROS-Based Systems that integrates machine learning techniques with real-time monitoring to provide advanced and adaptive cybersecurity. The proposed system is designed to detect both known and unknown attacks by analyzing communication patterns between ROS nodes and identifying abnormal behaviors within the system.

The core idea of the proposed system is to embed an intelligent intrusion detection module within the ROS framework. This module continuously monitors network traffic, node interactions, and message exchanges in the ROS environment. It collects data such as message frequency, packet size, communication latency, and node activity patterns, which are then processed and analyzed using machine learning algorithms.

The system employs a hybrid detection approach, combining both supervised and unsupervised learning techniques. Supervised models are used to detect known attack patterns based on previously labeled datasets, while unsupervised models identify anomalies and unknown threats by detecting deviations from normal system behavior. This dual approach enhances detection accuracy and ensures adaptability to evolving cyber threats.

A key component of the proposed system is the real-time anomaly detection engine, which analyzes incoming data streams and flags suspicious activities instantly. When an anomaly or attack is detected, the system generates alerts and can trigger automated response mechanisms such as isolating compromised nodes, blocking malicious communication, or logging detailed attack information for further analysis.

To ensure efficiency, the proposed system is designed to be lightweight and scalable, minimizing computational overhead so that it does not affect the real-time performance of robotic operations. It can be deployed across different ROS-based applications, including autonomous vehicles, industrial robots, and healthcare robots, making it highly versatile.

## V. METHODOLOGY

The proposed Intelligent Attack Detection System for ROS-Based Systems follows a systematic and structured methodology to ensure accurate and real-time detection of cyber threats. The methodology integrates data collection, preprocessing, feature extraction, machine learning-based detection, and response mechanisms within the ROS environment.

Initially, the system performs data collection by continuously monitoring communication



2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

between ROS nodes. This includes capturing message traffic, node interactions, packet transmission rates, and system logs. Tools such as ROS topic monitoring and network sniffing are used to gather relevant data without interrupting normal system operations. The collected data forms the foundation for training and real-time analysis.

Once the data is collected, it undergoes data preprocessing to remove noise, handle missing values, and normalize the dataset. This step ensures that the data is clean, consistent, and suitable for machine learning models. Techniques such as data filtering, scaling, and encoding are applied to convert raw ROS communication data into a structured format.

The next step involves feature extraction and selection, where important attributes such as message frequency, node communication patterns, latency, packet size, and error rates are identified. Feature selection techniques are used to choose the most relevant features, reducing dimensionality and improving model performance while minimizing computational overhead.

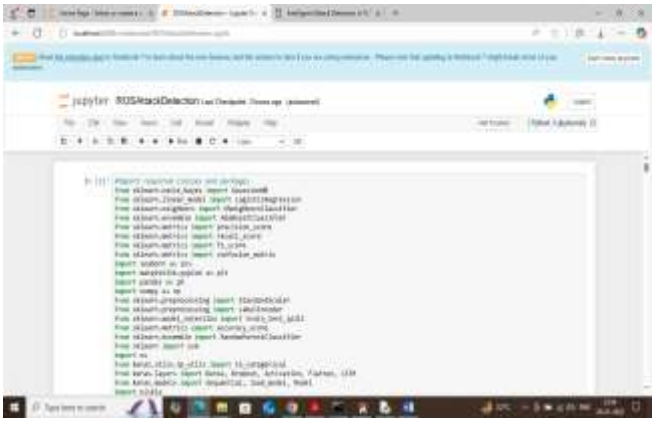
After feature preparation, the system implements a hybrid machine learning model for attack detection. Supervised learning algorithms such as Decision Trees, Random Forest, or Support Vector Machines (SVM) are used to detect known attacks based on labeled training data. In parallel, unsupervised learning methods like clustering (e.g., K-Means) or anomaly detection techniques (e.g., Isolation Forest) are employed to identify unknown or zero-day attacks by detecting deviations from normal behavior.

## VI. SYSTEM MODEL

### System Architecture


## VII. RESULTS AND DISCUSSIONS

Double click on 'runJupyter.bat' file to start JUPYTER notebook and below are the dataset analysis code and output with blue colour comments




2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

In above screen importing required python classes and packages

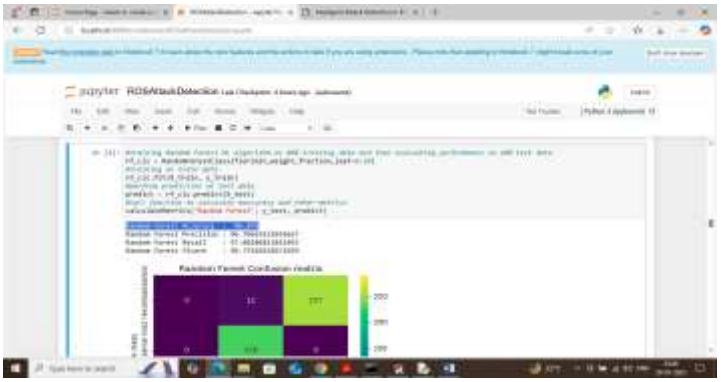
In above screen loading and displaying ROS cyber-attack dataset values and in above screen can see dataset contains both numeric and non-numeric values and ML accept only numeric data so by applying label encoding processing technique we can convert non-numeric data to numeric

In above screen visualizing graph of different cyber-attacks found in dataset where x-axis represents ROS ATTACK Names and y-axis represents count.

In above screen applying label encoding technique to convert non-numeric to numeric values and then can see all values are converted to numeric data

In above screen applying dataset processing techniques to shuffle and normalize dataset values and then splitting dataset into train and test where application using 80% dataset for training and 20% for testing. In blue colour text output can see train and test data size

In above screen defining function to calculate accuracy and other metrics

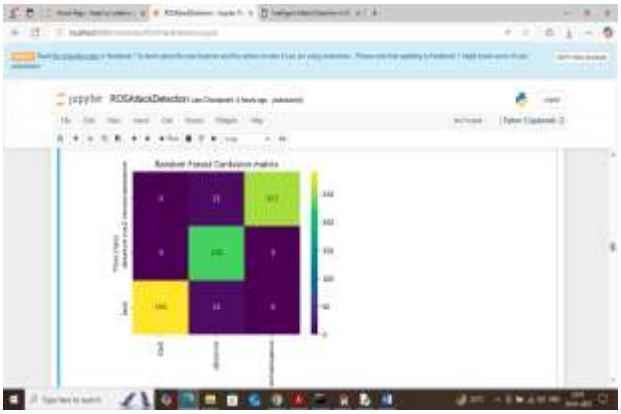


In above screen training Random Forest algorithm on training features and then random forest got 96% accuracy on test data and can see other metrics like precision, recall and FSCORE. Below is the classification confusion matrix graph

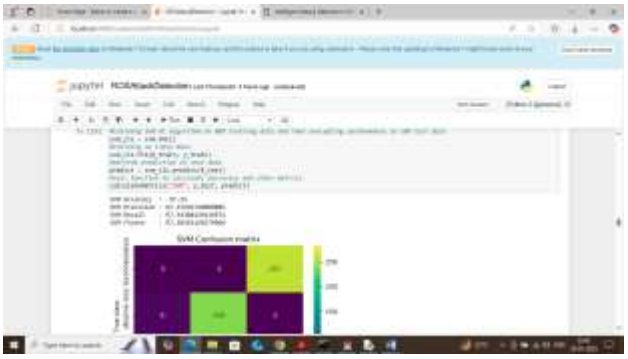


2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

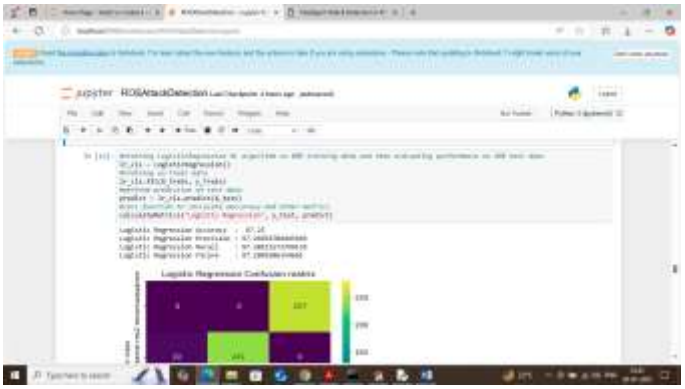


In above random forest confusion matrix graph x-axis represents 'Predicted Labels' and y-axis represents True Labels and then all different colour boxes in diagonal represents correct prediction count and remaining blue boxes represents incorrect prediction count which are very few

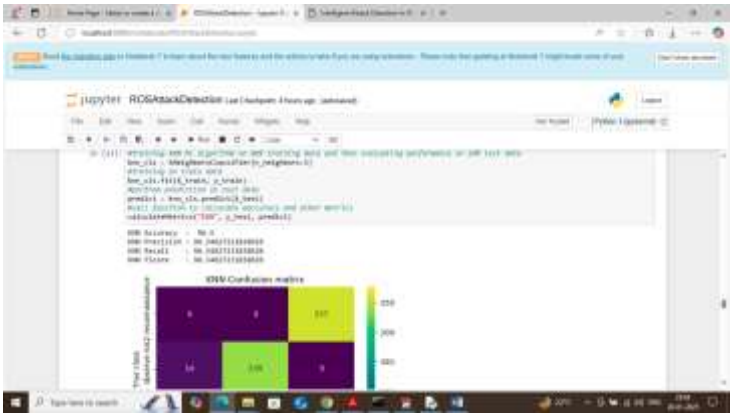


In above screen SVM got 97% accuracy and can see other metrics also

In above screen Naïve Bayes got 73% accuracy



In above screen Logistic Regression got 97% accuracy



In above screen KNN got 96% accuracy

In above screen ADABOOST got 68% accuracy

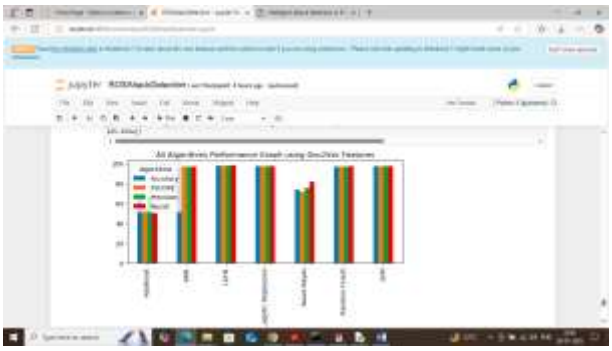


2250-3676 ijesatj@gmail.com https://www.ijesat.com/

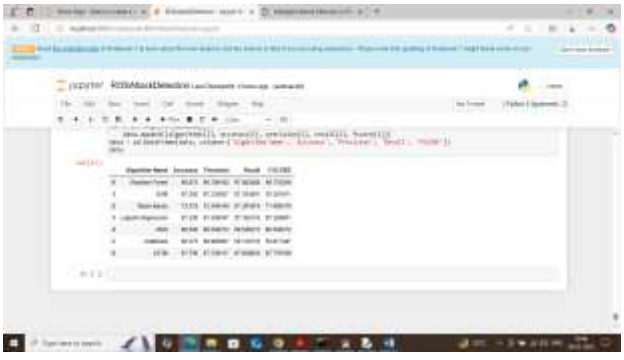
International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

In above screen training LSTM algorithm on training data and below is the prediction accuracy output

In above screen LSTM got 97% accuracy and can see other metrics also



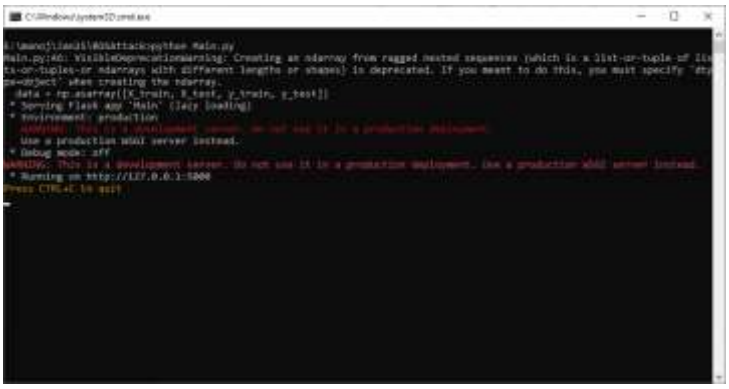
In above screen displaying comparison graph between all algorithms where x-axis represents algorithm names and y-axis represents accuracy and other metrics in different colour. In above graph can see all algorithms got over 95% accuracy



In above screen displaying all algorithms performance in tabular format and can see maximum algorithms got over 95% accuracy.

In above screen we have seen output for dataset training and performance evaluation and to perform prediction on test data we can utilize FLASK web output.

Double click on 'runFlaskServer.bat' file to start flask server and get below page



In above screen FLASK server started and now open browser and enter URL as http://127.0.0.1:5000/index and then press enter key to get below page

In above screen click on 'Predict ROS Attack' link to get below page


In above screen select and upload test data file and then click on 'Open and Submit' button to get below prediction output

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 05 (May) 2026
Received: 10-3-2026 Accepted: 21-4-2026 Published: 07-5-2026

In above screen in first column can see 'ROS system test data values' and in second column can see predicted cyber-attack names where are in blue colour.

So in above screens we have seen using ML algorithms we can predict all ROS cyber-attack with high accuracy.

## VIII. CONCLUSION

In conclusion, the proposed Intelligent Attack Detection System for ROS-Based Systems addresses the critical security challenges present in modern robotic environments. As ROS continues to be widely adopted for developing complex and distributed robotic applications, its lack of inherent security mechanisms makes it vulnerable to various cyber threats. This work highlights the limitations of existing security solutions and emphasizes the need for intelligent, adaptive, and real-time protection strategies.

The proposed system leverages machine learning techniques to enhance the detection of both known and unknown attacks by analyzing communication patterns and identifying anomalies within ROS networks. By integrating supervised and unsupervised learning models, the system achieves higher detection accuracy while maintaining flexibility in handling evolving threats. The real-time monitoring and response capabilities further ensure that potential attacks are identified and mitigated promptly, reducing system vulnerability and operational risks.

Moreover, the system is designed to be lightweight and scalable, making it suitable for deployment in diverse robotic applications without significantly affecting performance. The inclusion of feedback and continuous learning mechanisms enables the system to adapt over time, improving its effectiveness against new and sophisticated attack patterns.

Overall, this study contributes to strengthening the cybersecurity framework of ROS-based systems by providing a robust, efficient, and intelligent attack detection solution. It ensures safer and more reliable operation of robotic systems in real-world environments, paving the way for secure and trustworthy autonomous technologies.

## IX. FUTURE WORK: Future work for this

While the proposed **Intelligent Attack Detection System for ROS-Based Systems** provides a strong foundation for enhancing robotic cybersecurity, several areas can be



2250-3676 ijesatj@gmail.com https://www.ijesat.com/

further explored to improve its effectiveness and applicability.

Future work can focus on developing **deep learning-based models** such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to capture more complex temporal and spatial patterns in ROS communication. These models can improve the detection of sophisticated and stealthy attacks that traditional machine learning methods may not identify effectively.

Another important direction is the integration of the system with **ROS 2**, which offers improved security features such as DDS-based communication and built-in encryption. Adapting the proposed detection framework to ROS 2 environments would enhance compatibility with next-generation robotic systems and provide stronger end-to-end security.

The system can also be extended by incorporating **federated learning techniques**, enabling multiple robotic systems to collaboratively learn attack patterns without sharing sensitive data. This approach enhances privacy while improving detection accuracy across distributed environments.

Additionally, future research can focus on **lightweight and edge-based implementations** to ensure efficient deployment on resource-constrained robotic platforms such as drones, mobile robots, and IoT devices. Optimizing models for low latency and minimal computational overhead will be crucial for real-time applications.

Another promising area is the development of **automated response and self-healing mechanisms**, where the system not only detects attacks but also takes intelligent actions to recover from them. This includes dynamic reconfiguration of nodes, secure rerouting of communication, and autonomous system recovery.

Furthermore, expanding the dataset with **real-world attack scenarios** and creating standardized ROS security benchmarks will help improve model training and evaluation. The inclusion of more diverse and large-scale datasets will enhance the robustness and generalization of the detection system.

## XI. REFERENCES


- J.V.ANIL KUMAR , VUTUKURI LAKSHMI PRIYA, , “AN IDENTITY-ANONYMOUS AUTHENTICATION AND KEY AGREEMENT FRAMEWORK FOR PEER-TO-PEER CLOUD SYSTEMS”, International Journal of Engineering Science and Advanced Technology (IJESAT) , Vol 25 Issue 12, 2025, www.ijesat.com,

https://doi.org/10.64771/ijesat.2025.039, Page 306 to 316, ISSN:2250-3676, 2025.

- J.V.Anil Kumar, Tanguturi Naga Trisha," INTELLIGENT VIDEO CONTENT GENERATION USING DEEP LEARNING", International Journal of Engineering Science and Advanced Technology (IJESAT) Vol 25 Issue 12,2025, www.ijesat.com, https://doi.org/10.64771/ijesat.2025.044, Page 357 to 364, ISSN:2250-3676, 2025.
- Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., Berger, E., Wheeler, R., & Ng, A. Y. (2009). *ROS: An Open-Source Robot Operating System*. IEEE International Conference on Robotics and Automation (ICRA) Workshop.
- White, R., Christensen, H., & Quigley, M. (2016). *Security Analysis of the Robot Operating System (ROS)*. IEEE International Conference on Robotics and Automation.
- Dieber, B., White, R., Taurer, S., & Christensen, H. (2017). *Penetration Testing ROS*. IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS).
- Dieber, B., White, R., & Christensen, H. (2017). *Secure ROS (SROS): Security Enhancements for ROS*. ROSCon Proceedings.
- Mitchell, R., Chen, I. R., & others (2019). *A Survey of Intrusion Detection Techniques for Cyber-Physical Systems*. ACM Computing Surveys.
- Park, J., Kim, H., & Lee, K. (2020). *Machine Learning-Based Intrusion Detection System for ROS Environments*. Journal of Robotics and Autonomous Systems.
- Shin, S., Lee, J., & Kim, D. (2021). *Deep Learning-Based Intrusion Detection for Robotic Systems*. IEEE Access.
- Giaretta, A., et al. (2022). *Hybrid Intrusion Detection Systems for Cyber-Physical and Robotic Systems*. Future Generation Computer Systems.
- Kwon, Y., Park, S., & Choi, J. (2023). *Unsupervised Anomaly Detection in ROS-Based Systems Using Lightweight Models*. Sensors Journal.
- Humayed, A., Lin, J., Li, F., & Luo, B. (2017). *Cyber-Physical Systems Security—A Survey*. IEEE Internet of Things Journal.