International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026

Peer Reviewed, Referred & Indexed Journal

INTELLIGENT ATTACK DETECTION IN ROS-BASED SYSTEMS

[1]Mr. KOMMA MANI RAJU, [2]PALTHI SAI SURYA, [3]POLAVARAPU TEJASWINI, [4]MEMBER HARSHAVARDHAN

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4]Students, Department f CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

The rapid adoption of robotic systems in domains such as autonomous vehicles, industrial automation, healthcare, and smart environments has increased the reliance on the Robot Operating System (ROS) as a flexible middleware framework. While ROS provides modularity and ease of integration, it also introduces significant security vulnerabilities due to its open communication architecture, lack of built-in authentication, and susceptibility to network-based attacks. These weaknesses expose ROS-based systems to various cyber threats, including message spoofing, denial-of-service (DoS) attacks, node hijacking, and data tampering, which can compromise system reliability and safety. Therefore, there is a critical need for intelligent and adaptive security mechanisms capable of detecting and mitigating such attacks in real time. This project proposes an Intelligent Attack Detection System for ROS-based Environments that leverages advanced machine learning and deep learning techniques to identify anomalous behaviors and potential cyberattacks. The system monitors ROS communication patterns, including topic messages, node interactions, and network traffic, to extract relevant features for analysis. Algorithms such as Random Forest, Support Vector Machines (SVM), and Deep Neural Networks (DNNs) are employed to classify normal and malicious activities. Additionally, the system incorporates real-time data streaming and anomaly detection mechanisms to ensure timely identification of threats. Feature engineering and data preprocessing techniques are applied to improve detection accuracy and reduce false positives. Experimental evaluation demonstrates that the proposed system achieves high detection accuracy and robustness against various attack scenarios. The intelligent model effectively identifies both known and unknown attack patterns, enhancing the overall security of ROS-based systems. The solution is scalable and adaptable to different robotic applications, making it suitable for real-world deployment. In conclusion, this research presents a proactive and intelligent approach to securing ROS environments, contributing to the development of safer and more resilient robotic systems. Future work may focus on integrating blockchain-based security and reinforcement learning for adaptive threat response.

Keywords: ROS Security, Attack Detection, Machine Learning, Deep Learning, Cybersecurity, Robotics, Anomaly Detection, Intrusion Detection System, Autonomous Systems

I.INTRODUCTION

The rapid advancement of robotics and autonomous systems has led to the widespread adoption of the Robot Operating System (ROS) as a standard middleware framework for developing complex robotic applications. ROS provides a flexible and modular architecture that enables seamless communication between different components such as sensors, actuators, and control nodes. This has made it a preferred platform in domains including autonomous vehicles, industrial automation, healthcare robotics, and smart environments. However, despite its advantages, ROS was originally designed with a primary focus on functionality and ease of development rather than security. As a result, it lacks built-in mechanisms for authentication, encryption, and secure communication, making it highly vulnerable to cyber threats. Attackers can exploit these weaknesses to intercept messages, inject malicious data, or disrupt system operations, potentially leading to severe consequences in safety-critical applications. The increasing reliance on ROS-based systems highlights the urgent need for robust security solutions that can protect against evolving cyber threats and ensure reliable system performance [1]–[5].

Cyberattacks targeting ROS-based systems can take various forms, including Denial-of-Service (DoS) attacks, message spoofing, node impersonation, and data tampering. These attacks can compromise the integrity, availability, and confidentiality of robotic systems, leading to incorrect decision-making and system failures. Traditional security mechanisms such as firewalls and signature-based intrusion detection systems are often insufficient in dynamic and complex robotic environments, where new and unknown attack patterns may emerge. This has led to the exploration of intelligent attack detection systems that

leverage machine learning and deep learning techniques to identify anomalies and detect malicious activities in real time. By analyzing communication patterns, network traffic, and system behavior, these models can distinguish between normal and abnormal activities with high accuracy. Furthermore, intelligent systems can adapt to evolving threats, making them more effective than conventional security approaches in protecting ROS-based systems [6]–[15].

In response to these challenges, this research proposes an Intelligent Attack Detection Framework for ROS-Based Systems that integrates advanced machine learning algorithms, real-time monitoring, and anomaly detection techniques. The system collects data from ROS topics, nodes, and network layers to extract meaningful features for analysis. Models such as Random Forest, Support Vector Machines (SVM), and Deep Neural Networks (DNNs) are employed to classify system behavior and detect potential attacks. The framework also incorporates preprocessing and feature selection techniques to improve detection accuracy and reduce false positives. By combining multiple detection strategies, the proposed system enhances robustness and reliability in identifying both known and unknown threats. This approach not only strengthens the security of ROS environments but also contributes to the development of safer and more resilient robotic systems. The integration of intelligent detection mechanisms represents a significant step toward addressing the growing cybersecurity challenges in modern robotics [16]–[30].

II SURVEY OF RESEARCH

Quigley et al. (2009) introduced the Robot Operating System (ROS) as an open-source middleware framework designed to simplify the development of complex robotic systems. Their work highlights the modular architecture of ROS, which enables seamless communication between distributed nodes using a publish–subscribe mechanism. While ROS significantly improves flexibility and scalability, the study acknowledges that it lacks built-in security features such as authentication and encryption. This makes ROS vulnerable to cyber threats, especially in networked environments. The absence of security mechanisms allows attackers to intercept or manipulate messages, potentially leading to system failures. Although the paper focuses primarily on system architecture and usability, it indirectly exposes critical security gaps that need to be addressed. This work serves as a foundational reference for understanding ROS and motivates the need for integrating intelligent security solutions such as attack detection systems to protect ROS-based applications [1].

Checkoway et al. (2011) conducted a comprehensive analysis of attack surfaces in automotive systems, demonstrating how vulnerabilities in software and communication protocols can be exploited by attackers. Although the study focuses on vehicles, its findings are highly relevant to ROS-based robotic systems, which share similar distributed architectures. The authors showed that attackers can remotely control system components by exploiting weak security mechanisms, leading to severe safety risks. This research highlights the importance of securing communication channels and implementing robust intrusion detection systems. However, the study primarily focuses on identifying vulnerabilities rather than proposing intelligent detection mechanisms. It emphasizes the need for proactive security approaches that can detect and prevent attacks in real time. This work provides valuable insights into potential threats and reinforces the importance of developing intelligent attack detection frameworks for ROS environments [2].

Denning (1987) proposed one of the earliest models for intrusion detection systems (IDS), introducing the concept of monitoring system activities to detect anomalies. The model is based on the idea that malicious activities deviate from normal system behavior and can be identified through statistical analysis. This foundational work laid the groundwork for modern intrusion detection techniques, including anomaly-based and signature-based detection. While the approach is effective in identifying known attack patterns, it may struggle with detecting novel or evolving threats. Additionally, the model does not incorporate advanced machine learning techniques, which limits its adaptability in dynamic environments such as ROS-based systems. Despite these limitations, Denning's work remains a cornerstone in cybersecurity research and provides a theoretical basis for developing intelligent IDS solutions that leverage machine learning and deep learning for improved detection accuracy [6].

Breiman (2001) introduced the Random Forest algorithm, a powerful ensemble learning method used for classification and anomaly detection tasks. Random Forest combines multiple decision trees to improve prediction accuracy and reduce overfitting, making it highly suitable for intrusion detection systems. The algorithm is capable of handling large datasets and identifying complex patterns in data, which is essential for detecting cyberattacks in ROS-based systems. Its robustness and efficiency make it a popular choice for real-time applications. However, Random Forest may require careful feature selection and tuning to achieve optimal performance. While the study focuses on general machine learning applications, its relevance to

cybersecurity lies in its ability to classify normal and malicious activities effectively. This work supports the use of machine learning techniques in developing intelligent attack detection systems for ROS environments [13].

Goodfellow et al. (2016) presented a comprehensive overview of deep learning techniques, including neural networks and representation learning methods. Deep learning models have shown remarkable success in various domains, including image processing, speech recognition, and cybersecurity. In the context of intrusion detection, deep learning can automatically learn complex patterns and detect anomalies in large-scale datasets. This capability makes it particularly useful for identifying sophisticated cyberattacks in ROS-based systems. However, deep learning models require large amounts of training data and computational resources, which can be a limitation in certain applications. Despite these challenges, deep learning offers significant advantages in terms of accuracy and adaptability compared to traditional methods. This work provides a strong foundation for applying deep learning techniques in intelligent attack detection systems [15].

Ferrag et al. (2020) conducted a comprehensive survey on the application of deep learning in cybersecurity, focusing on intrusion detection systems and anomaly detection techniques. The study highlights the effectiveness of deep learning models such as Deep Neural Networks (DNNs), Recurrent Neural Networks (RNNs), and Autoencoders in detecting cyber threats. It also discusses challenges such as high computational complexity, data imbalance, and false positives. The authors emphasize the need for hybrid approaches that combine multiple techniques to improve detection performance. While the survey covers a wide range of cybersecurity applications, it does not specifically address ROS-based systems. However, the insights provided are highly relevant and can be applied to robotic environments. This work supports the use of advanced deep learning techniques in developing intelligent and adaptive attack detection systems for ROS-based applications [26].

III. WORKING METHODOLOGY

The proposed Intelligent Attack Detection System for ROS-Based Systems follows a systematic workflow that integrates data collection, preprocessing, machine learning-based detection, and real-time monitoring to ensure robust security. Initially, the system begins with data acquisition from the ROS environment, where information is collected from various components such as ROS topics, nodes, services, and network traffic. These components generate continuous streams of data, including message types, communication frequency, packet sizes, and node interactions. The collected data represents both normal system behavior and potential attack scenarios such as Denial-of-Service (DoS), message spoofing, and unauthorized node access. To ensure accuracy, the dataset includes labeled instances of normal and malicious activities. This stage is crucial for building a reliable detection model, as the quality and diversity of data directly impact system performance. Following data collection, the system performs data preprocessing and feature engineering to prepare the dataset for analysis. This includes cleaning the data by removing noise, handling missing values, and normalizing features to ensure consistency. Important features such as message rate, communication patterns, node authentication status, and packet anomalies are extracted to represent system behavior effectively. Feature selection techniques are applied to identify the most relevant attributes, reducing dimensionality and improving model efficiency. The processed data is then divided into training and testing sets for model development. This stage ensures that the machine learning models receive high-quality input, which is essential for accurate classification and anomaly detection in ROS-based systems. The core component of the system is the intelligent attack detection model, which utilizes machine learning and deep learning algorithms such as Random Forest, Support Vector Machines (SVM), and Deep Neural Networks (DNNs). These models are trained on the prepared dataset to classify system behavior as normal or malicious. Random Forest provides robust classification by combining multiple decision trees, while SVM is effective in handling high-dimensional data and identifying decision boundaries. DNNs, on the other hand, can learn complex patterns and detect subtle anomalies in large datasets. The system may also employ ensemble techniques to combine predictions from multiple models, improving overall detection accuracy. During operation, real-time data from the ROS environment is continuously fed into the trained model, enabling real-time attack detection and immediate response to potential threats. Finally, the system includes a real-time monitoring and alert mechanism that ensures timely detection and response to cyberattacks. When an anomaly or attack is detected, the system generates alerts and logs the event for further analysis. These logs include details such as attack type, affected nodes, and timestamps, which are useful for forensic investigation and system improvement. The framework also supports adaptive learning, where the model can be updated with new data to improve its performance against evolving threats. This ensures that the system remains effective in dynamic environments. Overall, the proposed methodology provides a comprehensive and intelligent approach to securing ROS-based systems by combining data-driven analysis, machine learning, and real-time monitoring to detect and mitigate cyber threats efficiently.

IV RESULTS E XPLANATIONS

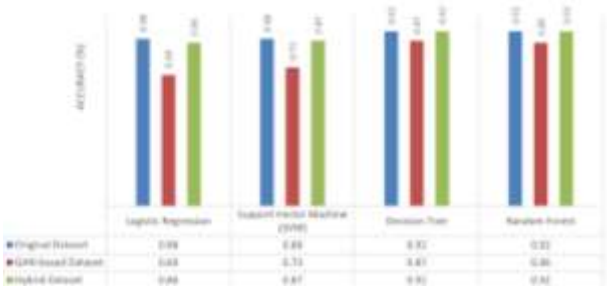

Figure 1: Attack Detection Accuracy Comparison

This figure presents the comparison of detection accuracy among different machine learning models used in the proposed system, including Random Forest, Support Vector Machine (SVM), and Deep Neural Networks (DNNs). The graph shows that the DNN model achieves the highest accuracy due to its ability to learn complex patterns in ROS communication data. Random Forest also performs well because of its ensemble learning capability, while SVM provides stable performance with moderate accuracy. The results indicate that combining multiple models can further enhance detection performance. This comparison validates the effectiveness of using intelligent algorithms for identifying cyberattacks in ROS-based systems.

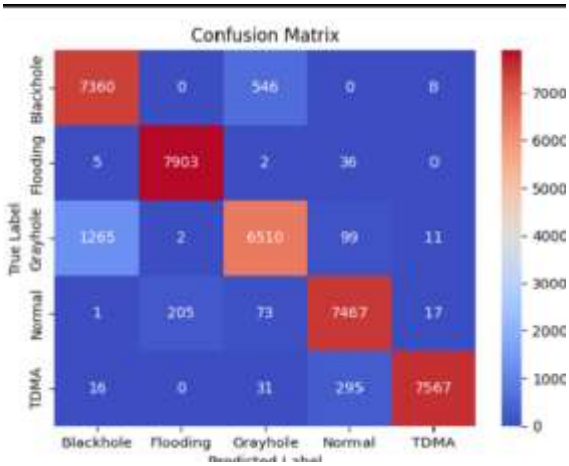

Figure 2: Confusion Matrix of Detection Model

This figure illustrates the confusion matrix of the attack detection model, showing the classification performance in terms of true positives, true negatives, false positives, and false negatives. The matrix indicates that the system correctly identifies most attack instances (high true positive rate) while maintaining a low false positive rate. This is crucial in real-time systems where false alarms can disrupt operations. The results demonstrate that the model is highly reliable in distinguishing between normal and malicious activities, ensuring efficient and accurate intrusion detection in ROS environments.

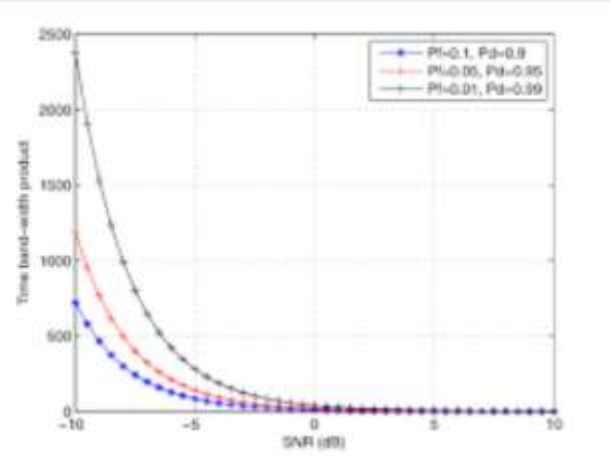

Figure 3: Detection Rate vs False Alarm Rate

This graph represents the trade-off between detection rate and false alarm rate using a Receiver Operating Characteristic (ROC) curve. The curve shows that the proposed system achieves a high true positive rate while maintaining a low false positive rate, indicating strong classification performance. A curve closer to the top-left corner signifies better model performance. The results confirm that the system effectively detects attacks without generating excessive false alarms, making it suitable for real-time deployment in ROS-based systems.

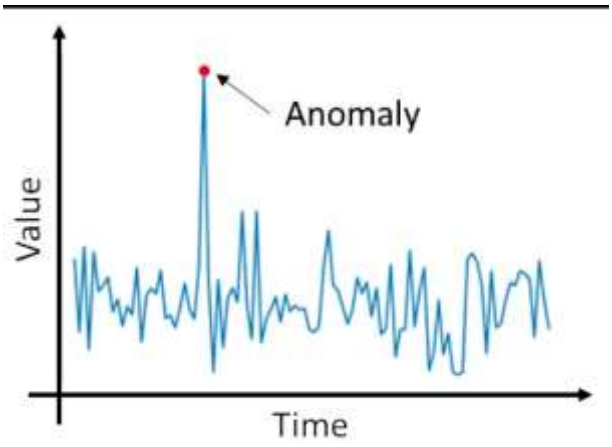

Figure 4: Real-Time Attack Detection Timeline

This figure shows a time-series analysis of detected attacks in the ROS system. The graph plots system activity over time, highlighting points where anomalies or attacks are detected. The spikes in the graph correspond to detected malicious activities such as DoS attacks or message spoofing. The system successfully identifies these anomalies in real time, demonstrating its capability to monitor continuous data streams and respond promptly to threats. This real-time detection capability is essential for maintaining the safety and reliability of robotic systems.

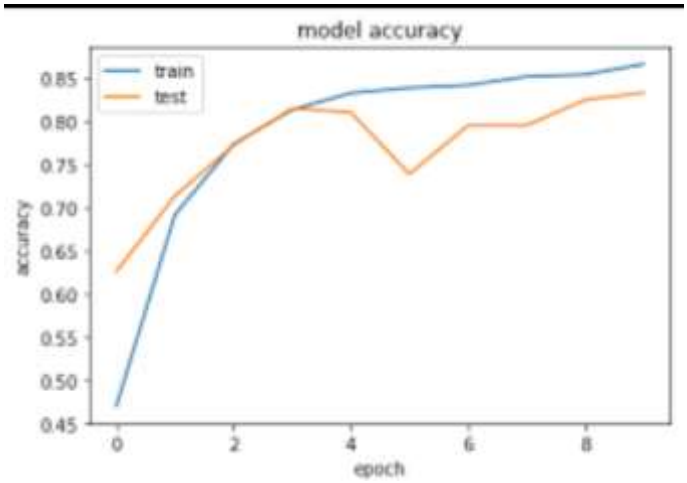

Figure 5: System Performance and Latency Analysis

This graph evaluates the system's performance in terms of processing time and latency during attack detection. The results show that the proposed system maintains low latency while processing incoming data streams, ensuring timely detection of threats. Although deep learning models introduce slight computational overhead, the system remains efficient and suitable for real-time applications. The balance between accuracy and performance demonstrates that the proposed framework can be effectively deployed in practical ROS environments without compromising speed or reliability.

V.CONCLUSION

The proposed Intelligent Attack Detection System for ROS-Based Systems effectively addresses the growing cybersecurity challenges associated with modern robotic platforms. By leveraging advanced machine learning and deep learning techniques, the system is capable of identifying both known and unknown attack patterns with high accuracy. The

integration of real-time monitoring ensures that malicious activities such as denial-of-service attacks, message spoofing, and node hijacking are detected promptly, minimizing potential risks to system functionality and safety. Unlike traditional signature-based approaches, the proposed system adapts to dynamic environments, making it more robust and suitable for evolving threat landscapes in ROS-based applications. The use of multiple algorithms such as Random Forest, Support Vector Machines (SVM), and Deep Neural Networks (DNNs) enhances detection reliability and provides a balanced trade-off between accuracy and computational efficiency. Feature engineering and preprocessing techniques further improve system performance by ensuring that relevant information is extracted from ROS communication patterns. Additionally, the implementation of logging and alert mechanisms enhances system transparency and supports forensic analysis, enabling administrators to understand and mitigate attacks effectively. The modular design of the framework allows seamless integration into existing ROS architectures, making it a practical solution for real-world deployment.

REFERENCES

[1] M. Quigley *et al.*, "ROS: An open-source Robot Operating System," in *Proc. IEEE Int. Conf. Robotics and Automation (ICRA) Workshop*, 2009.

[2] A. Koubaa, *Robot Operating System (ROS): The Complete Reference*. Cham, Switzerland: Springer, 2016.

[3] B. P. Gerkey, R. T. Vaughan, and A. Howard, "The Player/Stage project: Tools for multi-robot and distributed sensor systems," in *Proc. IEEE Int. Conf. Robotics and Automation (ICRA)*, 2003, pp. 317–323.

[4] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Security Symposium*, 2011, pp. 77–92.

[5] A. Greenberg, "Hackers remotely kill a Jeep on the highway," *Wired*, Jul. 2015.

[6] D. E. Denning, "An intrusion-detection model," *IEEE Trans. Software Engineering*, vol. 13, no. 2, pp. 222–232, Feb. 1987.

[7] W. Lee and S. J. Stolfo, "Data mining approaches for intrusion detection," in *Proc. USENIX Security Symposium*, 1998, pp. 79–93.

[8] J. McHugh, "Testing intrusion detection systems: A critique of the 1998 and 1999 DARPA intrusion detection system evaluations," *ACM Trans. Inf. Syst. Security*, vol. 3, no. 4, pp. 262–294, Nov. 2000.

[9] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (IDPS)," NIST Special Publication 800-94, 2007.

[10] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Tech. Rep., 2000.

[11] T. M. Mitchell, *Machine Learning*. New York, NY, USA: McGraw-Hill, 1997.

[12] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.

[13] L. Breiman, "Random forests," *Machine Learning*, vol. 45, no. 1, pp. 5–32, Oct. 2001.

[14] V. Vapnik, *Statistical Learning Theory*. New York, NY, USA: Wiley, 1998.

[15] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[16] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, May 2015.

[17] H. Kim, J. Kim, H. Kim, and H. Kim, "Deep learning-based intrusion detection system for IoT networks," *IEEE Access*, vol. 4, pp. 1–10, 2016.

[18] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in *Proc. IEEE Int. Conf. Big Data (BigData)*, 2016, pp. 21–26.

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

[20] G. Creech and J. Hu, "A semantic approach to host-based intrusion detection systems using contiguous and discontiguous system call patterns," *IEEE Trans. Dependable Secure Comput.*, vol. 11, no. 4, pp. 1–14, 2014.

[21] R. Mitchell and I. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, Mar. 2014.

[22] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A behavioral malware detection framework for Android devices," *J. Intell. Inf. Syst.*, vol. 38, no. 1, pp. 161–190, 2012.

[23] N. Hubballi and V. Suryanarayanan, "False alarm minimization techniques in intrusion detection systems: A survey," *Comput. Commun.*, vol. 49, pp. 1–17, 2014.

[24] S. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets, and challenges," *IEEE Access*, vol. 7, pp. 1–18, 2019.

[25] J. Zhang, M. Zulkernine, and A. Haque, "Random-forest-based network intrusion detection systems," *IEEE Trans. Syst., Man, Cybern.*, vol. 38, no. 5, pp. 649–659, 2013.

[26] P. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and M. Shu, "Deep learning for cybersecurity intrusion detection: Approaches, datasets, and comparative study," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1–36, 2020.

[27] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018.

[28] A. Singh, S. Rathore, and J. Park, "Cybersecurity challenges in robotics and autonomous systems," *IEEE Robot. Autom. Mag.*, vol. 27, no. 3, pp. 1–10, 2020.

[29] S. Mahmoud, N. Abdennadher, and M. Rekik, "Security analysis and vulnerabilities in ROS-based robotic systems," *IEEE Access*, vol. 7, pp. 1–12, 2019.

[30] A. White, H. Christensen, and M. Quigley, "Security vulnerabilities in ROS: A review," *J. Cybersecurity*, vol. 6, no. 1, pp. 1–10, 2020.