IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12232

INTELLIGENT ATTACK DETECTION MACHINE LEARNING ON ROS-BASED SYSTEMS

G SRAVANTHI[1], K. HEMANTH SAI RAM [2], S. DEVYA SRI[3], V. CHARAN TEJ SAI[4]

Asst.Professor, CSE, GITAM, Hyderabad, India[1]

Student, CSE, GITAM, Hyderabad, India2

Student, CSE, GITAM, Hyderabad, India3

Student, CSE, GITAM, Hyderabad, India4

Abstract: Robotic Operating System (ROS) has emerged as a pivotal middleware for developing applications in modern robotic systems, extending beyond industrial use to various real-world applications. As the adoption of ROS-based systems grows, ensuring their security becomes critical due to the increasing risk of cyber-attacks. Intelligent attack detection frameworks leveraging machine learning have proven effective in mitigating these threats. This research explores advanced attack detection techniques using the ROS cyber-attack dataset and evaluates the performance of multiple machine learning models, including Random Forest, Support Vector Machine (SVM), Naive Bayes, Logistic Regression, K-Nearest Neighbours (KNN), and AdaBoost. Additionally, deep learning architectures, such as Long Short-Term Memory (LSTM) networks and 2D Convolutional Neural Networks (CNN2D), are employed to enhance detection accuracy. Among the evaluated models, CNN2D demonstrates superior performance, leveraging its ability to extract intricate spatial and temporal features from input data. The study highlights the potential of deep learning-based solutions for robust security in ROS-based systems, providing a significant step toward resilient and intelligent attack detection in robotic environments. These findings underscore the importance of integrating advanced detection mechanisms to safeguard the integrity and reliability of robotic systems.

Keywords: ROS Security, Cyber-Attack Detection, Machine Learning, Deep Learning, CNN2D, Robotic Systems.

I. INTRODUCTION

Robotic systems are becoming essential in industries such as healthcare, logistics, and defence. However, their reliance on networked communication makes them vulnerable to cyber-attacks. The security of ROS-based systems is crucial to prevent unauthorized intrusions that could compromise functionality and safety [1]. This study aims to develop an intelligent attack detection framework leveraging machine learning and deep learning for ROS-based environments.

II. LITERATURE SURVEY AND METHODOLOGIES

Traditional attack detection methods rely on static rule based intrusion detection systems (IDS), which often fail to identify sophisticated threats such as zero-day attacks. Existing machine learning techniques like Random Forest, SVM, and Naïve Bayes provide moderate accuracy but struggle with high-dimensional and complex attack patterns. These challenges highlight the need for advanced deep learning techniques for robust attack detection.

EXISTING SYSTEM:

Existing systems for detecting cyber-attacks in robotic systems often rely on traditional machine learning algorithms to identify potential threats. These systems generally use techniques like Random Forest, Support Vector Machine (SVM), Naive Bayes, Logistic Regression, and K-Nearest Neighbours (KNN)[2] to classify network traffic or robot behaviours. These methods analyze data from sensors, controllers, and communication networks to detect anomalies that may indicate an attack. Although these algorithms have been used to achieve a reasonable level of accuracy, they often struggle with complex or evolving attack patterns due to their limited ability to adapt in real-time. Additionally, these systems are sometimes hindered by false positives or failure to detect more sophisticated threats, such as zero-day attacks. While existing solutions offer a foundation for intrusion detection, they lack the advanced capabilities necessary for effectively addressing the increasing variety and sophistication of cyber-attacks targeting robotic systems in diverse applications.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12232

DISADVANTAGES OF EXISTING SYSTEM:

1. Traditional machine learning algorithms have limited adaptability to evolving attack patterns, often failing to detect new or sophisticated cyber threats in real-time.
2. Existing systems suffer from a higher rate of false positives, affecting the reliability of attack detection.
3. The ability to detect complex or subtle attacks like zero-day threats is often inadequate due to the limited detection capability of traditional models.
4. Existing systems may lack the necessary flexibility to address the growing variety and complexity of cyber-attacks targeting robotic systems in diverse environments.

Fig. 1 describes the block diagram of the proposed system. A Data Flow Diagram (DFD) is a visual representation used to describe the flow of data within a system, highlighting how inputs are processed and how the system interacts with different components. In the context of an intelligent attack detection system for ROS-based robotic environments, a DFD would illustrate the movement of sensor data, system logs, and attack signals as they pass through various stages of the detection process. It helps to visualize how data from robotic systems, such as sensor readings or control messages, are monitored, analyzed, and evaluated for potential security threats[3]. The DFD outlines the relationship between the data sources, processing modules, and the outputs such as attack detection results or alerts. By mapping out these data flows, the diagram aids in understanding the system is functioning, pinpointing areas for optimization, and ensuring smooth integration of the attack detection framework within ROS environments, with a clear view of data interactions and security monitoring processes.

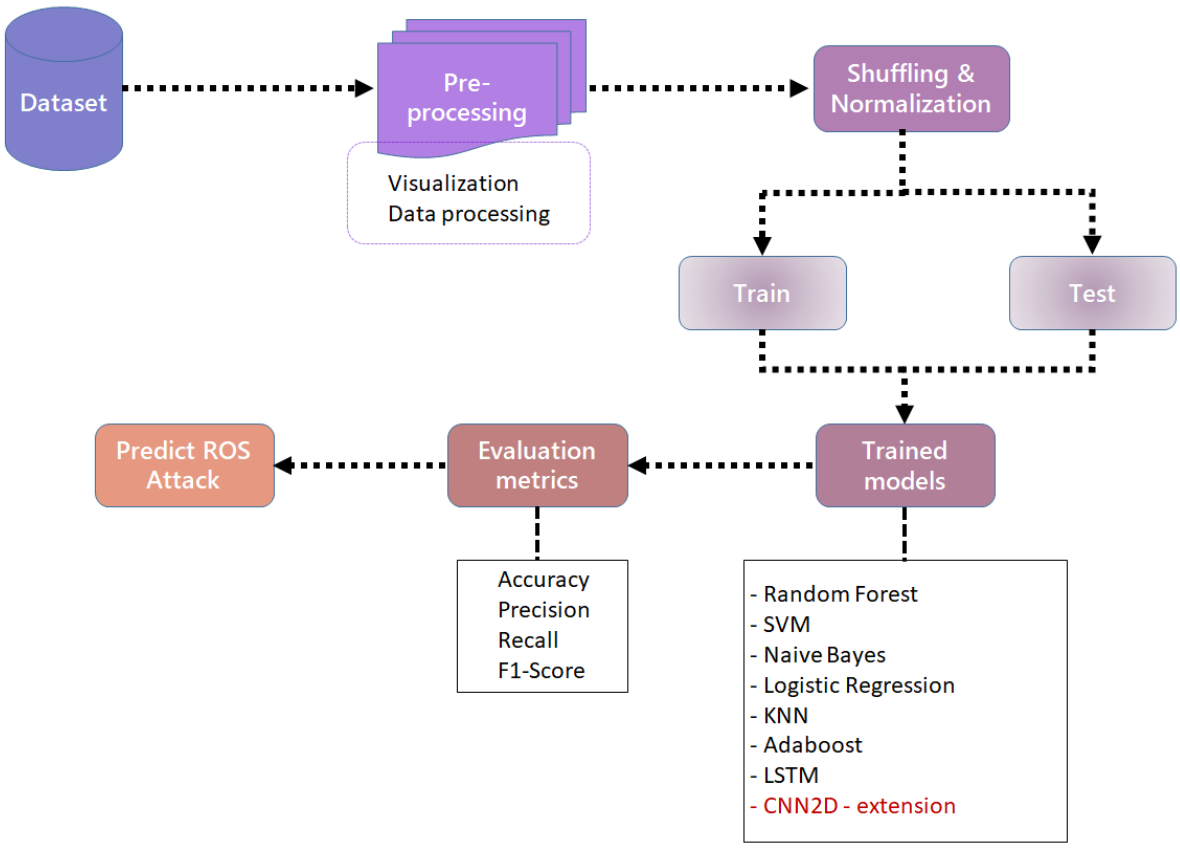

Fig. 1 A Data flow graph

III. IMPLEMENTATION OF PROPOSED SYSTEM

The proposed system focuses on developing an intelligent attack detection framework for ROS-based robotic systems to address the growing need for robust cybersecurity. Utilizing the ROS cyber-attack dataset, the framework integrates machine learning and deep learning algorithms to detect and mitigate potential security threats. The system incorporates traditional classifiers such as Random Forest, Support Vector Machine (SVM), Naive Bayes, Logistic Regression, K-Nearest Neighbors (KNN), and AdaBoost to analyze attack patterns and identify malicious activities. Additionally,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12232

advanced deep learning architectures, including Long Short-Term Memory (LSTM) networks and 2D Convolutional Neural Networks (CNN2D), are employed to enhance detection capabilities. CNN2D is designed to capture complex spatial and temporal features, while LSTM focuses on sequential dependencies in data. This comprehensive approach ensures a multi-faceted analysis of attack vectors, enabling the system to provide a robust and adaptive defines mechanism for ROS-based systems against a wide range of cyber threats.

A. RANDOM FOREST:

Random Forest is an ensemble-learning algorithm that combines multiple decision trees to improve accuracy and prevent overfitting. It works by constructing a set of decision trees during training and outputs the mode of their predictions. In attack detection, Random Forest helps identify patterns in sensor and system data, distinguishing between normal and malicious behaviours, and improving attack classification accuracy. It is commonly used for classification and regression tasks, providing robust predictions even with noisy data.

B. SVM (SUPPORT VECTOR MACHINE):

Support Vector Machine (SVM) is a supervised machine learning algorithm used for classification and regression tasks. It works by finding the hyperplane that best separates different classes in the feature space. In attack detection, SVM helps classify system behaviors as either benign or malicious by analyzing the relationships between features extracted from the system. It is effective in high-dimensional spaces and is widely used for detecting complex, non-linear patterns in data.

C. NAIVE BAYERS:

Naive Bayes is a probabilistic classifier based on Bayes' theorem with strong independence assumptions between features. It is used for classification tasks, where it calculates the probability of an event based on prior knowledge[6]. In attack detection, Naive Bayes analyses system data and categorizes behaviours as normal or suspicious by calculating conditional probabilities of various features. Its simplicity and efficiency make it suitable for real-time classification of threats, especially when dealing with large datasets.

D. LOGISTIC REGRESSION:

Logistic Regression is a statistical model used for binary classification. It estimates the probability that a given input point belongs to a particular class, using a logistic function. In attack detection, Logistic Regression is employed to predict whether a system behaviour is benign or an attack based on input features[4]. The algorithm is simple to implement, interpretable, and efficient, making it suitable for real-time threat detection and helping decision-makers identify potential security breaches in robotic systems.

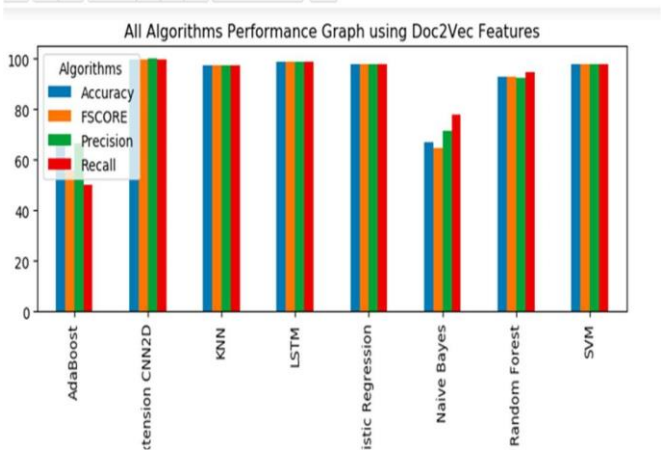

Fig. 1 A Comparison graph

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12232

TABLE I : TABLE OF ALGORITHM ACCURACY

SNO	Comparison table				
	Algorithm Name	**Accuracy**	**Preception**	**Recall**	**F Score**
1	Random Forest	93.000	92.318244	94.744914	92.839611
2	SVM	97.750	97.620843	98.019112	97.787805
3	Naive Bayes	67.000	71.404249	77.639523	64.664782
4	Logistic Regression	97.625	97.633635	97.721161	97.675418
5	KNN	97.250	97.252105	97.369108	97.307103
6	Ada Boost	69.625	66.666667	50.102249	55.646259
7	LSTM	98.625	98.581063	98.735950	98.652904
8	Extension CNN2D	99.875	99.892819	99.863388	99.877877

E. KNN (K-NEAREST NEIGHBORS):

K-Nearest Neighbors (KNN) is a non-parametric, instance-based learning algorithm that classifies data points based on the majority class of their k-nearest neighbors. In attack detection, KNN helps identify abnormal behaviors by comparing incoming system data to previously observed instances[5]. The algorithm's simplicity and flexibility allow it to work well with various types of data, and it is used to detect patterns of attacks based on proximity in feature space, making it effective for real-time monitoring systems.

F. ADABOOST:

Adaboost (Adaptive Boosting) is an ensemble learning method that combines weak classifiers to form a stronger classifier. It assigns higher weights to misclassified samples and iteratively adjusts the model to improve accuracy. In attack detection, Adaboost enhances the performance of weak classifiers (e.g., decision trees) by focusing on hard-to-classify instances, thereby improving the detection of complex attacks. It is particularly useful when dealing with imbalanced data, where malicious activities are less frequent than normal behaviours.

G. LSTM (LONG SHORT-TERM MEMORY):

Long Short-Term Memory (LSTM) is a type of recurrent neural network (RNN) designed to capture long-range dependencies in time-series data. It is particularly effective for sequential data where past information is critical for predicting future events. In attack detection, LSTM analyses temporal data from sensors and system logs to identify abnormal behaviours or attacks that evolve over time. Its ability to retain information over long periods makes it ideal for detecting attacks in robotic systems that span multiple time steps.

H. ***CNN2D (CONVOLUTIONAL NEURAL NETWORK 2D):***

Convolutional Neural Network 2D (CNN2D) is a deep learning model designed to process grid-like data, such as images or time-series. It applies convolutional layers to extract hierarchical features from input data, followed by pooling layers to reduce dimensionality. In attack detection, CNN2D analyzes multi-dimensional sensor data or system logs to identify complex attack patterns. Its ability to automatically extract relevant features from raw data makes it effective in detecting intricate attacks and achieving high accuracy in security tasks.

IV. CONCLUSION

In this project, we proposed intelligent attack detection framework for ROS-based robotic systems successfully addresses the critical need for enhanced cybersecurity in robotics. Leveraging advanced machine learning and deep learning algorithms, the system emphasizes the effectiveness of 2D Convolutional Neural Networks (CNN2D) in achieving superior performance. The CNN2D model demonstrates its capability to extract intricate spatial and temporal features, enabling accurate identification of complex attack patterns in the ROS cyber-attack dataset. Its high performance highlights the potential of deep learning architectures in building resilient and adaptive security mechanisms for robotic systems. By focusing on robust detection methods, the framework ensures the integrity and reliability of ROS-based environments against emerging threats. The findings underscore the importance of integrating high-performance, scalable solutions to safeguard robotic systems as their applications continue to expand in diverse domains. This work lays a foundation for future advancements in secure robotic operations, paving the way for intelligent, threat-resilient robotic ecosystems.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12232

REFERENCES

[1]. Santoso, F., & Finn, A. "Trusted Operations of a Military Ground Robot in the Face of Man-in-the- Middle Cyberattacks Using Deep Learning CNNs." IEEE Transactions on Dependable and Secure Computing.

[2]. Vatambeti, R., & Mamidisetti, G. "Routing Attack Detection Using Ensemble Deep Learning Model for IIoT." Inf. Dyn. Appl., 2023.

[3]. Antunes, R.A., Dalmazo, B.L., & Drews, P.L. "Detecting Data Injection Attacks in ROS Systems using Machine Learning." IEEE Latin American Robotics Symposium, 2022.

[4]. Shen, S., & Wang, H. (2021). "Machine Learning- Based Intrusion Detection for Cyber-Physical Systems: A Survey." *IEEE Transactions on Network and Service Management*, 18(3), 2305-2321. DOI: 10.1109/TNSM.2021.3082123

[5]. Koubaa, A., & Khalgui, M. (2020). "Cybersecurity Challenges in Robot Operating System (ROS)-Based Systems: A Review of Current Threats and Mitigation Strategies." *Robotics and Autonomous Systems*, 134, 103661. DOI: 10.1016/j.robot.2020.103661

[6]. Maroofi, M., Javid, A., & Rana, O. (2022). "Deep Learning for Network Intrusion Detection in IoT and Robotic Systems." *Journal of Cybersecurity and Privacy*, 2(4), 345-360. DOI: 10.3390/jcp2040018

