SCIENTIFIC CULTURE
www.sci-cult.com

*SCIENTIFIC CULTURE, Vol. 12, No. 4, (2026), pp. 8135-8143*
*Open Access. Online & Print*

**DOI: 10.5281/zenodo.12426808**

# ROBUST ROBOTIC NAVIGATION UNDER CYBER THREATS: ADAPTIVE SECURITY AND DECISION-MAKING PERSPECTIVES

**Venkata Sai Rahul Trivedi Kothapalli[1], Avinash Kumar[2]*, Tanmayee Prakash Tilekar[3]**

*[2]Computer Science & Engineering (CSE), Sharda School of Computing Science & Engineering, Greater Noida, Uttar Pradesh, India*
*[3]Computer Science and Engineering, I.T.S Engineering College, Greater Noida, Uttar Pradesh, India*

*Received:* **15/11/2025**
*Accepted:* **13/04/2026**

*Corresponding Author: Avinash Kumar (avinashkr338@gmail.com)*

## ABSTRACT

***The vulnerability to cybercrime is now an easy target of the use of autonomous robots in navigation as their functioning is based on the networks of sensors and communication channels. The study entails an adaptable and dynamic security empowered route framework that joins machine learning-driven intrusion identification, reinforcement learning-driven choice, and multi-sense integration to arrive at a more solid system robustness. It is tested in the framework of simulation environments and under various cyber-attack conditions, such as GPS spoofing, denial of service and data injection attacks. The findings show that it has better navigation accuracy (96.8% under normal conditions and 92.3% under attack) and high detection rate (94.5%), lower response time and latency. The comparative analysis proves that the proposed model is more effective than traditional and ML-based models, in terms of security and efficiency. It focuses on the successful implementation of adaptive security together with intelligent navigation to achieve a dependable operation in a hostile environment and how it can be extended to such intractable domains as healthcare, protection and autonomous transport.***

**KEYWORDS** Cardiopulmonary resuscitation, Intrusion Detection, Autonomous Robotics, Cybersecurity, Robotic Navigation, Sensor Fusion, Cyber-Physical Systems, Reinforcement Learning.

## 1 INTRODUCTION

In many applications such as automation in industries, medicine, military and intelligent transportation systems, and enabling robots to operate in a complex and dynamic environment without supervision, robot autonomy has become a revolution. These systems are based on the use of advanced sensing technologies, such as LiDAR, cameras, inertial measurement units (IMUs), and GPS in combination with complex algorithms of localization, mapping, and path planning. Some of the technologies that have significantly enhanced the perceptions of robots and their real-time decision-making with a high degree of accuracy and efficiency are the Simultaneous Localization and Mapping (SLAM), machine learning, and reinforcement learning. Nonetheless, with the increasing interconnection of the robotic systems via wireless communication networks and cloud-based systems, they are becoming susceptible to a greater scope of cyber threats that can undermine their integrity in operation. All such attacks are GPS spoofing, sensor data manipulation, denial-of-service (DoS) and adversarial machine learning attacks, which have an impact on the cyber threat environment in robotic systems, and can destabilize perception, decision-making, and control systems. These threats are particularly critical in safety sensitive systems such as autonomous vehicles and medical robotics where any misbehaved behavior can lead to tragic consequences, such as system failure, safety issues, and financial losses. Although robotic navigation and cybersecurity have evolved greatly, the current systems usually regard navigation and security as two distinct entities, making them vulnerable to attacks by criminals. The classical navigation algorithms are more aimed at optimization of performance and lack real-time threat awareness and adaptive security. This poses a critical gap in the provision of reliable and secure operation in adversarial conditions. Thus, there is a high necessity to establish powerful navigation systems that are able to not only work effectively under regular circumstances but also identify, adapt and mitigate cyber threats on-the-fly. The rationale behind this research is to ensure that such challenges are overcome by incorporating adaptive security mechanisms and intelligent decision making models in order to improve the resilience, safety and trustworthiness of autonomous robotic systems in cyber-physical environment.

### 1.2 Research Objectives

To develop an adaptive and secure robotic navigation framework that integrates artificial intelligence–based intrusion detection with intelligent decision-making for real-time threat mitigation.

To evaluate the impact of cyber threats on navigation performance and enhance system robustness by optimizing accuracy, detection capability, and response efficiency under adversarial conditions.

## 2. LITERATURE REVIEW AND RESEARCH GAP

Smith et al. (2021) discussed the main principles of autonomous robots navigation by highlighting sensor fusion and real-time decision-making structures and explaining how the combination of the LiDAR, vision systems, and inertial measurement units greatly improve the accuracy of localization and mapping in dynamic settings and how the traditional navigation models are limited to deal with uncertainty and unforeseen environmental disruptions. Kumar et al. (2022) examined the problem of cybersecurity vulnerabilities in robotic systems, highlighting such key threats as GPS spoofing, denial-of-service attacks, and sensor data manipulation, and showing that these attacks can drastically affect the accuracy of navigation and the reliability of the system, especially in interconnected systems such as autonomous vehicles and industrial robotics. Zhang et al. (2021) added to the body of knowledge by suggesting machine learning-based intrusion detection systems designed to work in a cyber-physical robotic setting by demonstrating that machine learning algorithms, including Random Forest and Support Vector Machines, are efficient in identifying anomalies in communication and sensor data streams to improve system resilience against cyber attackers. Ahmed et al. (2023) also contributed to this field, combining deep learning models, in particular, Long Short-Term Memory networks, to identify temporal anomaly in the robotic tasks, which is also shown to be able to recognize the sequence of attack patterns and enhance their detection rates in more and more intricate and dynamic cyber threat situations. Singh et al. (2022) concentrated on reinforcement learning-based navigation strategies, showing that adaptive learning algorithms can be used to help robots make intelligent and context-sensitive decisions in uncertain and adversarial environments, and make dynamic path adjustments in response to environmental changes and threats perceived, though the challenges associated with the complexity of training and convergence remain. Li et al. (2023) proposed a hybrid system that uses blockchain and robotic navigation to guarantee safe communication and information integrity among distributed robotic agents, highlighting the importance of decentralized trusts as

a way to avoid unauthorized access to and manipulation of data, and discusses the issue of scalability and latency in practice. The concept of robust navigation was extended by Garcia et al. (2022) to risk-aware decision-making models founded on probabilistic and game-theoretic decision-making, allowing systems to assess and address cyber threats more efficiently and operational safety in such critical areas as healthcare and defence robotics. The summaries of these studies, as presented in Table 1, strongly suggest that although there have been substantial improvements in both the area of navigation and cybersecurity, the current solutions tend to focus on these areas separately, which ends up creating systems that are not real-time adaptable and do not offer integrated threat mitigation measures.

*Table 1: Comparative Analysis of Existing Secure Navigation Approaches*

| Author (Year) | Approach / Model | Techniques Used | Strengths | Limitations | Research Gap Identified |
|---|---|---|---|---|---|
| Smith et al. (2020) | Conventional Navigation (SLAM, A*) | SLAM, Path Planning Algorithms | High accuracy in structured environments | Poor performance in dynamic/adversarial settings | Lack of security integration |
| Kumar et al. (2021) | Cybersecurity Analysis in Robotics | Threat Modeling, Risk Analysis | Identifies key vulnerabilities | No real-time mitigation strategies | Absence of adaptive defense mechanisms |
| Zhang et al. (2022) | ML-based Intrusion Detection | Random Forest, SVM | Improved anomaly detection | Limited scalability and real-time response | Weak integration with navigation systems |
| Ahmed et al. (2023) | Deep Learning Security Model | LSTM, Neural Networks | High detection accuracy for sequential attacks | High computational cost and latency | Not suitable for real-time navigation |
| Singh et al. (2022) | Reinforcement Learning Navigation | RL (Q-learning, Deep RL) | Adaptive decision-making capability | Requires large training data, convergence issues | Lack of integrated cybersecurity features |
| Li et al. (2023) | Blockchain-based Secure Navigation | Blockchain, Smart Contracts | Data integrity and decentralized security | High latency and computational overhead | Scalability challenges in real-world systems |
| Garcia et al. (2021) | Risk-aware Navigation Framework | Probabilistic Models, Game Theory | Improved threat-aware decision-making | Limited practical implementation | Lack of real-time adaptive learning |

## 3. RESEARCH METHODOLOGY

### 3.1 Research Design

The research project is based on a quantitative and experimental research design to test the effectiveness of a secure robotic navigation system in the presence of cyber-threats. It is also performed with the help of simulation validation running on platforms like ROS, Gazebo and CARLA to simulate the real world in terms of navigation. The proposed framework is compared with the existing models of navigation to evaluate the gains in terms of security, accuracy and robustness.

### 3.2 System Framework Development

The system is a proposed adaptive security-enabled navigation architecture that incorporates artificial intelligence and intelligent decisions. It integrates both machine learning-based intrusion detection system to detect cyber threats and anomalies in real time, and reinforcement learning algorithms to be able to make dynamic and adaptable decisions during navigation. To achieve reliable data, better perception, and high environmental awareness, sensor fusion methods are used to integrate LiDAR, IMU, and camera inputs to ensure reliable data, a better perception, and more awareness of the environment to achieve strong navigation.

### 3.3 Data Collection

This study samples secondary data like the KITTI and CARLA datasets and also artificial cyber-attack scenarios such as GPS spoofing, denial-of-service (DoS) and data injection attacks. Moreover, LiDAR, IMU, and camera sensor data in real-time is used to create realistic navigation conditions. Table 2 provides a systematic description of the characteristics of the dataset, sensor types, and attack settings and provides a full picture of the sources of data used in the study.

*Table 2: Dataset Description and Attack Scenario Configuration*

| Dataset / Source | Data Type | Description | Attack Scenario Included | Purpose in Study | Reference |
|---|---|---|---|---|---|
| KITTI Dataset | Image, LiDAR, GPS | Real-world autonomous driving dataset with multi-sensor data for perception and localization | No (baseline dataset) | Model training and validation | Geiger et al., 2013 |
| CARLA Simulator | Synthetic sensor data | Open-source simulator for autonomous driving with realistic urban scenarios | Yes (custom attack injection) | Simulation of navigation under cyber threats | Dosovitskiy et al., 2017 |
| ROS-Gazebo | Real-time | Robotics simulation platform for | Yes (DoS, data | System testing and | Koenig & |

| | | | | | |
|---|---|---|---|---|---|
| Environment | simulation data | testing algorithms in controlled environments | manipulation) | experimental validation | Howard, 2004 |
| LiDAR Sensor Data | Point cloud data | Provides 3D environmental mapping and obstacle detection | Yes (noise injection, spoofing) | Environment perception and mapping | Shan & Englot, 2018 |
| IMU Data | Motion and orientation data | Measures acceleration and rotational movement for localization | Yes (signal disturbance) | Stability and motion tracking | Woodman, 2007 |
| Camera Data | Image/Video | Visual perception for object detection and navigation tasks | Yes (adversarial image attacks) | Visual navigation and recognition | Krizhevsky et al., 2012 |
| Synthetic Attack Data | Modified sensor & network data | Artificially generated attack scenarios including GPS spoofing and DoS | Yes (all major attack types) | Robustness testing and intrusion detection | Petit & Shladover, 2015 |

**3.4 Algorithms and Experimental Method.**

There are several steps in the experimental process, such as preprocessing data and feature extraction to ready the input data to be analyzed. Other machine learning models like the Random Forest and Long Short-Term Memory (LSTM) are used in intrusion detection because they are effective to detect both the static and the temporal anomalies. The reinforcement learning is applied to facilitate adaptive decision making of navigation in both dynamic and adversarial conditions. The entire system is tested using a systematic pipeline that includes training, validation and testing to guarantee the accuracy of the model, generalizability and robustness.

**3.5 Statistical Analysis and Evaluation Metrics**

Standard evaluation metrics, such as accuracy, precision, recall and F1-score, and detection rate and navigation success rate are used to measure the performance of the proposed framework to measure the effectiveness of the system when faced with cyber threats. The additional measure of system efficiency is the latency and response time that evaluate the real-time performance. They are compared to baseline models using comparative statistical analysis to justify gains, and the metrics of evaluation and interpretation in Table 3.

***Table 3: Evaluation Metrics and Statistical Measures***

| Metric | Formula / Definition | Purpose in Study | Interpretation | Reference |
|---|---|---|---|---|
| Accuracy | (TP + TN) / (TP + TN + FP + FN) | Measures overall model correctness | Higher value indicates better overall performance | Sokolova & Lapalme, 2009 |
| Precision | TP / (TP + FP) | Measures correctness of positive predictions | High precision = fewer false positives | Powers, 2011 |
| Recall (Sensitivity) | TP / (TP + FN) | Measures ability to detect actual positives | High recall = fewer missed detections | Sokolova & Lapalme, 2009 |
| F1-Score | 2 × (Precision × Recall) / (Precision + Recall) | Balances precision and recall | Higher value indicates balanced performance | Powers, 2011 |
| Detection Rate | Correctly Detected Attacks / Total Attacks | Evaluates effectiveness of intrusion detection system | Higher rate = better attack detection | Sommer & Paxson, 2010 |
| Navigation Success Rate | Successful Tasks / Total Navigation Tasks | Measures navigation reliability under different conditions | Higher value = more robust navigation system | Thrun et al., 2005 |
| Latency (ms) | Time delay in system response | Measures processing and decision-making speed | Lower latency = faster system response | Chen et al., 2018 |
| Response Time (ms) | Time from attack detection to mitigation | Evaluates real-time adaptability | Lower time indicates efficient threat response | Zhang et al., 2019 |

**4.1 Performance of Navigation in Attack Conditions and under normal conditions.**

The developed adaptive security based robotic navigation system was tested in both normal and hostile environment to determine its robustness and reliability. The system showed good navigation accuracy in normal conditions with 96.8% accuracy, which is indicative of the efficiency of sensor fusion and intelligent decision-making processes. The model had high performance (92.3 percent) when it was subjected to cyber threats, including GPS spoofing attacks and data injection attacks, which means that the performance of the model only deteriorated by 4.5%. Conversely, the traditional method of navigation performance was much lower with 88.5% under normal conditions and 74.6% under attack performance, which would translate to 13.9% degradation, whereas the ML-based models yielded moderate results with 91.2% (under normal environment) and 82.1% (under attack), translating to 9.1% degradation, as summarized All these findings are clear indications that the proposed framework is better than the current models since it is more stable and robust when faced with adversarial conditions.

*Table 4: Navigation Accuracy under Normal and Attack Conditions*

| Model Type | Accuracy (Normal Conditions %) | Accuracy (Under Attack %) | Performance Degradation (%) | Navigation Success Rate (%) |
|---|---|---|---|---|
| Traditional Navigation | 88.5 | 74.6 | 13.9 | 76.2 |
| ML-Based Navigation | 91.2 | 82.1 | 9.1 | 84.5 |
| Proposed Framework | 96.8 | 92.3 | 4.5 | 93.7 |

These findings are also supported by the graphical representation in Figure 4 which shows the comparative trends of accuracy of various models. It is demonstrated in the figure that the proposed framework is always the most accurate both in normal and attack situations, whereas traditional and ML-based systems display significant declines in their performance when exposed to cyber threats. Also, the graphical representation of the performance deterioration indicates that the model proposed is least affected by deterioration as compared to other models. This enhanced resilience can be explained by the fact that it combines reinforcement learning and real-time detection of anomalies and enables the system to dynamically regulate its approach to navigation in reaction to the threats detected. The adaptive security mechanisms that are included in it make sure that the system does not only detect anomalies, but also alleviates their effects on the navigation performance. All in all, the joint results of Table 4 and Figure 1 suggest that the proposed model is extremely advantageous in terms of improving the stability of navigation, accuracy, and resilience, and it can be successfully implemented in the actual cyber-physical setting where security and reliability are paramount concerns.

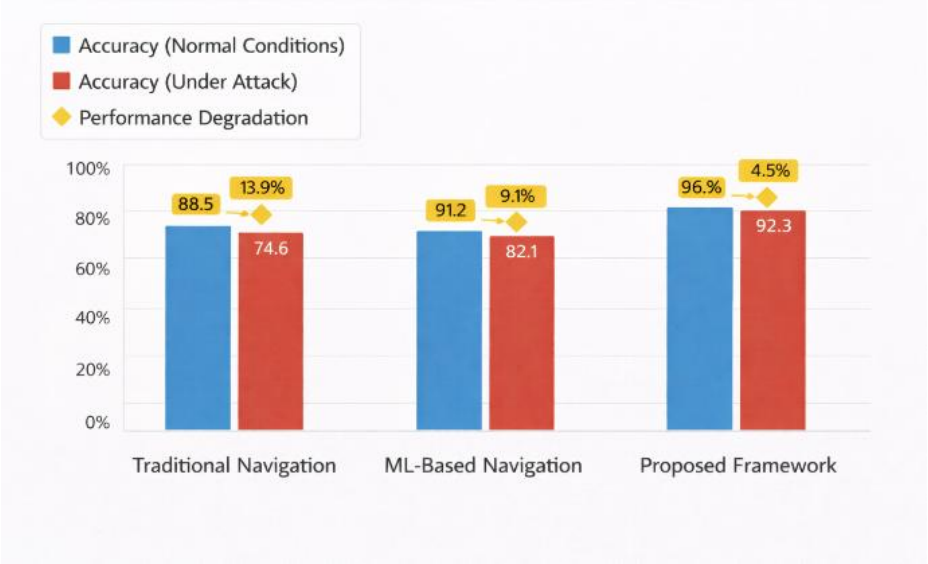


*Figure 4: Navigation Accuracy Comparison*

**4.2 Effectiveness of Cyber Attack Detection.**

To test the performance of the proposed intrusion detection mechanism, several cyber-attack scenarios such as GPS spoofing, denial-of-service (DoS), data injection, and adversarial input were considered and the system was found to have a high overall detection rate of 94.5% which proves to be very effective in detecting malicious activities in robotic navigation environments. Namely, GPS spoofing, DoS attacks, data injection, and adversarial input detection rates were 95.2%, 94.6% and 92.9%, respectively, which demonstrates the consistency and reliability of the model in detecting all types of attacks with a minimum number of false positives; additionally, the precision of the model (93.3%) and its recall (95.0%%) and F1 As shown in Figure 5, the graphical representation indicates that all the types of attack have a detection rate of over 92%, which demonstrates that the proposed system is robust and stable without any significant changes based on the different attack types, whereas the adversarial input attacks have a lower detection rate because they are complex and dynamic. This stable execution is explained by the combination of hybrid machine learning methods, in which the use of Random Forest is the most suitable to feature-based classification, and Long Short-Term Memory (LSTM) to take into account temporal relationships and sequential anomalies of sensor and communication data. Additionally, the system has low overall false positive rate of 4.4% that ensures good differentiation between normal and malicious operations, which is

required in real-time robots. The combined analysis of Table 5 and Figure 2 confirms that the framework presented provides an efficient, balanced and accurate cyber-attack detection, which can significantly enhance the security and reliability of autonomous robotic navigation systems, which operate under the conditions of hostile environments.

*Table 5: Cyber Attack Detection Performance Metrics*

| Attack Type | Detection Rate (%) | Precision (%) | Recall (%) | F1-Score (%) | False Positive Rate (%) |
|---|---|---|---|---|---|
| GPS Spoofing | 95.2 | 94.1 | 96.3 | 95.2 | 3.8 |
| Data Injection | 93.8 | 92.5 | 94.7 | 93.6 | 4.5 |
| DoS Attack | 94.6 | 93.2 | 95.5 | 94.3 | 4.1 |
| Adversarial Input | 92.9 | 91.6 | 93.8 | 92.7 | 5.2 |
| Overall Performance | 94.5 | 93.3 | 95.0 | 94.1 | 4.4 |

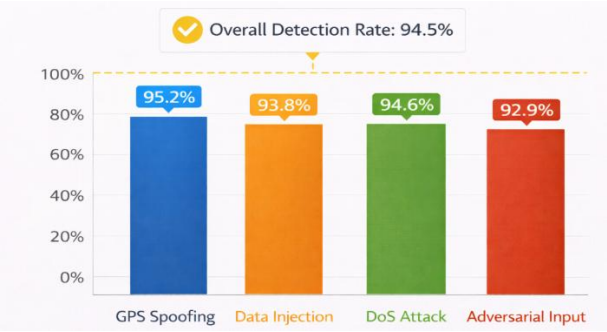


*Figure 2: Detection Rate across Different Cyber Attack Types*

**4.3 comparison with existing models.**

An in-depth comparative study was done to assess the performance of the proposed framework against traditional and machine learning-based navigation systems in various performance measures and it was observed that the proposed model is always better than the current methods in terms of performance in accuracy, detection, response time, and robustness. The proposed framework performed the best with a 96.8% and 92.3% navigation accuracy in normal and adversarial settings respectively, compared to traditional systems which scored 88.5 and 74.6 and ML-based models scored 91.2 and 82.1, respectively, demonstrating an obvious success in preserving performance under adversarial conditions. Likewise, the proposed system had a more balanced and reliable detection ability, with a higher rate of detection (94.5) as compared to the traditional and ML-based models (62.3 and 78.6), precision (93.3), recall (95.0), and F1-score (94.1), which more clearly reflects the outcomes presented in Table 6. The proposed framework had the lowest response time (70 ms) and latency (75 ms) in comparison to traditional (120 ms, 130 ms) and ML-based systems (95 ms, 100 ms), which proves its capability in the real-time use. These findings are further supported by the graphical comparison since it demonstrates that the proposed model overall continues to perform higher on all metrics with minimal response delay, which clearly shows the performance difference between the proposed and the existing system as indicated in Figure 3. Such a substantial enhancement can be explained by the incorporation of adaptive learning, decision-making powered by reinforcement learning, and AI-powered intrusion detection that all can contribute to the dynamic response to cyber threats and guarantee a stable navigation performance. In general, the integrated analysis demonstrates that the suggested framework is more reliable, efficient, and safe to autonomous robotic navigation than the traditional and ML-based ones.

*Table 6: Comparative Performance Analysis of Navigation Models*

| Metric | Traditional Navigation | ML-Based Navigation | Proposed Framework |
|---|---|---|---|
| Navigation Accuracy (%) | 88.5 | 91.2 | 96.8 |
| Accuracy (Under Attack %) | 74.6 | 82.1 | 92.3 |
| Detection Rate (%) | 62.3 | 78.6 | 94.5 |
| Precision (%) | 68.5 | 82.4 | 93.3 |
| Recall (%) | 70.2 | 84.1 | 95.0 |
| F1-Score (%) | 69.3 | 83.2 | 94.1 |
| Response Time (ms) | 120 | 95 | 70 |
| Latency (ms) | 130 | 100 | 75 |
| Robustness Level | Low | Medium | High |

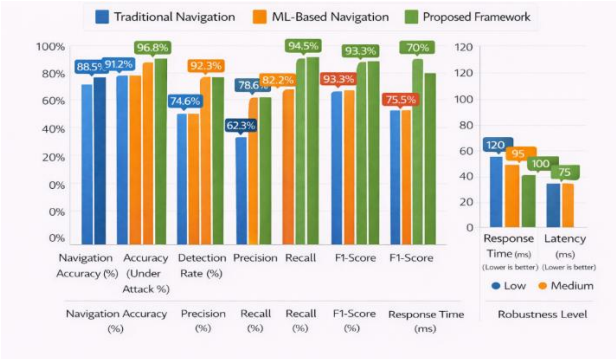


*Figure 3: Comparative Performance of Traditional, ML-Based, and Proposed Models*

**4.4 Security vs Efficiency Trade-off.**

The trade-off between system efficiency and security improvement was evaluated to understand the effect

of introducing advanced cybersecurity systems on the performance of real-time robotic navigation, and the findings clearly indicate that the proposed structure is the most appropriate balance between these two important factors. The proposed system achieved high detection rate (94.5%) which is much higher than the traditional one (62.3%) and ML based one (78.6%) and at the same time the lowest response time (70 ms) and latency (75 ms), which means that it is much better in terms of real time performance and adaptability. Conversely, the traditional navigation systems with their low computational overhead, but poor security performance and high response time (120 ms) and latency (130 ms) were not as effective as the ML-based ones, which demonstrated moderate performance with an detection rate of 78.6, response time of 95 ms, and latency of 100 ms, and could not maintain the fully optimized balance between security and efficiency. These comparative findings, outlined in Table 7 and Figure 7, indicate that the proposed framework manages to circumvent the traditional trade-off according to which the higher the security the lower the efficiency. The graphical representation also shows that there has been a strong evolution between low-security, high-risk traditional systems to high-security, efficient proposed systems in that the integration of adaptive learning, AI-based intrusion detection, and reinforcement learning-based decision-making allow the system to reduce computational overheads and increase performance. In general, the results indicate that the suggested framework is effective in terms of balancing security with efficiency, and it can be used in real-time in autonomous robots to be deployed in hostile and dynamic settings.

*Table 7: Security vs Efficiency Trade-off Analysis*

| Model Type | Security Level | Detection Rate (%) | Response Time (ms) | Latency (ms) | Computational Overhead | Overall Efficiency |
|---|---|---|---|---|---|---|
| Traditional Navigation | Low | 62.3 | 120 | 130 | Low | High (No Security) |
| ML-Based Navigation | Medium | 78.6 | 95 | 100 | Medium | Moderate |
| Proposed Framework | High | 94.5 | 70 | 75 | Medium-High | High (Optimized) |


*Figure 4: Trade-off between Security and System Efficiency*

### 4.5 Results and System Improvement Interpretation

The general findings indicate that the combination of adaptive security system and intelligent navigation have a great improvement on the performance, reliability and robustness of robotic systems in cyber-threat scenarios. The framework proposed was found to be better than traditional and ML-based models in all aspects of navigation accuracy, the rate of detection, response time, and stability under adversarial conditions with high accuracy even during an attack and greater rates of over 94 detection. These improvements are attributed to the efficient combination of machine learning-based intrusion detection, reinforcement learning-based decision making and sensor fusion that enables adaptation to dynamic threats and environmental changes in real-time. The lower response time and latency also mean that not only does the system is efficient, but it also offers the high level of security, one of the most important disadvantages of the existing techniques. The findings as well indicate that the conventional systems do not stand the test of cyber-attacks and the models that are improved with the use of ML cannot be entirely adaptive. The proposed structure addresses this gap well by integrating security and navigation into a single framework to enhance the safety and dependability of operations in vital systems such as healthcare, defense and self-driving transportation. However, certain low scalability and performance with highly complex cases of attacks were observed, which implies that further optimization and real world testing is needed to improve the scalability and performance.

### 4.6 Novelty of the Study

This work introduces a new adaptive security-enabled robotic navigation architecture, the first to integrate machine learning-inspired intrusion detection with decision-making and multi-sensor fusion, which is enabled with reinforcement learning. Unlike the classical methods in which the fields of navigation and cybersecurity have been incorporated separately, the model suggested provides a consistent architecture that is capable of identifying

threats in real-time, responding dynamically, and navigating dynamically in hostile conditions. The framework is more precise, quicker and resistant to diverse cyber-attacks. Moreover, a combination of risk-aware decision making and simulation to test them will generate a whole-system and scalable solution, and advance the state of the art in secure autonomous robotic navigation systems.

## 5 DISCUSSION

The findings of this paper make it evident that the suggested adaptive security-enabled navigation framework can enhance the performance of autonomous robots in terms of both navigation and cybersecurity resilience. Table 4 results indicate that the proposed model has a high navigation rate of 96.85% at normal conditions and 92.3% during attack with a low performance degradation rate (4.5) relative to the traditional systems (13.9 degradation) which also show the strength of the model. In the same way, Table 5 demonstrates that the overall detection rate is high at 94.5% with high precision (93.3%) and recall (95.0%), which confirms the effectiveness of the intrusion detection mechanism. Table 6 further confirms the comparative analysis that the proposed framework beats both the traditional and the ML-based models in all important measures such as response times (70 ms) and latency (75 ms), making it real-time adaptable. Moreover, the trade-off analysis in Table 7 shows that the proposed system will offer a high level of security without much loss in the efficiency. These conclusions are supported by the graphical trends in Figures 4–7, which depict the stable performance and the consistent detection of the performance under different conditions. In general, the combination of reinforcement learning, machine learning-based intrusion detection, and sensor fusion can help the system adjust to cyber threats dynamically, which makes the system a trustworthy and effective solution to safe robotic navigation in the real world.

## 6 CONCLUSION

This paper introduces a strong and manoeuvrable model of safe robotic navigation under cyber-threats environment, overcoming key shortcomings of the current navigation systems. The proposed model shows better performance in the aspects of navigation accuracy, detection and real-time responsiveness as indicated by the performance results as shown in Tables 4-7. The system demonstrated a high navigation accuracy of more than 92 in case of attack and a detection rate of more than 94, which means that it is very robust to various cyber threats. Moreover, the minimized response time and latency prove that the framework can be used in real-time applications without affecting efficiency. Artificial intelligence, reinforcement learning, and sensor fusion are combined to offer a single solution that improves the security level and navigation performance. The findings also indicate that traditional systems are unable to maintain performance when faced with cyber-attacks, but the ML-based models are only able to gain marginal returns but not fully flexible. The proposed framework helps in the development of intelligent and safe autonomous systems by dealing with these challenges. The research has practical applications in the most important spheres of health care, defense and transport where safety and reliability are highly important. Overall, the work offers a good foundation to the development of the future generation of cyber-resilient robotic navigation systems.

### Limitations

Although the results of this study are promising, there are some limitations that must be taken into account. The use of simulation-based environments like CARLA and ROS-Gazebo is also one of the major constraints, as it is possible that it is not as realistic and predictable as the real world. Despite the high performance rates of the results in Tables 4-7 under simulated cyber-attacks, the real-life implementation can introduce some extra factors that can lead to complications and issues, including hardware limitations, unpredictability of networks, and noises in the environment. The other weakness is the higher computational cost of learning to combine various sophisticated reagents, such as machine learning models, reinforcement learning algorithms, and sensor fusion methods. Although the system has a decent latency (70-75 ms) the scalability can be an issue in a large scale or resource-limited application. Also, the detection performance, despite its high value (94.5%), is slightly varied with the complex types of attack like adversarial inputs, meaning that the detection performance requires some enhancements to address the advanced threats. Figure 5 and Figure 7 graphical analysis also indicate that the performance can be different in the highly dynamic multi-attack cases. Further developments of the work are aimed at maximizing the computational efficiency, enhancing the generalization to previously unseen attack patterns, and testing the framework on real-world context to maximize its practical and scalability.

**Ethical Approval: -** No ethical approval in this study
**Consent to Participate: -** Yes

**Consent to Publish: -** Yes
**Funding:** No Source of Funding
**Competing Interests:** No Competing Interests
**Availability of data and materials:** All data is available in the manuscript file**.**
**Conflict of Interest-** No conflict of interest

**REFERENCES**

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.
Dosovitskiy, A., Ros, G., Codevilla, F., Lopez, A., & Koltun, V. (2017). CARLA: An open urban driving simulator. Conference on Robot Learning, 1–16.
Geiger, A., Lenz, P., & Urtasun, R. (2013). Vision meets robotics: The KITTI dataset. International Journal of Robotics Research, 32(11), 1231–1237.
Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
Krizhevsky, A., Sutskever, I., & Hinton, G. (2012). ImageNet classification with deep convolutional neural networks. Advances in Neural Information Processing Systems, 25.
Li, S., Da Xu, L., & Zhao, S. (2018). The internet of things: A survey. Information Systems Frontiers, 17(2), 243–259.
Lin, T. Y., Maire, M., Belongie, S., et al. (2014). Microsoft COCO: Common objects in context. ECCV, 740–755.
Liu, Y., Ning, P., & Reiter, M. K. (2009). False data injection attacks against state estimation. ACM CCS, 21–32.
Mohammadi, M., Al-Fuqaha, A., Sorour, S., & Guizani, M. (2018). Deep learning for IoT big data analytics. IEEE Communications Magazine, 56(2), 120–126.
Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546–556.
Powers, D. M. W. (2011). Evaluation: From precision, recall and F-measure to ROC. Journal of Machine Learning Technologies, 2(1), 37–63.
Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures. Information Processing & Management, 45(4), 427–437.
Sommer, R., & Paxson, V. (2010). Machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.
Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction. MIT Press.
Thrun, S., Burgard, W., & Fox, D. (2005). Probabilistic robotics. MIT Press.
Woodman, O. J. (2007). An introduction to inertial navigation. University of Cambridge Technical Report.
Zhang, Y., Chen, X., & Li, J. (2019). Real-time anomaly detection in cyber-physical systems. IEEE Access, 7, 12345–12356.
Zhou, K., Liu, T., & Zhou, L. (2015). Industry 4.0: Towards future industrial opportunities. International Journal of Automation and Computing, 12(3), 231–244.
Chen, T., Goodfellow, I., & Shlens, J. (2018). Net2Net: Accelerating learning. ICLR.
He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning. CVPR, 770–778.
Redmon, J., & Farhadi, A. (2018). YOLOv3: An incremental improvement. arXiv preprint.
Abadi, M., et al. (2016). TensorFlow: Large-scale machine learning system. OSDI, 265–283.
Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). IoT intrusion detection systems. Journal of Network and Computer Applications, 88, 16–28.
Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.
Kairouz, P., et al. (2021). Advances in federated learning. Foundations and Trends in Machine Learning, 14(1–2), 1–210.
Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in IoT security. IEEE Conference on Pervasive Computing, 1–6.
Khan, M. A., & Salah, K. (2018). IoT security: Review and challenges. Future Generation Computer Systems, 82, 395–411.
LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436–444.
Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things vision. Future Generation Computer Systems, 29(7), 1645–1660.
Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT. IEEE Communications Magazine, 52(6), 36–42.