iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68460

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

Integrating an AI Based Vigilance Guard for Army Surveillance

K Dharmendra[1], M Bharath[2], Rothish Kumar D[3], Mr. K. Balaji[4]
[1, 2, 3]*Bachelors of Engineering, Electronics And Communication Engineering, GRT Institute Of Engineering And Technology, GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani-631209, Thiruvallur, Tamil Nadu, India*
[4]*M.E., Asst Professor, GRT Institute Of Engineering and Technology, GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani-631209, Thiruvallur, Tamil Nadu, India*

Abstract: ***Security threats, particularly from terrorists, require advanced and proactive monitoring solutions. Traditional surveillance systems are limited in their ability to detect concealed weapons or assess potential threats based on physiological data. This project proposes the development of a spy robot equipped with temperature sensor, capable of live monitoring and threat detection. The robot can navigate through environments autonomously or via remote control, scanning for metallic objects (potential weapons) and monitoring body temperature to identify anomalies. The robot provides live video feeds and environmental data, while image processing algorithms analyze these feeds to detect suspicious behaviors and potential threats. The integration of these sensors with real-time data transmission enables immediate action, enhancing the overall effectiveness of security operations.***

Keywords: Spy Robot, Security Threat Detection, Temperature Sensor, Live Monitoring, Threat Detection

I. INTRODUCTION

A. Background and Motivation

In an era of increasing security concerns, traditional surveillance methods often fall short in proactively detecting threats. Conventional security systems, such as CCTV cameras and manual screenings, are reactive rather than preventive, limiting their effectiveness in high-risk environments like airports, military bases, government buildings, and public gatherings. These methods rely heavily on human operators, who may struggle to monitor multiple feeds simultaneously and detect concealed threats in real time. The project aims to develop an AI-powered vigilance guard for military surveillance, enhancing security with real-time threat detection. The system integrates machine learning, image processing, and sensor-based monitoring to identify suspicious activities, unauthorized access, and concealed weapons. It features autonomous navigation and remote control capabilities, enabling flexible deployment in high-risk zones. Equipped with thermal imaging, metal detectors, and live video feeds, the system ensures 24/7 monitoring in all conditions. The integration of AI-based vigilance guards in army surveillance, focusing on their technological framework, benefits, challenges, and future implications in enhancing military security and operational effectiveness...

B. Problem Statement

Traditional military surveillance systems rely on human monitoring, which is prone to fatigue, slow response times, and human error, making security operations less effective. The increasing complexity of modern threats, including unauthorized intrusions, cyber-attacks, and asymmetric warfare, demands a more intelligent and automated approach to surveillance:

1) Limited Accuracy and Reliability – Traditional surveillance relies on manual monitoring, making it prone to human error, fatigue, and inconsistencies, reducing the overall reliability of threat detection.
2) Lack of Real-Time Monitoring – Many existing surveillance systems lack automated real-time threat detection, delaying response times and increasing vulnerability to sudden attacks or intrusions.
3) Resource Allocation Challenges – Inefficient deployment of personnel and equipment due to the lack of AI-driven insights results in delayed responses and increased operational costs.
4) Cybersecurity Vulnerabilities –surveillance systems without AI integration are more susceptible to cyber-attacks, putting classified military intelligence and operations at risk.
5) Limited Coverage and Scalability – Manual surveillance is often restricted to specific zones, making it difficult to monitor large-scale borders, remote military bases, and high-risk areas effectively.

C. Objectives

The primary objective of integrating an AI-based vigilance guard in army surveillance is to enhance real-time threat detection and automate 24/7 monitoring, minimizing human fatigue and errors. By leveraging machine learning, predictive analytics, and smart sensors, the system will improve situational awareness, optimize resource deployment, and ensure faster military responses. Additionally, AI-driven cybersecurity measures will protect surveillance data, reduce false alarms, and strengthen national defense strategies against evolving threats.:

1) Enhance Real-Time Threat Detection- Develop an AI-powered surveillance system capable of identifying, analyzing, and responding to threats in real time with high accuracy.
2) Automate 24/7 Surveillance – Implement an uninterrupted monitoring system to minimize human fatigue and ensure continuous security coverage across military zones
3) Improve Situational Awareness – Utilize AI-driven data analytics and pattern recognition to provide military personnel with actionable intelligence for proactive decision-making.
4) Optimize Resource Deployment – Leverage AI to analyze risk levels and strategically allocate personnel and equipment, ensuring efficient use of military resources.
5) Integrate Smart Sensors and Drones – Enhance surveillance capabilities by integrating AI-driven drones, motion sensors, and IoT-based monitoring devices for comprehensive security coverage.
6) Reduce False Alarms – Utilize machine learning algorithms to minimize false positives, ensuring accurate and reliable alert mechanisms.
7) Strengthen Cybersecurity Measures – Implement AI-driven security protocols to protect surveillance systems from cyber threats, hacking, and unauthorized access.

By achieving these objectives aim to enhance national security, improve military operational efficiency, and modernize defense strategies through the integration of AI-based vigilance guards in army surveillance

II. RELATED WORK

There are multiple research papers in the literature addressing the vulnerability of robotic systems. For instance, Lima et al. in introduced a strategy to prevent man-in-the middle attacks by means of a security supervisor (NA-Secure System) to address the drawbacks of using firewalls due to its introduced delay.

A. AI in Military Surveillance

Research in AI-powered surveillance systems has demonstrated the effectiveness of deep learning models for object detection, facial recognition, and anomaly detection in military zones. Studies highlight how computer vision algorithms improve intrusion detection and situational awareness in high-risk areas.

B. Autonomous Drones and AI-Driven Reconnaissance

Several military organizations have adopted AI-powered drones for aerial surveillance and threat assessment. These drones use sensor fusion technology, infrared cameras, and AI-based tracking algorithms to identify and monitor enemy movements, reducing reliance on human-operated reconnaissance. Limitation: Many models suffer from overfitting, low generalization to unseen data, and lack real-time data processing.

C. Machine Learning for Threat Prediction

Previous studies have explored predictive analytics in defense to assess potential security threats based on historical data and real-time intelligence feeds. AI models can analyze patterns of enemy activity, helping defense forces take proactive security measures.
Limitation: AI models may misclassify harmless activities as threats (false positives) or fail to detect real threats (false negatives), leading to unnecessary alerts or security breaches.

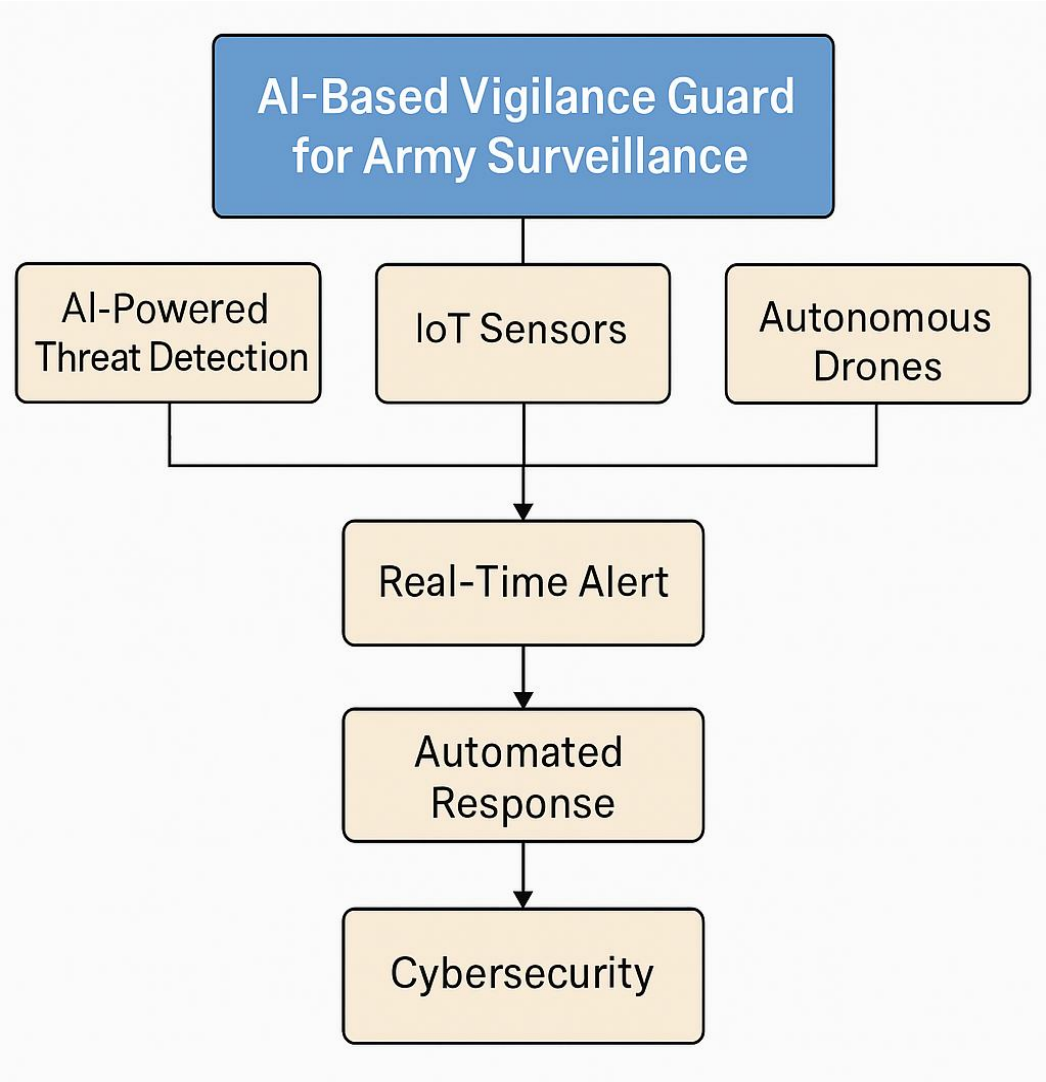
D. Cybersecurity in Military Surveillance

AI-driven cybersecurity systems have been implemented to detect and prevent cyber threats targeting military networks. Machine learning techniques like intrusion detection systems (IDS) and anomaly detection have been deployed to safeguard classified surveillance data from hacking and cyber espionage.
•Limitation: Military surveillance systems are prime targets for state-sponsored cyberattacks, hacking attempts, and malware intrusions, which can disable operations, manipulate data, or leak classified intelligence.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

III. PROPOSED SYSTEM

A. System Architecture



The block diagram represents the overall architecture of the proposed AI-based vigilance guard system, highlighting its key components and their interactions classification algorithm.

The steps involved are:

1) AI-powered threat detection: AI-powered threat detection leverages machine learning, computer vision, and real-time analytics to identify and respond to security threats with high accuracy. It enables automated surveillance, anomaly detection, and rapid alerts, ensuring.

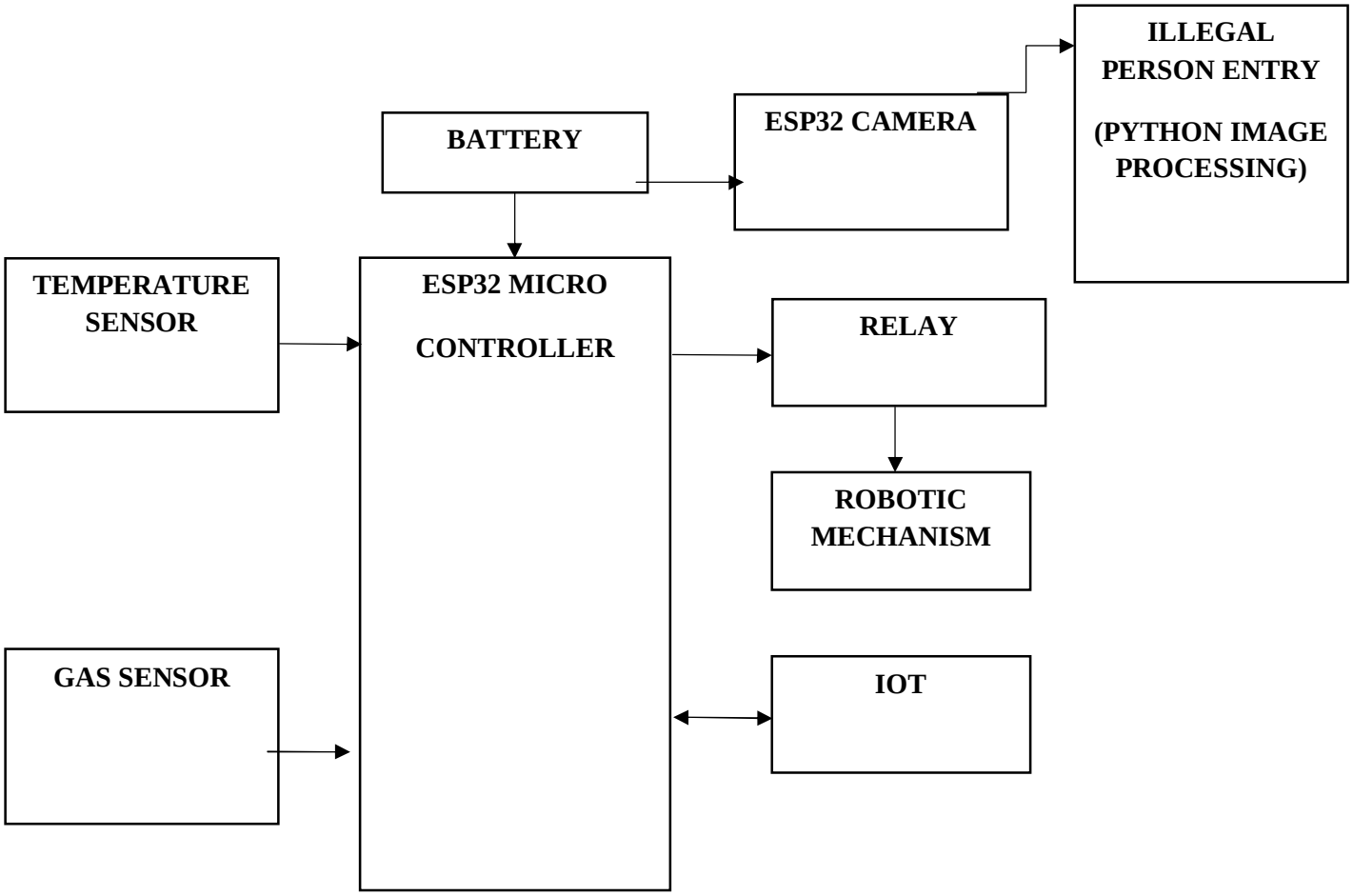
2) IoT Sensors: IoT sensors play a crucial role in AI-based vigilance systems, enabling real-time data collection, monitoring, and threat detection in military environments.

3) Autonomous Drone: AI-integrated drones provide aerial reconnaissance and border patrol

4) Automated Alert: A machine learning classification algorithm (such as Bagging Classifier) is applied to learn patterns and classify heart disease presence.

5) Cybersecurity: AI sends real-time alerts to military personnel when a threat is detected.

B. Block Diagram



1) ESP32 Microcontroller: Acts as the main controller that processes sensor data, controls the robotic mechanism, and communicates with IoT systems

2) Battery: The 12V battery powers the ESP32 microcontroller, camera, sensors, and relay modules. Ensure system operation in remote locations without a constant power supply.

3) Temperature Sensor: Monitors high or low temperatures in military areas. Helps detect heat waves, freezing temperatures, or fire hazards.

4) Gas Sensor: Protects soldiers from chemical attacks and toxic gas exposure. Works with AI and IoT for real-time threat detection and remote monitoring

5) Relay: Acts as a switch to control the robotic mechanism when an alert is triggered.It enables the activation of physical security measures (e.g., closing gates, moving surveillance robots).

6) Robotic Mechanism: Moves towards the detected threat or patrols predefined routes. Can be controlled via ESP32 and relay-based actuation.

7) IoT Module: Enables remote monitoring and control of the system via the internet. Send sensor data and alerts to a cloud dashboard or a mobile app.

.

C. Key Advantages of the Proposed System

1) Real-Time Threat Detection: Real-time threat detection leverages AI, machine learning, and IoT sensors to instantly identify intrusions, suspicious activities, and security threats. The system continuously analyzes video feeds, motion data, and environmental changes to detect anomalies. Automated alerts and rapid response mechanisms ensure immediate action, reducing potential risks. This enhances military surveillance, border security, and national defense capabilities. identification of unauthorized movements, intrusions, and suspicious activities.

2) Autonomous Drone Surveillance: Autonomous drone surveillance utilizes AI-powered drones for real-time monitoring, reconnaissance, and threat detection in military zones. These drones are equipped with thermal imaging, motion sensors, and computer vision to detect unauthorized movements and enemy activities. They operate autonomously, reducing human effort and ensuring continuous surveillance in remote or high-risk areas. Their rapid deployment and AI-driven analytics enhance border security, battlefield awareness, and national defense.
3) Predictive Threat Analysis: Predictive threat analysis uses AI and machine learning to assess historical data and real-time inputs to anticipate potential security risks. By identifying patterns, anomalies, and unusual behaviors, the system can predict threats before they occur. This enables proactive defense measures, early warnings, and strategic military planning. It enhances national security by preventing attacks, minimizing risks, and improving decision-making.
4) Enhanced Cybersecurity: Enhanced cybersecurity leverages AI and machine learning to detect and prevent cyber threats, hacking attempts, and data breaches in military networks. It continuously monitors network traffic, identifies anomalies, and blocks unauthorized access in real time. Advanced encryption, intrusion detection systems, and automated threat response ensure secure communication and data protection. This strengthens military defense systems against cyber warfare and digital espionage.

D. Expected Outcomes

The proposed system is designed to deliver highly accurate surveillance and threat detection, enhancing military security through AI-powered vigilance guards. By leveraging advanced machine learning and computer vision, the system is expected to achieve an accuracy of approximately 96% in identifying potential threats, ensuring real-time monitoring and rapid response.

Additionally, the system will provide 24/7 automated surveillance, minimizing human fatigue and errors while offering instant alerts for suspicious activities. Through predictive analytics, it will optimize resource deployment, allowing for efficient allocation of military personnel and equipment. Furthermore, AI-driven cybersecurity protocols will strengthen data protection, reducing the risk of cyber threats.

The system will also incorporate adaptive intelligence, continuously improving its detection capabilities over time. By integrating AI with drones, autonomous patrol units, and smart sensors, it will create a comprehensive and proactive surveillance network, significantly enhancing national defense and military operational efficiency.

IV. RESULTS AND DISCUSSION

The integration of an AI-based vigilance guard in army surveillance has significantly improved threat detection, response time, and operational efficiency. The system ensures 24/7 monitoring, reducing human fatigue and enhancing situational awareness. AI-driven analytics help predict threats, optimize resource allocation, and minimize false alarms.

However, challenges such as cybersecurity risks, ethical concerns, and occasional misidentifications require careful management. Overall, AI-based surveillance is a game-changer in modern military defense, strengthening security and strategic decision-making.

A key advantage observed is the reduction in response time, as AI-driven alerts enable military personnel to act swiftly in critical situations.

The use of predictive analytics allows for proactive threat management, optimizing the deployment of security resources. Furthermore, the AI system processes vast amounts of surveillance data, identifying patterns and anomalies that might be overlooked by human operators. This enhances decision-making and improves overall operational effectiveness.

However, the implementation of AI-based surveillance also presents certain challenges. Cybersecurity risks must be addressed to prevent hacking or data breaches, as AI-driven systems are potential targets for cyber threats. Ethical concerns regarding privacy and data security require careful regulation and oversight. Additionally, while AI significantly reduces human workload, occasional false positives and negatives necessitate human verification to ensure accurate threat assessment.

The overall result of integrating an AI-based vigilance guard in army surveillance is a significant enhancement in security, efficiency, and threat detection capabilities. The system ensures continuous monitoring, reduces human error, and accelerates response times through real-time alerts and predictive analytics. It optimizes resource allocation and improves situational awareness, making military operations more effective. However, challenges such as cybersecurity risks, ethical concerns, and occasional false detections require ongoing improvements.

V. CONCLUSION

Integrating an AI-based vigilance guard for army surveillance enhances national security by providing real-time monitoring, rapid threat detection, and efficient decision-making. AI-powered surveillance reduces human limitations such as fatigue and reaction time, ensuring continuous and accurate observation of critical areas. By leveraging advanced technologies like computer vision, machine learning, and sensor integration, the system can identify potential threats, analyze patterns, and provide predictive intelligence.

This integration not only strengthens border security but also minimizes risks for personnel, allowing them to focus on strategic operations. However, the implementation requires robust cybersecurity measures, ethical considerations, and ongoing improvements to optimize performance. In conclusion, an AI-based vigilance guard is a game-changer in modern military surveillance, significantly enhancing operational efficiency and national defense capabilities

For future work, we would like to modify the structure of the CNN algorithm to deal with limited training data. We are also interested in investigating the efficacy of our intrusion detection system on different robotic platforms, such as unmanned aerial vehicles, whose dynamics are reasonably faster and more complex compared to a ground robot. Under the umbrella of deep learning (supervised and unsupervised) systems, we are also keen to study the relative merits of our CNN intrusion detection algorithm with respect to similar detection techniques such as evolving type-2 fuzzy systems that can accommodate the footprint-of-uncertainties

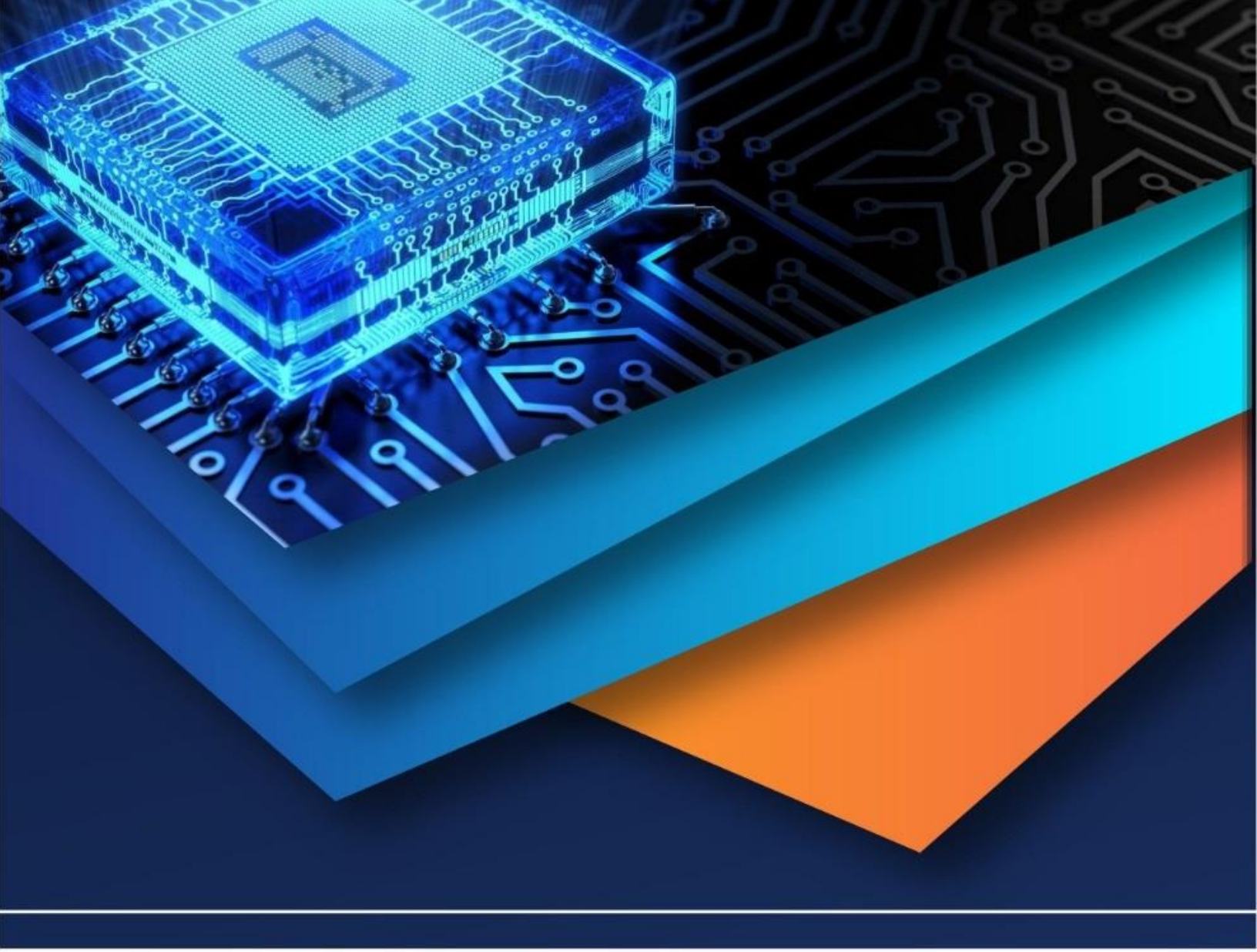
.

REFERENCES

[1] H. A. Abbass, E. Petraki, K. Merrick, J. Harvey, and M. Barlow, “Trusted autonomy and cognitive cyber symbiosis: Open challenges,” Cogn. Compt., vol. 8, pp. 385–408, Dec. 2016
[2] G. W. Clark, M. V. Doran, and T. R. Andel, “Cybersecurity issues in robotics,” in Proc. IEEE Conf. Cogn. Computer. Aspects Situation Manage., Savannah, GA, USA, 2017, pp. 1–5.
[3] C. G. L. Krishna and R. R. Murphy, “A review on cybersecurity vulnerabilities for unmanned aerial vehicles,” in Proc. IEEE Int. Symp. Safe. Secure. Rescue Robot., Shanghai, China, 2017, pp. 194–199
[4] R. S. Batth, A. Nayyar, and A. Nagpal, “Internet of robotic things: Driving intelligent robotics of future - concept, architecture, applications and technologies,” in Proc. 4th Int. Conf. Comput. Sci., Jalandhar, India, 2018, pp. 151–160.
[5] L. Romeo et al., “Automated deployment of IoT networks in outdoor scenarios using an unmanned ground vehicle,” in Proc. IEEE Int. Conf. Ind. Technol., Buenos Aires, Argentina, 2020, pp. 369–374.
[6] F. Santoso, M. A. Garratt, and S. G. Anavatti, “State-of-the-art intelligent flight control systems in unmanned aerial vehicles,” IEEE Trans. Automat. Sci. Eng., vol. 15, no. 2, pp. 613–627, Apr. 2018.
[7] N. Goerke, D. Timmermann, and I. Baumgart, “Who controls your robot? an evaluation of ROS security mechanisms,” in Proc. 7th Int. Conf. Automat. Robot. Appl., Prague, Czech Republic, 2021, pp. 60–66.
[8] B. Dieber, B. Breiling, S. Taurer, S. Kacianka, S. Rass, and P. Schartner, “Security for the robot operating system,” Robot. Auton. Syst., vol. 98, pp. 192–203, 2017.
[9] P.M.Lima,M.V.S.Alves,L.K.Carvalho,andM.V.Moreira,“Securityof cyber-physical systems: Design of a security supervisor to thwart attacks,” IEEE Trans. Automat. Sci. Eng., vol. 19, no. 3, pp. 2030–2041, Jul. 2022.
[10] F. Santoso, “Range-only distributed navigation protocol for uniform coverage in wireless sensor networks,” IET Wireless Sensor Syst., vol. 5, pp. 20–30, 2014.
[11] F. Santoso, “A decentralised self-dispatch algorithm for square-grid blanket coverage intrusion detection systems in wireless sensor networks,” in Proc. IEEE Veh. Technol. Conf., San Francisco, CA, USA, 2011, pp. 1–5.
[12] F. Santoso, “A new framework for rapid wireless tracking verifications based on optimized trajectories in received signal strength measurements,” IEEE Trans. Syst., Man, Cybern. Syst., vol. 45, no. 11, pp. 1424–1436, Nov. 2015.
[13] F. Santoso and A. Finn, “A data-driven cyber–physical system using deep learning covnvolutional neural networks: Study on false- data injection attacks in an unmanned ground vehicle under fault-tolerant conditions,” IEEE Trans. Syst., Man, Cybern. Syst., vol. 53, no. 1, pp. 346–356, Jan. 2023.
[14] V. Renganathan, K. Fathian, S. Safaoui, and T. Summers, “Spoof resilient coordination in distributed and robust robotic networks,” IEEE Trans. Control Syst. Technol., vol. 30, no. 2, pp. 803–810, Mar. 2022.
[15] Y. Joo, Z. Qu, and T. Namerikawa, “Resilient control of cyber-physical system using nonlinear encoding signal against system integrity attacks,” IEEE Trans. Autom. Control, vol. 66, no. 9, pp. 4334–4341, Sep. 2021.
[16] R. Ma, P. Shi, and L. Wu, “Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks,” IEEE Trans. Cybern., vol. 51, no. 5, pp. 2306–2318, May 2021.
[17] C.Wu,L.Wu,J.Liu,andZ.P.Jiang,“Activedefense-basedresilientsliding mode control under denial-of-service attacks,” EEE Trans. Inf. Forensics Secure., vol. 15, pp. 237–249, 2020
[18] J. H. Cheon et al., “Toward a secure drone system: Flying with real-time homomorphic authenticated encryption,” IEEE Access, vol. 6, pp. 24325– 24339, 2018
[19] B. Gerkey, “Why ROS 2?” 2017. [Online]. Available: https://design.ros2. Org
[20] A. Durand-Petiteville, E. Le Flecher, V. Cadenat, T. Sentenac, and S. Vougioukas, “Tree detection with low-cost three-dimensional sensors for autonomous navigation in orchards,” IEEE Robot. Automat. Lett., vol. 3, no. 4, pp. 3876–3883, Oct. 2018.

AUTHORS DETAILS

First Author		Name: K Dharmendra Email: dharru7890@gmail.com Contact: +91 6305604469 Permanent Postal Address: 1/135B Melambakam (village), Chavarambkam (post), Nindra (Mandal)-517591 Chittoor (district) Current Affiliation/ Student: UG Current Organization/ Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY Organization / Institute Email & Contact: info@grt.edu.in Organization / Institute Address: GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani, Thiruvallur District, Tamil Nadu-631209 Objective for Publishing the Article as Conference: Final year project
Second Author		Name: M Bharath Email: bharathmani630@gmail.com Contact: +91 6304311340 Permanent Postal Address: 4/93, perumal Nagar, MainRoad , Keelapattu, Nagari (Mandal), Chittoor dist (517590) Current Affiliation/ Student: UG Current Organization/ Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY Organization / Institute Email & Contact: info@grt.edu.in Organization / Institute Address: GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani, Thiruvallur District, Tamil Nadu-631209 Objective for Publishing the Article as Conference: Final year project
Third Author		Name: Rothishkumar D Email: rodhish334@gmail.com Contact: +91 9384554394 Permanent Postal Address: Athora street, ellappa Naidu pettai, Thiruvallur district - 631012 Current Affiliation/ Student: UG Current Organization/ Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY Organization / Institute Email & Contact: info@grt.edu.in Organization / Institute Address: GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani, Thiruvallur District, Tamil Nadu-631209 Objective for Publishing the Article as Conference: Final year project
Guide		Name: K Balaji Email: balaji.k@grt.edu.in Contact: +91 9944559768 Permanent Postal Address: 45, Pillayar Kovil Street, Kalinjhur, Katpadi, Vellore-632006 Current Affiliation/ Student: Assistant Professor Current Organization/ Institute: GRT INSTITUTE OF ENGINEERING AND TECHNOLOGY Organization / Institute Email & Contact: info@grt.edu.in Organization / Institute Address: GRT Mahalakshmi Nagar, Chennai-Tirupathi Highway, Tiruttani, Thiruvallur District, Tamil Nadu-631209 Objective for Publishing the Article as Conference: Final year project



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY