IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Review On Surveillance Robot With Target Detection And Engagement

Assistent Prof.Minal.K
CSE HKBK College of Engineering
HKBK College of Engineering
Banglore India

Vishwa Patil
CSE HKBK College of Engineering
HKBK College of Engineering
Bangalore India

Shashank V
CSE HKBK College of Engineering
HKBK College of Engineering
Bangalore India

Sangmesh
CSE HKBK College of Engineering
HKBK College of Engineering
Bangalore India

Suhas HS
CSE HKBK College of Engineering
HKBK College of Engineering
Bangalore India

***Abstract*—**This paper proposes a cyber-physical system employing Convolutional Neural Networks (CNN) for ensuring reliable operation of military ground robots in adversarial envi- ronments. Focusing on the vulnerabilities of the Robot Operating System (ROS), the system is tested against man-in-the-middle cyberattacks on the GVR-BOT, a military-grade unmanned ground vehicle. By transforming ROS network traffic into RGB or grayscale images, the CNN is able to detect cyber intrusions. The proposed framework outperforms state-of-the-art methods such as Bag-of-Features and Support Vector Machines, with low rates of false positives and fast detection times, enabling improved cybersecurity in autonomous systems.

I. Introduction

In today's digital battlefield, robotic systems are now central to military operations, including unmanned ground vehicles (UGVs), air drones, and autonomous naval platforms, all under the banner of advanced situational awareness, reduced human risk, and optimized operational performance. However, the increasing deployment of networked, autonomous sys- tems poses a fundamental problem: cybersecurity. As robotic systems become more intelligent and networked, they be- come more susceptible to cyber attacks that can degrade their functionality, integrity, and reliability. One of the most sinister threats under this system is the man-in-the-middle (MitM) cyberattack—a type of intrusion wherein an attacker covertly intercepts and possibly alters the communication between two systems. When aimed at military robots, the consequences can be catastrophic, from mission failure to collateral engagement. This research tackles the problem of ensuring the trusted functioning of a military ground robot in hostile environments by incorporating cybersecurity defenses through deep learning. In particular, it explores the design and implementation of an Intrusion Detection System (IDS) based on Convolutional Neural Network (CNN) technology with the capability to detect Man-in-the-Middle (MitM) attacks in real-time. The robot under consideration is simulated from the GVR-BOT, a military-grade Unmanned Ground Vehicle (UGV) developed by the U.S. Army Combat Capabilities Development Command (CCDC). Based on the Robot Operating System (ROS), the GVR-BOT is an actual testbed for testing cybersecurity threats and defenses on robotic platforms. The basic premise of trusted operations is based on the trust that a robot system will perform its intended task without any compromise even in high-risk or adversarial environments. Traditional cybersecurity techniques such as firewalls and encrypted communication protocols, though helpful, may not be enough in scenarios where adaptive and dynamic response to attacks is essential. Deep learning based on the Convolutional Neural Networks (CNNs) is a trustworthy solution. Learning and classifying network traffic data patterns—presented as images by preprocessing techniques—CNNs can identify subtle patterns of anomalies indicating possible cyber intrusions. The research methodology involves collecting malicious and benign ROS network traffic, transforming the data into image representations most appropriate for CNN processing, and training the CNN to detect and classify attacks at high levels of accuracy. Experimental results confirm that the system can record detection accuracies over 99Furthermore, the re- search contributes to the vibrant debate surrounding trusted autonomy, a concept that encompasses both the reliability of technology and human trust in robotic agents. In high-risk domains such as military operations, this trust must be built through thorough verification of the robot's immunity against cyber attacks and its ability to recover from them. Not only does the work highlight the promise of deep learning for real-time intrusion detection.

II. A. Literature servey

[1].The research paper entitled ”An Ensemble Deep Learning Model for Vehicular Engine Health Prediction” by Chukwudi et al. in 2024 presents a robust and intelligent method of predicting vehicular engine health leveraging the strength of advanced supervised machine learning and ensemble learning techniques. The primary objective of this study was to create a real-time predictive model that can detect potential engine issues early and classify engine health status into classes such as Good, Minimal, Moderate, and Critical. Early prediction allows for timely interventions, avoids operational disruptions, and reduces maintenance costs. The authors developed a comprehensive dataset of 3003 clinical engine records, where features were extracted from a set of onboard sensors that accurately capture real-world engine behaviors

[2]. The research article ”An Improved Framework for Detecting Thyroid Disease Using Filter-Based Feature Selection and Stacking Ensemble,” by Obaido et al. (2024), suggests a novel state-of-the-art framework for early and precise diagnosis of thyroid disease by utilizing a blend of feature selection methods and machine learning methods. The research emphasizes the need for high-performance prediction systems in the healthcare sector, especially in the case of thyroid diseases that are extremely misdiagnosed because of similar symptoms and the lack of the appropriate diagnostic equipment. To address these challenges, the authors utilized a collection of supervised machine learning methods, such as Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), K-Nearest Neighbors (KNN), and Artificial Neural Networks (ANN). The models were used in a Stacked Ensemble Framework, which combines individual classifier predictions with a meta-learner to provide overall accuracy and stability.

[3].The research paper entitled ”An Ensemble Deep Learning Model for Vehicular Engine Health Prediction,” authored by I. J. Chukwudi et al. in 2024, is concerned with the enhancement of early vehicular engine health condition prediction through advanced ensemble machine learning and deep learning techniques. The primary goal is to predict the condition of a vehicle engine—classified as Good, Minor, Moderate, or Critical—by aggregating multiple classifiers. The authors employed an ensemble learning strategy, specifi- cally the stacked ensemble approach, which aggregates the predictive outcomes of multiple base models and applies a meta-learner to enhance the ultimate prediction. Precisely, three distinct stacked models were developed: Stacked Model 1 comprises Random For- est, SVM, Gradient Boosting, Decision Tree, and K-Nearest Neighbors; Stacked Model 2 aggregates Logistic Regression, SVM, Linear Discriminant Analysis, Gradient Boosting, and AdaBoost; while Stacked Model 3 entails Logistic Regression, KNN, SVM, LDA, Gradient Boosting, AdaBoost, Decision Tree, Random Forest, and Gaussian Naive Bayes.

[4].The research article ”Sensing Technologies for Crowd Management Adaptation and Information Dissemination in Public Transportation Systems: A Review” highlights the importance of advanced sensing technologies and machine learning algorithms in crowd prediction and management in public transport systems. Authors present a wide range of methodologies, including visual-based (VB) and non-visual-based (NVB) sensing techniques such as optical cameras, thermal cameras, LiDAR, pressure sensors, and acoustic/ultrasound systems. Machine learning (ML) algorithms including Support Vector Machines (SVM), Convolutional Neural Networks (CNN), and Deep Learning (DL) techniques are used to enhance the accuracy of prediction and operational efficiency. For instance, a CNN-based passenger count system showed significant improvement in metro platform crowd density estimation. In another study, SVM models reported high accuracy (above 80)

[5].This study aims to predict the mode of delivery (cesarean or normal) based on supervised machine learning models. The data used were 1200 clinical records with features like maternal age, fetal weight, gestational weeks, and medical history. The algorithms employed are Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Gradient Boosting (GB). All the algorithms were trained and evaluated based on cross-validation methods. Among all models, Random Forest yielded the maximum accuracy of 91.3

[6].Title: State-of-the-Art Intelligent Flight Control and Path Planning Systems in Unmanned Aerial Vehicles This paper shows a detailed survey of intelligent control and path planning mechanisms in UAVs, via soft computing and bio-inspired methodologies. Algorithms addressed are Artificial Neural Networks (ANN), Genetic Algorithms (GA), Particle Swarm Optimization (PSO), Neuro-Fuzzy systems, and hybrid paradigms such as Genetic Learning-PSO and ANFIS (Adaptive Neuro-Fuzzy Inference System). These were all employed for different scenarios of UAV navigation and control. For example, hybrid NN-based Model Predictive Controllers (NN-MPC) proved to be superior to traditional PID controllers in disturbance conditions. GL-PSO proved to have better search ability than PSO or GA alone. The ANN controllers offered

strong flight performance with little steady-state error. Experiment results indicated that hybrid and evolutionary methods resulted in better adaptability, stability, and performance over conventional methods, rendering them effective for real-time UAV applications though with increased computational requirements

[7].Title: Towards a Secure Drone System: Flying with Real-Time Homomorphic Authenticated Encryption This pa- per presents a security-oriented solution for drone control systems with the application of cryptographic methods instead of conventional ML algorithms. More specifically, it suggests a linearly homomorphic authenticated encryption (LinHAE) scheme intended to protect real-time controller actions in drones. The goal was to avoid controller key management vulnerabilities and forgery or tampering of control messages. LinHAE promotes computational operations on ciphertext (e.g., addition, multiplication with constants) without having to decrypt at computation time, allowing safe and real-time control. The experiments in the field using flights proved that drones using LinHAE had a steady autonomous flight in the face of typical cyberattacks. As an unconventional machine learning research piece, this article shows a secure and new mechanism for improving reliability of autonomous UAV systems.

[8].The research article ”Modelling of Mobile Robot Dynamics” by Edouard Ivanjko et al., 2010 deals with im- proving mobile robot navigation precision through modeling their dynamic behavior employing physical modeling and experimental identification methods. The authors discuss the drawbacks of conventional kinematic odometry-based localization, particularly when they are exposed to high-speed maneuvers, sudden acceleration, or rough terrain, leading to pose prediction errors most of the time. Two modeling methods are introduced: one based on physical principles such as mass, inertia, torque, and friction through Euler- Lagrange formulations, and one based on experimental curve fitting of actual velocity measurements of a Pioneer 3DX mobile robot. The physical model combines units such as DC motors, PI controllers, gearheads, and encoder feedback, whereas the experimental model encompasses significant dy- namic response scenarios such as step changes, ramps, and steady-state velocities. While no supervised machine learning algorithms such as Decision Tree or SVM were used, the models are created to capture real-world dynamics properly and are coded using MATLAB/SIMULINK for verification. Performance was quantified in terms of average and maximum velocity errors. The model based on experiments revealed lesser mean translational and rotational velocity errors (1.62 mm/s and 0.48°/s respectively) than the physical model (3.36 mm/s and 0.81°/s), which reflects its general greater precision. Nonetheless, the physical model was superior under sharp transitions because it incorporated internal system dynamics.

[9]. This research measures the open-source autonomous driving system’s resilience and security through simulation of adversarial scenarios. Machine learning algorithms are integrated into perception and control layers for object detection and path planning. The primary algorithms and tools used are: Kalman Filter for tracking objects, Hungarian Algorithm for matching tracks, Search based on the cost function for path planning,Utilization of CNNs in visual perception. Although not predicting childbirth per se, ML application in real- time decision-making in safety-critical systems is the core. Accuracy is not given in terms of percentages but assessed in terms of system robustness against adversarial attacks. The performance of the system is gauged by its capacity to sustain control in the presence of injected faults and disturbances

[10]. This paper uses machine vision and specially designed algorithms for tree trunk localization in orchards based on stereo camera data: Concavity Detection Algorithm: Designed specifically to identify tree shadows in point clouds. Algorithms Employed: Custom-designed concavity exploration, Coin-based random descent technique for image exploration, RANSAC for ground detection,Density-based filtering for candidate verification. Performance: Precision: 97Recall: 90Processing time: 10–15 ms with CUDA.

[11]. Internet of Robotic Things: Driving Intelligent Robotics of Future” This review paper presents the Internet of Robotic Things (IoRT), integrating: Machine Learning, AI, IoT, and Cloud Computing for smart decision-making, Explores supervised learning and deep learning for real-time robotics applications,Healthcare, industry, military, and smart environment applications.Although it does not provide new experimental findings or accuracies, it highlights the significance of ML models such as ANN (Artificial Neural Networks) and reinforcement learning in autonomous operations. It focuses on adaptive and modular ML deployment in cyber-physical systems

[12]. Toward a Secure Drone System Using Real-Time Homomorphic Authenticated Encryption” Homomorphic Authenticated Encryption (LinHAE) is employed in this work to safely manage autonomous drones, emphasizing real- time computation: ML is not applied directly to predic- tion, yet encryption-based computation simulates prediction logic.The controller employs:Homomorphic functions to ma- nipulate encrypted data, Authenticated encryption to assure integrity and confidentiality.Performance:Attained real-time autonomous flight with encrypted signal processing within 1 s per evaluation. Proven resistance against forgery, replay, and eavesdropping attacks that are critical for trustworthy CPS (Cyber-Physical Systems)

[13]. The research article ”Cybersecurity Issues in Robotics” by George W. Clark Jr. et al., 2018, explores the increased vulnerabilities and attack surfaces in robotic systems used in different applications such as manufacturing, elderly care, autonomous vehicles, and military drones. Instead of utilizing predictive machine learning algorithms, the emphasis of this research is classification and simulation of cyber-physical attacks against embedded systems with robotic architectures. The authors group attacks into hardware-level (such as hardware trojans and kill-switches), firmware/OS-level (such as DDoS, malware injections), and application-level (such as buffer overflows, Stuxnet-type malware). No individual machine learning classifiers were actually tried or compared, but the paper is well-organized to illustrate in detail how such systems could be compromised and used for ill. Scenarios are constructed in order to emulate hijacking of eldercare robots for identity theft, firmware tampering in autonomous cars, and GPS spoofing-based deactivation of drones. The primary contribution of the paper is that it focuses on highlighting human safety and economic threats posed by insecure autonomous systems. It gives suggested countermeasures and a security framework instead of empirical accuracy measures. The merit of this research lies in its strategic threat modeling and possible combination with predictive AI-driven intrusion detection in future research.

[14]. The research article ”Trusted Autonomy and Cognitive Cyber Symbiosis: Open Challenges” by Hussein A. Abbass et al., 2015, addresses the incorporation of trust in autonomous and semi-autonomous systems, a fundamental need for future AI decision-making systems. In contrast to the common prediction problem with machine learning classifiers, this article addresses the psychological, social, and computational aspects of trust between intelligent agents and humans. It formalizes and conceptualizes trust and distrust models, citing behav- ioral game theory, fuzzy logic, and cognitive computation. Algorithms mentioned are trust calibration functions, social dilemma games for cooperation of agents, and trust-based risk models, which function as high-level cognitive control mechanisms. Although empirical outcomes are not compared in terms of F1 scores or classification accuracy, the paper formulates a layered system architecture for trust-aware autonomous systems and identifies performance bottlenecks in existing human-machine teams. Theoretical frameworks outlined are meant to be used in the future in areas like autonomous vehicles, surgical robots, and collaborative decision-making agents. This study is seminal in its focus on trustworthiness as the precondition to broad deployment of AI, as opposed to conventional ML performance measures.

[15]. The article ”A Simplified Model-Free Self-Evolving TS Fuzzy Controller for Nonlinear Systems with Uncertainties” by Ayad Al-Mahturi et al., 2020, presents a new self-evolving fuzzy logic controller specifically suited for non-linear system control. The work is centered on real-time adaptive control instead of static prediction with a Takagi-Sugeno (TS) fuzzy inference framework. The authors use model-free design, avoiding dependence on prior knowledge of plant dynamics. The controller learns through a rule-evolution mechanism such that fuzzy rules are added or trimmed online according to performance. A gradient-descent derived sliding surface method is employed to optimize fuzzy parameters so as to minimize error between desired and actual outputs. The controller has been applied to an inverted pendulum system in a disturbed scenario. Compared to an adaptive model- based fuzzy controller, the developed model-free controller yielded improved tracking performance and robustness. The method is not assessed in terms of accuracy percentages but control error metrics and uncertainty stability. Some of the important contributions are the minimal need for a priori system knowledge, high adaptability, and robustness under uncertainty. This positions it for applications like robotics, UAVs, and other real-time autonomous systems.

III. PROPOSED SYSTEM

The existing literature on cyber-physical systems, such as unmanned aerial vehicles (UAVs) and ground robots, highlights several vulnerabilities and limitations in the attainment of strong operational efficiency. Homomorphic encryption research highlights controller-level security at the cost of adaptive, deep-learning-based intrusion detection systems for facilitating dynamic interactions in real-time environments. Likewise, UAV flight control system and mobile robot dynamics research highlights non-linear dynamics and advanced localization, but they fail to integrate fault-tolerant cybersecurity models based on convolutional neural networks (CNNs) effectively. Although ROS 2 effectively addresses modular- ity and security-related issues, the use of proactive deep- learning methods for cyberattack prevention remains poorly explored. Furthermore, intrusion detection methods used cur- rently largely lack thorough benchmarking against advanced counterparts such as fuzzy systems or hybrid models, hence rendering them less effective in addressing changing threats. To fill these gaps, an integrated approach with adaptive deep learning, secure middleware advancements, and comparative performance analysis must be taken, with the aim of attaining scalable, secure, and resilient operations in cyber-physical systems.

IV. . LOAD DATASETS

The measurements utilized here are ROS network traffic measurements taken under two scenarios: normal operation and malicious attacks. The measurements were taken while conducting real-time penetration testing on the GVR-BOT ground vehicle, a proof-of-concept of a military robot

A. Dataset Characteristics

Data Type: The data regards network traffic gathered from the ROS system, including multivariate time-series data.

B. Data Processing

The data was normalized using the min-max normalization method, scaling it between -1 and +1. The data was normalized into RGB or grayscale images for CNN training

C. Data Configuration

Taken during experiments in indoor and outdoor environments. The document encompasses a range of robotic states, including forward and angular velocities, motor dynamics, battery status, and acceleration

D. Cyberattack Scenario

The data includes the the time when man-in-the-middle attawere executed, namely on ROS topics such as One for training the convolutional neural network Intrusion detection system and another fortesting and validation

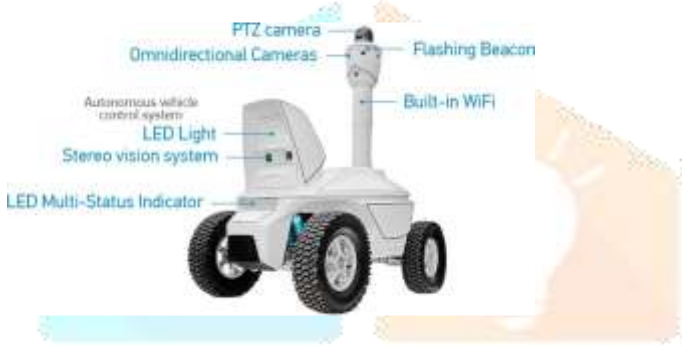

Fig. 1: system Architecture of surveillance robot

V. GAP OF THE PAPER

Current literature for cyber-physical systems, including UAVs and ground robots, emphasizes a range of vulnerabilities and limitations in providing robust operational efficiency. Research pertaining to homomorphic encryption tends to concentrate on controller-level security at the cost of adaptive, deep-learning-based intrusion detection systems, which can enable dynamic interactions in real-time domains. Likewise, research in UAV flight control systems and mobile robot dynamics concentrates on non-linear dynamics and localization improvement, but fails to provide effective integration of fault-tolerant cybersecurity models using convolutional neural networks (CNNs). While ROS 2 effectively addresses issues pertaining to modularity and security, the integration of proactive deep-learning techniques to counter cyberattacks remains poorly explored. Additionally, existing intrusion detection techniques tend to lack comprehensive benchmarking with sophisticated alternatives like fuzzy systems or hybrid models, thereby restricting their effectiveness in countering evolving threats. Addressing these limitations requires an integrated approach that combines adaptive deep learning, secure middleware enhancements, and relative performance analysis to provide scalable, secure, and resilient operations in cyber-physical systems.

VI. SUMMARY

Comparison of results presented in the provided paper confirms the effectiveness of the suggested CNN-based intrusion detection system in the detection and blocking of man-in-the-middle cyberattacks on the GVR-BOT ground vehicle.Short detection time, which is merely 3 consecutive epochs or less.Works better than standard algorithms, such as Bag-of-Features (BoFs) and Support Vector Machines (SVMs), on key parameters like accuracy, precision, recall, F1-score, and robustness.The system attains almost ideal sensitivity (True Positive Rate) and specificity (True Negative Rate) with both values approximating 1.F1-scores also approach 1, which indicates high and balanced recall-precision performance. The false negatives are minimal as well, showing the system's ability to catch almost all bad traffic

TABLE I: Summary of review on Surveillance Robot

Sl No.	Title	Algorithms / Techniques	Limitations
1	An Ensemble Deep Learn- ing Model for Vehicular Engine Health Prediction	RF , SVM , KNN	High Dimensionality Challenges,Computational Overhead
2	Sensing Technologies for Crowd Management Adaptation and Information Dissemination in Public Transport System	VB , NVB	High Cost of Deployment Data Privacy Concerns
3	This research will attempt to forecast the mode of delivery	LR , DT , RF	Training and Evaluation.Data Imbalance, Feature Dependence
4	Smart Flight Control and Path Planning Systems Flight Control Algorithms	ANNS , GAS , PSO	High Computational Demand Complexity of Hybrid Method
5	Towards a Secure Drone System	Real-Time Homomorphic Authenticated Encryptions	Simulation of motion of two independently powered wheels of a robot.
6	open-source autonomous driving system's resilience and security	LiDAR , Sensor Fusion Algorithms	Open-source systems are vulnerable to exploitation because codebases are open.
7	Machine vision and algorithms designed specifically for tree trunks,	RGB cameras, LiDAR	Environmental Variations: Performance may be degraded in poor conditions, e.g., irregular lighting, shadows, or dense
8	Internet of Robotic Things	KNN , LIDAR	Network Dependence o IoRT is dependent largely on stable low-latency network connections.
9	Towards a Secure Drone System Based on Real-Time Homomorphic Authenticated Encryption	AE , KNN	Energy Consumption Heavy encryption/decryption consumes drone battery quicker.Can decrease flight duration and flying stamina
10	Cybersecurity Challenges in Robotics Intrusion Detection Systems	Bayesian Networks , Reinforcement Learning	Resource Constraints: The majority of robots have limited computational power and battery life, which restricts the use of advanced security measures.
11	Traffic Signal Control Using End-to-End Off-Policy Deep Reinforcement Learning	BGR ResNet, Rainbow RL	Simulator only, struggles with imbalanced traffic
12	A Simplified Model-Free Self-Evolving TS Fuzzy Controller for Uncertain Nonlinear Systems	Fuzzification	Fuzzy rules are dynamically developed and tuned according to observed data and system performance.
13	Cybersecurity Issues in Robotics	SVM or neural networks	Robotics platforms possess minimal processing power, which renders sophisticated cybersecurity algorithms difficult to execute
14	Trusted Autonomy and Cognitive Cyber Symbiosis	Human-Machine Interaction Algorithms	Technique, Employ cognitive architectures High Computational Overhead
15	Minimizing Delay at Closely Spaced Signalized Intersections Through Green Time Ratio Optimization: A Hybrid Approach With K-Means Clustering and Genetic Algorithms	K-Means, Genetic Algorithm	No left turns, fixed cycles, no pedestrians, no real-time data

VII. FUTURE WORK

The authors propose a number of avenues for future research aimed at enhancing both the efficacy and adaptability of their intrusion detection system Describe the performance of the implemented intrusion detection system for different robotic platforms,unmanned aerial vehicles (UAVs), which have more dynamic and advanced behavior compared to ground robots.Apart from algorithm optimization to enable quicker real-time processing with high precision and low false positives,Through addressing these areas, the framework can be made more potent, adaptable, and scalable for wider uses in civilian and military robot systems.

VIII. CONCLUSION

We performed live cyberattack testing on the ROS-based GVR-BOT ground vehicle and recorded network traffic for training a CNN-based intrusion detection system. The results reveal that the proposed algorithm is efficient, secure, and feasible. It performs well with high accuracy, sensitivity (true positive rate, TPR) and specificity (true negative rate, TNR) approaching 1, which reflects superior detection performance. Moreover, the system also produces near-perfect F1-scores, which reflect good precision and recall, with low false positive rates and fast detection times in three epochs. Further, it surpasses the conventional approaches like Bag-of-Features (BoFs) and Support Vector Machines (SVMs), which are commonly deployed in image classification. In the future, we will continue to improve the CNN algorithm to enhance its robustness with minimal training data and test its effectiveness on faster and more advanced platforms, like drones. We are also keen to explore other deep learning methods, like type-2 fuzzy systems, to discover their advantages in dealing with uncertainties compared to our CNN approach.

REFERENCES

[1] Abbass,H.A.Petraki,E.Merrick, K., Harvey,J Barlow, M”Trusted autonomy and cognitive cyber symbiosis: Open challenges,” Cognitive Computation, 2016.

[2] Clark, G. W., Doran, M. V., and Andel, T. R. (2017). ”Cybersecurity issues in robotics.” In IEEE Conference on Cognitive and Computational Aspects of Situation Management.

[3] Clark,G.W.Doran,M. V and Andel, T. R. (2017). ”Cybersecurity issues in robotics.” In IEEE Conference on Cognitive and Computational Aspects of Situation Management.

[4] Batth, R.S Nayyar, A Nagpal, A. ”Internet of robotic things: Driving intelligent robotics of the future,” 4th International Conference on Computational Science and Computational Intelligence, 2018.

[5] Romeo, Letal. ”Automated deployment of IoT networks in outdoor scenarios using an unmanned ground vehicle,” IEEE International Conference on Industrial Technology, 2020.

[6] Santoso,F,Garratt,M.A,and Anavatti, S. G. (2018). ”State-of-the-art intelligent flight control systems in unmanned aerial vehicles.” IEEE Transactions on Automation Science and Engineering.

[7] Goerke, N.Timmermann,D Baumgart, I. ”Who controls your robot? An evaluation of ROS security mechanisms,” 7th International Conference on Automation and Robotics Applications, 2021.

[8] Dieber,Betal. ”Security for the Robot Operating System.” Robotics and Autonomous Systems, 2017.

[9] Lima,P.Metal.”Security of cyber-physical systems: Design of a security supervisor to thwart attacks,” IEEE Transactions on Automation Science and Engineering, 2022.

[10] Joo,Y,Qu,Z, Namerikawa, T. ”Resilient control of cyber-physical systems using nonlinear encoding signal against system integrity attacks,” IEEE Transactions on Au- tomatic Control, 2021.

[11] Ma,R,Shi, P, Wu, L. ”Dissipativity-based sliding-mode control of cyber-physical systems under denial-of-service attacks,” IEEE Transactions on Cybernetics, 2021. [12] Wu, C., et al. ”Active defense-based resilient sliding mode control under denial-of-service attacks,” IEEE Transactions on Information Forensics and Security, 2020.

[13] Cheon et al. ”Toward a secure drone system: Flying with real-time homomorphic authenticated encryption,” IEEE Access, 2018.

[14] Farivar et al. (2020). ”Artificial intelligence for the detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems.” IEEE Transactions on Industrial Informatics.

[15] Nowak, E.Jurie,F Triggs, B. ”Sampling strategies for bag-of-features image classification,” European Conference on Computer Vision, 2006