2025 Volume: 01 Issue: 06 www.ijrpa.com Review Article

International Journal Research Publication Analysis

Page: 01-13

AUTONOMOUS SYSTEMS FOR PRIVACY AND INFORMATION SECURITY

Olajide Olatunde Adeola*[1] and Oluwatoyin Yemi Obansola[2]

[1]Department of Computer Science, Oyo State College of Agriculture and Technology, Igboora, Oyo State, Nigeria.

[2]Federal School of Surveying, Oyo, Oyo State, Nigeria.

Article Received: 23 September 2025
Article Revised: 13 October 2025
Published on: 03 November 2025

***Corresponding Author: Olajide Olatunde Adeola**
Department of Computer Science, Oyo State College of Agriculture and Technology, Igboora, Oyo State, Nigeria.

ABSTRACT

The rapid proliferation of autonomous and robotic systems in domains such as smart manufacturing, healthcare, transportation, and home assistance has intensified concerns over privacy and cybersecurity. Modern autonomous systems rely heavily on machine learning for perception, decision-making, and control, which both exacerbates and mitigates security risks. On the one hand, machine learning components introduce new attack surfaces (adversarial examples, model poisoning), while on the other hand machine learning methods are essential tools for detecting intrusions, securing communications, and preserving data privacy. This review surveys recent advances at the intersection of autonomy, robotics, machine learning, privacy, and cybersecurity. We examine machine learning-driven techniques for securing robotic systems, including network intrusion and anomaly detection, secure authentication, and resilient control. The machine learning approaches that enhance privacy, such as federated and distributed learning, differential privacy, and novel sensor designs that obfuscate sensitive data were explored. Case studies span autonomous vehicles, drones, industrial robots, medical robots, and service robots. Our findings highlight the promise of machine learning in improving detection accuracy and adaptive defenses, while also underscoring challenges like data scarcity, adversarial vulnerabilities, and regulatory compliance. It is concluded by recommending integrated "secure-by-design" frameworks, interdisciplinary standards and privacy-by-design principles (for example. inherent privacy-preserving sensors) to ensure that future autonomous systems are both effective and trustworthy.

KEYWORDS: Autonomous, Cybersecurity, Data Privacy, Machine Learning, Sandbox, Robotics.

1.0 INTRODUCTION

Autonomous systems and robotics are transforming many sectors, from driverless vehicles and delivery drones to surgical robots and home assistants. These systems typically fuse advanced sensing, connectivity, and intelligent decision-making to operate with minimal human intervention. However, their complexity and connectivity also make them vulnerable to cyber threats. Prior work has shown that the most cybersecurity-vulnerable parts of robot technologies are robots' data, software, networks, and hardware, [2]. For example, autonomous vehicles depend on data links (V2X), sensors (LiDAR, cameras), and control software, any of which can be targeted by attackers. Likewise, service robots in homes or hospitals collect personal data, raising privacy concerns, [8]. Ensuring the confidentiality, integrity, and availability of autonomous systems is thus a critical challenge.

Machine learning has become deeply embedded in modern autonomy. Machine learning is used for perception (for example. object recognition), navigation (for example. localization and planning), and control (for example. reinforcement learning). These machine learning capabilities can help address security issues: for instance, machine learning-based intrusion detection systems (IDS) can learn network traffic patterns to spot anomalies [3]. However, machine learning also introduces new risks. Neural models can be fooled by adversarial inputs or data poisoning, and centralized machine learning can leak sensitive data. Recognizing this dual role, current research increasingly applies machine learning to cybersecurity and designs machine learning that respects privacy.

The aim of this paper is to provide an in-depth review of recent developments in machine learning-driven autonomous and robotic systems for privacy and cybersecurity. In doing so, we address the following questions:

1. What are the main security and privacy threats facing autonomous robots and vehicles? We survey vulnerabilities (for example. sensor spoofing, network attacks, data breaches) across different robotic platforms.
2. How are machine learning methods used to enhance security in autonomous systems? We review machine learning-based intrusion detection, anomaly detection, authentication schemes, and resilient control strategies in robotics.

3. How can autonomous systems use machine learning to preserve privacy? We examine federated learning, differential privacy, secure aggregation, and privacy-preserving sensor designs that keep data local or obfuscated.
4. What are the challenges faced by stakeholders in managing autonomous systems?

2.0 LITERATURE REVIEW

2.1 Security and Privacy Challenges in Autonomous Robotics

Autonomous systems combine sensing, computation and actuation, often in complex environments. This diversity of components gives rise to a wide threat landscape. For example, autonomous vehicles rely on camera, radar, and LiDAR feeds; attackers can manipulate these (for example. projecting fake obstacles) to cause misperceptions. In a comprehensive survey of AV cybersecurity, sensor manipulation (spoofing, jamming) and remote hacking (exploiting wireless links) are key threats [9]. Similarly, service robots (for example. elder-care helpers) collect personal data; such continuous monitoring raises significant privacy concerns and that robots suffer from the same cybersecurity problems as computers [8].

Machine learning, encryption, and blockchain-based mechanisms may be used to prevent or detect cyber-attacks in robotic systems [4]. [2] emphasize that robots' networks, software, and data are vulnerable, and advocate for security to be integrated early in design. Their analysis of a database of vulnerabilities highlights common trends in attacks against robots. In the context of multi-robot swarms, [14] studied coordinated attacks on UAV swarms and identified attack strategies that can compromise swarm consensus. The data issue in terms of its persistence and complexity is the key one. This includes: data collection issues, consistent labelling ensuring high quality of annotations; effective addressing of extreme data imbalance and heterogeneous data integrating data; network flows, sensor readings, system logs, security events, etc [12]. Although it looks promising in regards to its ability to generate new data through GANs, the quality of these generation is still subject to improvement, particularly when it comes to complex cyber-physical environments.

Overall, the literature identifies frequent concerns for autonomous systems: unauthorized access to control systems, data theft or leakage, tampering with sensor inputs, and exploitation of communication links. It is also mentioned that many autonomous platforms (drones, mobile robots) operate in partially known or open environments which then complicates security. For example, [11] categorise various kinds of attacks on mobile robot navigation (spoofing, DoS, hijacking, etc.), and propose models to classify the impact of such attacks. These baseline threat analyses reveal clearly the requirement for both preventive and detective security mechanisms which are tailored specifically to robotic autonomy.

2.2 Machine Learning-Based Intrusion and Anomaly Detection

Machine learning has emerged as a core method of IDS and anomaly detector for autonomous systems. Traditional signature-based security is constrained for dynamic robotic environments; machine learning can learn patterns from data to recognise novel threats. [10] said focusing on Greater Explainability AI(XAI), Highly Resistant to Adversarial AI, Public Quality Datasets and Industry Control System (ICS)-Specific Solutions to improve cyber defence of systems. Network-based intrusion detection is one area that is prominent. [3] provide a survey of network-based IDS (NIDS) for industrial and robotic systems; They report that detection accuracy and false-positive rates are greatly enhanced by machine learning (including deep learning) [3]. For example, neural classifiers and ensemble techniques can detect malicious network traffic to a robot's control unit. Similarly, anomaly detection can be used on the robot’s behavioral data (sensor readings, motion patterns). A recent CAV (connected autonomous vehicle) study used a stacked LSTM to predict vehicle trajectories and flagged large deviations as anomalies, achieving near-perfect regression accuracy ($R^2 \approx 0.9998$) [27]. Such data-driven detectors can reveal cyber-attacks that subtly alter vehicle behavior.

At the system level, multi-agent machine learning methods help detect distributed attacks. For example, Self-Evolving Host-based IDS (SEHIDS) for robotic systems dynamically updates its detection rules using reinforcement signals when an attack is suspected [4]. Other works explore unsupervised learning: clustering or autoencoders trained on “normal” robot sensor data can detect outliers from attacks [11]. The anomaly detection survey by [16] classifies anomalies by spatial and temporal features in robotic missions, reflecting the varied forms anomalies can take in robots.

The model enables users, customers, and workers to post digital news directly to the verification system, which contributes to the creation of a quicker and more precise counterfeit news detection system utilizing the Decision Tree algorithm [28]. Besides detection, machine learning also supports authentication and authorization in robotic contexts. [7] design a privacy-preserving, transformer-based multi-factor authentication for delivery robots, noting that robots are vulnerable to machine learning-driven impersonation and adversarial attacks (for example. FGSM/PGD). Machine learning models (for example. facial or voice recognition) are integrated with cryptographic credentials to verify users or devices in robot networks. In essence, AI strengthens authentication but also must itself be secured (for example. with defenses to adversarial input [7].

Collectively, these works demonstrate that machine learning can greatly enhance cyber defenses in autonomous systems. By learning from large-scale logs and sensor streams, machine learning-enabled IDS adapt to complex patterns that rule-based systems miss [3]. However, several challenges are noted: models require high-quality training data (often scarce in niche robotic applications) and machine learning detectors may struggle to distinguish attacks from rare but benign anomalies [11]. Ensuring machine learning models remain robust under adversarial conditions is an ongoing concern (for example. incorporating adversarial training in detectors as part of "security by design" [2].

2.3 Machine Learning for Privacy-Preserving Autonomy

Privacy concerns arise when autonomous robots collect or transmit personal data. Here, machine learning techniques are being developed to protect data at various stages. One major approach is federated learning (FL), where multiple robots or devices collaboratively train a shared model without exchanging raw data. [5] introduce a multi-agent federated reinforcement learning framework for collaborative robots in smart manufacturing. Their MARL-FL scheme integrates FL with RL and differential privacy: each robot (agent) trains locally on its data, then only encrypted model updates are shared. This preserves sensitive information (compliant with GDPR/CCPA) while enabling effective joint learning [5]. Their experiments in a simulated assembly task achieved ~91% accuracy with 41.5% less privacy leakage than a central approach. Similarly, [26] propose Federated Deep Reinforcement Learning (FDRL) for robotic-assisted surgery, using secure aggregation and homomorphic encryption to protect patient data. They reported a 60% reduction in privacy leakage compared to conventional methods [26]. These works show that FL/RL can give robots high-quality learning without pooling sensitive data into a single vulnerable repository.

Other machine learning privacy methods include differential privacy (DP). While not many robotics-specific DP implementations are published yet, DP techniques are mentioned as complementary. [5] suggests adding DP to FL updates to satisfy rigorous privacy guarantees. Another direction is multi-party computation and homomorphic encryption, enabling robots to run joint computations on encrypted data as in [6].

At the sensor level, innovative privacy-by-design concepts are emerging. [1] argue that some robotics vision tasks should avoid forming human-interpretable images altogether. They propose a novel hardware concept where analog optical processing generates “hashes” of the scene that are sufficient for robot vision tasks (for example. localization) but intractable to invert [1]. The underlying principle is “shift processing out of the digital domain” and maximize irreversible transformations. This preserves privacy because the robot never acquires raw images of people or environments. For example, their simulated robot could localize using privacy-preserving visual hashes with accuracy comparable to conventional SIFT-based methods [1]. Such work exemplifies how machine learning-aligned robotics design can ensure data never leaves the device unprotected.

Federated and encrypted learning methods are also applied to specific robotic services. For autonomous driving, one FL study addressed data privacy among vehicles, customizing FL to account for vehicle-specific data distributions. In robotics teleoperation, secure machine learning ensures that private telemetric streams are only shared in encoded form. The [7] authentication scheme mentioned earlier also uses machine learning-based biometric features in a multi-factor protocol to preserve user identity.

In summary, privacy-preserving machine learning enables collaborative autonomy without exposing raw data. By keeping training data local (FL) or encrypting it, robots can benefit from shared intelligence while respecting individual privacy [5]. Nonetheless, these methods trade off some performance and require additional overhead (for example. encryption costs, communication rounds). Designing efficient, low-power privacy protocols for resource-constrained robots is an active research area.

3.0 Case Studies and Domain Applications

i. Autonomous Vehicles (AVs): AVs are a flagship example of machine learning-driven autonomous systems. As noted earlier, AV cybersecurity surveys emphasize intrusion detection and anomaly detection using artificial intelligence [9]. [9] discuss adaptive machine learning-based IDS and blockchain for securing AV data. The stacked Long-Short Term Memory (LSTM) anomaly detector for CAVs (mentioned above) specifically targeted AV trajectories [27]. Other AV-focused work applies CNNs to detect spoofing in camera feeds or adversarial perturbations on road signs. Overall, machine learning aids AV security by continuously learning driving patterns and flagging deviations (for example. recognizing that sensor readings are inconsistent with physical reality).

ii. Unmmaned Aerial Vehicles (UAVs) and Swarm Robots: Drones/UAVs combine autonomy with mobility, making them susceptible to GPS spoofing and jamming. [11] via a machine learning approach) achieved >92% spoofing attack detection on UAVs. The "Threats to the Swarm" analysis by [14] highlighted potential coordinated swarm attacks, motivating machine learning-based defenses in swarm coordination. Machine learning is used to fuse multi-sensor drone data, enabling anomaly detectors that alert on control signal inconsistencies. Additionally, secure multi-agent RL is a direction where drones learn collaboratively under adversarial conditions.

iii. Industrial and Collaborative Robots: In smart factories, robots work alongside humans. Here, privacy concerns focus on human worker data (for example, gestures) and network security on the shop floor. Federated learning for human-robot collaboration as in the work of [5] directly addresses this. Machine Learning-based IDS for industrial control networks (often sharing protocols with robotics) are surveyed in [24]. Authenticated safety protocols (with Machine learning biometric checks) are also investigated for robots in public spaces.

iv. Healthcare and Surgical Robots: Medical robotics requires strict privacy. The FDRL surgical framework is a prime example of Machine learning security in healthcare robotics [26]. More generally, Machine learning helps in anomaly detection in medical robotic motion to ensure patient safety. Privacy-preserving data sharing (for example, federated learning on patient datasets) is an active area, though specific papers from 2021–2025 are still emerging.

v. Mobile and Service Robots: Robots in homes or public venues often have cameras and microphones, [26]. There is also work on encrypting audio streams or using on-device machine learning to process personal data without cloud uploads. Multi-factor authentication is aimed at secure access for delivery robots [7].

In each domain, the integration of machine learning with security/privacy measures is context-specific, but common themes emerge: learning-based detection, decentralized learning for privacy, and sensor-level data protection.

4.0 Machine Learning Techniques and Issues

Across the surveyed literature, a wide range of machine learning approaches are employed. Supervised learning (for example, CNNs, random forests) is popular for classifying attack types once labeled data is available [11]. Unsupervised learning (clustering, autoencoders) is used for anomaly detection where attack labels are unknown [27]. Deep learning (LSTM, CNN) handles complex data (sequences, images) to detect subtle anomalies [27]. Reinforcement learning appears both as a target (secure RL algorithms) and as a tool (RL controllers that are robust to attacks). For example, secure RL can adapt a robot's policy if an attack is detected mid-operation.

Adversarial machine learning is a growing focus: many researchers note the need to defend ML models themselves. Techniques like adversarial training, model distillation, and input sanitization are beginning to be applied. [7] specifically mention defending against FGSM/PGD adversarial examples in robotic authentication.

Resource constraints are also a challenge: embedded robots may not handle huge machine learning models or encryption computations. Several works suggest using lightweight models or offloading computation to edge servers, with secure channels. Federated approaches inherently distribute the computation, but at the cost of communication overhead. Emerging work on swarm federated reinforcement learning (RL) shows how clustering-based FL can reduce bandwidth [15].

Finally, regulatory requirements such as General Data Protection Regulation (GDPR), Central Consumer Protection (CCPA), and industry standards (for example, ISO 21434 for automotive) influence design. The reviewed works. Machine learning solutions often incorporate privacy-by-design principles such as data minimization (only exchanging model weights, not raw data) or deploying encryption [5].

In summary, a diverse machine learning toolkit is employed in securing autonomous systems. Supervised machine learning excels in recognizing known threats, unsupervised machine learning flags unknown anomalies, and federated/differentially-private machine learning protects data. However, all approaches must be carefully validated, as false positives in intrusion detection system (IDS) can disrupt operations, and missed detections can be catastrophic.

5.0 FINDINGS

First, methods based on machine learning have measurable benefit for security in autonomy. In studies, it is consistently shown that with machine learning, there are greater detection rates and lower false positives. [3] state that machine learning based NIDS significantly outperforms traditional rule-based IDS. The trajectory predictor based on LSTM for vehicles had R2 about 99.9%, which allows very accurate detection of anomalies [27]. These results have shown that learning from complex data patterns is very well-suited to the robotic domain.

Second, privacy-preserving machine learning is becoming practical. Federated frameworks indicate the fact that robots can collaboratively learn models without raw data sharing [5]. The cited studies show large reductions in the amount of privacy leaked (30% - 60%) while maintaining performance. This is important for compliance: rather than creating one central data lake (breeding a single point of breach), robots create ad-hoc learning networks. Methods such as differential privacy and secure aggregation further make these schemes more difficult, though they do come with utility trade-offs.

Third, new sensor designs for privacy are emerging. [1] prove that it is possible to make robotic vision inherently privacy-preserving. This "in-the-camera" approach, while still being experimental, constitutes a paradigm shift: privacy does not just need to be software-enforced, it could be built into the hardware. We expect to see more such multi-disciplinary approaches (optics, machine learning hardware) in the future.

Fourth, despite the gains, there are important challenges ahead. A recurring problem is data availability: real attack data sets for robots are scarce. Many studies are based on simulated attacks or use datasets that were re-used, possibly not reflecting field conditions. Machine learning methods work best when information about the processes of the system has already been studied and initial conditions determined - a luxury not always available [11]. Adversarial robustness is another problem. Robots are often used in safety-critical environments, so it is necessary for machine learning models to be resistant to adversarial inputs. Few reviewed works give this full treatment; most mention this as an open problem.

There are also issues of system-level integration. Security patches or machine learning model need to be updated over-the-air and security update mechanisms in robots are still immature. Autonomous systems tend to have long lifecycles (for example, cars, industrial arms); maintainable ML components are required. Moreover, interdisciplinary coordination is required: researchers in machine learning, engineers in robotics and experts in security must collaborate.

In terms of domain gaps, it was noted that little work is done in ethics or human factors. For example, trust in AI decisions, user consent on collecting data, and legal accountability are not really part of technical papers, but will affect adoption. Nonetheless, [8] begin to address these aspects, emphasising that privacy is not only a technical problem, but a social one.

6.0 CONCLUSION AND RECOMMENDATIONS

In this work, we have examined how machine learning is leveraged to secure autonomous systems and protect privacy. The reviewed literatures consistently show that machine learning can greatly enhance detection of cyber threats and enable new privacy-preserving architectures in robotics.

Machine Learning-based Intrusion Detection System (IDS) and anomaly detectors significantly improve security monitoring; federated and encrypted learning can allow collaborative robotics without centralized data exposure; and privacy-by-design sensors (for example. obfuscating vision streams) can prevent leaks before they happen. However, robust implementation requires overcoming data scarcity, adversarial risks, and integration challenges.

Based on the findings, the following are recommended

1. Adopting secure-by-design frameworks for robotics. This means incorporating machine learning-based security modules from the outset, not retrofitting them. Robot system architectures should include monitoring components that use machine learning to detect intrusions in real time.
2. Investing in federated and decentralized learning. Robot manufacturers and service providers should share model architectures and aggregated parameters rather than raw logs, enabling a community-wide machine learning improvement without sacrificing privacy.
3. Using standardized benchmarks and datasets. The community needs open, realistic datasets of robotic attacks and normal operations to train and evaluate machine learning models.
4. Considering regulation and ethics. Autonomous systems often collect personal data; thus compliance with privacy laws (GDPR, etc.) must be baked into design. Methods like anonymization and DP should be applied whenever possible.

In conclusion, machine learning is a powerful tool for advancing autonomous systems, but it must be used carefully. By integrating machine learning into security and privacy mechanisms, future robots and vehicles can be both intelligent and trustworthy. Continued research—especially in adversarial robustness, explainability of security models, and cross-domain standards—will be essential to ensure these systems benefit society safely.

REFERENCES

A. K. Taras, N. Suenderhaufb, P. Corkeb, D. G. Dansereau, “Inherently Privacy-Preserving Vision for Trustworthy Autonomous Systems: Needs and Solutions,” J. Responsible Tech., vol. 17, p. 100079, 2024, taras2024inherently.pdf

A. Botta, C. Rotbei, V. Zinno, and G. Ventre, “Cyber Security of Robots: A Comprehensive Survey,” J. Intell. Syst. Appl., vol. 18, 2023, DOI: 10.1016/j.iswa.2023.200237

1. R. Holdbrook, O. Odeyomi, S. Yi, and K. Roy, “Network-Based Intrusion Detection for Industrial and Robotics Systems: A Comprehensive Survey,” Electronics, vol. 13, no. 22, p. 4440, 2024, https://doi.org/10.3390/electronics13224440
2. N. Verma, N. Kumar, C. Verma, Z. Illés and D. Singh. Central Unive., “A Systematic Review on Cybersecurity of Robotic Systems: Vulnerabilities Trends, Threats, Attacks, Challenges, and Proposed Framework,” Int. J. Inf. Secur., vol. 24, no. 3, 2025,
3. M. Rahmati, “Federated Learning for Privacy-Preserving AI in Human–Robot Collaboration for Smart Manufacturing,” J. Intell. Manuf. Smart Equip., 2025, https://doi.org/10.1108/JIMSE-03-2025-0003
4. M. Hafeez, B. Qiu, and N. Mohammed, “Federated Deep Reinforcement Learning for Privacy-Preserving Robotic-Assisted Surgery,” https://doi.org/10.48550/arXiv. 2505.12153
5. Y. Yang, A. M. Pasikhani, P. Gope, B. Sikdar, “Privacy-Preserving Robotic-based Multi-factor Authentication Scheme for Secure Automated Delivery Systems,” 2024, https://doi.org/10.48550/arXiv.2411.18027
6. J. Rajamäki and J. Helin, “The Ethics and Cybersecurity of Artificial Intelligence and Robotics in Helping The Elderly to Manage at Home,” Information, vol. 15, no. 11, p. 729, 2024, https://doi.org/10.3390/info15110729

I. Durlik, T. Miller, E. Kostecka, Z. Zwierzewicz and A. Łobodzińska “Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge?,” Electronics, vol. 13, no. 13, p. 2654, 2024, https://doi.org/10.3390/electronics13132654

7. O.O. Adeola, B. K. Alese, A. E. Akinwonmi, O. Owolafe and V. I. Omoniyi, “Detection of Real-Time Anomalies in Network Environment Using Deep Learning”. Journal of Current Research and Studies. Vol. 2, no. 4, pp. 103-119, 2025, https://journalcurrentresearch.com/pub/jcr/article/view/49/42

8. E. Basan, A. Basan, A. Mushenko, A. Nekrasov, C. Fidge, A. Lesnikov, “Analysis of Attack Intensity on Autonomous Mobile Robots,” Robotics, vol. 13, no. 7, p. 101, 2024, DOI: https://doi.org/10.3390/robotics13070101
9. O.O. Adeola, B. K. Alese, A. E. Akinwonmi, O. Owolafe and V. I. Omoniyi “The Evolution of Malware Sandboxing and Artificial Intelligence for Smart Threat Detection”. International Journal of Advance Research Publication and Reviews. Vol. 2, no. 8, pp. 303 -31, 2025, https://ijarpr.com/uploads/V2ISSUE8/IJARPR0826.pdf
10. E. Dritsas and M. Trigka, “Machine learning for Blockchain and IoT Systems in Smart Cities: A Survey,” Future Internet, vol. 16, p. 324, 2024.
11. F. Higgins, A. Tinson, and K. Martin, “Threats to the Swarm: Modeling Attacks on UAV Swarms,” J. Intell. Robotic Sys., vol. 107, no. 1, pp. 329–344, 2021.
12. S. Na, T. Roucek, J. Ulrich, J. Pikman, T. Krajnik, B. Lennox and F. Arvin, “Federated Reinforcement Learning for Collective Navigation of Robotic Swarms,” IEEE Trans. Cogn. Dev. Syst., vol. 15, no. 4, pp. 2122–2131, 2023, https://doi.org/10.1109/tcds.2023.3239815
13. S. C. Nandakumar, D. Mitchell, M. S. Erden, D. Flynn and T. Lim “Anomaly Detection Methods in Autonomous Robotic Missions,” Sensors, vol. 24, no. 4, p. 1330, 2024, https://doi.org/10.3390/s24041330
14. R. Noorian et al., “Secure Multi-Agent Reinforcement Learning for Autonomous Robotics,” Autonomous Robots, 2023.
15. J. Liu and P. Zhao, “Blockchain-Based Security in IoT-Enabled Robotic Systems,” IEEE Trans. Ind. Informatics, 2022.
16. Y. Chen et al., “Federated Perception for Privacy in Autonomous Vehicles,” IEEE Trans. Vehicular Technology, 2025.
17. X. Zhang and L. Qian, “Differential Privacy for Federated Learning in Autonomous Driving,” IEEE Internet Things J., 2024.

A. Khan, “Adversarial Machine learning in Cyber-Physical Robotic Systems,” IEEE Trans. Neural Netw. Learn. Syst., 2024.

18. R. Kumar and S. Patel, “Machine learning for Intrusion Detection in Industrial Robot Networks,” IEEE Access, 2023.
19. P. Müller, “Secure and Privacy-Preserving Localization for Edge-Assisted Robotic Navigation,” in IEEE/RSJ IROS, 2022.
20. H. Singh and M. Johansson, “Privacy-Preserving Deep Learning in Autonomous Service Robots,” Robotics and Autonomous Systems, 2023.

21. O. Verma, A. Rodriguez, "Deep Learning based Secure Object Detection in Autonomous Vehicles," in Proc. IEEE ITSC, 2022.
22. S. Hafeez, S. R. Mulkana, M. A. Imran and M. Sevegnani, "Federated Deep Reinforcement Learning for Privacy-Preserving Robotic-Assisted Surgery", https://arxiv.org/pdf/2505.12153
23. P. K. R. Lebaku, L. Gao, Y. Zhang, Z. Li, Y. Liu and T. Arafin, "Cybersecurity-Focused Anomaly Detection in Connected Autonomous Vehicles Using Machine Learning", https://arxiv.org/htmachine learning/2506.22984v1
24. O. O. Adeola, G. R. Bello, B. S. Oluwasola and K. R. Lateef, "Development of a Fake News Detection Model Using Decision Tree Algorithm", Advances in Multidisciplinary & Scientific Research Journal Publication, vol. 2, no. 2, pp. 81-88, 2023, DOI: 10.22624/AIMS/CSEAN-SMART2023P10