AUTONOMOUS YET VULNERABLE: DATA SECURITY, PRIVACY AND ETHICAL CHALLENGES IN AUTONOMOUS SYSTEMS

Vrushank CJ, K.L.E. Society's Law college, Bangalore

ABSTRACT

Artificial intelligence (AI) is fast evolving, and everyone is accustomed to it. large manufacturers are investing billions of dollars to manufacture Autonomous vehicles and Drones. Autonomous vehicles are a growing trend in U.S domestic market and drones are being used almost in every corner of the world and these drones can be warfare ready too i.e. Unmanned Aerial Vehicle (UAV) which has become an efficient tool in defense and disaster response. Autonomous vehicles have more benefits providing safety, traffic optimization and fuel efficient.

However, this transformation in technology involves greater risks in privacy and data security, as these machines are based on real-time data processing and self-learning AI mechanism. Autonomous vehicles are based on LIDAR, high resolution cameras and self-learning AI algorithm which dynamically changes based on location, behavioral patterns and real time data. This flexibility may lead to unauthorized access to private data, data harvesting and raises other security concerns. The capability and adaptable nature of such AI driven machines raises a challenge to bring in advanced security frameworks ensuring data protection and public trust.

This research paper examines privacy concerns in three key areas: (1) Unauthorized surveillance and data harvesting by drones and autonomous vehicles, (2) (V2X) vehicle to everything vulnerabilities in wireless data connectivity, (3) Usage of AI in high data-sensitive areas. The goal is to provide more transparency and protection of private data by being accountable to users on how the data is being collected and where it is being applied. We can overcome these complications by having legal and ethical frameworks, also by providing a well secured experience to users with full autonomy.

Introduction:

Artificial Intelligence is stimulating technological innovation, transforming industries from transportation to surveillance. Autonomous vehicles (AVs) and drones are at the forefront of technological progress. According to *Research and markets* report, the global autonomous vehicle market is predicted to develop at compound annual growth rate (CAGR) of 21.9% and reach USD 214.32 billion by 2030[1]. The technologies which include artificial intelligence (AI), sensors and real-time data processing, provide fine efficiency and functionality. For instance, Tesla's neural network to monitor road conditions and Amazon's drone delivery program optimizes operation with even little human interaction.

As autonomous vehicles and drones become more intelligent and adapt to the changing environment, it becomes more efficient. However, this technological progress may give rise to security threats and risk pertaining to private data as they collect vast data such as location data, environmental visuals and different behavioral patterns. In July 2015, Charlie Miller and Chris Valasek at Black Hat USA demonstrated hacking a Jeep Cherokee SUV which was 18 kilometers away. They were able to hack into the vehicle's computer which is primarily known as ECU (Electronic control unit) and control vehicle speed and direction. This incident led to recall of 1.4 million vehicles for software security update across USA[2]. Whereas drones have potential advantage over commercial helicopters when it comes to cost and budget. However, drones are not only limited to such tasks, but they can also be used for military surveillance, border security and rescue operations. In fact, drones can carry armed explosives and pose a threat to the target by bombing or self-detonation due to its stealth capabilities. Privacy, safety and security are the key components required for Internet of things (IoT) technology, which helps in adopting strict legal compliances to prevent illegal or unauthorized operation of drones.

The societal impact of this progress is complex. Therefore, this paper analyzes security and privacy issues in autonomous vehicles and drones, in three different key areas i.e. Unauthorized

[1] *Autonomous vehicle market by autonomy level, powertrain type, components and supporting technologies,* Research and markets, (May. 25, 2025, 9:00 PM), https://www.researchandmarkets.com/report/autonomous-vehicles?utm_source=GNE&utm_medium=PressRelease&utm_code=tn3hcb&utm_campaign=1927494+-+Autonomous+Vehicle+Market+Projected+to+Reach+%24214.32+Billion+by+2030+with+North+America+Taking+the+Lead%3a+Comprehensive+Global+Industry+Analysis+Report&utm_exec=jocamsai

[2] Andy Greenberg, *Hackers remotely kill a jeep on the highway-with me in it*, Wired, (May.26, 2025, 7:55 PM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

surveillance and data harvesting by drones, Vehicle to everything (V2X) vulnerabilities in autonomous vehicles and usage of AI in high data sensitive areas. By analyzing the existing gaps and required actionable solutions, the paper aims to contribute to the ongoing debate on creating safer, user-friendly and privacy-respecting technological solutions.

Understanding autonomous systems:

This section of the paper describes architecture of autonomous vehicles and drones, data dependency of autonomous systems and importance of security in data utilization.

➢ **Architecture of autonomous vehicles and drones:**

Autonomous vehicles rely upon complex hardware and software which operates independently. These systems use:

- RADAR: Radio Detection and Ranging

  RADAR in autonomous vehicles are used to scan the surroundings and detect the presence of other vehicles and objects. This sensor emits laser beams which can detect objects ranging from 5m to 200m. The radars have anti-blocking and anti-pollution feature, which is helpful during extreme conditions like rain, fog and low-light situations[3].

- LIDAR: Light Detection and Ranging

  LIDAR uses single beam laser which is mounted on top of the car and rotates as the speed of the car increases by emitting beams. Laser beams reflect from obstacles and emit back to the device which helps to calculate the distance, depth and shape of the obstacle. LIDAR play a vital role in providing safety and reliability for Advanced Driver Assistance System (ADAS) and autonomous driving systems. LIDAR has the characteristic of having night-vision, long-range object recognition

[3] Igal Bilik, Oren Longman, Shahar Villeval and Joseph Tabrikian, *The rise of radars for autonomous vehicles,* IEEE Signal processing magazine, (May. 27, 2025, 1:05 PM), https://forms1.ieee.org/rs/682-UPB-550/images/The%20Rise%20of%20Radar%20for%20Autonomous%20Vehicles.pdf

and wide field of view (FOV) cameras to measure the distance precisely[4].

- Vehicle to everything communication (V2X):

V2X communication technology enable autonomous vehicles to interact with other vehicles, infrastructure and external systems. This technology builds foundation to improve road safety, optimize traffic management and enable smart mobility in urban areas. For instance, Vehicle-to-Vehicle (V2V) system shares technical data like speed of the vehicle and braking system to prevent collisions. Vehicle-to-pedestrian (V2P) system detects pedestrian carrying smartphones and analyzes behavioral pattern of the pedestrian. Vehicle-to-infrastructure (V2I) system recognizes the pattern of traffic signals and other road signs[5].

Drones, or Unmanned aerial vehicle (UAV) share similar characteristic like autonomous vehicles but with different operating modules, like:

- Flight controller unit:

Flight controller unit is considered as the drone's central processing unit (CPU). The onboard processor integrates data from sensors, process data from Ground control station (GCS) and ensures real-time environmental condition to perform the task by following the flight path. Modern flight controllers also use AI to unlock functionalities like autonomous navigation, real-time obstacle detector and object tracking. `

- Ground Control Station (GCS):

GCS serves as the operational unit, providing accessibility to operate and monitor the drone remotely. It consists of On-Land facility (OLF), which varies in difficulty based on size, type and mission. For small drones, GCS are often handheld, or software based on tablets or smartphone. For military grade drones/UAVs, GCS is more sophisticated with multiple console and user

[4] Saad ul Hassan, Lidar sensors in autonomous vehicles, Researchgate, (May. 27, 2025, 1:25 PM), https://www.researchgate.net/publication/359263639_Lidar_Sensor_in_Autonomous_Vehicles
[5] Jacob Biba, *what is Vehicle-to-everything technology,* Builtin, (May.27, 2025, 2:58 PM), https://builtin.com/articles/v2x-vehicle-to-everything

interfaces, providing unmatched efficiency in real-time data analysis, live video streaming and aerial route configurations.

- Communication Datalink (CDL):

  Communication Datalink is the backbone of drone operations, providing seamless data transfer between the drone and GCS. This wireless communication controls the flow of commands, telemetry data and payload information. It is based on two different operational range:

  1) Visual Line-of-sight (VLOS) distance: This relies on direct radio waves for transmitting control signals from drone and GCS. This method is used in short-range commercial drones, as it ensures reliable connection without any additional features.

  2) Beyond Visual Line-of-sight (BVLOS) distance: This method is used for long-range missions, BVLOS rely on satellite-based communication to maintain connectivity for long-distance delivery, rescue missions, disaster response or surveillance in remote areas[6].

Privacy and security challenges:

Autonomous systems depend on more than a dozen sensors and cameras placed around the body of autonomous vehicles and drones, to detect traffic signs, pedestrians, vehicles and other objects. Some of the challenges regarding privacy and security includes:

- Unauthorized surveillance: Drones are used for surveillance purpose, often disrupting the gap between security and privacy violations. Moreover, there should be a strict approach in limiting the drone's ability to capture pictures and videos without any authorized permission. Drones can be armed with explosives and harmful chemicals to carry out attack on innocent people or critical infrastructure. In 2023, A drone disrupted the operations of Kempegowda International airport in Bengaluru, as the drone was

[6] Jean-paul Yaccoub, Hassan Noura, Security analysis of drone's systems: attacks, limitations and recommendations, (May.27, 2025, 3:58), https://www.sciencedirect.com/science/article/pii/S2542660519302112?ref=pdf_download&fr=RR-2&rr=8e8b8b6eec2eb297#abs0001

found flying too close to the aircraft filled with passengers. The pilots alerted the Air Traffic Controller tower and immediate investigation was taken right away by airport authorities[7]

- Vulnerabilities in communication protocols: The communication pattern is integral in drones and autonomous vehicles but are also a main issue of vulnerability. V2X communication allows autonomous vehicles to share data with other vehicles, infrastructure, and pedestrians. However, with weak encryption in the system will leave them exposed for hacking and data theft.

  The Black Hat Jeep Cherokee incident[8] is the prime example, where hackers demonstrated remotely gaining access to vehicle's data, controlling its steering and braking through a weak encryption in Uconnect car software. This incident raised alarms to develop a robust authentication and encryption to protect communication systems. Similarly, drones are known for vital threat to information security as they are prone to spoofing, data interference and interception, manipulation and Wi-Fi communication jamming issues.

- Ethical concerns in AI decision making: AI decision making in autonomous vehicles and drones raises a significant ethical challenge where it involves human lives or privacy. An ethical dilemma known as "Trolley problem", where autonomous systems must choose between two outcomes, such as saving passengers at the cost of pedestrian safety or vice versa[9]. These dilemmas indicate difficulty in programming ethical decision-making into the system, which includes societal values and moral judgement which vary widely. Whereas Drones rely on AI for surveillance which may misidentify individuals or targets which makes it difficult to hold these systems accountable when errors or harm occur, this is commonly known as "Black Box problem". These concerns reinforce the need for ethical consideration in AI development, including diverse

[7] Petlee Peter, *In Bengaluru, drones fly dangerously close to 2 indigo planes*, Times of India, (May.27, 2025, 9:27 PM), https://timesofindia.indiatimes.com/city/bengaluru/in-bengaluru-drone-flies-dangerously-close-to-2-indigo-planes-probe-on/articleshow/104030546.cms

[8] Andy Greenberg, *Hackers remotely kill a jeep on the highway-with me in it*, Wired, (May.26, 2025, 7:55 PM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[9] Lee kai-fu, *AI's trolley problem can lead us to surprising conclusions*, World Economic Forum, (May.28, 2025, 7:18 PM), https://www.weforum.org/stories/2022/05/ai-s-trolley-problem-debate-can-lead-us-to-surprising-conclusions/

datasets, transparent algorithms and accountability mechanisms to ensure public trust and safety.

Recommendations:

Addressing the difficulties of Autonomous vehicles (AV) and drones require a multidimensional approach that includes technological developments, legal reforms, and ethical behaviors. On the technological part, better encryption methods, such as quantum-resistance cryptography can protect systems like Vehicle-to-everything (V2X) communications. Blockchain technology is an appropriate choice for maintaining data integrity, providing stable operational records, and improving transparency. Privacy-preserving AI techniques, such as federated learning, allow data processing to take place locally on private devices rather than centralized servers, minimizing the risk of data breach and improving user privacy.

Regulatory reforms must prioritize worldwide standardization to create a consistent framework for manufacturers and operators. This includes establishing comprehensive data protection laws that addresses the specific challenges faced by autonomous vehicles and drones, such as collection and processing of location and biometric data. Policy makers must regulate security audits, Data reduction policies and stringent penalties for non-compliance. Establishing international agreements can make cross-border data sharing easier while protecting security and privacy.

Transparency, fairness and accountability are all essential components of ethical practices. Companies should implement clear consent mechanisms, allowing users to know about how their data is being collected and used. Algorithms must be made transparent to address the "Black box" problem and establish accountability regarding AI-driven decisions.

An Overview of autonomous systems in India:

India is a fast-developing country with diverse socio-economic background, holds enormous opportunity for the adoption of autonomous vehicles and drones. These technologies have the potential to transform key sectors like agriculture, logistics and urban mobility by increasing efficiency, scalability and innovation. However, implementing them involves distinct problems, particularly in infrastructure, legal and public acceptance. To accomplish its full

potential, a careful balance of innovation and governance is required and this includes consideration of privacy, security and societal concerns.

1) Regulatory landscape in India: India has made amazing progress, but it is still in the early stages of tackling autonomous system technology. The drone rules of 2021[10] simplified the procedure of purchasing and operating the drones, encouraging innovation in both commercial and recreational use. The guidelines established classification based on weight, ranging from nano (<250g) to big (>25kg), and encouraged use of Digital sky platform for registration and clearance purpose. Key features were introduced like No permission, No takeoff (NPNT) ensure that drones can operate with proper authorization, limiting unauthorized usage and improved airspace security. However, these regulations are still under development with limited focus on long-term problems like cybersecurity and data protection. Long distance operations of drones are limited by connectivity issues in rural and remote regions. While 5g networks promise enhanced connectivity, due to lack of consistent internet access hampers the usage of drones to their full potential. While urban areas offer better connectivity, pose challenges such as high human population which may lead to accidents and privacy violations.

2) Emerging opportunities in India: Despite facing challenges, India still offers significant opportunities for autonomous vehicles and drones, particularly in such sectors which yield high economic benefit:

    - Agriculture: Drones integrated with sensors and cameras are transforming Indian agriculture by precise farming. They keep track of crop health, optimize pesticide spraying and survey the farmland quickly and efficiently. State Governments, including Maharashtra and Karnataka are testing drone program to increase productivity and reduce costs.

    - Logistics and E-commerce: India's booming e-commerce platforms such as Amazon, Flipkart and Zomato, is looking forward to implementing drone delivery program to overcome logistics cost and save time. Drones have the potential to

[10] Ministry of civil aviation, *The drone rules, 2021,* Ministry of information and broadcasting GOI, (May.28, 2025, 8:24 PM), https://static.pib.gov.in/writereaddata/specificdocs/documents/2022/jan/doc202212810701.pdf

transform the logistics chain by reducing delivery time and cost, especially in the countries with poor road infrastructure.

- Disaster management: Drones have been used in natural disasters like Kerala floods, to survey affected areas, deliver medical kit and locate the survivors. They are well equipped with infrared thermal detection cameras, they play an important role in search and rescue operations, particularly in those areas where rescue crews cannot reach.

3) Policy recommendations for India: To realize the potential of autonomous vehicles and drones addressing the problems, India must develop comprehensive policies and initiatives. A dedicated autonomous system framework is needed to set clear criteria for testing, deployment, and liability. By considering accidents involving autonomous vehicles, such as assigning determined insurance claims, the framework ensures legal clarity and encourage manufacturers to invest in Indian market. Simultaneously, the 'Personal Data Protection Bill' must be facilitated to secure data collected by autonomous vehicles and drones. Furthermore, Infrastructure development is crucial for seamless operation of autonomous systems. Investment in infrastructure development must be encouraged, for instance: connected traffic lights, geofencing and reliable 5g networks, would enhance the working of Vehicle-to-everything(V2X) communications. Together, these policies and initiatives offer an established path for promoting autonomous technology into India's socio-economic infrastructure, assuring long-term growth and global competitiveness.

Conclusion:

The introduction of Autonomous vehicles (AV) and Drones represents an important chapter in technical innovation, with the potential to transform industries, enhance efficiency and improve quality of life. These technologies have the potential to transform a variety of industries including transportation, logistics, agriculture, rescue operations and urban planning. However, by implementing them in the society comes with numerous challenges, particularly in terms of privacy, security and regulatory control.

One of the most serious concerns is the privacy and security acquired by autonomous vehicles and drones. These systems significantly rely on Real-time data, location tracking, user behavior

patterns and environmental scanning, making them subject to hacking and abuse. Incidents like Jeep Cherokee hack and unlawful drone monitoring highlights dangers posed by inadequate safety measures. Cyberattacks on Autonomous systems and drones may jeopardize safety due to weak encryption; this calls for an urgent need for robust regulatory frameworks that address these vulnerabilities, particularly in growing technological market.

India, provides a unique insight for the adoption of autonomous vehicles and drones, with its diverse landscape, complex traffic system and growing demand for new solutions, the country is at stake of new opportunities and challenges. While the Government has taken step to standardize drone operations with the drone rules 2021, a different framework for autonomous vehicles remains undiscovered. Without appropriate criteria for testing, development and liability, the adoption to change remains stagnant. Addressing these gaps through policies such as Personal Data Protection Bill and development of smart infrastructure, will be essential to unlock the potential of these technologies.

To address the concerns, including "Black box" and "Trolley problem", developers must prioritize fairness, inclusivity and transparency in AI algorithm. Furthermore, public education and awareness are vital for building public trust and acceptance, ensuring they are informed about benefits, risks and safety measures associated with Autonomous vehicles and drones.

Collaboration with Government, industrialists, technologists and ethicists would bring out more innovative solutions, enforce robust regulatory standards and promote ethical practices. India's path in this arena has the ability to reshape its worldwide technology by establishing standards in developing 5g connectivity, AI driven systems and data encryption frameworks, this approach not only promises to use autonomous vehicles and drones for long-term growth, but an opportunity to establish itself as a global leader in autonomous technological innovation. In doing so, India can demonstrate how emerging economies can use cutting-edge technologies by preserving privacy, security and data inclusivity.