Artificial Intelligence (AI) is transforming the technology landscape. What is understood to be "**inventive**" is changing as AI systems move from experimental algorithms to important infrastructure in data security, autonomous mobility, and healthcare industries. This article studies two recent Indian patent applications that mark important developments in computer science domain. These applications tackle the **lack of high-quality training data** and **data privacy in real-time object detection**, two of the most important bottlenecks in contemporary AI deployment.

The first of these applications is "System and Method for Privacy-Preserving Object Detection Using Federated YOLOv8 in Connected and Autonomous Vehicles" which proposes a decentralized approach to machine learning. It addresses the privacy risks inherent in cloud-based processing for autonomous vehicles and smart wheelchairs. The second application is titled as "Generative AI for Synthetic Data Generation in Machine Learning Models" tackles the issue of data scarcity and bias by utilizing Generative Adversarial Networks (GANs) to create robust synthetic datasets. Both inventions highlight the increasing sophistication of Indian innovation in the AI sector and underscore the critical role of **Intellectual Property (IP) protection** in securing algorithmic methodologies.

Patent Application 1

“Privacy-Preserving Object Detection in Autonomous Systems”

Application Details-

- **Title:** System and Method for Privacy-Preserving Object Detection Using Federated YOLOv8 in Connected and Autonomous Vehicles
- **Application Number:** 202531105457
- **Applicant:** Indian Institute of Technology (Indian School of Mines), Dhanbad

Understanding the Invention- The core objective of this invention is to enable real-time object detection in Connected and Autonomous Vehicles (CAVs) and assistive mobility systems, specifically smart wheelchairs, **without compromising user privacy**. Traditional object detection systems in autonomous vehicles often depends on a centralized architecture where raw sensory data (images and videos) is transmitted to a central server for processing. This approach poses significant privacy risks, as the raw data often contains sensitive information such as facial images, license plates, and location data, which risks privacy of data provider’s.

The inventors suggest a **Federated Learning** (FL)-based framework to reduce these risks. The system utilizes a client-server architecture where the "clients" are the edge devices—specifically, the GPU modules (such as NVIDIA Jetson Nano) embedded in smart wheelchairs or vehicles. The "server" acts as a central aggregator.

Technical Elements The technical novelty of this invention lies in the integration of the **YOLOv8 (You Only Look Once, version 8)** deep vision model with a federated learning infrastructure.

1. **Local Training on Edge Devices:** Unlike traditional systems, the raw sensor data never leaves the client device (the wheelchair or vehicle). The YOLOv8 model is trained locally on the device using its specific environment data.
2. **Model Weight Transmission:** Instead of sharing raw images, the devices transmit only the updated "model weights" (mathematical parameters representing what the model has learned) to the central server. This is done via secure channels like HTTPS or 5G-V2X.
3. **Federated Averaging (FedAvg):** The central server aggregates these weights using the FedAvg algorithm to create a refined global model. This global model is then sent back to the devices.
4. **Handling Non-IID Data:** A significant technical achievement claimed is the system's ability to handle "non-identically distributed" (non-IID) data. Real-world environments vary wildly; the data seen by a wheelchair in a hospital differs from one on a street. The invention demonstrates that this federated approach achieves a high mean Average Precision (mAP) of **80.3%**, outperforming centralized benchmarks while maintaining privacy.

IP Protection's Significance Because this invention asserts a particular system architecture and methodology, patent protection is important. The patent safeguards the novel application of Federated Learning and the YOLOv8 algorithm to edge devices with limited resources, such as smart wheelchairs. The applicant keeps rivals from copying this privacy-preserving architecture in the cutthroat market for autonomous mobility aids by protecting this intellectual property. It turns a theoretical idea in computer science into a tangible asset with direct commercial use in improving disabled users' privacy and safety.

Patent Application 2: Generative AI for Synthetic Data Creation

Application Details

- **Title:** Generative AI for Synthetic Data Generation in Machine Learning Models
- **Application Number:** 202541095529
- **Applicant:** J.J. College of Engineering and Technology

Understanding the Invention- The second patent application goes through a fundamental issue in the development of robust Machine Learning (ML) models: **data scarcity**. High-quality, diverse datasets are the fuel for AI, but obtaining them is often difficult due to privacy regulations (like GDPR), high costs, or the rarity of specific events (e.g., rare disease data or extreme driving scenarios). This invention introduces a system using Generative AI to manufacture "synthetic data" that statistically mirrors real-world data without containing any personally identifiable information (PII).

Technical Elements The invention relies on two advanced generative architectures: **Generative Adversarial Networks (GANs)** and **Variational Autoencoders (VAEs)**.

1. **Adversarial Training (GANs):** The specification describes a "game-like" training process involving two neural networks: a *Generator* and a *Discriminator*. The Generator creates synthetic data samples, while the Discriminator find them against real data. Through iterative adversarial training, the Generator improves until the synthetic data is indistinguishable from real data in terms of statistical distribution.
2. **Latent Space Mapping (VAEs):** The invention also employs VAEs to map high-dimensional real data into a lower-dimensional "latent space." New data points can be generated by sampling from this space and decoding them. This is particularly effective for complex data types like images or time-series data.
3. **Bias Reduction:** A key technical feature is the ability to augment underrepresented classes. If a dataset is biased (e.g., lacking data from a specific demographic), this system can generate specific synthetic samples to balance the dataset, leading to fairer AI models.

Relevance of IP Protection The process of creating data to train other models is the main focus of IP protection. The capacity to train models on privacy-compliant synthetic data is a huge commercial advantage as AI regulations tighten globally. This patent describes how GANs and VAEs are specifically used to enhance real datasets in order to eliminate bias and privacy issues. By obtaining patent rights over this data generation pipeline, the applicant can license the technology to sectors like healthcare and finance that handle sensitive data, giving them a distinct competitive advantage over organizations that depend on costly manual data collection.

Conclusion

The two patent applications studied in this article shows the maturing landscape of Indian innovation in Artificial Intelligence. They evolved beyond simple software applications to address foundational challenges in AI infrastructure: privacy and data availability.

The "Federated YOLOv8" patent represents a shift towards **Edge AI**, recognizing that for autonomous systems to be safe and accepted, they must process data locally and respect user privacy. It effectively utilizes the patent system to protect a specific hardware-software architecture. Meanwhile, the "Generative AI for Synthetic Data" patent represents the **Data-Centric AI** movement, acknowledging that the future of model performance lies not just in better algorithms, but in better, unbiased, and privacy-compliant data.

When taken as a whole, these applications show how important intellectual property protection is to contemporary computer science. It encourages researchers to take on challenging ethical and technical issues like privacy and bias by providing the legal framework required to monetize complex algorithmic innovations. The leaders of the upcoming technological era will be determined by how technical creativity and intellectual property strategy interact as AI develops.