AI-Based Aadhaar Fraud Detection: Overview, Steps, Challenges, and Impact

The AI-based Aadhaar fraud detection project leverages advanced technologies to automate the verification of Aadhaar cards, ensuring security and authenticity. It addresses the increasing misuse of Aadhaar-linked services by identifying tampered, fake, or duplicate IDs, reducing manual errors and enhancing trust in identity verification processes.

Steps Involved

1. **Data Cleaning**: Raw image data is preprocessed by resizing, normalizing, and enhancing quality to improve detection accuracy.
2. **Data Classification**: The system classifies images into Aadhaar or non-Aadhaar categories to streamline further processing.
3. **Detection**: YOLOv11 is used to detect tampered regions, such as altered text, fake overlays, or mismatched fields.
4. **OCR**: Extracts text from Aadhaar cards for detailed analysis, such as verifying names, addresses, or unique numbers.
5. **Matching Scoring Logic**: Verifies extracted data against a reference database to determine authenticity.
6. **Frontend & Backend Integration**: A user-friendly interface enables file uploads and displays fraud detection results, while the backend processes the data.

Challenges

- Handling poor-quality images.
- Managing diverse Aadhaar formats.
- Ensuring real-time detection without compromising accuracy.

Tech Stack

- **YOLOv11**: For object detection.
- **OCR (EasyOCR)**: For text extraction.
- **Flask**: Backend development.
- **HTML/CSS/JS**: Frontend.
- **TensorFlow**: Deep learning models.

Impact:

This project automates fraud detection, preventing misuse of Aadhaar-linked services in banking, subsidies, and government schemes, fostering trust and reducing fraud significantly.