AI-DRIVEN FORGERY OF AADHAAR AND PAN CARDS

ADVISORY REPORT

2025

CCCMH_CA_2025_02

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The rapid growth of Artificial Intelligence (AI) has introduced new risks to digital and document security.

A major concern is the use of AI to create fake government identity cards, like Aadhaar and PAN Cards, for activities such as identity theft, financial fraud, and unauthorized access.

This advisory sheds light on the misuse of AI in crafting highly convincing fake identities that can evade preliminary verification mechanisms. It addresses the ramifications of such acts, which jeopardize national security, undermine public trust, and destabilize financial frameworks. Furthermore, it provides insights into how these forgeries are produced, methods to identify counterfeit IDs, potential legal repercussions, and available verification tools.

Src: x.com/RisingPiku
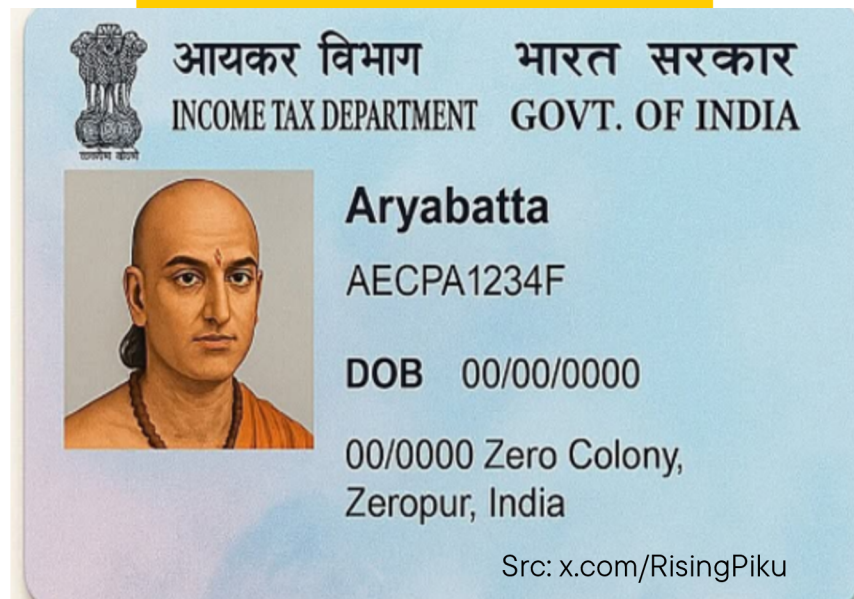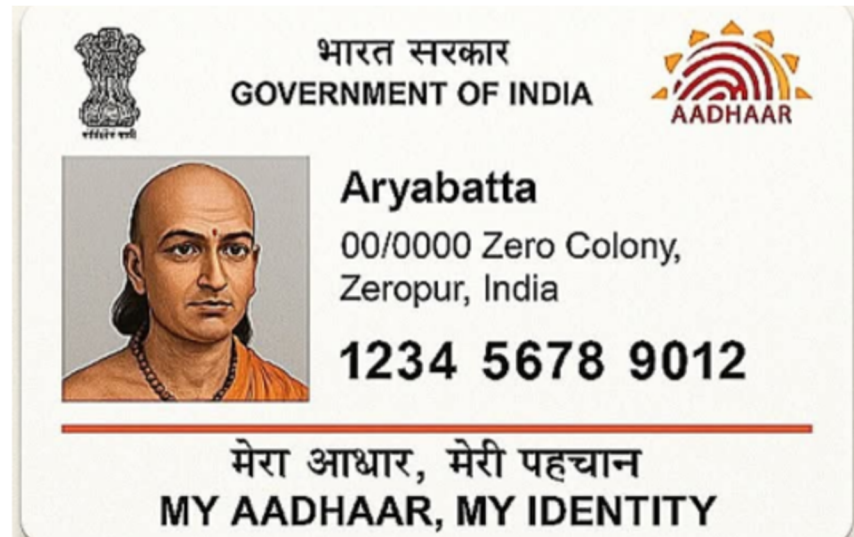
INTRODUCTION

In the digital era, Artificial Intelligence (AI) has emerged as a powerful tool with the potential to transform various sectors. However, alongside its benefits, AI is increasingly being exploited for unlawful activities. One alarming trend is the use of AI-based technologies to forge critical identity documents such as Aadhaar Cards and Permanent Account Number (PAN) Cards—both essential for identity verification and access to financial and government services in India.

Src: moneylife.in

These AI-generated forgeries are becoming more sophisticated, making it difficult to distinguish fake documents from genuine ones with the naked eye. The misuse of such forged IDs can lead to serious consequences, including financial fraud, identity theft, and unauthorized access to sensitive systems.

This issue not only threatens individual privacy but also poses a wider risk to national security and public trust in digital systems.

This document aims to raise awareness about the methods, implications, and preventive strategies related to AI-driven identity forgery, while also highlighting the importance of verification and legal action to counter such threats.

Advanced Forgery Techniques

AI tools enable criminals to create fake IDs using deepfakes, template editing, and spoofed QR codes that look real but fail official verification

Financial Fraud

Fake documents are exploited for financial crimes such as opening accounts, securing loans, bypassing KYC checks, and laundering money.

Identity Theft & Privacy Violation

AI-generated or stolen personal data is used for identity theft, cybercrimes, and illegally claiming government benefits.

THREAT LANDSCAPE

ID THEFT

Criminal Activities

Financial Impact

Legal Implications
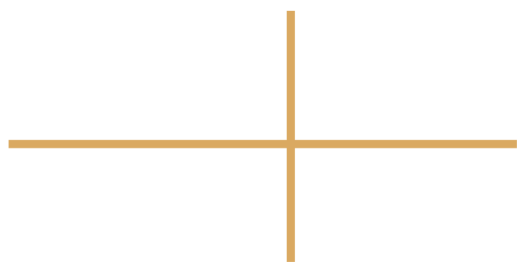
AI-Based Photo Replacement

Using deepfake image tools, photos on Aadhaar or PAN cards can be altered, enabling identity theft when paired with authentic card numbers and forged names.

QR Code Manipulation

AI tools, combined with Python libraries like qrcode and segno, can generate fake QR codes that appear genuine, leading to manipulated data or counterfeit UIDAI websites, risking verification processes and deceiving officials

IMPACT

The misuse of advanced AI tools has enabled the creation of highly convincing fake Aadhaar and PAN cards, posing serious threats to individuals, financial institutions, and national security. As traditional verification methods struggle to detect such forgeries, there is a pressing need for robust regulatory measures and AI-proof authentication systems.

Impacts of AI-Driven Forgery of Aadhaar and PAN Cards

1. PERSONAL & FINANCIAL HARM

Fake IDs lead to identity theft, financial fraud and emotional distress for individuals.

2. INSTITUTIONAL & GOVERNMENT SYSTEM MISUSE

Banks, service providers, and government schemes are exploited through fraudulent accounts, loan scams, and illegal subsidy claims.

3. CYBERSECURITY & NATIONAL THREATS

AI-generated IDs are used to commit cybercrimes, evade law enforcement, and support illegal or terrorist activities.

RECOMMENDATIONS

API-Based Document Verification
Always use UIDAI/NSDL official APIs to verify Aadhaar & PAN details. Avoid relying on static images or scans- validate QR codes and digital signatures in real time.

AI & Deepfake Detection
Deploy AI tools trained to detect synthetic images, font mismatches or GAN noise in forged IDs. Use facial recognition with liveness detection to prevent photo or video deepfakes.

Multi-Factor & Biometric Authentication
Combine OTP, biometrics and facial recognition during onboarding or eKYC, Implementation, liveness tests to prevent spoofing with AI-generated faces.

Portal & Bot Protection
Secure form with CAPTCHA, rate limiting and behavior- based bot detection. Monitor for bulk fake identify creation or AI-driven submissions.

Training & Legal Enforcement
Train bank staff, telecoms and police to spot AI-based identity forgeries.

India Today

- https://www.indiatoday.in/india/story/chatgpt-made-fake-aadhaar-pan-voter-ids-raise-forgery-concerns-2704189-2025-04-04?utm_source=chatgpt.com

Money Control

- https://www.moneycontrol.com/news/india/chatgpt-can-now-generate-fake-aadhaar-pan-cards-a-new-cybercrime-concern-12985641.html?utm_source=chatgpt.com

The Indian Express

- https://indianexpress.com/article/technology/artificial-intelligence/chatgpt-can-generate-fake-aadhaar-pan-cards-why-not-to-worry-9925025/?utm_source=chatgpt.com

The Economic Times

- https://economictimes.indiatimes.com/wealth/save/chatgpt-for-fake-aadhaar-and-pan-the-artificial-intelligence-tool-can-be-misused-to-generate-photorealistic-fake-ids/articleshow/119979257.cms

🚨 REPORTING HELPLINES

Want to report Cyber Crime

- Website: https://www.mhcyber.gov.in
- Helpline: 📞 1945 (24x7 Cyber Fraud Helpline)