DSCI
PROMOTING DATA PROTECTION

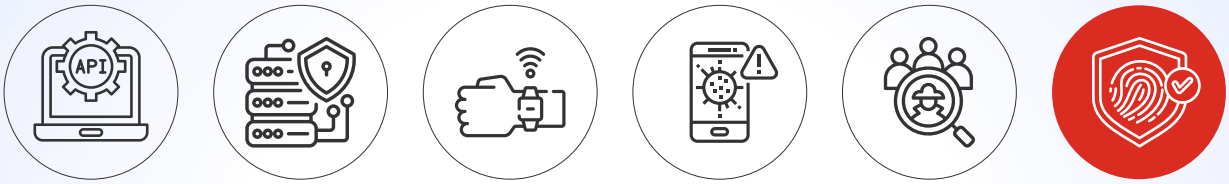
Ministry of Electronics & Information Technology
Government of India
सत्यमेव जयते

CYBERSECURITY GRAND CHALLENGE 2.0
INNOVATE TO SECURE

Promoting Cyber Security Entrepreneurship in India

06

Securing Next-Generation Biometric Systems



Securing Next-Generation Biometric Systems

PROBLEM STATEMENT

Defending against vectors targeting next-generation biometric identification and authentication systems that withstand AI-powered threats.

BUSINESS CONTEXT

Biometric systems, driven by advancements in AI and machine learning, have evolved into robust tools for secure, efficient, and user-friendly authentication. Future systems will integrate multi-modal biometrics, edge computing, and real-time analytics to adapt to diverse and dynamic operational contexts. However, these advancements introduce novel attack surfaces. The fusion of AI capabilities with biometric systems presents opportunities for attackers to exploit system vulnerabilities, including adversarial manipulation, synthetic biometric data generation, and hardware-specific exploits. Proactively addressing these challenges is critical to safeguarding sensitive systems and ensuring the integrity of biometric identification and authentication mechanisms.

ISSUES AND THREATS

Biometric systems face advanced and futuristic threats, such as adversarial generative attacks, where malicious actors use generative adversarial networks (GANs) to craft imperceptible perturbations that mislead biometric recognition systems in real-time; contextual spoofing via dynamic adversarial inputs, exploiting changing environmental factors (e.g., lighting, motion, or acoustic interference) to degrade system reliability; quantum-assisted biometric decryption, leveraging quantum algorithms to undermine current encryption schemes protecting stored biometric templates; temporal identity drift exploitation, using subtle, time-based variations in behavioural biometrics (e.g., typing cadence, gait) to create attack patterns mimicking authorized users over time; synthetic multimodal fusion attacks, generating artificial biometric identities by fusing AI-generated fingerprints, facial patterns, and voice signals into unified profiles that bypass current detection mechanisms; edge AI

poisoning, where attackers compromise localized biometric processing on edge devices to subtly alter training data or inference results; continuous system adversarial feedback loops, wherein attackers use iterative testing to adapt and bypass adaptive learning algorithms in biometric systems; and predictive biometric mapping, employing AI to analyze collected biometric patterns and predict future changes, enabling pre-emptive attacks on long-term identification systems.

POSSIBLE TARGETS

Any of the following, combination of them, but not limited to:

Advanced payment systems using biometric transaction verification

Critical infrastructure access control with multi-modal biometrics

Biometric-enabled authentication in autonomous systems (e.g., vehicles, drones)

Healthcare systems leveraging biometrics for patient identification and monitoring

IoT ecosystems integrating biometric gateways for device authentication

INDUSTRY USE CASES

AI Risk Scoring
Real-time risk evaluation of biometric authentication attempts.

Edge Ledger Systems
Decentralized identity models for secure biometric management.

Predictive Security
AI modelling future biometric changes for pre-emptive protection.

Self-Learning Engines
Autonomous updates to authentication baselines against attacks.

Context Fusion
Verifying biometrics from multiple devices for enhanced accuracy.