STUDY NOTES · BASIC CONCEPT

India’s Cybersecurity Shift: Device Identity and AI Defence Explained

Defence & Security

26 Apr 2024

Rising Digital Expansion and Growing Threat Landscape

India’s fast-growing digital ecosystem—spanning smartphones, IoT devices, cloud systems, and critical infrastructure—has significantly increased the attack surface for cybercriminals. As more services move online, the risk of data breaches, ransomware attacks, and infrastructure disruption also rises. This expansion demands a stronger and more proactive cybersecurity framework.

BECOME IAS
AI-Powered UPSC Preparation by TINKPOT

Concept of Digital Identity for Every Device

Experts are proposing that every connected device should have a unique, verifiable digital identity—similar to how individuals have identification systems. This would help in authenticating devices on networks, ensuring that only trusted devices can access systems. A device-level identity can reduce risks such as unauthorized access, spoofing, and malicious device infiltration.

Role of AI in Strengthening Cyber Defence

Artificial Intelligence can play a crucial role in detecting and preventing cyber threats in real time. AI-powered systems can analyze vast amounts of data, identify unusual patterns, and respond to threats faster than traditional methods. This makes cybersecurity more adaptive and capable of handling sophisticated attacks that evolve rapidly.

Protection of Critical Infrastructure

Sectors like power grids, banking, telecom, and healthcare are increasingly dependent on digital networks. A cyberattack on these systems can have widespread consequences. By combining device identity frameworks with AI-driven monitoring, authorities can better secure these critical systems against disruptions and breaches.

Benefits for Citizens and Data Security

A robust cybersecurity system not only protects infrastructure but also safeguards individual users. With device

authentication and AI surveillance, risks like identity theft, financial fraud, and data leaks can be minimized. This builds trust in digital services and encourages wider adoption of technology.

Challenges in Implementation

While the idea is promising, implementing a digital identity for every device comes with challenges. These include ensuring privacy, managing large-scale infrastructure, standardizing protocols, and preventing misuse of data. Balancing security with user rights will be a key concern.

Way Forward for India

To effectively curb cyber threats, India needs a coordinated approach involving government, private sector, and technology experts. Investment in AI-based cybersecurity, clear regulatory frameworks, and awareness among users will be essential. A secure digital ecosystem will be critical for sustaining India’s growth in the digital age.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT