

## Indian Financial Institutions See Spike in Deepfake-Based Fraud Attempts, Report



Deepfake-enabled fraud, powered by artificial intelligence, is emerging as a new high-impact attack vector that targets financial institutions, customers and transaction ecosystems, a report said on Monday.

The report from Seqrite, the enterprise security arm of cybersecurity solutions provider Quick Heal Technologies Limited said AI-driven impersonation attacks that use synthetic voice, video and identity manipulation are increasingly able to bypass traditional verification mechanisms.

Attackers can mimic executives, relationship managers, or customers with high accuracy, enabling fraudulent authorisations, account takeovers, and real-time payment manipulation.

These attacks are particularly effective in environments where speed of transaction often outweighs verification depth, the report noted.

Over 265.52 million detections across more than 8 million endpoints were recorded between October 2024 and September 2025 with an average of 505 detections every minute.

Trojans accounted for about 43 per cent of detections and file infectors about 35 per cent, the report said, noting many campaigns relying on social engineering and identity deception to initiate compromise.

Financial institutions, by design, operate on trust-driven interactions across customers, vendors, and internal systems.

Deepfake-based fraud exploits this trust layer, embedding itself within legitimate communication channels such as calls, video verifications, and approval workflows, making detection significantly more complex.

Under the Digital Personal Data Protection (DPDP) Act, 2023, financial institutions are required to safeguard personal data and ensure secure processing across digital interactions.

A deepfake-led breach can lead to unauthorised access, identity misuse, and compliance violations, exposing organisations to regulatory penalties and reputational damage.

The report urged a shift from static identity verification to dynamic, behaviour-led validation. Institutions must strengthen multi-layered authentication, deploy anomaly detection across transaction flows, and monitor communication channels for manipulation signals.

The next phase of threats will be increasingly AI-driven, adaptive, and capable of bypassing conventional controls, it forecasted.

—IANS