

Anthropic Mythos Sparks Concern: Are Indian Banks Ready For AI-Powered Cyberattacks?

Anthropic Mythos, an autonomous AI cyberattack model, alarms experts and Indian banks, prompting RBI, MeitY and CERT-In to push systemic, real-time cybersecurity upgrades



AI vs banks: Why Mythos is forcing India's financial sector to rethink security

A yet-to-be-launched AI model, widely referred to as Anthropic Mythos, is already sparking concern across governments, banks, and cybersecurity experts. The reason isn't hype alone — it's what the model represents: a leap from human-led cyberattacks to autonomous, AI-driven exploitation at scale.

The model hasn't been released by Anthropic yet. It is being allowed for a restrictive use by the company in the US. However, some reports say that a group of hacker broke into the system to access the model.

What is the threat?

At its core, Mythos signals a shift in how cyberattacks can be executed. Traditionally, hackers needed time, skill, and coordination. That assumption is now breaking.

As Sanjay Katkar of Quick Heal puts it, the real concern is not just the model itself but what it proves: "AI has crossed a threshold where the full workflow of a sophisticated cyberattack... can now run autonomously."

This compresses the time between finding a flaw and exploiting it. Hackers can use the vulnerabilities in the financial system to exploit it.

Another expert, Parag Khurana of Barracuda Networks, highlights that the capability isn't entirely new — but the speed is unprecedented: These models “accelerate AI-enabled threats and compress the time between vulnerability discovery and exploitation.”

Why is this different from existing AI models?

Most current AI tools assist humans — they don't fully replace them in executing attacks. Mythos changes that equation.

Mythos brings autonomy, scale and speed that make it more dangerous than any prior existing models. It could lead to increase of more personalized phishing, and cybercrime becomes harder to detect and cheaper and more scalable.

Are Indian banks prepared?

India's banking ecosystem, known for its robust digital infrastructure and scale, faces a unique paradox. Its sophistication is also its exposure.

There has been visible institutional response. The Finance Ministry has convened meetings involving the RBI, MeitY and banking leaders. CERT-In has issued high-severity alerts, and efforts are underway to build a coordinated cybersecurity response framework.

Arjun Nagulapally, CTO at AIONOS, highlights that most banking security systems were designed for a slower threat landscape. He points out that these systems were built assuming attackers would need time, but “that architecture starts to break down when the window between vulnerability discovery and exploitation collapses to hours.”

Another layer of risk lies in the ecosystem surrounding banks. A large share of banking technology is managed by third-party vendors, where security standards are uneven. Notably, early reports around Mythos itself suggest unauthorised access occurred via a third-party environment, underlining how supply chain vulnerabilities can become entry points.

Is this threat overhyped?

While the reaction may appear alarmist, experts suggest the concern is justified — but often misdirected.

Katkar makes it clear that the focus should not be on Mythos as a standalone product. Instead, it is about what the model proves — that such capabilities are now achievable.

Even if access to Mythos is restricted, similar or more advanced models are expected to emerge. In fact, competing AI systems are already being developed. This makes it nearly impossible to contain the risk by controlling a single model.

The real challenge, therefore, is systemic. Governments and institutions need to shift from reacting to individual technologies to preparing for an entire class of AI-driven

What needs to change in cybersecurity strategy

The rise of AI-driven attacks demands a shift from reactive defence to continuous and predictive security models. Organisations will need to rethink how they monitor systems, detect anomalies and respond to threats in real time.

Experts emphasise that improving cyber resilience is not just about deploying advanced tools. It also involves strengthening basic practices such as faster patch management, tighter access controls and better employee awareness against AI-powered phishing attempts.