eMudhra Highlights Emerging 'Behavioral Trust' Risks in Autonomous AI Systems

As AI agents act independently, eMudhra highlights the need for behavioral trust frameworks to ensure accountability, security, and verifiable decisions.

BENGALURU, KARNATAKA, INDIA, March 11, 2026 /EINPresswire.com/ -- eMudhra today called attention to a growing cybersecurity and governance challenge as humanoids and physical AI systems begin operating in real-world environments: how organizations verify not just the identity of autonomous machines, but their behavior.

As AI-powered robots, autonomous devices, and intelligent systems increasingly perform tasks across manufacturing, healthcare, logistics, and public infrastructure, traditional security models focused on authentication alone may not address emerging risks, the company said.

eMudhra described a potential “behavioral trust gap,” where systems may be verified as legitimate but could still act unpredictably, be manipulated, or deviate from intended operational parameters. The company said this creates new attack surfaces, including unauthorized behavior changes, system compromise, and operational safety risks.

The issue is gaining urgency as organizations deploy physical AI systems capable of interacting with critical infrastructure and public environments without direct human oversight.

“Digital trust has historically focused on verifying identity — users, devices, and systems,” said Kaushik Srinivasan, EVP, eMudhra. “As autonomous machines begin making decisions in the physical world, the next challenge is verifying how they behave. Without behavioral trust, autonomy introduces systemic risk.”
eMudhra said emerging trust models may need to combine cryptographic identity, behavioral monitoring, policy enforcement, and continuous verification of autonomous actions to ensure operational integrity and safety.

The company noted that the challenge extends beyond enterprise environments to digital public infrastructure (DPI), smart cities, industrial automation, and AI-driven services. As adoption accelerates, establishing governance frameworks for autonomous behavior may become a priority for regulators and industry leaders.

eMudhra said the shift reflects a broader transformation in digital infrastructure, where trust

must extend beyond human users and devices to autonomous systems operating independently.

As global investment in robotics and AI accelerates, the company said addressing trust in physical AI will be critical to ensuring resilience, safety, and public confidence in the emerging autonomous economy.

About eMudhra

eMudhra is a global provider of digital identity, authentication, and trust services, enabling secure digital transformation for enterprises and governments. With a strong foundation in PKI, digital signatures, certificate lifecycle management, and identity and access management (IAM), eMudhra powers secure transactions and digital public infrastructure at population scale.

Serving customers across more than 35+ countries, eMudhra partners with leading technology providers and governments worldwide to deliver compliant, scalable, and high-assurance digital trust solutions.

As global cyber threats continue to evolve, eMudhra said establishing verifiable trust across users, devices, and digital services will be essential to protecting digital economies and public infrastructure.

Sudesh Kumar
eMudhra Limited
email us here
Visit us on social media:
LinkedIn