Short Description: How the adoption of digital identity solutions can address generative AI threats?

Meta Description: The US Financial Services Committee has held a hearing with innovative leaders of finTECH to discuss potential opportunities and risks connected to generative AI.

Description: Experts estimate that nearly 90% of online content could be generated artificially by 2026. As governments and other entities grapple with the challenges associated with AI, the implementation of digital IDs, and the incorporation of biometrics and advanced technologies emerge as safeguards against looming threats. Does the adoption of digital solutions help to address concerns raised by generative AI?

Should Governments Consider Adoption of Digital Identity to Address Generative AI Threats?

With the rise of generative AI, the vulnerability to sophisticated crimes has increased, putting stress on the adoption of applications that strengthen fraud detection and combat financial crimes. The US Financial Services Committee conducted a hearing with innovative leaders in financial technology to discuss the potential opportunities and risks associated with the use of artificial intelligence (AI). Certain members of the Committee expressed a clear interest in the prospects of utilizing digital IDs to counter fraud and enhance financial inclusion, reported Biometric update.

The increased use of AI introduces the possibility of sophisticated fraud, enabling the generation of texts or messages to execute deepfake attacks. Donna Murphy, Deputy Comptroller at Office of the Comptroller of the Currency (OCC), an independent bureau within the US Department of Treasury, reportedly remarked, “OCC supervised institutions are generally approaching generative AI with caution and its use is not widespread.”

Attendees of the Committee hearing also talked about how technology can drive financial innovation, emphasizing the importance of customer protection and regulatory compliance.

What are the threats associated with the use of AI?

The capability of AI to generate ultra-realistic content erases the boundaries between what is real and what is artificially crafted. The fabricated content can be exploited by illicit actors for various purposes such as spreading false information and impersonating individuals. Moreover, another concern arises from the generative AI to autonomously generate phishing content, elevating the risks of falling prey to online fraud and cyber attacks.

Deep fakes, particularly, have become powerful tools for malicious actors, enabling them to generate images and videos that appear authentic and can deceive even the most discerning individuals. The widespread use of misleading content not only harms trust but also poses a serious threat to the foundation of the information ecosystem.

Under ‘Facing Reality? Law Enforcement and the Challenge of Deep Fakes Report’ by Europol, experts estimate that by 2026, nearly 90% of online content could be generated artificially.

Illicit actors make use of AI to generate fake information and then use this information to conduct criminal activities. Sometimes, they take advantage of vulnerable individuals and target them by using phishing techniques. Identity Theft Fraud Survey 2023 by US News, inquired about 2,000 US adults who had fallen prey to identity theft. They were asked about their encounter with identity theft, social media identity theft, SMS phishing, and the precautions they took after the incidents. The survey findings revealed that 73% of the victims encountered at least one type of identity theft while 23% of respondents stated they had experienced identity theft more than one time.

In the year 2022, the Federal Trade Commission recorded over 1.1 million cases of identity theft. Experts predict the likelihood of a continuous surge in identity theft as cybercriminals find sophisticated ways to scam vulnerable individuals and often the most discerning individuals also fall prey to their scams.

It is the need of the hour to take decisive actions to keep individuals safe against identity theft and other potential threats imposed by the use of AI. Governments and businesses are making efforts to keep their societies safe and looking forward to implementing digital IDs as a shield against risks and challenges associated with generative AI.

How Does Digital Identity Can Fight Against AI Threats?

Globally, businesses and government bodies are taking active steps to secure their systems, and putting efforts to develop digital IDs ensuring protection against risks and challenges linked to the use of AI. The integration of biometrics in digital ID systems enhances security against unauthorized access and identity theft.

Biometrics involves the use of distinct physical and behavioral traits to verify the identity of individuals and presents an unparalleled verification standard. The traits may include fingerprints, facial features, iris patterns, and voice patterns. Governments can establish identity verification protocols by integrating biometrics into digital ID frameworks. The adoption of biometrics ensures the legitimacy of interactions conducted online.

Governments have the potential to implement digital identity solutions to actively address the challenges introduced by generative AI. For instance, authorities can mitigate the risks of deep fakes by employing facial recognition technology in ID verification systems, thereby preventing the exploitation of illicit activities like impersonation and spreading misinformation. Adopting this strategy not only strengthens security but also empowers users to navigate digital systems more confidently. It also enables individuals to know how their data is used and shared.

WorldID Powered by Worldcoin Introduces Facial Biometrics in its Digital ID System

one way to counter the threat of AI-generated deepfakes is through digital identities that use biometric data. Projects like World ID aim at using iris scans to create identity for humanity so that it is easy to differentiate between fake IDs and real ones. Reflecting on current events, OpenAI, through Worldcoin, a cryptocurrency issued in exchange for iris scans, has expanded its digital ID verification by integrating facial biometric verification and guaranteed capability with several widely adopted online services. This approach aims to empower individuals to verify their distinct human identity online, ensuring privacy protection and allowing users to control their data.

AI makes it easy to create deepfakes which can exacerbate identity theft. An effective solution to this problem calls for a robust identity verification solution that uses the biometric data available in the form of easy-to-prove credentials.

Digital Identities issued by governments and digital identity verification solutions by private sectors can play a significant role in differentiating spoofed identities and the real ones.

No doubt, digital solutions have already been adopted by various organizations and government bodies however, the fusion of advanced digital solutions with adaptive security measures could be essential in addressing AI-related threats. How can we strike the right balance between security and privacy while fostering innovation?

Also Read: Why Even a Least Developed Country Like Bhutan is Turning To Self-Sovereign Identity for Citizens?