AI and Digital Identity: Unleash the Power, Tame the Beast!

As digital identity continues to evolve, artificial intelligence presents both opportunities and threats. Providing jaw dropping case studies, our esteemed panel of experts will delve into various aspects of AI in digital identity, discussing the implications for security, fraud, and the future of trust in the digital domain.

**1.**  **How is AI currently being used to deliver more effective outcomes for ID/V processes and controls?**

**Ans**. I can tell you that Banks are still very much using Traditional Monitoring approach to detect **financial crime**. This is largely driven by static rules and alerts. Most of the time it means that Banks react to a suspicious event after event has taken place.

Of late, Banks have also started adopting AI, which enables you to detect events before they have taken place using **predictive analysis**.

A lot of this shift to AI will now be driven by MSA (**Monitoring for Suspicious Activity**) guidance by Wolfsberg Group. Published in July this year, it talks about enhanced focus on Client Due diligence, more effective reporting than quantity, and adoption of innovative technology.

So we will see in coming times banks adopting new technology more like - AI for proactive fraud detection, Blockchain to track transactions, and BI tools for data visualisation.

**2.**  **What are the biggest areas of risk from the proliferation of data and the use of foundation models, including generative AI?**

*comment on foundation models, transparency index, DORA and using 3rd party solutions. Prompt injection, data leakage, inherent bias etc.*

**3.**  **How do we solve these risks and is there an opportunity for even more effective IDV leveraging the latest technology?**

To mitigate the risks associated with data proliferation and the use of foundation models, we need a multi-faceted approach.

1. Choose your LLMs based on transparency index.

2. Data protection

3. Be aware of and compliant with regulations.

4. When leveraging biometrics for ID verification, combine multiple biometric factors like finger print, face match, iris match, even voice.

5. External audits and certifications.

6. Finally, employing AI and machine learning for real-time fraud detection and adopting a multi-layered approach to security along with TMs.

**4.**  **What are some of the broader constraints in combating the threat of AI and leveraging the opportunities?**

Yes, the regulatory landscape is forever evolving. This year we had EU AI act going live which is seen as a game changer as far as regulations around AI are concerned. The act classifies ai usage to 4 risk categories as per use case. The use of AI in identity verification (ID/V) is categorized under the "high-risk" category, due to the potential impact on fundamental rights such as privacy and data protection.

Digital identities are the key to how we can solve the fundamental trust issues with today’s internet.

A digital identity = unique id of person + its relationships to other entities.

**Biometrics** are one of the commonly used methods for authenticating digital identities. Other ways include passwords, OTPs, MFAs, smart cards, etc.

EU Digital Identity Wallets initiative: by 2030, all EU citizens to have single digital id and a wallet to share digital documents.

The UK is also rolling out a similar [**GOV.UK**](https://gov.uk/)**One Login**, which aims to provide a more straightforward and secure way for people  to prove their identity and access government services online.

----

AI in Identity:

1. Proactive fraud monitoring.
2. Streamline KYC by automatic document verification.
3. Biometrics – voice, iris face, fingerprint.

Use of AI in Identity help standardise login experience as well. Otherwise, every app uses it's own mechanism, some have user passwords, some use federations with third party social logins.

--

One innovative technique to prevent deepfake frauds is the use of heatmaps

Heatmaps can help detect anomalies in images or videos by visualizing areas with unusual patterns or inconsistencies.

Here's how it works:

Facial Feature Analysis: Heatmaps can highlight facial features and track their movements. Any unnatural movement or inconsistency in facial features can be flagged as a potential deepfake

Pixel-Level Analysis: By analysing the pixel-level data, heatmaps can identify subtle changes that are not easily visible to the naked eye.

Behavioural Patterns: Heatmaps can also be used to monitor behavioural patterns in videos, such as eye movements and blinking patterns, which are often difficult for deepfake algorithms to replicate accurately.

This technique, combined with other AI-driven solutions like anomaly detection and predictive analytics, can significantly enhance the ability to detect and prevent deepfake frauds.

Other techniques to safeguard against deepfakes are:

MFA, Blockchain - temper proof record of document creation.

Face recognition - asks for video recording, and moving of head to detect any mask being used. If you use a recording of head movement, then heatmap would detect it that it is a screen recording as pixels would vary from a real video.

-

In realm of Identity, authenticity and privacy are always pitted against each other. You can't achieve both. E.g. in the realm of KYC checks in Banking, they ask for lot of your documents. As they want to check your application thoroughly, but this comes at the cost of privacy.

Imp regulations for security of ID/V systems: GDPR (UK GDPR is the UK version of GDPR post Brexit),

This act requires explicit consent before collecting biometric data and mandates the secure storage of data.

There can be region specific regulations as well – such as **CCPA** – also known as California’s GDPR, because California houses many tech giants that process data, separate regulation had to be made around it.

**Time value and cost of privacy**: People are more concerned about privacy of their recent data. Old data like previous address being used for AI – person might not be concerned.

With Biometrics, there are 2 approaches – either you save biometric template of the user (taken at time of registration) on the device or on cloud. With device, if its stolen, so is your data, but with cloud, you are saving it on a 3rd party entity altogether.

To reduce the risk of storing biometrics on cloud, techniques like **MPC (Multi Party Computation)** can be used, to ensure that the saved biometric is not exposed to a single party. Many parties participate in computing the encryption value, each using their own private keys.

To further increase effectiveness of Biometrics, say for facial biometrics, instead of reading entire face, area around eyes (**Periocular**), or ears is captured, to prevent use of a face mask. Doesn’t require lot of CPU of your device.

Face is considered a safe way of biometrics, but there are privacy concerns with this.

Minor cosmetic operations etc. does not change your enrolment. But say a surgery after a major accident etc, there can still be a provision to re-enrol.

On average, a password reset costs companies around $70 per instance. Based on cost on helpdesk resource, verifying user identity again, cost of IT systems – sending emails/OTP, etc., potential loss of business if customer uses another platform for the transaction.

**How does gen ai help with id/v?**

By generating potential fraud vectors and help train the system.

Help customers fill out forms during enrolment and KYC.