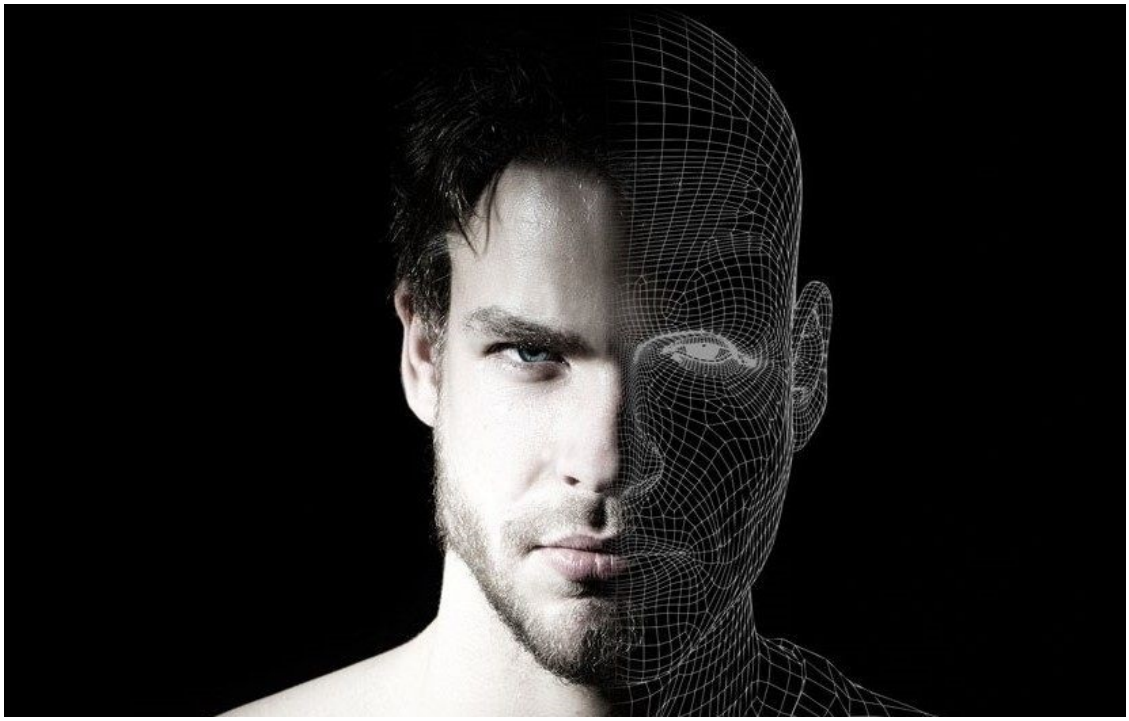
Neural biometric - the next generation of security

With security as the watchword at every turn and in practically every transaction in modern-day life, the unsettling reality remains that fraud, identity theft, and cybercrime are rapidly on the increase globally.



In South Africa, the SA Fraud Prevention Services reports that identity theft has increased by 200% over the past six years, and the Global Economic Crime and Fraud Survey 2018 conducted by PWC states that South Africa's rate of reported economic crime is at 77%, way above the global average of 49%.

Even as technology advances and security solutions are touted as 'the answer' to threats, shortfalls are revealed.

"Unfortunately, biometric data can also be hacked. There have already been a number of large-scale breaches, including a 2015 incident in which the fingerprints of 5.6 million workers were stolen from the [US] Federal Government Office of Personnel Management," states a *Fortune* magazine article, *'How Biometrics are Worse than Passwords'* (May 2016). It continues, "Even worse, when biometric security is compromised, the damage is long-lasting. You can change your password after a data breach, but you can't change your fingerprint."

In April, in South Africa, it was reported that a flaw in the Department of Home Affairs website exposed details of people

contacting the department, including name and surname, ID number or case number, cell phone number, and query details (www.mybroadband.co.za: 19 April 2018).

aiThenticate Cognitive Computing Labs recently launched a new biometric, Neural Biometric, that mimics human cognition – how the human brain naturally and instinctively recognises people. Because the human brain's ability to process information and to make sense of things far exceeds the most advanced supercomputer imaginable, aiThenticate used the human brain as its model to develop its new Neural Biometric.

Home Affairs' biometric ID verification a big step towards curbing crime

15 Jun 2018

Andrè Immelman, CEO of aiThenticate, points out that biometric identities can be stolen or reused. "There is no way to prevent criminals or computer malware from hacking or stealing biometric identities from the places that store them, or lifting them from wherever we leave them – Facebook or anywhere we touch."

In spite of the large-scale adoption of biometrics by almost every private and public organisation in the world, identity theft now ranks as the foremost blue-collar crime in the world.

"Much of this has to do with the false sense of security that biometric features on smartphones tend to foster – fingerprint, facial recognition, retinal and iris scan systems built into mobile phones add absolutely nothing to the security of a transaction," says Immelman. "That is because every on-device biometric is premised on simple faulty logic: the user is asked to tender a fingerprint or faceprint or voiceprint as 'proof' of his identity, when the device has absolutely no way of knowing whether the biometric actually belongs to that user.

"Technologies such as Apple's touch ID or Face ID all assume that the person who registers his fingerprint, faceprint or voiceprint on his phone is being truthful – that he actually is who he says he is. If the growing scourge of identity theft in the world has taught us anything, then it is the fact that we simply cannot trust a person's own say-so," he adds.

aiThenticate's Certified Programme on the other hand, ensures that every user actually is who he says he is – no credence is given to the user's own testimony or credentials.

Graham Croock, director: IT Audit, Risk & Cyber Lab at BDO, says, "Conventional biometrics have long since passed their sell-by date. Our post 9/11 world wherein we are able to connect with anyone, anywhere at any time in any number of different ways, demands an authentication technology that extends beyond the conventional. And aiThenticate's next-generation neural biometric does exactly that!"

aiThenticate's biometric technology answers five of the most important security-related questions:

- Is someone actually who he says he is? (Authentication)
- Who is this? (Identification)
- Is this an actual live person? (Liveness, proof-of-life, anti-spoofing)
- Does this person match his or her identity credentials? (Verification)
- Did the right person authorise the transaction? (Authorisation)

Says Immelman, "aiThenticate's Neural Biometric recognises that we each possess a unique identity that inalienably and immutably persists with us for the duration of our lives, that we are each so much more than just a few whorls and arches at the end of our fingertips or a few key landmark points on our faces.

Like the human brain, aiThenticate's Neural Biometric is able to interpret a person's true identity using any camera on a

phone or desktop computer or at an ATM or kiosk, and then express that information as a complex, anonymous, irreversible, de-identified ‘crypto hash’ that is utterly unintelligible to anyone who is able to access it.”

The fact is that the volume of information contained in a person’s identity is far more than is available in any fingerprint or faceprint or voiceprint – and whereas conventional biometrics only make around 182,000 unique permutations possible, aiThenticate’s Neural Biometric, on the other hand, makes a staggering 29.2x1032 unique permutations possible – that is nearly 30 billion times more than there are planets in the universe.

“Now aiThenticate is advancing this breakthrough discovery as the next generation biometric to replace biometric conventions that are rapidly becoming obsolete,” says Immelman.