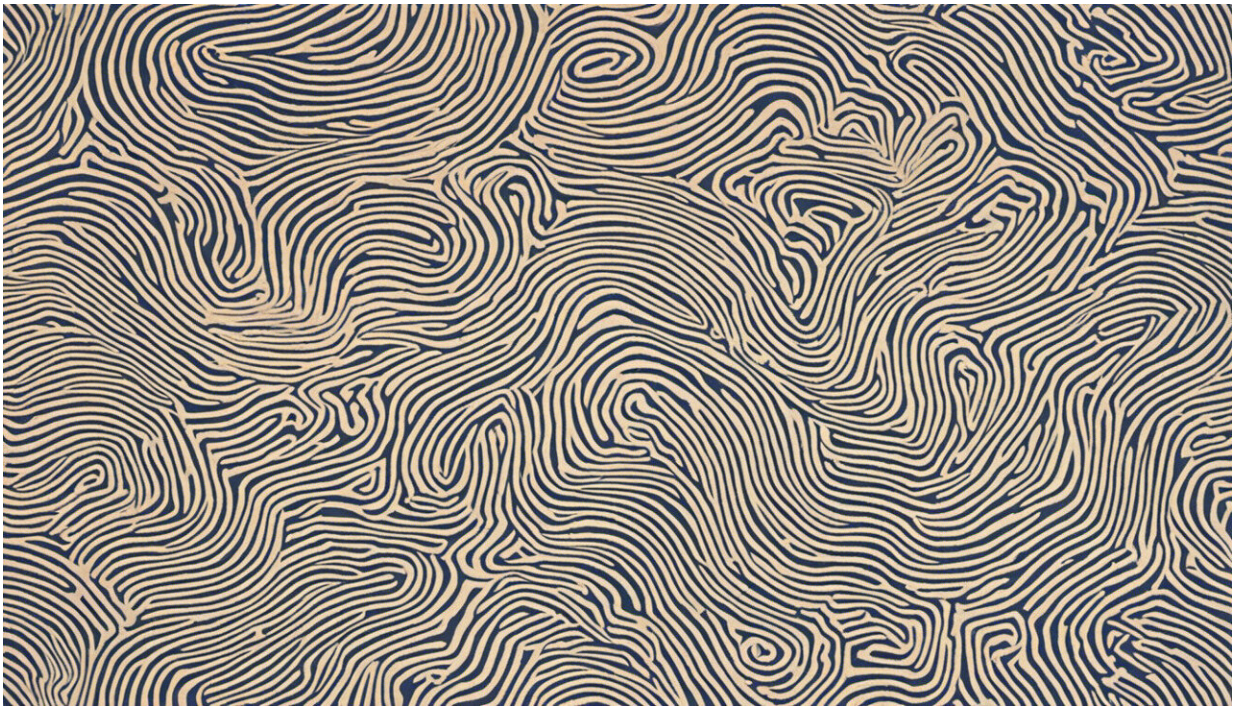
Stolen fingerprints could spell the end of biometric security – here's how to save it

August 20 2019, by Chaminda Hewage



Credit: AI-generated image (disclaimer)

The biggest known biometric data breach to date was reported recently when researchers managed to access a 23-gigabyte database of more than 27.8m records including fingerprint and facial recognition data.

The researchers, working with cyber-security firm VPNMentor, said that

they had been able to access the Biostar 2 biometrics lock system that manages access to secure facilities like warehouses or office buildings. This control mechanism, run by the firm Suprema, is reportedly part of a system used by 5,700 organisations in 83 countries, including governments, banks and the UK's Metropolitan Police.

This breach highlights a major problem with biometric security systems that effectively use people's biological measurements as passwords. Unlike usernames and passwords, biometric data can't be changed if it is stolen.

Given that data breaches have become an inevitable part of our increasingly digital world, does that mean biometric security doesn't have a long-term future, as it's likely that one day almost everyone's data will be floating around cyberspace? Perhaps in its current format, but there are also ways we could rescue biometrics and make it more secure.

Traditional passwords are something you know. Biometric features are something you are. Fingerprints, iris scans, voice patterns, face and ear photos and facial recognition data can all be used as a way to check if someone is who they say they are and are very hard to fake.

Authentication systems securely store a copy of the raw biometric data and when a user wants to login to the system, their features are compared with the stored data. Once only a feature of science fiction, biometric systems are now widely used in real-life secure facilities, passports and even the fingerprint authentication in your smartphone.

But the unique nature of biometrics is also its flaw. Biometric data might provide a way to identify people with a high degree of accuracy but once it is stolen there is nothing you can do to make it secure again. Of course, if your fingerprint is stolen you could always use another finger, but you could only do this 10 times.

Once someone has your fingerprint data, it is possible to print a replica using conductive ink that can fool biometric scanners. There are also examples of researchers fooling voice scanners with sound-morphing tools, iris scanners with replica images and face scanners with photos and even 3-D-printed heads.

This means it's really important to protect your raw biometric data from leaking to unwanted parties. But this will become an increasingly difficult task as we reveal our biometric data to more and more service providers.

Barely a week goes by without news of another company having its customers' data stolen. You've probably had to change your own passwords on at least one occasion because of this. If enough people have their biometric data exposed, eventually some systems could become unusable because so many users won't be able to securely log in to them.

In the recent biometric data breach, more than 1m people had their fingerprints, facial recognition data, face photos, usernames and passwords revealed. It was also discovered that outsiders could replace biometric records in the database with their own details, exposing another way to overcome the security checks.

Improving security

So what can be done to make biometrics security stronger? One simple way is passwords. It's a common practice to store passwords by first encrypting them or "hashing" them. This is essentially a one-way version of encryption that transforms the passwords into a string of characters known as a message digest that it is almost impossible to decrypt.

This means that even if the encrypted passwords are leaked, hackers

can't obtain the passwords. Modern systems would never store passwords in their original plain text format.

This method can also be applied to biometric data so that only encrypted or message digest versions of the biometric features are stored. In the recent biometric database breach, all the data was stored in raw format without encryption. This means hackers could access the raw biometric features of the users directly and replicate them for getting into critical services.

Another way to make biometric systems more secure would be to use blockchain, the system behind cryptocurrencies such as Bitcoin. With blockchain technology, you can store customer data in a distributed ledger protected by cryptography in multiple computers across the world. This means only authorised parties can access the data (or data blocks), and any attempt to modify the data will be detected by any other user subscribed to the blockchain. It's also possible to create private distributed ledgers that only certain people can access.

Even this might not be enough to keep biometric systems secure forever. Researchers recently demonstrated that it's possible to fool fingerprint scanners using artificial intelligence to generate replica prints that can beat the system. So one day, advanced computers might be able to recreate any features in order to fool biometric security system into letting an impostor through. But for now, if biometric service providers would take some simple steps to make their data more secure, we could more avoid breaches that will eventually make these systems obsolete.

Provided by The Conversation