It’s Time for Multimodal Biometric Verification. Here’s why

If you have ever watched one of the *Mission: Impossible* movies, then you’ve definitely seen biometric verification in action. A ton of characters in the franchise have used their eyes, voices, faces, and fingerprints to access a ridiculously fortified system. For the scriptwriters, it’s an easy way to say “here’s a very secure thing Ethan Hunt will have to break into - again.”

However, biometric verification is hardly just a plot device for fictional stories. Today, more and more companies, products, and services are outsourcing development to take full advantage of it. The main objective of this growing popularity is obviously offering more protection.

Yet, as it stands today, biometric verification systems still face a lot of challenges. From ensuring the right verification and avoiding the noise to prevent spoofing attacks, these technologies are still trying to provide a more robust service. That’s where multimodal biometric verification might help.

A Quick Recap of the Essentials

When you use your fingerprint or voice to lock or unlock your smartphone, you’re using biometric verification. In other words, you’re using a physical or behavioral biometric to enter a system. That’s what biometric verification is all about: using biometric data for access.

Said data can be classified into 2 categories:

Physical biometrics: fingerprints, veins, iris, facial features, and hand geometry
Behavioral biometrics: gestures, handwritten text, voice recognition, and walking patterns

Basically, any biometric verification system could use any one of the above to allow or deny access to a product or service. Each of those systems would be a single biometric verification platform.

The idea of using a biometric verification system is to replace traditional authorization systems with much stronger protection. You can forget, lose or get your identification numbers, passwords, or IDs stolen. That’s hardly the case with things that are inherently yours like your fingerprints or your face.

Why Multimodal Biometric Verification?

If no one can copy or steal your biometric features, why would companies work with outsourcing services to combine more than one verification system? Wouldn’t one be enough? You’d think so. But the reality shows that using single biometric verification systems is problematic for a number of reasons, including:

Environmental effect: the surrounding might become a problem when capturing or reading

your biometric feature. This is a very common issue for facial recognition, which is very affected by lighting conditions and is prone to errors.

Noise: though you might think that noise is only a problem for voice recognition systems, there are other kinds of noise that affect other systems. A new scar on your finger, an injury that's impairing your gestures, even your growing a beard - all can be detected as noise that can lead to a single biometric verification system to fail. In the same way, defective or improperly maintained sensors can also lead to faulty (AKA noisy) readings.

Variations over time: the verification process implies that every time you try to access the system, it will compare the current reading of the biometric feature with the one stored on the database. But there are features that change naturally over time: your face gets wrinkles, your voice changes, even your walking patterns might suffer.

Non-universal: though software outsourcing companies like to think they are creating biometric verification systems that work for everyone, that might not be the case. There are some people with disabilities or illnesses that won't be able to provide a specific biometric credential. If the system only uses that biometric feature, then those people will be left out.

Spoofing: spoofing attacks happen when someone impersonates a user to gain access to a system. This might seem impossible with fingerprints or faces, but the possibilities are there and a single verification system is less secure than a combination of them.

So, if using just one of the biometric verification systems available can lead you to those problems, then why do you need to use multimodal biometric ones becomes more evident. That's because combining 2 or more of those single systems complement their individual strengths while reducing the impact of their weaknesses.

For example, a multimodal biometric verification system could combine fingerprint and voice recognition to provide access to a user. Thus, the whole verification would be more reliable. That's because you'd be using independent biometric traits, limiting the effect of noise and variations and making it harder for malicious actors to impersonate you.

Advantages of Multimodal Biometric Verification Systems

This multilayered approach to verification tackles all of the issues described above in one way or another. Here are some of the most important benefits you can get out of using multimodal biometric verification systems:

Accuracy: if the conditions where the capture/reading takes place can affect the process, then having multiple biometric features will reduce its impact. Sure, a facial recognition system might not be able to determine if you are you due to poor lighting. But if you pair it

up with a fingerprint scanner and/or a voice reader, then chances are you won't be locked out of the system. That's because it's highly unlikely for multiple systems to be affected all at the same time.

Reduced noise and variation impact: the accuracy that you get doesn't just allow you to limit the environmental impact on the capture or reading. It also helps with noise and variations. A noisy signal could be problematic but if you pair it with other biometrics, you can ensure that the system knows who you are. The same goes for variations - maybe you have a new scar on your finger, but if your voice is the same, you will be able to gain access.

Universal: this is simple. If a person or several can't provide a biometric because of disability or illness, multimodal verification allows you to take one or more extra biometrics to ensure that everyone can use the system.

Security: spoofing attacks are hard to carry out - but not impossible. By using several biometric readings, you make it even harder for intruders to gain access to your system. That's because they might be able to spoof one trait of a user but spoofing several is highly unlikely and difficult.

That's not all. If you own a business and use multimodal biometric verification, you'll have one cost-effective solution to provide access for sensitive systems and areas in your company. While it's true that implementing the verification process might require a significant investment, the costs of an attack or of data loss are far greater.

It's Time to Start Using Multimodal Biometric Verification

In a world where cyberattacks are getting more vicious and effective, implementing biometric verification is almost mandatory today. Yet, the sophistication level of those attacks is so high that using just one of them won't cut it anymore. Besides, there are other problems when you use single systems, like noisy biometrics and non-universal approaches.

The combination of several of those systems is the perfect way to avoid those issues. Of course, things are so simple. There isn't a one-size-fits-all way to solve problems for everyone. Thus, each company and industry has to find its own verification solution that's able to tackle their specific needs. The success of the verification approach and the advantages described above depend on finding the right combination.

Even when you may think that's more of a gimmick out of Tom Cruise's movies, the time of multimodal biometric verification has come. The technology is ripe for adoption and the benefits greatly surpass the costs. So if you truly want to up your security game, then you have no other choice: you have to bet on this new trend.