AWARE

# Mobile Biometric Authentication:

## Pros and Cons of Server and Device-Based

# Table of Contents

# Introduction

Multiple biometric modalities for authentication can achieve higher biometric performance.

Biometrics use "inherent" factors (something the user is) to authenticate a user's identity. Relative to knowledge- and possession-based authentication methods (something the user knows and something the user has), inherent authentication factors like biometrics are difficult to steal and spoof. We can't easily tell when a fraudster uses a stolen password or mobile device, but with biometrics and liveness detection we can better detect when a fraudster is at work so that their access can be prevented.

Increasingly, modern smart phones incorporate biometric authentication capabilities, often using custom sensors.

But incorporating biometrics into the mobile application achieves several goals:

- Authentication performance that is known, and not dependent on user's device.
- Flexibility to apply different biometric modalities and matching thresholds.
- Consistent user experience between devices.
- Universal support for password free experience regardless of user device.

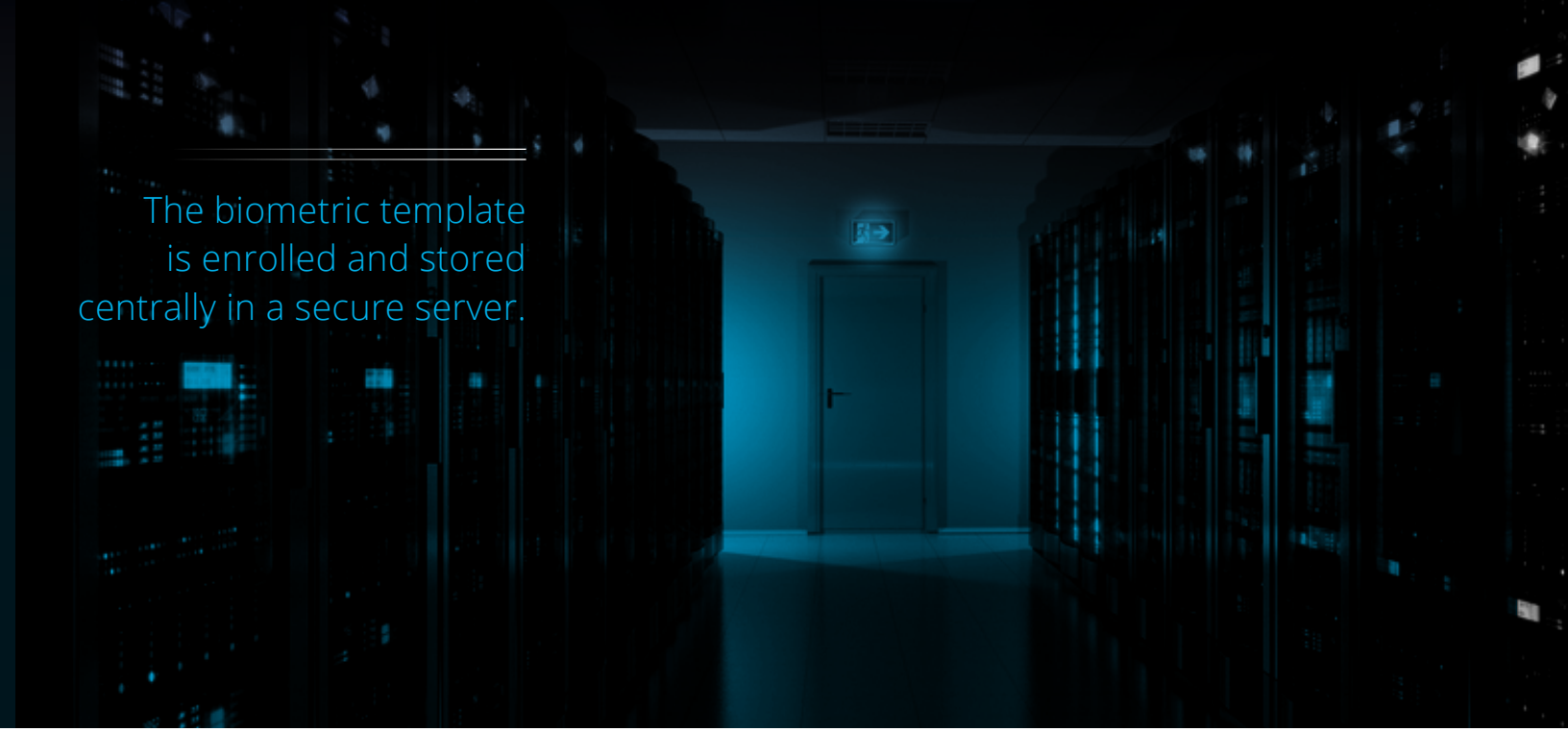
Using multiple biometric modalities for authentication (e.g. keystroke analysis with facial recognition) can achieve higher biometric performance by creating more obstacles for cybercriminals without compromising convenience.

## The Ongoing Debate

While most security experts can see eye-to-eye on the benefits of biometric-based mobile authentication, the underlying architecture with which to implement biometrics is less clear; more specifically, whether a server or device-centric architecture is more effective and secure.

The client-versus-server debate is as old as computing itself; we have seen it take place in countless other computing applications and environments. There have been ebbs and flows as mobile devices, networks, and software have become much more powerful and sophisticated. At its most basic level, biometric authentication has a lot in common with other classic computing tasks; the need to capture data, analyze the data, provide a result, and do it in a secure and efficient fashion. So we see some of same issues with biometrics that we have seen before.

This paper illuminates some of the question around device and server-centric biometric authentication by identifying their respective strengths and weaknesses and providing examples of where one may be preferred over the other.




## Server-Centric Architecture

In this setup, the biometric template is enrolled and stored centrally in a secure server. Matching and liveness detection upon an authentication attempt are performed centrally, as opposed to on each individual device. Each time the user performs a verification attempt, the captured sample is sent to the central matching engine, where it is processed and matched against the enrolled template stored centrally.

## Device-Centric Architecture

The analysis, biometric template creation, storage, and matching all occur locally on the device. In a FIDO-compliant system, a successful biometric match grants access to a private key stored on the device, which is in turn used to respond to a PKI challenge from a relying party, such as a bank or retailer whose app is running on the device. The private key never actually leaves the mobile device.

## Advantages of Each

Clearly there are advantages, disadvantages, and tradeoffs associated with both architectures. These characteristics will lend themselves to distinct use cases.

Where one method may excel another may fall short, but one is not necessarily better than the other.

| Issue | Advantage: Device-Centric | Advantage: Server-Centric | Reason |
|---|---|---|---|
| **Large-scale data breaches** | ✓ | | A single breach of the central storage location exposes many more. |
| **Perimeter defense** | | ✓ | Central storage and processes means that the perimeter is smaller and therefore easier to defend. |
| **Lost or stolen devices** | | ✓ | Server-centric architect segregates biometric data from other PII. A lost or stolen device contains the sample but also an individual's identity. |
| **Device dependencies** | | ✓ | Reduces mobile app size, easier downloads and takes up less space on the device. |
| **Man-in-the-middle attacks** | ✓ | | Biometric templates and other private data are less vulnerable to interception since they never leave the device. |
| **Use on multiple devices** | | ✓ | By storing and matching on the server, multiple devices can be used for authentication. |
| **Cross-jurisdictional mobility** | ✓ | | No cross-jurisdictional transit of biometric data since the credentials are only ever with the device. |
| **Scalability** | ✓ | | Processing and storage of biometric data is distributed across devices instead of all being done in a central location. |
| **Data analysis** | | ✓ | Observe, analyze, and learn from data to improve biometric matching and liveness detection algorithms. |
| **Bandwidth and data consumption** | ✓ | | Less data transmitted between device and server. Faster authentication. |
| **Device support** | | ✓ | Works on devices with less processing power sometimes needed for device-side biometrics. |
| **Biometric data validation** | | ✓ | Supervise and validate enrolled biometrics (e.g. as part or a more thorough identity proofing process). |
| **Multi-purpose biometric matching** | | ✓ | Use biometric data for other matching purposes (e.g. identity proofing, search against other data). |

| Priorities | |
|---|---|
| **Device-centric** | **Server-centric** |
| • Prevention of large scale breach.<br>• High scalability.<br>• Avoid mobile app complexity and large downloads.<br>• Enable modern devices.<br>• Avoidance of cloud resource consumption. | • Control and oversight of authentication process.<br>• Analysis of data to improve matching and livenes detection performance.<br>• Support for less powerful devices.<br>• Support for multiple devices for each user. |

A FIDO Certified approach allows an organization to enable strong biometric authentication into their mobile app.

**A server-centric approach** is likely preferred for organizations that desire a high degree of control and oversight over the mobile authentication function, and the capacity to manage and secure the proper storage and use of the biometric data. Organizations can also analyze the biometric data they collect to improve the performance of matching and liveness algorithms. By storing more resources and functions in the cloud rather than on the device itself, it reduces app size and complexity, but can be a bigger challenge to scale. As a result, server-centric authentication may also function more effectively with devices that have limited memory and processing power. However, mobile network bandwidth constraints can slow the authentication process.

**A device-centric approach** is likely the best option for organizations with a primary objective of preventing large-scale breaches of customer data. A FIDO Certified approach allows an organization such as a bank to enable strong biometric authentication into their mobile app without having to store, manage, and process customer data on a central server.

The tradeoff is that there is more size and complexity in the app, since the biometric processes all take place on the app, which less powerful devices may not easily support. That said, a device-centric approach is more scalable, and the FIDO Alliance provides for a standards-based approach and a marketplace of vetted products.

# Both Have Their Place in Biometric Authentication

Biometrics make mobile authentication more convenient and more secure. As a result, it is quickly becoming **the preferred authentication method** in multiple industries and in countries across the globe, according to Frost & Sullivan.

The availability of multiple storage methods may further expedite the spread of biometric authentication, since server and device-side architecture provide flexible options for organizations that would seek to implement it.

Therefore, both storage architectures have their place, and organizations are encouraged to select one based on their needs, capabilities, risk profiles, and available resources.

AWARE

www.aware.com/contact

Sources:
https://ww2.frost.com/frost-perspectives/biometric-technology-rapidly-becoming-preferred-technology-identity-and-authentication-across-sectors-globally/
https://fidoalliance.org/specifications/overview/