Editorial
Volume 12:5, 2021

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

What is Biometrics? 10 Physical and Behavioral Identifiers that can be Used for Authentication

Kouji Yamamoto[1*] **and Sadao Tomizawa**[2]

[1]*Center for Clinical Investigation and Research, Osaka University Hospital, 2-15, Yamadaoka, Suita, Osaka, Japan*

[2]*Department of Information Sciences, Faculty of Science and Technology, Tokyo University of Science, Noda City, Chiba, Japan*

Introduction

Biometrics are physical or behavioral human characteristics to that can be used to digitally identify a person to grant access to systems, devices or data. Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence. Each of these identifiers is considered unique to the individual, and they may be used in combination to ensure greater accuracy of identification. Because biometrics can provide a reasonable level of confidence in authenticating a person with less friction for the user, it has the potential to dramatically improve enterprise security. Computers and devices can unlock automatically when they detect the fingerprints of an approved user. Server room doors can swing open when they recognize the faces of trusted system administrators. Help desk systems might automatically pull up all relevant information when they recognize an employee's voice on the support line.

According to a recent Ping Identity survey, 92 percent of enterprises rank biometric authentication as an "effective" or "very effective" to secure identity data stored on premises, and 86 percent say it is effective for protecting data stored in a public cloud. Another survey, released last year by Spiceworks, reports that 62 percent of companies are already using biometric authentication, and another 24 percent plan to deploy it within the next two years. However, companies need to be careful about how they roll out their biometric authentication systems to avoid infringing on employee or customer privacy or improperly exposing sensitive information. After all, while it's easy to issue a new password when the old one has been compromised, you can't issue someone a new eyeball. According to the Spiceworks survey, 48 percent cite the risks of stolen biometric data as a top security risk with the technology. Other barriers to adoption include costs, cited by 67 percent of respondents, followed by reliability concerns at 59 percent. For companies specifically using biometrics to secure IT infrastructure in cloud, SaaS, on-prem and hybrid environments, adoption rates are even lower, according to the Ping Identity survey. Only 28 percent of companies use biometrics on premises, and even fewer, 22 percent, use it for cloud applications.

Types of biometrics

A biometric identifier is one that is related to intrinsic human characteristics. They fall roughly into two categories: physical identifiers and behavioral identifiers. Physical identifiers are, for the most part, immutable and device independent:

Fingerprints:

Fingerprint scanners have become ubiquitous in recent years due to their widespread deployment on smartphones. Any device that can be touched, such as a phone screen, computer mouse or touchpad, or a door panel, has the potential to become an easy and convenient fingerprint scanner. According to Spiceworks, fingerprint scanning is the most common type of biometric authentication in the enterprise, used by 57 percent of companies.

Photo and video:

If a device is equipped with a camera, it can easily be used for authentication. Facial recognition and retinal scans are two common approaches. Physiological recognition: Facial recognition is the second most common type of authentication, according to Spiceworks, in place at 14 percent of companies. Other image-based authentication methods include hand geometry recognition, used by 5 percent of companies, iris or retinal scanning, palm vein recognition, and ear recognition.

Voice:

Voice-based digital assistants and telephone-based service portals are already using voice recognition to identify users and authenticate customers. According to Spiceworks, 2 percent of companies use voice recognition for authentication within the enterprise.

How to cite this article: Yamamoto, Kouji. "What is Biometrics? 10 Physical and Behavioral Identifiers that can be Used for Authentication ." *J Biom Biostat*12 (2021) : 5

***Corresponding author:** Center for Clinical Investigation and Research, Osaka University Hospital, 2-15, Yamadaoka, Suita, Osaka, Japan; E-mail: kouji@yamamoto.com

Received: May 04, 2021; **Accepted:** May 21, 2021; **Published:** May 28, 2021