Editorial
Volume 12:7, 2021

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

Behavioral Patterns, not Physical Characteristics, are the Emphasis of Behavioral Metrics

Dongfeng Wu*

Department of Biostatistics and Bioinformatics, University of Louisville, USA

Introduction

Behaviometrics is a term derived from the words behavior and biometrics. It refers to the study of a person's conduct rather than physical attributes in order to uniquely identify him. Learn more about Voice Biometrics: The Promising Future of Authentication in the Internet of Things in the article Voice Biometrics: The Promising Future of Authentication in the Internet of Things Secured Touch detects fraud early in the client journey by providing real-time, adaptive fraud detection. For a variety of use scenarios, such as ATO, bots, and no-transaction fraud, our technology ensures precise risk-based prevention. Behavioral biometrics is a type of fraud protection technology that examines a user's digital physical and cognitive activities. Behavioral biometrics can distinguish between the activities of a geologist and those of a geologist since each person's interactions with a technology are distinct.

Continuous authentication is a method of providing users access to internet services depending on risk levels or contextual information that is acceptable. If the user makes a financial transaction during the session, the user will be asked to provide an authentication factor for payment authorization. Buguroo, a pioneer in behavioral biometrics-based online fraud prevention, revealed today that it has received a patent for its technology. Financial institutions, businesses, government facilities, retail point of sale (POS), and a growing number of other venues use behavioral biometrics for secure authentication. Biometrics are proven to be superior than passwords because they are easier to use, give more privacy and security, and are becoming more widely accepted across a wide range of mobile, desktop, and cloud-based devices.

People leaving unprotected and unattended workstations are the biggest risk element in computer security. Continuous authentication also enables a risk engine, which is at the heart of a fraud protection system, to monitor and analyses all data associated with the banking session, the customer, and their device in order to assess the likelihood of fraud. Biometric matching or verification is the first function, while biometric identification is the second. There are two types of biometric systems. The FBI and Interpol, for example, use biometrics in criminal investigations. They utilise a variety of biometric technologies, the most prevalent of which is a fingerprint scanner.

The verification procedure, on the other hand, entails confirming that identity data is linked to a specific person, such as comparing a person's date of birth to their name. Behavioral biometric authentication recognises a person based on the patterns they display when interacting with a device such a tablet, smartphone, or computer (including the mouse and keyboard). These patterns enable genuine frictionless authentication that is less intrusive to the user. In general, fingerprint recognition software is less safe than a good, strong password. If fingerprints are compromised, they can't be changed, and they can't be changed between accounts or devices.

Even commonplace products like playthings can be used to hack fingerprint readers. The use of a mobile device plus one or more authentication techniques to verify a user's identity for safe access is referred to as mobile authentication. Out-of-band authentication occurs when a user dials a phone number to request authentication. Using phone apps or SMS messaging to create One-Time Passwords (OTP). On a broad scale, dictionary attacks are used to crack traditional text-based password schemes.

How to cite this article: Wu, Dongfeng. "Behavioral Patterns, not Physical Characteristics, are the Emphasis of Behavioral Metrics." *JBMBS*12 (2021) : 7

***Corresponding author:** Dongfeng Wu, Department of Biostatistics and Bioinformatics, University of Louisville, USA, E-mail: dongfeng.wu@louisville.edu*

Received Date: July 01, 2021; **Accepted Date:** July 16, 2021; **Published Date:** July 23, 2021