Artificial Intelligence-Based Behavioral Biometrics

Muskan Gupta
Vellore Institute of Technology, Vellore, India

B. K. Tripathy
Vellore Institute of Technology, Vellore, India

INTRODUCTION

The traditional authentication methods are based on passwords or PINs, which are not suited to the kind of interaction a user has with more and more portable devices. The problem arises as these authentication methods are based on point-of-entry, where they check a user once before he starts a session, and keep you logged in until a user exits that session (Clarke and Furnell, 2007). This leads to several vulnerabilities to the systems, where a person may target a post-login session.

With the advancements of technology, we have turned towards the usage of biometric security (Gorman, 2003). Biometric security ("Something you are") is a reliable solution that is much preferred over a password ("Something you know") or a token ("Something you have"). Biometric characteristics, being inherently individual are difficult to mimic or change. Studies suggest that biometrics recognition has the potential to support distinctive personality traits, can associate itself with the current system, and become an essential part of the present validation system.

Now, depending on the number of traits that are used for validation a biometric system can be divided into two systems: Uni-modal biometric system and Multimodal biometric system. The Uni-model systems use one biometric trait that can be an aid in the process of recognition. But the use of a single trait has proved to have many drawbacks such as restricted degree of freedom, spoofing and presence of noise in sensed data (A. Buriro,2016), (Kresimir and Mislav, 2004). On the other hand; we have a multi-modal biometric system that uses multiple traits for verification.

Based on this, in this chapter, we are trying to understand the two systems, in one of the emerging fields in this sector, Behavioral Biometrics which proposes a system of continuous authentication which is also non-intrusive in the workflow of the user. In general, they are particularly well equipped for verification of people who make use of laptops, smartphones, smart cars, or points of sale terminals. As the amount of digital appliances used in our surroundings is increasing exponentially (De et al, 2020), so does the prospects for utilization of this up-and-coming technology. It also provides numerous benefits over traditional biometric technologies. Collection of data for behavioral biometric verification often does not require any peculiar hardware and is also cost-efficient and can be cumulated non-obtrusively or without even the awareness of the patron. While most behavioral biometrics are not adequately distinctive to support trustworthy human identification, they have been manifested to yield rapturous accuracy for identity verification. So to explore this field more we did a comprehensive review in the paper is done

DOI: 10.4018/978-1-7998-9220-5.ch051

by comparing different parameters for verification of behavioral biometric approaches, and addressing the evolution of study and applications of behavioral biometrics (Fairhurst et al, 2017).

BIOMETRIC AND ITS TYPES

Let's, first understand the term "biometrics", it is extracted from the Greek words 'bio' which infers life and 'metric' means to measure. So in simple words, Biometrics refers to the study of metrics or traits associated with life, and interestingly it is used in the field of computer science as a technique to identify individuals.

Biometric identifiers can be seen as differentiating, quantifiable traits which are manipulated to label and characterize an individual.

Biometric is broadly segmented into two parts: physiological versus behavioral characteristics.

Physiological Biometric

Physiological characteristics are linked to the static traits of an organism that are not prone to variation over time. Some implementation of physiological traits is face recognition (Tripathy and Sasikumar, 2012), (Debgupta et al, 2020), hand geometry, fingerprint (Tripathy et al, 2012), iris recognition, DNA, retina and many more. A useful face identification technique with masks is given in (Surya et al, 2021).

Behavioral Biometric

The behavioral avenue of biometrics is restricted to the behavioral traits of an organism that is related to the personal behaviour of an individual such as voice recognition, signature recognition, gait and keystroke dynamics and based on the number of features or metrics it is segmented as uni and multimodal.

Physiological Versus Behavioral Biometric

If we use physical biometric techniques to authenticate users in an online platform it can be considered that the use of a single physical biometric data point for authentication at the time of login, is the same as entering a static second password – as it can never be changed (due to human constraints) if compromised. Thus the major issue with physiological biometrics is that it can be compromised or leaked. For instance, a fingerprint– the use of such a physical biometric attribute is the same as saving a list of passwords in your laptop, but instead of it being just on their laptop, they simply leave a copy on everything they touch to be a cup they pick up or a chewing gum they discard.

So as a solution we have a more secure, user-friendly technique that makes use of the signals generated by how a person interacts with their surroundings. When these behavioral signals are accumulated they are highly effective at authenticating as they are not only self enrolling but also tolerant to change in the behavioral pattern of the users. Unlike physiological biometrics, behavioral biometrics data points cannot be duplicated or stolen thus is of no use to a malicious user and even if there is a case of high fidelity copy of legitimate user interaction, the attempt to recreate a previous interaction would be considered as an anomaly.

Now, as the prominence of behavioral over physiological biometrics is clear let's delve deep into the domain of behavioral biometrics. The classification of behavioral biometrics is detailed in Figure 1.