BIOMETRIC:

Biometrics is a technology used to identify, analyze, and measure an individual's physical and behavioral characteristics.
Each human being is unique in terms of characteristics, which make him or her different from all others. The physical attributes such as finger prints, color of iris, color of hair, hand geometry, and behavioral characteristics such as tone and accent of speech, signature, or the way of typing keys of computer keyboard etc., make a person stand separate from the rest.
This uniqueness of a person is then used by the biometric systems to −

- Identify and verify a person.
- Authenticate a person to give appropriate rights of system operations.
- Keep the system safe from unethical handling.

Biometrics refers to metrics related to human characteristics. Biometric authentication is a type of system that relies on the unique biological characteristics of individuals to verify identity for secure access to electronic systems.

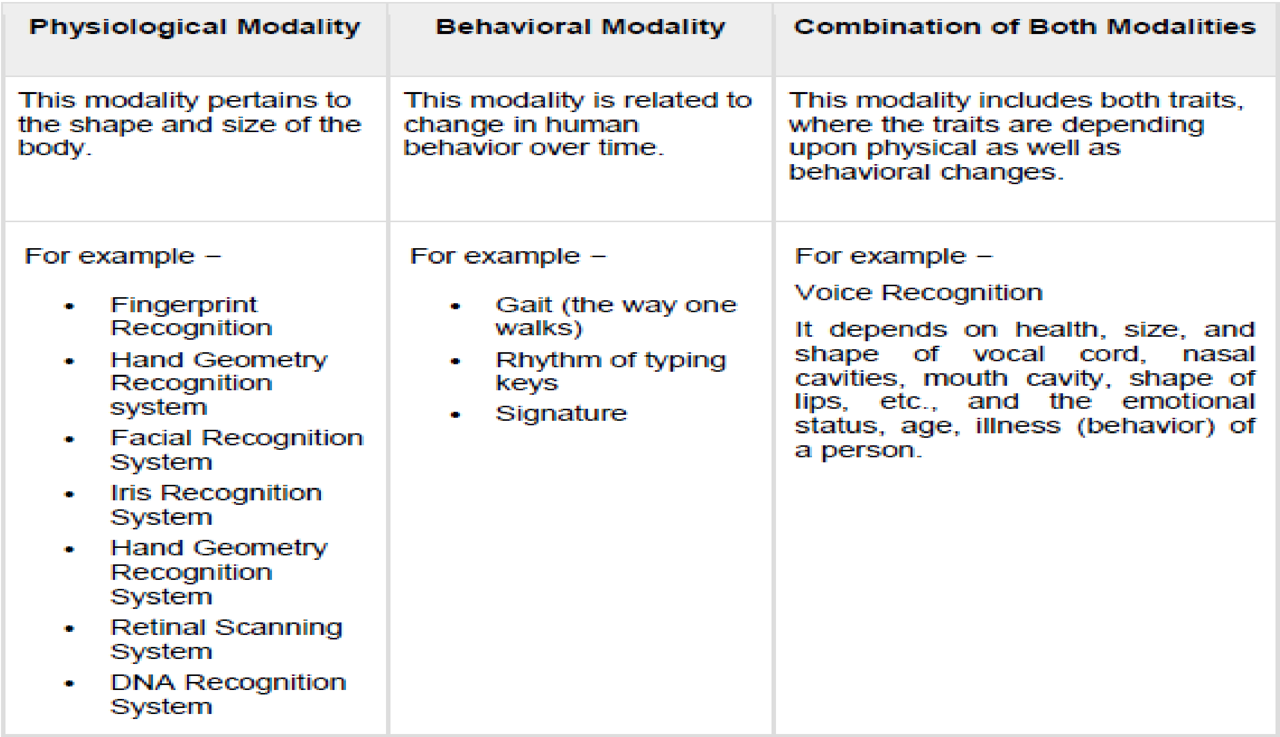
The oldest known use of biometric verification is fingerprinting. Thumbprints made on clay seals were used as a means of unique identification as far back as ancient China.

Types of Biometric Modalities

There are various traits present in humans, which can be used as biometrics modalities. The biometric modalities fall under three types −

- • 1. Physiological
- • 2. Behavioral
- • 3. Combination of physiological and behavioral modality

The following table collects the points that differentiate these three modalities –



Physiological Modality	Behavioral Modality	Combination of Both Modalities
This modality pertains to the shape and size of the body.	This modality is related to change in human behavior over time.	This modality includes both traits, where the traits are depending upon physical as well as behavioral changes.
For example – • Fingerprint Recognition • Hand Geometry Recognition system • Facial Recognition System • Iris Recognition System • Hand Geometry Recognition System • Retinal Scanning System • DNA Recognition System	For example – • Gait (the way one walks) • Rhythm of typing keys • Signature	For example – Voice Recognition It depends on health, size, and shape of vocal cord, nasal cavities, mouth cavity, shape of lips, etc., and the emotional status, age, illness (behavior) of a person.

Ear

Visual Biometric The identification of an individual using the shape of the ear.

Eyes - Iris Recognition

Visual Biometric The use of the features found in the iris to identify an individual.

Eyes - Retina Recognition

Visual Biometric The use of patterns of veins in the back of the eye to accomplish recognition.

Face Recognition

Visual Biometric The analysis of facial features or patterns for the authentication or recognition of an individuals identity. Most face recognition systems either use eigenfaces or local feature analysis.

Fingerprint Recognition

Visual Biometric The use of the ridges and valleys (minutiae) found on the surface tips of a human finger to identify an individual.

Finger Geometry Recognition

Visual/Spatial Biometric The use of 3D geometry of the finger to determine identity.

Gait

Behavioural Biometric The use of an individuals walking style or gait to determine identity.

Hand Geometry Recognition

Visual/Spatial Biometric The use of the geometric features of the hand such as the lengths of fingers and the width of the hand to identify an individual.

Odour

Olfactory Biometric The use of an individuals odor to determine identity.

Signature Recognition

Visual/Behavioural Biometric The authentication of an individual by the analysis of handwriting style, in particular the signature. There are two key types of digital handwritten signature authentication, Static and Dynamic. Static is most often a visual comparison between one scanned signature and another scanned signature, or a scanned signature against an ink signature. Technology is available to check two scanned signatures using advances algorithms. Dynamic is becoming more popular as ceremony data is captured along with the X,Y,T and P Coordinates of the signor from the signing device. This data can be utilised in a court of law using digital forensic examination tools, and to create a biometric template from which dynamic signatures can be authenticated either at time of signing or post signing, and as triggers in workflow processes.

Typing Recognition

Behavioural Biometric The use of the unique characteristics of a persons typing for establishing identity.

Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger or palm.

Voice / Speaker Recognition

There are two major applications of speaker recognition:

Voice - Speaker Verification / Authentication

Auditory Biometric The use of the voice as a method of determining the identity of a speaker for access control.
If the speaker claims to be of a certain identity and the voice is used to verify this claim. Speaker verification is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model"). Speaker verification is usually employed as a "gatekeeper" in order to provide access to a secure system (e.g.: telephone banking). These systems operate with the user's knowledge and typically require their cooperation.
For example, presenting a person’s passport at border control is a verification process - the agent compares the person’s face to the picture in the document.

Voice - Speaker Identification

Auditory Biometric Identification is the task of determining an unknown speaker's identity.

Speaker identification is a 1:N (many) match where the voice is compared against N templates. Speaker identification systems can also be implemented covertly without the user's knowledge to identify talkers in a discussion, alert automated systems of speaker changes, check if a user is already enrolled in a system, etc.

For example, a police officer compares a sketch of an assailant against a database of previously documented criminals to find the closest match(es).

In forensic applications, it is common to first perform a speaker identification process to create a list of "best matches" and then perform a series of verification processes to determine a conclusive match.

Note: There is a difference between speaker recognition (recognising who is speaking) and speech recognition (recognising what is being said). These two terms are frequently confused, as is voice recognition. Voice recognition is a synonym for speaker, and thus not speech, recognition. In addition, there is a difference between the act of authentication (commonly referred to as speaker verification or speaker authentication) and identification.