BIOMETRICS

1. **General:** The term "biometrics" is derived from the Greek words "bio" meaning life and "metric" meaning to measure. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the "automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic".

2. There are two main types of biometric identifiers:

   (a) Physiological characteristics: The shape or composition of the body.

   (b) Behavioral characteristics: The behavior of a person.

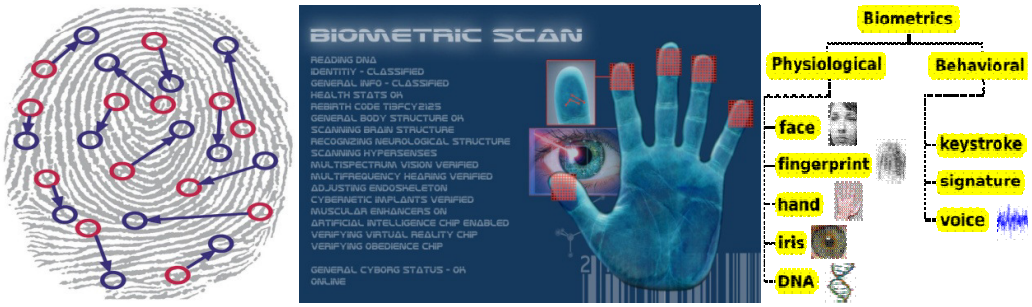

Fig.1: Biometric Scans

3. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for various reasons such as: The person to be identified is required to be physically present at the time-of-identification. Identification based on biometric techniques obviates the need to remember a password or carry a token. Examples of physiological characteristics used for biometric authentication include fingerprints; DNA, face, hand, retina or ear features and odour. Behavioural characteristics are related to the pattern of the behaviour of a person, such as typing rhythm, gait, gestures and voice. Certain biometric identifiers, such as monitoring keystrokes or gait in real time, can be used to provide continuous authentication instead of a single one-off authentication check.

4. Other areas that are being explored in the quest to improve biometric authentication include brainwave signals, electronic tattoos, and a password pill that contains a microchip powered by the acid present in the stomach. Once swallowed, it creates a unique ID radio signal that can be sensed from outside the skin, turning the entire body into a password.

5. Biometric devices, such as fingerprint readers, consist of:

   (a) A reader or scanning device.

(b) Software that converts the scanned information into digital form and compares match points.

(c) A database that stores the biometric data for comparison.

Accuracy of biometrics

6. The accuracy and cost of readers has until recently been a limiting factor in the adoption of biometric authentication solutions but the presence of high quality cameras, microphones, and fingerprint readers in many of today's mobile devices means biometrics is likely to become a considerably more common method of authenticating users, particularly as the new FIDO(Fast Identity Online) specification means that two-factor authentication using biometrics is finally becoming cost effective and in a position to be rolled out to the consumer market.

7. The quality of biometric readers is improving all the time, but they can still produce false negatives and false positives. One problem with fingerprints is that people inadvertently leave their fingerprints on many surfaces they touch, and it's fairly easy to copy them and create a replica in silicone. People also leave DNA everywhere they go and someone's voice is also easily captured. Dynamic biometrics like gestures and facial expressions can change, but they can be captured by HD cameras and copied. Also, whatever biometric is being measured, if the measurement data is exposed at any point during the authentication process, there is always the possibility it can be intercepted. This is a big problem, as people can't change their physical attributes as they can a password. While limitations in biometric authentication schemes are real, biometrics is a great improvement over passwords as a means of authenticating an individual.

8. **Working**: A biometric system can be either an 'identification' system or a 'verification' (authentication) system, which are defined below.

(a) Identification - One to Many: Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database.

(b) Verification - One to One: Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

9. Biometric authentication requires to compare a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, the one captured during a login). This is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process. During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner or video camera. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrolment. Here the processed sample (a mathematical representation of the biometric - not the original biometric sample) is stored / registered in a storage medium for future comparison during an

authentication. In many commercial applications, there is a need to store the processed biometric sample only. The original biometric sample cannot be reconstructed from this identifier.

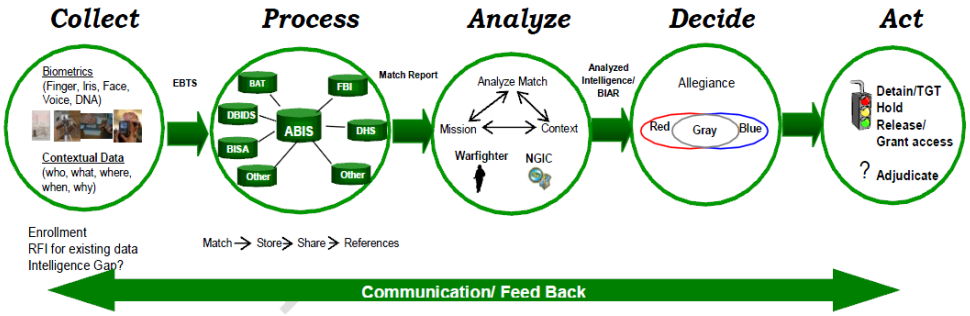

Fig.2: Process cycle of biometrics

10. A number of biometric characteristics may be captured in the first phase of processing. However, automated capturing and automated comparison with previously stored data requires that the biometric characteristics satisfy the following characteristics:

(a) Universal: Every person must possess the characteristic/attribute. The attribute must be one that is universal and seldom lost to accident or disease.

(b) Invariance of properties: They should be constant over a long period of time. The attribute should not be subject to significant differences based on age either episodic or chronic disease.

(c) Measurability: The properties should be suitable for capture without waiting time and must be easy to gather the attribute data passively.

(d) Singularity: Each expression of the attribute must be unique to the individual. The characteristics should have sufficient unique properties to distinguish one person from any other. Height, weight, hair and eye color are all attributes that are unique assuming a particularly precise measure, but do not offer enough points of differentiation to be useful for more than categorizing.

(e) Acceptance: The capturing should be possible in a way acceptable to a large percentage of the population. Excluded are particularly invasive technologies, i.e. technologies which require a part of the human body to be taken or which (apparently) impair the human body.

(f) Reducibility: The captured data should be capable of being reduced to a file which is easy to handle.

(g) Reliability and tamper-resistance: The attribute should be impractical to mask or manipulate. The process should ensure high reliability and reproducibility.

(h) Privacy: The process should not violate the privacy of the person.

(j) Comparable: Should be able to reduce the attribute to a state that makes it digitally comparable to others. The less probabilistic the matching involved, the more authoritative the identification.

(k) Inimitable: The attribute must be irreproducible by other means. The less reproducible the attribute, the more likely it will be authoritative.

11. A biometric system can also be classified into two modules i.e. Database reparation Module and Verification Module. The Database Preparation Module consists of two sub-modules i.e. Enroll Module and Training Module while the other module, Verification module can be divided into two modules that is Matching Module Decision Module.

Multimodal Biometric Systems

12. Multimodal biometric systems are those that utilize more than one physiological or behavioural characteristic for enrolment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of

(a) Reducing false non-match and false match rates,

(b) Providing a secondary means of enrolment, verification, and identification if sufficient data cannot be acquired from a given biometric sample.

(c) Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

13. Conclusion. Recently, another approach to biometric security was developed, this method scans the entire body of prospects to guarantee a better identification of this prospect. This method is not globally accepted because it is very complex and prospects are concerned about their privacy. Certain members of the civilian community are worried about how biometric data is used but full disclosure may not be forthcoming. In particular, the Unclassified Report of the Defense Science Board Task Force on Defense Biometrics states that it is wise to protect, and sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This also potentially applies to Biometrics. It goes on to say that this is a classic feature of intelligence and military operations. In short, the goal is to preserve the security of 'sources and methods'.