AN INTRODUCTION OF TECHNOLOGY FOR HUMAN IDENTIFICATION-BIOMETRICS

Praveen kumar
Assistant Professor , Amity University, Noida, India

Seema Rawat
Assistant Professor , Amity University, Noida, India

Neeraj Kumar
Stydent, M.Tech(CSE), Amity University, Noida, India

Veenita Gupta
Stydent, M.Tech(CSE), Amity University, Noida, India

Abstract- Biometrics is the combination of two words: Bio means Life and Metrics means Measurement. Biometric Identification which identify the particular person from all those enrolled in all walks of life. The identification of the valid user is now a key issue and is being driven by increased security threats and the rising problem of identity threats, Biometrics is proved to be the best option.

I.. BIOMETRICS: INTRODUCTION

Biometrics is the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Technically, biometrics is the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purpose of recognizing that individual.

A. COMMON HUMAN BIOMETRICS CHARACTERISTICS

Physiological Biometrics is related to the shape of the body. It includes

- Finger print -analyzing fingertip patterns
- Facial Recognition -measuring facial characteristic
- Hand Geometry - measuring the shape of the hand
- Iris Scan - analyzing features of colored ring of the eye
- Retinal Scan - analyzing blood vessels in the eye
- Vascular Patterns - analyzing vein patterns
- DNA - analyzing genetic makeup

Behavioral Biometrics is related to the behavior of a person. It includes

- Speaker Recognition - analyzing vocal behavior
- Signature - analyzing signature dynamics
- Keystroke - measuring the time spacing of typed words

Behavioral Biometrics is generally used for verification while Physical biometrics can be used for either identification or verification.

II. USES OF BIOMETRICS

We can also use token, credit card, PIN no. for identification and verification purpose but why biometrics because it has number of advantages like

- Eliminate memorization: Users don't have to memorize features of their voice, face, eyes or fingerprints.
- Eliminate misplaced tokens: Users won't forget to bring fingerprints to work
- Can't be delegated: Users can't lend fingers or faces to someone else
- Often unique: Save money and maintain database integrity by eliminating duplicate enrollments.
- Less requirements for users such that they do not have to go through a separate process for verification .

Figure 1. Biometrics Device

Very little hardware is required and ideally suited to telephone-based system for a remote identification, Zero client-side cost, no special reader needs to be installed

III.. PRINCIPLE

Biometric devices consist of a reader or scanning device, software that converts the gathered information into digital form and a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data in the database.

A. Advantages of Biometric Scanning System

Biometric scanning can be used for almost any situation calling for a quick, correct answer to the question, "Who are you?" The unique advantage of biometric scanning is that it bases recognition on an intrinsic aspect of a human being. Recognition systems that are based on something other than an intrinsic aspect of a human being are not always secure. For example, keys, badges, tokens and access cards (or things that you physically possess) can be lost, duplicated, stolen or forgotten at home. Passwords, secret codes and personal identification numbers (Pin's) (or things that you must know) can easily be forgotten, compromised, shared or observed.

Biometrics, on the other hand, is not susceptible to these particular problems. According to Dr. J. Campbell, Jr., a National Security Agency (NSA) researcher and chairman of the Biometric Consortium, no one technology has emerged as the "'perfect biometric,' suitable for any application" [9]. While there is no "perfect biometric," the characteristics of a good biometric scanning system are speed, accuracy, user friendliness and low cost.

B. *Comparison Of Biometrics*

Physical and Behavioral characteristics should meet some requirements in order to be used as biometrics methods. These requirements are either theoretical or practical. Theoretical requirements include:

- Universality: Each person should have the biometric characteristic.
- Distinctiveness: Any two persons are not equal in terms of the characteristic.
- Permanence: The characteristic remains the same over time or has no abrupt changes.
- Collectabillity: The characteristic should be able to be measured quantitatively. The practical requirements are traditionally related to the functionality of the computational systems.
- Performance: The achievable recognition accuracy speed that the biometric system can achieve.
- Acceptability: The acceptance of the end users in using the biometric system in their daily lives.
- Circumvention: The degree of security of the system given fraudulent attacks.

C. *Table Of Comparisons*

Comparison among different types of biometrics characteristics:-

Biometric characteristic	Universality	Unicity	Persistence	Colectability	Performance	Acceptability	Circumvention
Face	high	low	medium	high	low	high	low
Fingerprint	medium	high	high	medium	high	medium	high
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Iris	high	high	high	medium	high	low	high
Retinal Scan	high	high	medium	low	high	low	high
Signature	low	low	low	high	low	high	low
Voice	medium	low	low	medium	low	high	low
Thermogram	high	high	low	high	medium	high	high

Table 1. Biometric Characteristic

D. *BIOMETRIC APPLICATIONS*

a) Biometric Authentication ATMs, Law enforcement and Airports

Iris recognition in Law enforcement: In 1996, the prison in USA became the first correctional facility to use iris scanning. Sometimes the facility would need to release a prisoner on short notice and could not wait for the fingerprint tests. ATM iris recognition: Using iris recognition ATM, a customer simply walks up to the ATM and looks in a sensor camera to access their accounts. The camera instantly photographs the customer's iris. If the customer's iris data matches the record stored, a database access is granted. At the ATM, a positive authentication can be read through glasses, contact lenses and most sunglasses. Iris recognition proves highly accurate, easy to use and virtually fraud proof means to verify customer's identity. Iris recognition in Airports: In July 2000, iris authentication entered a new area of use as two airports began scanning passenger's irises as part of an effort to streamline boarding and security processes. The airports rollouts are among the first major applications for iris scanning. The system used a 30 frame/sec, black and white camera to take a picture of the eye from 6 to 36 inches away. Once passengers enroll, their codes will be stored for further use. Airline passengers will step up to a terminal kiosk and get scanned in one second. The iris is compared to a database of customers to authenticate. Then the passenger can be issued a boarding pass.

b) Biometric authentication in Networking

A host of networking associated companies has recently added biometric authentication features to their products. Companies such as Novell, Baltimore Technologies are some of the first to take advantage of biometric scheme.

Internet Banking , One area where the tool kit could be used is for enhancing security for Internet banking. A bank, contracting with an ASP (application service provider), could require biometric verification for a high-value transaction over the Internet. A vendor seeking to wire money using the Internet would go to the bank's Web page, fill out the required information and submit the transaction. If the transaction is for a high value, the bank would decide it needs biometric verification and automatically send a message to the Key ware LBV server requesting that the vendor speak a pass phrase and use the fingerprint scanner. The LBV server would then verify the pass phrase and the fingerprint and notify the bank if the request is accepted or rejected. No biometric templates leave the Key ware server, keeping them away from possible public access, according to Key ware.

c) Employee Recognition

Biometrics is the cheapest solution for employee recognition as very few people lose their fingers or eyes when compared with those who lose their smartcards or forget passwords.

d) Time and Attendance Systems

Biometrics is the cheapest solution for employee recognition as very few people lose their fingers or eyes when compared with those who lose their smartcards or forget passwords.Time and Attendance has always been a problem in some industries and other institutions. Biometrics can effectively eliminate problem with buddy clocking by ensuring that the employee in question is present.

IV. CONCLUSION

Biometrics is a new technology that is being deployed in a variety of public and private sector applications. It protects information integrity in both the private and public sector by restricting access to personal information .Biometrics has become the most appropriate means considering the factors such as account cost, convenience and level of security.

V. REFERENCES

[1] W. J. Clinton, commencement address at Morgan State University, Baltimore, MD, May 18, 1997.

[2] R. Chandrasekaran, “Brave new whorl: ID systems using the human body are here, but privacy issues persist,” Washington Post, Mar. 30, 1997.

[3] A. Davis, “The body as password,” Wired, July1997.

[4] F. James, “Body scans could make ID process truly personal,” Chicago Tribune, June 4, 1997.

[5] D. R. Richards, “Rules of thumb for biometric systems,” Security Manage, Oct. 1, 1995.

[6] R. Ryan: The importance of biometric standards. Biometric Technology Today, 17(7):7-10, 2009.

[7] F. Deravi: Biometrics standards. Advances in biometrics, 473-489, 2008.

[8] C. Tilton: Biometric standards – an overview. 2009. White paper available at http://www.daon.com/.

[9] A.K. Jain, A. Ross, S. Prabhakar: An Introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):4-20, 2004.