Biometrics for Identification

Priyanka Kapoor
Dept of Computer Science
GGN khalsa College

Abstract- *Biometrics is vital authentication technology used for determining the identity of person in information society. It deals with identification of individuals based on their biological or behavioral characteristics. Biometric technology is used for various types of application from modest to extensive type. Biometrics will become considerable component of the identification technology as people are known to the strengths and limitation of technology.*

Keywords- authentication; biometric; enrolment; identification; privacy; security

I. INTRODUCTION

Biometric word comprises bio (body) + metrics (to measure). Biometrics is an automated method of identifying a person which is based on characteristics such as physiological or behavioral. The physiological features measured are face, fingerprints, iris, retinal, vein, DNA and so on whereas behavioral characteristics include voice, gait, keystrokes , handwriting and soon . Biometric data are distinctive from personal information. Biometric templates cannot be recreated and stolen and used to access personal information, it is best and easiest way of authentication and security. Globally, biometrics market is rising at rapid rate to combat the higher need of security, data hacking and theft of identity. Therefore, it is extremely unlikely that intruders can false the user's identity.

II. METHODS OF BIOMETRIC IDENTIFICATION

A. ***Face:*** Face is the most common method of identification. To verify user, facial scan technology is used for unique features of the human face. Face appearance is a significant biometric because of its everyday use by nearly everyone as the primary source of recognizing other humans. Because of its genuineness, it is more acceptable than other biometrics. Faces have been officially used for identity in identity cards and passports for well structured system.

B. ***Fingerprints*****:** fingerprints are ridges on human fingers. Fingerprint image is captured in scanner as biometric identification Fingerprints have been used by humans for personal identification. The accuracy for matching identification using the biometric system is very high. Fingerprints of twins are different and the prints on each finger of the same person are also different which increases the rate of accuracy.

C. ***Iris*****:** Iris as the colored part of the eye bounded by the pupil and sclera. Iris scan technology uses the unique characteristics of the human iris in order to identify or verify the identity of the users. Iris scan technology has the prospective to play an important role in the biometric technology.

D. ***Retinal scan:*** A retinal image is captured by using scanner device then template is designed by using special software that compiles the unique feature of retinal blood vessels. Retinal scan algorithms require a high-quality image and will not allow a user to enroll until the system is able to capture an image of adequate quality. The template of retina is usually one of the smallest of any biometric technology. Retinal scan is a highly reliable technology because it is highly accurate and difficult to spoof in terms of identification.

E. ***Keystrokes:*** Keystroke is the behavioral biometric identification. These unique behavioral characteristics are measured by using keystroke recognition include:

1. The cumulative typing speed;
2. The time that elapses between consecutive keystrokes;
3. The time that each key is held down;
4. The frequency of the individual in using other keys on the keyboard, such as the number pad or function keys;
5. The sequence utilized by the individual when attempting to type a capital letter-for example, does the individual release the shift key or the letter key first?

F. ***Hand geometry****:* Hand scan technology makes use of the unique parts of the hand. Mainly it includes height and width of the back of the hand and the fingers. Hand scan is an application specific solution than majorities of biometric technologies and is used exclusively for physical access and also, time and attendance applications.

G. ***Gait:*** Analysis for gait is used to assess individuals with their ability to walk. The parameters taken into account for the gait analysis are as follows:

1. Step length
2. Speed
3. Dynamic Base
4. Progression Line
5. Foot Angle
6. Hip Angle and so on.

H. ***Voice:*** Voice recognition actually comprised of two different types of technology which are voice scan and speech recognition. Voice scan technology makes use of the distinctive aspects of the voice to identify and verify the identity of users.

I. ***DNA***: If you see blood, urine or any other liquid that has come from a human then DNA can be taken. One thing about DNA technology is the speed of it. This means that the results of a DNA test will be available in very less minutes. This gives a huge advantage, for example, some crime investigator and police who need to track down a killer. For crime cases, fast biometric results are a key thing for people to solve problems.

J. ***EAR:*** The term ear biometrics refers to automatic human identification on the basis of the ear physiological features. The identification is performed on the basis of the features which are usually calculated from captured 2D or 3D ear images.

III. TRENDS IN BIOMETRIC TECHNOLOGY

1. ***Mobile Biometrics:*** Mobile Biometric functionality can be obtained to speed up the processing of human identification on mobile device through inbuilt biometric sensors and by attaching portable hardware

2. ***Online Banking:*** Biometrics in online banking helps banks and retailers to achieve safe and convenient payments and transfers. It lowers the risk of that password can be stolen and customers can authenticate themselves by using face, fingerprints, eyes for making transactions

3. ***Immigration Services:*** Biometrics identifications are being used in immigration agencies around the world. They are considering fingerprints as most reliable identification method for safe traveling around the world by preventing criminals and deported people to get visa.

4. ***E-Government processes***: governments are providing public services to the citizens by using internet and e-commerce technologies. For this purpose, the Internet can be used to provide access to centrally stored data to support services and transactions. The permanent storage of confidential and personal data present significant security challenges. Citizens are exposed to threats to data privacy and the security of information. Privacy, security and confidentiality are thus natural concerns for citizens in these e- government processes. Many citizens may feel that their privacy is threatened if personal data is stored centrally. So, an emerging technology, biometrics is being used which provides two important capabilities: firstly, the trustworthy identification of an individual from the extent of a physiological property, secondly which provides the ability to control and protect the integrity of sensitive data stored in information systems.

5. ***Internet of things*****:** The Internet of Things (IoT) is a concept that involves connecting endpoint devices and physical objects to the Internet. These objects can communicate with other objects to know each other's status and share data. An IoT object has an ability to communicate with each other and eliminates need of human interference. Conventional methods like login - password for authentication on a smart node does not actually compliment the IoT technology. As Passwords can be guessed, forgotten or shared, all these standards of conventional authentication methods can be fixed by using biometrics for IoT authentication. Biometrics makes use of an individual's physiological and behavioral characteristics like fingerprint patterns, iris patterns, vein pattern, etc., to identify the user. All these characteristics are unique to an individual and they can be used as a secure method of authentication. Biometric characteristics also do not change with time or age nor are they easy to replicate or spoof. All these qualities give biometrics an edge over traditional method of identification. Biometrics eliminates standards of passwords and offers a better-quality authentication solution.

6. ***Cloud based biometric:*** In biometric authentication, cloud platform/ service provider provides biometric system for cloud users for enrolment. In biometric security systems, fingerprints, iris, face or any human traits that is unique to each individual are used to authenticate the person's identity. In today's era, Fingerprint technology is one of the most widely used biometric authentications. Users are required to register multiple biometric fingerprints during the enrollment process which are then stored as templates at the cloud provider's section. Each moment to access cloud based services, the person is prompted to provide

his fingerprint image and that is compared with the stored template. On a Comparison between the stored template and the person's current fingerprint scan, the person is authenticated and granted access. The fingerprint templates and the images that the person provides for getting access are encrypted for enhanced security.

7. ***Enrollment Management:*** Enrolment management is the act of managing presence in a work setting to minimize loss due to employee downtime. Traditionally, Enrollment control has been approached using time clocks and timesheets, but enrollment management goes beyond this to provide a working environment which maximizes and motivates employee attendance

7.1 Types of Enrollment Management System

Management System falls into two categories namely

a. Conventional and
b. Automated methods.

Conventional methods include

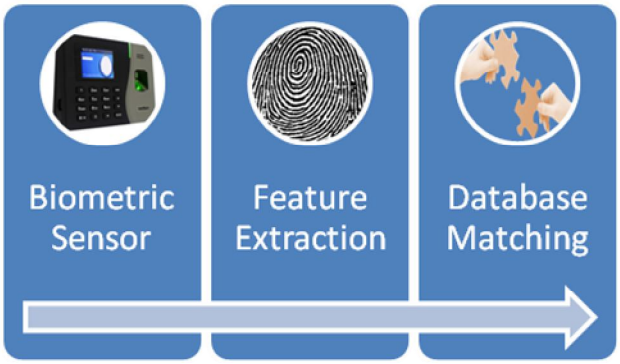
a) Attendance register: Attendance register is an official list of people who are present at an institution or organization.
b) Time clock: Time clock which is an electronic device used to assist in tracking the hour worked by an employee in an organization.
c) Time sheet: Time sheets are documents that record what time was spent by the employee on what tasks in an organization.

Automated methods include

a) Barcode system attendance system
b) Magnetic stripe attendance system,
c) Radio Frequency Identification (RFID) and
d) The biometric attendance system.

IV. ARCHITECTURE OF BIOMETRIC SYSTEM

The design/ architecture of biometric system are made up of the following:



i . Enrolment
ii . Authentication
iii . System database

Enrolment

The task of enrollment is to enroll users and their Biometric identity into the system database. For example, during enrolment, the fingerprint and other bio-data of the employee is captured and the unique features are extracted from the fingerprint image and stored in a database with the employee's ID. Employee's bio data to be captured includes: employee number, surname, sex, phone number, email, department and passport photograph and so on.

Authentication

The task of the authentication is to validate the identity of the person who intends to access the system. The person to be authenticated indicates his/her biometric identity. For example, employee places his/her finger on the fingerprint scanner. The fingerprint images captured is enhanced and thinned at the image processing stage, and at feature extraction stage, the biometric template is extracted. It is then fed to a matching algorithm, which matches it against the person's biometric template stored in the system database to establish the identity. During authentication, for enrolment, employee places his/her finger over the fingerprint reader, the fingerprint recognition unit compares the fingerprint features with those stored in the database, after a successful match, the employee number is sent to the database. Employee attendance is captured twice a day for both arrival and departure time.

The Database

The system database consists of tables that stores records, each of which corresponds to an authorized person that has access to the system. Each record may contain for example the employee's fingerprint and employee id of the person or other information. The system implements relational

data model for database design which is a collections of tables in which data are stored. The database can be maintained by using SQLServer, is fast and easy, it can store a very large record and requires little configuration.

V. BENEFITS OF BIOMETRIC IDENTIFICATION

1. No more forgotten or stolen passwords: there is no need of remembering and learning passwords and not to worry about to be forgotten / stolen.
2. Positive and accurate Identification: Biometric identification is accurate and consistent method of authentication.
3. Highest level of security: it provides high level of security as nobody can steal the biometric identity
4. Offers mobility: it offers the facility of mobility of identification
5. Safe & user friendly: it provides user friendly , easy and safe to use environment

VI. CONS OF BIOMETRIC TECHNOLOGY

1. One of the major drawbacks of technology is COST. A different biometric technology uses the different devices that have a high range of costs.
2. Second disadvantage is concerned with health as touching the device by everyone leads to spreading of germs.
3. Third disadvantage is related to face recognition as faces of people change over time.
4. There is need of large device for hand geometry verification which also cost high.

VII. CONCLUSION

As the world is evolving around the technology, more and more trends are there in the field of identity management for the purpose of security. In this paper we have presented a biometrics as digital identification system. It describes the basics trends in the technology, methods used for identification, how its architecture work which include enrollment, then authentication by matching the enrolled feature template from the database. Globally biometrics is being adopted to gain competitive advantage for the need of accurate and secure way of identifying individuals.

REFERENCES

[1] Jain, A. K., Bross, A. A., & Kumar, K. N. (2011). *Introduction to Biometrics.* US: Springer.

[2] C.O, A., A.O, A., O.O, O., & E.O, I. (2013). Fingerprint-Based Attendance Management System. *Journal of Computer Sciences and Applications* , 5.

[3] Bailey, K. O., Okolica, J. S., & Peterson, G. L. (2014). User identification and authentication using multi-modal behavioral biometrics. *Elsevier* , 77-89.

[4] Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM* , 90-98.

[5] Thakkar, D. (2017, Feburary 8). *Bayometric.* Retrieved December 7, 2017, from https://www.bayometric.com: https://www.bayometric.com/biometric-technology-trends/

[6] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology* , 4-20.

[7] Wang, L., & Geng, X. (2010). *Behavioural Biometrics for Human Identification: Intelligent Applications.* New York: Medical Information Science Reference.