Information Systems Security and Integrity

IT 6252

The Evolution of Biometric Security in Information Technology

Submitted to:
Ajarn Thotsaporn Sortrakul
11/29/2019

By: Anas A
ID: 6119488

Table of Contents

Introduction

The term biometric security refers to devices that measure unique characteristics of a person with functions such as the voice pattern, the retina or iris pattern of the eye, fingerprint patterns. This term can be related to our human body itself that refers to the measurements and differences in calculations.

Once again, security is one of the most crucial aspects of the technological world. Without security, we will not feel safe as there are a lot of potential risks. In general terms, security means safety, confidence and reassurance from any potential threats or harms. We require security because when entering in the technological world, we want to keep our data and information secret from being able to access by other unwanted users or threats. The information and data that we carry with our self is vital such as our personal information like bank account, PIN, and many other access codes.

Likewise, using biometric system makes our lives easier through enhancing the security. Through research and development from a long period, this unique system has evolved throughout decades which continues to provide extra or added layer of security in each tech involved.

Background

Recent study shows that many people are leaving the authentication on their online platform unfinished mainly due to the long and tiresome process of creating and typing their passwords and PIN codes. This concludes that security checks all over the world are boring in every facility where it functions. Therefore, many countries and places have adopted the use of Biometric security systems to change the entire process and perception of security to make everything easy, fast and simple from the user’s point of view. In Japan, their airports have adopted facial recognition gates that scans the passersby face automatically and keeps them in a record. Similarly, many airports are using iris scan as a biometric security system. Countries like Ukraine are now using biometric system to keep track of the border control. It is arguably the most time saving, hassle free, and also cost saving of security control and evaluation method.

History

The discovery of biometric can be rooted back to the 1800s where fingerprint was introduced in the identification of criminal’s record. It was used to analyze and store the fingerprint in police files. Over the past few decades, the importance of biometric system has increased significantly as biometric authentication is even found in our handheld devices like smartphones. Now, even different parts of the body is used for biometric system which includes:

- Finger vein
- Palm Vein
- Iris Scan
- Voice Recognition

More advance and but not yet common:

- Brain Waves
- Heart Signars
- DNA identification
- Behavioral biometrics

The most significant and early discoveries of Biometrics

1858 - First identification of Hand Captured images for ID purpose
Sir William Hershchel first used recorded handprint on the contract for each workers to distinguish employees regarding their payday. It was the first systematic capture of hand and finger image used for ID purposes.

1870 - Alphonse Bertillon introduced what's called Anthropometries which is a method of identifying individuals based on detailed records of their body measurements and physical descriptions photographs.

1892 and 1896 - Developing a classification system for fingerprints. Sir Francis Galton began writing a detailed study of fingerprints that presented a classification system using prints from ten fingers. It uses detailed measurements for identification which are still used today. Then in 1896, Sir Edward Henry researched a method of identification to implement and replace anthropometrics. Consulting with sir Francis regarding fingerprinting as a method of identifying criminals. When this was implemented, his worker, Azizul Haque, developed a method of classifying and storing information so that searching could be performed easily and efficiently.

1903 - The state prisons in NY begins using fingerprint. As learned from the recent development of fingerprinting ID into collecting criminal data, the state prisons are starting to adopt this which also later in 1904 spread into the police department. Eventually, more local police department began using this system as it brought many advantages.

1936 - Concept of using Iris pattern as identification was proposed by Frank Burch who was an ophthalmologist. He wanted to find a different method to recognize individuals apart from fingerprints.

1960s - First semi-automatic facial recognition system developed. It was developed by Woodrow W. Bledsoe in the US which required administrator to locate features such as eyes, ears, nose and mouth in the photographs. This relied solely on the ability to extract usable feature points and calculated distances and ratios to a common reference point that was compared to the reference data.

1960 - Also in the same year, the first model of acoustic speech production was created. Gunnar Fant, a Swedish Professor was able to identify the physiological components of acoustic speech production

1965 - The research for Automated Signature recognition begins.

1970 - First model of Behavioral components of Speech.

1980 - NIST Speech Group established. They developed and promoted the study of speech processing techniques.

1988; 1991 - First semi-automatic Facial Recognition system deployed and pioneered. Making real time facial recognition possible. Research study found that eigenfaces techniques could be used to detect faces in images as residual errors.

1993 - FacE REcognition Technology or FERET program is initiated. Algorithms were created by agencies that developed and researched on this technology.

1997 - First commercial and generic biometric interoperability standard published.

2001 - Face recognition is used at the Super Bowl in Florida. This was implemented in attempt to find wanted individuals entering the stadium.

2005 - Face Recognition algorithms developed to improve specific identified areas of interest in face recognition.

2011 - Biometric identification was used to identify the body of Osaba bin Laden

2013 - Apple introduces fingerprint scanners into the handheld devices. It was initially started by the iPhone 5S.

Technical Analysis

Biometrics allows a person to be identified and authenticated based on a set of recognizable and verifiable data which are unique and specific to them.

The authentication is the process of comparing data for the person's characteristics to that person's biometric template to determine the resemblance.

The reference model is usually stored in a database or a secured portable element. After that, the stored data can then be compared to that person's biometric data to be authenticated which will be the person's identity that is being checked and verified.

The technical aspect of biometric identification consists of determining that person's identity therefore, the goal is to capture the component of biometric data from that person first which can be a photo of their face, their vocal record or an image of their fingerprint. Once again, this data is compared to the biometric data of several other persons recorded database.

There are two main components of Biometric Measurements

1) Physiological measurements

Mostly morphological or biological, these consists mainly of fingerprints, hand pattern, vein pattern, eye or iris and retina, shape of the face. In criminal investigation cases, biological analyses the DNA, blood, saliva or urine for medical terms.

2) Behavioral measurements

In behavioral measurements, the most common ones are voice recognition, signature dynamics such as the speed of pen movement, accelerations, pressure exerted and many other factors. This part of the method is still being researched and developed for more improvements.

Applications

As we learned, historically the application of biometric security was initiated by the law enforcement and authorities which eventually transferred to the bigger fields such as FBI and military. These were mainly used for criminal or civil identification records under tightly regulated legal and technical framework.

Nowadays, many sectors such as banks, mobile commerce, retail markets are using a real deal for the advantages of biometrics. Also, due to the vast number of mobile developers using fingerprint and facial recognition has boosted the awareness publicly.

Overview of typical use case of biometric technology:

1. Law enforcement and public security (criminal/suspect identification)
2. Military (enemy/ally identification)
3. Border, travel, and migration control (traveler/migrant/passenger identification)
4. Civil identification (citizen/resident/voter identification)
5. Healthcare and subsidies (patient/beneficiary/healthcare professional identification)
6. Physical and logical access (owner/user/employee/contractor/partner identification)
7. Commercial applications (consumer/customer identification)

Advantages

We can identify several advantages of Biometrics security system as this is the most convenient method of authentication and validation process which has made the overall framework much more flexible without any hassle. It collects several human characteristics which are:

- Universal, as they can be found in all individuals
- Unique, as they make it possible to differentiate one individual from another
- Permanent, allowing for change over time
- Recordable (with or without consent)
- Measurable, allowing for future comparison
- Forgery-proof (a face, a fingerprint)

Conclusion

Overall, Biometrics can satisfy two unmistakable capacities, confirmation and distinguishing proof as we have learned. Distinguishing proof answers the inquiry "Who are you?". For this situation, the person is distinguished as the one among a group of others (1: N coordinating). The personal information of the individual to be recognized are compared and the information of different people put away in a similar database or perhaps other connected databases.

In this case, biometrics allow a person's identity to be authenticated by comparing the information they provide to the person they claim to be (1:1 matching) with pre-recorded data. These two technical solutions call upon different techniques. Identification generally requires a centralized database to compare multiple people's biometric data. Without such a centralized database, authentication can do. The data, like one of our smart cards, can simply be stored on a decentralized device. A process of authentication with a decentralized device should be preferred for data protection. There is less risk involved in such a process. Hence, biometrics security is a highly developed method that has been continuously developed researched throughout many years. It will be very interesting to see what the future holds for this category in technology and how far the human can reach to broaden the security aspect.

References

1. http://www.m2sys.com/blog/important-biometric-terms-to-know/the-history-of-biometrics-technology/
2. https://www.biometricupdate.com/201802/history-of-biometrics-2
3. http://www.m2sys.com/automated-fingerprint-identification-system-afis-border-control-and-border-protection/?utm_source=blog&utm_campaign=border%20control&utm_medium=m2sys%20landing%20page
4. https://www.gemalto.com/govt/inspired/biometrics
5. https://www.gemalto.com/govt/biometrics