ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

An Analytical Survey on Biometric Access Control for Physical Security

Sunil S. Shah[1], Kunal J. Pithadiya[2]

Sr. Lecturer, Dept. of Computer, BBIT, V.V.Nagar, Gujrat Technological University, Gujrat, India[1]

Sr. Lecturer, Dept. of EC, BBIT, V.V.Nagar, Gujrat Technological University, Gujrat, India[2]

ABSTRACT: With the increasing concern of security, Biometric access control is very effective tool. Biometric access control is the science with technology of the business as it relates to analyzing biological data as a means to control access. Biometric access control can measure various human characteristics with its features like a person's fingerprint, eye retinas and irises, vocal patterns, facial shapes, signature and writing patterns, keystrokes, hand measurements etc. Biometric access control is very effective within professional companies to promote security, as it would be extremely impossible to fake a biological imprint. In this paper, we have tried to present brief overview of different biometrics access control with its pros and cons.

KEYWORDS: Biometrics, access control, authentication, identification, recognition

I. Introduction

It is understood that transaction fraud increases as the level of security breaches. Today, the need of personal verification technology with highly secure identification becomes very much crucial. Biometric technologies are becoming the foundation of highly secure identification and physical verification solutions. Biometric-based solutions are able to provide confidential and financial transactions with personal data privacy. The key advantages of biometrics are easy and safe to use, accountability, time saving, secure and robust against potential hackers, ease of convenience, non-repudiation, non-guessable, etc. The rest of the paper is organized as follows: In Section-1 Introductory part is discussed, In Section-2 overview of biometric system is given, In Section-3, various Biometric access controls described with its pros and cons, In Section-4 we discuss about market share of biometric access control Section-5 concludes the paper.

II. Overview of biometric access control

Biometric access control can be classified into two main categories i.e. Physiological and Behavioral as shown in Fig.1.

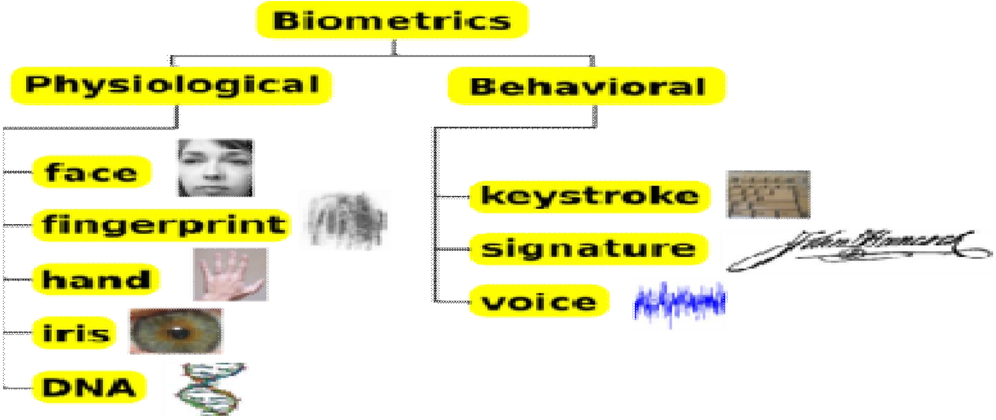

Fig 1. Types of Biometric Access Control
[Source: http://misbiometrics.wikidot.com]

DOI: 10.15680/IJIRCCE.2015. 0405109

1) Physiological: This is related to the shape of the body. This includes fingerprint, palm prints, hand geometry, hand veins, iris recognition, retina scan, ear canal, face recognition, facial thermo gram, DNA etc.
2) Behavioral: This is related to the behavior of a person. This includes signature and writing patterns, keystroke dynamics, voice patterns etc.
Components of a Biometric System as shown in Fig.2, a sensor that detects the characteristic being used for identification, the computer also called analyzer with comparator which reads and stores the necessary information. Resulted outcome is drawn by using analyzer with comparator from stored samples and data from the sensors. Analyzer that analyzes the characteristic, translates it into a graph or code and performs the actual comparison.

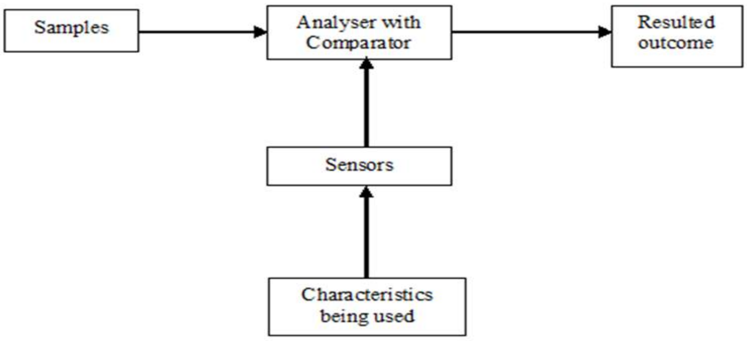

Fig.2Process of Biometric Access Control

III.TYPES OF BIOMETRIC ACCESS CONTROL

A. *Physiological Biometrics:*
1. *Fingerprints:* Fingerprints remain constant throughout person’s life. In over 140 years of fingerprint comparison worldwide, no two fingerprints however been found to be alike, not even those of identical twins. Good fingerprint scanners have been installed in PDAs; so scanner technology is also easy. It might not work in industrial applications since it requires clean hands [1]. Fingerprint identification involves comparing the pattern of ridges and furrows on the fingertips, as well as the minutiae points of a specimen print with a database of prints on file. As it is learnt from the study that it is highly accurate, standardized, most economical biometric user authentication technique mostly used and developed, easy to use and requires small storage space. It can make mistakes with the dryness or dirty of the finger’s skin, as well as with the age. Fig.3 shows fingerprint of the human being.

Fig.3 Fingerprint [6]

2. *Hand Prints:* Hand scan will measure hand geometry like finger lengths, widths, thickness, curves etc. It is most widely used technique for physical access. Though it requires special hardware to use, it can be easily integrated into other devices or systems. It is most commonly associated with authorized access so not have public attitude problem. It is very expensive, requires considerable size and it is not suitable to person who has problem of arthritic, since they cannot able to put the hand on the scanner properly. Fig.4 shows Handprint of the human being.

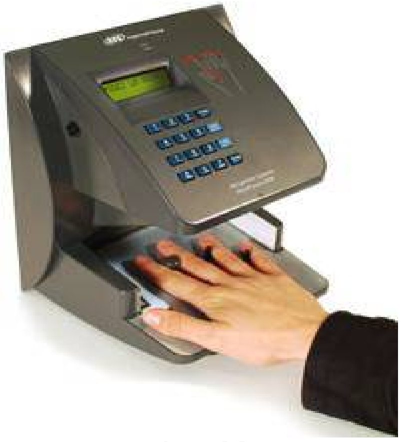

Fig.4 Hand Print [6]

3. *Retina Scanning:* A retinal scan is a biometric technique that uses the unique patterns on a person's retina to identify them [2]. The biometric use of this scan is used to examine the pattern of blood vessels and vein patterns at the back of the eye [3]. There is no known way to replicate a retina. As far as anyone knows, the pattern of the blood vessels at the back of the eye is unique and stays the same for a lifetime. However, it requires about 15 seconds of careful concentration to take a good scan. Retina scan remains a standard in military and government installations [4]. It is having high accuracy. There is no known way to replicate a retina. The eye from a dead person would deteriorate too fast to be useful, so no extra precautions have to been taken with retinal scans to be sure the user is a living human being. It is very intrusive. It has the stigma of consumer's thinking it is potentially harmful to the eye. It is very expensive. Fig.5A shows retina scanning of the human being and Fig 5B shows blood vessels and vein patterns of the eye.

Fig.5A Retina Scanning [6]

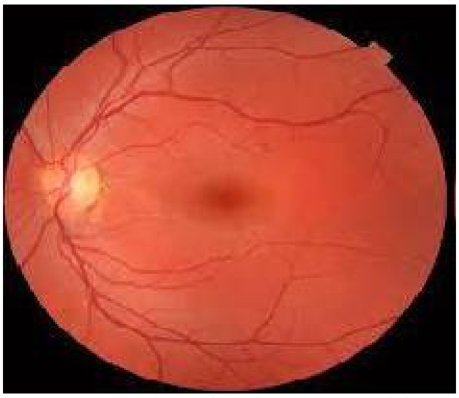

Fig.5B Blood vessels and Vein patterns [6]

B. *Behavioral Biometric:*

1. *Voice Patterns:* In Voice scan, it measures the sound waves of human speech including pitch, dynamics, and waveforms for recognition of person voice or speech. Voice scan could be based on either text-dependent or text-independent speech input. If it is text-dependent, user talks to a microphone a pass phrase and will repeat the same pass phrase when needed to be authenticated. A voice identification system firstly stores the sample of voice as reference so that it can be used to compare for subsequent voice identification. Voice scan Biometrics is currently used for low security applications because of high variability in an individual’s voice as it highly depends on mood of user and it is highly affected by background noise. In this users requirement is very low because users do not have to go through a separate process for verification. It requires very little hardware, and ideally suited for a remote identification, zero cost at client-side, no special reader needs to be installed. Verification time is about five seconds. It is highly depends on acoustic features like misspoken or misread phrases; the human voice's great amount of variation, due to colds, aging,

DOI: 10.15680/IJIRCCE.2015. 0405109

and simple tiredness. It is having low accuracy and can be captured secretly by a third party and replayed for unauthorized PC or network. Fig.6 shows voice pattern of the human being.

Fig.6 Voice Pattern
[Source: http://bankinnovation.net/2014/06/barclays-to-expand-voice-biometric-security/]

2. *Signature and Writing Patterns:* It is behavioral biometrics as people handwrite digits or their names in their own manners which is very personal and quite distinctive. It is used to analyze the dynamics inherent in writing the digits, characters, letters, words, and sentences. The other features that the system measures are how a person presses on the writing surface, how long a person takes to sign his or her name, how a person struggles to maintain verticality, angularity in letter forms and along the baseline, plus narrow letters. In signature, it measures the speed, pressure, stroke order and image of a signature. If a signature of a user is already recorded, this biometric technology adds an extra level of security with non-repudiation. It is low cost, non-intrusive, requires little time of verification generally five seconds. Individuals who do not sign regularly may face difficulty in enrolling and verifying in signature. Fig.7 shows signature and writing patterns of the human being.

Fig 7: Signature and Writing Pattern [6]

3. *Keystrokes:* Keystroke dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard [5]. Keystroke dynamics measures the time between strokes and duration of key pressed. It is purely software-based which does not requires sensor. Keystroke biometrics describes when person is typing keyboard exactly when each key was pressed and when it was released as a. Using keystroke dynamics in authentication software provides a solution that is fast, accurate, and scalable to millions of users. It is cost effective and easy to install and use, does not require end user training and taking less space. Typing patterns can be rather erratic, inconsistent and difficult when authorized person are injured also typing patterns are very much based on the keyboard being used and its layout. Fig.8 shows keystrokes of the human being.

Fig.8 Keystrokes [6]

IV. DISCUSSION

In this paper, we have analyzed different types of biometric access control system. Fig.9 shows the Biometric market share by its system types of January, 2016. By seeing below figure, it seems that in biometric security access dominated by fingerprint, iris scanning and face recognition. In future, we may have highly accurate and efficient sensors which will reduce the domination of above three.

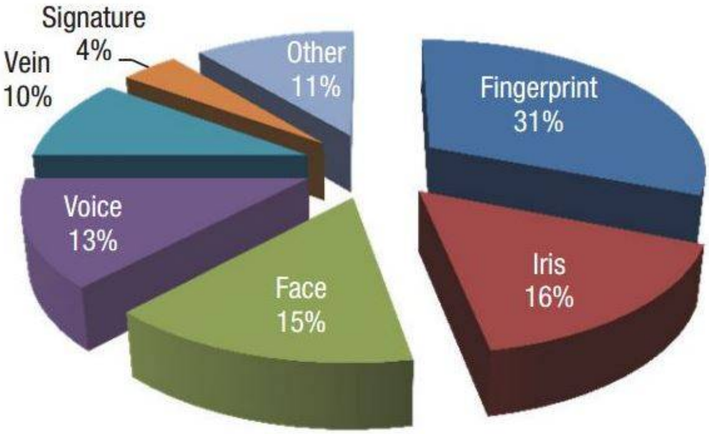

Fig.9 Biometric Market Share
[Source: http://image-sensors-world.blogspot.in/2016_01_01_archive.html]

The biometrics system market report covers the applications such as government, military and defense, healthcare, banking and finance, consumer electronics, travel and immigration, security and others [7]. We have tried to incorporate above all biometric application area into three basics application categories as shown in Fig.10. There are three categories, 1-Professional sector, 2-Confidential sector, 3-Financial sector. In Professional sector includes consumer electronics, travel and immigration, security etc. In Confidential sector includes government, military and defense, healthcare etc. In Financial sector includes banking and finance.

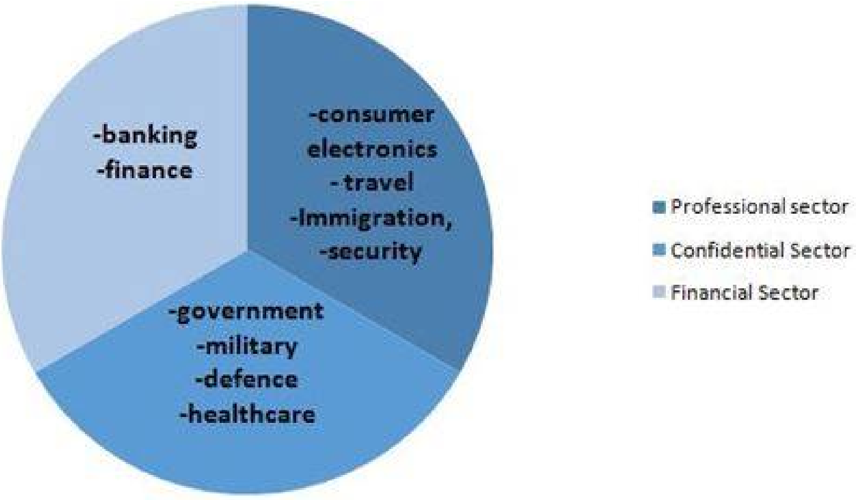

Fig.10 Biometric Access Control categories by Application

V. CONCLUSION AND FUTURE WORK

In this paper, hereby we suggest to use different biometric access control system by application. It means if someone is working in professional sector then one has to go through anyone of discussed above. If someone is working in confidential sector then one has to go through each and every one discussed according to its security level. If someone is working in financial sector then one has to go through any combination of above discussed biometric methods.

REFERENCES

1. Security and Access Control Using Biometric Technologies By Robert Newman
2. https://en.wikipedia.org/wiki/Retinal_scan
3. Advanced Criminal Investigations and Intelligence Operations: Tradecraft by Robert J Girod.
4. http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16
5. https://en.wikipedia.org/wiki/Keystroke_dynamics
6. Kaur et al., “Comparative Analysis of Biometric Modalities” International Journal of Advanced Research in Computer Science and Software Engineering 4(4), pp. 603-613,2014
7. http://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

BIOGRAPHY

Sunil S. Shah is a Sr. lecturer in the Computer Engineering Department, B & B Institute of Technology, V. V. Nagar, Gujarat Technological University, Gujarat, India. He received Master of Computer Engineering degree in 2012 from BVM Engineering college, V. V. Nagar, GTU, Ahmedabad, India. His research interests are Computer Networks (Wireless Networks), Computer Network and Security, Computer Algorithms etc.

Kunal J. Pithadiya is a Sr. lecturer in the Electronics & Communication Engineering Department, B & B Institute of Technology, V. V. Nagar, Gujarat Technological University, Gujarat, India. He received Master of Communication Engineering degree in 2009 from GCET, S P University, V. V. Nagar, India. His research interests are Machine Vision, Image processing, Edge Detection etc.